# 確定802.11 WLAN和CUWN快速安全漫遊的方法

## 目錄



## 簡介

本檔案介紹適用於整合無線網路(CUWN)上的IEEE 802.11無線LAN(WLAN)的無線和快速安全漫遊型別。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- IEEE 802.11 WLAN基礎
- IEEE 802.11 WLAN安全
- IEEE 802.1X/EAP基礎知識

### 採用元件

本檔案中的資訊是根據Cisco WLAN控制器軟體版本7.4。

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。

## 背景資訊

本檔案中的資訊是根據Cisco WLAN控制器軟體版本7.4，但大多數所述的偵錯輸出和行為可套用於支援所討論方法的任何軟體版本。後面的Cisco WLAN控制器代碼中此處介紹的所有方法的具體內容保持不變（本文更新時最多為8.3版）。

本檔案介紹適用於思科整合無線網路(CUWN)上支援的IEEE 802.11無線LAN(WLAN)的不同型別的無線漫遊和快速安全漫遊方法。

本文檔並未提供每種方法的工作方式或配置方式的所有詳細資訊。本文的主要目的是描述各種可用技術之間的差異、它們的優點和侷限性，以及每種方法上的幀交換。本文提供WLAN控制器(WLC)偵錯的範例，並使用無線封包映像來分析和說明所述的每個漫遊方法發生的事件。

在給出WLAN可用的不同快速安全漫遊方法的說明之前，必須瞭解WLAN關聯過程如何工作，以及在服務集識別符號(SSID)上未配置安全的情況下如何發生常規漫遊事件。

當802.11無線客戶端連線到接入點(AP)時，在它開始傳遞流量（無線資料幀）之前，它必須首先通過基本的802.11開放系統身份驗證過程。然後，必須完成關聯過程。開放系統身份驗證過程類似於客戶端選擇的AP上的電纜連線。這一點非常重要，因為選擇首選哪個AP的總是無線客戶端，而且決策取決於多個因素，這些因素因供應商而異。這就是客戶端通過向選定AP傳送身份驗證幀來開始此過程的原因，如本文檔稍後所示。AP無法請求您建立連線。

在成功完成開放系統身份驗證過程並收到來自AP的響應（「電纜連線」）後，關聯過程實質上會完成802.11第2層(L2)協商，該協商在客戶端和AP之間建立鏈路。如果連線成功，則AP會為客戶端分配一個關聯ID，如果配置在SSID上，則該AP會準備該關聯ID以便傳遞流量或執行更高級別的安全方法。開放系統身份驗證過程包括兩個管理幀以及關聯過程。身份驗證幀和關聯幀是**無線管**理幀，而不是資料幀，資料幀基本上用於與AP的連線過程。

以下是該過程的無線幀影象：

| No. | Time | Source | Destination | BSS Id | Protocol | Channel frequency | Info |
|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | Aironet_b7:ab:5c | Cisco_f0:68:d0 | 84:78:ac:f0:68:d0 | 802.11 | 2462 | Authentication, SN=2443, FN=0, Flags=.... |
| 2 | 0.000784 | Cisco_f0:68:d0 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d0 | 802.11 | 2462 | Authentication, SN=2771, FN=0, Flags=.... |
| 3 | 0.002428 | Aironet_b7:ab:5c | Cisco_f0:68:d0 | 84:78:ac:f0:68:d0 | 802.11 | 2462 | Association Request, SN=2444, FN=0, Flags |
| 4 | 0.007122 | Cisco_f0:68:d0 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d0 | 802.11 | 2462 | Association Response, SN=2772, FN=0, Flag |
| 5 | 0.995428 | 0.0.0.0 | 255.255.255.255 | 84:78:ac:f0:68:d0 | DHCP | 2462 | DHCP Discover - Transaction ID 0xba2bf0a4 |
| 6 | 2.996191 | 1.1.1.1 | 172.30.6.67 | 84:78:ac:f0:68:d0 | DHCP | 2462 | DHCP Offer - Transaction ID 0xba2bf0a4 |
| 7 | 2.998532 | 0.0.0.0 | 255.255.255.255 | 84:78:ac:f0:68:d0 | DHCP | 2462 | DHCP Request - Transaction ID 0xba2bf0a4 |
| 8 | 3.005016 | 1.1.1.1 | 172.30.6.67 | 84:78:ac:f0:68:d0 | DHCP | 2462 | DHCP ACK - Transaction ID 0xba2bf0a4 |

**註**意：如果您想瞭解802.11無線監聽技術，以及在Wireshark上用於本文檔中顯示的影象的濾鏡/顏色，請訪問思科支援社群文章802.11監聽器影象分析。

無線客戶端從身份驗證幀開始，AP使用另一個身份驗證幀進行應答。然後，客戶端傳送關聯請求幀，AP完成與關聯響應幀的回覆。如DHCP資料包所示，一旦通過802.11開放系統身份驗證和關聯過程，客戶端就開始傳遞資料幀。在這種情況下，SSID上沒有配置安全方法，因此客戶端立即開始傳送未加密的資料幀（本例中為DHCP）。

如本文檔稍後所示，如果在SSID上啟用了安全，則在關聯響應之後並在傳送任何客戶端流量資料幀(如DHCP、地址解析協定(ARP)和應用資料包（這些資料包經過加密）之前，特定安全方法有更高級別的身份驗證和加密握手幀。只有在客戶端完全通過身份驗證，並且根據配置的安全方法協商加密金鑰之前，才能傳送資料幀。

根據上一個映像，以下是在無線使用者端開始與WLAN的新關聯時，在WLC **debug client**命令的輸出中看到的訊息：

```
*apfMsConnTask_0: Jun 21 18:55:14.221: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID 84:78:ac:f0:68:d0
!--- This is the Association Request from the wireless client
     to the selected AP.

*apfMsConnTask_0: Jun 21 18:55:14.222: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d0
  (status 0) ApVapId 1 Slot 0
!--- This is the Association Response from the AP to the client.
```

**註**：用於本文檔中所示輸出的WLC調試是**debug client命令，示例僅顯示一些相關消息，而不是整個輸出。**有關此debug命令的詳細資訊，請參閱瞭解無線LAN控制器(WLC)上的偵錯使用者端的檔案。

這些消息顯示關聯請求和響應幀；初始身份驗證幀不會記錄在WLC中，因為此握手在CUWN的AP級別上快速發生。

客戶端漫遊時顯示什麼資訊？客戶端在與AP建立連線時總是交換四個管理幀，這歸因於客戶端建立關聯或漫遊事件。客戶端每次僅建立到一個AP的一個連線。在到WLAN基礎設施的新連線和漫遊事件之間的幀交換的唯一區別是漫遊事件的關聯幀稱為**Reassociation**幀，它表示客戶端實際上是從另一個AP漫遊，而沒有嘗試建立到WLAN的新關聯。這些幀可能包含用於協商漫遊事件的不同元素；這取決於設定，但這些詳細資訊不在本文檔的討論範圍之內。

以下是訊框交換的範例：

| No. | Time | Source | Destination | BSS Id | Protocol | Channel frequency | Info |
|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | Aironet_b7:ab:5c | Cisco_f0:2a:90 | 84:78:ac:f0:2a:90 | 802.11 | 2437 | Authentication, SN=2611, FN=0, Flags=..... |
| 2 | 0.001608 | Cisco_f0:2a:90 | Aironet_b7:ab:5c | 84:78:ac:f0:2a:90 | 802.11 | 2437 | Authentication, SN=3010, FN=0, Flags=..... |
| 3 | 0.003248 | Aironet_b7:ab:5c | Cisco_f0:2a:90 | 84:78:ac:f0:2a:90 | 802.11 | 2437 | Reassociation Request, SN=2612, FN=0, Flags |
| 4 | 0.008122 | Cisco_f0:2a:90 | Aironet_b7:ab:5c | 84:78:ac:f0:2a:90 | 802.11 | 2437 | Reassociation Response, SN=3011, FN=0, Flag |
| 5 | 4.291764 | Aironet_b7:ab:5c | Broadcast | 84:78:ac:f0:2a:90 | ARP | 2437 | Who has 172.30.6.254? Tell 172.30.6.67 |
| 6 | 4.293918 | Cisco_f5:4a:40 | Aironet_b7:ab:5c | 84:78:ac:f0:2a:90 | ARP | 2437 | 172.30.6.254 is at 00:1e:f7:f5:4a:40 |

這些消息顯示在調試輸出中：

```
*apfMsConnTask_2: Jun 21 19:02:19.709: 00:40:96:b7:ab:5c
  Reassociation received from mobile on BSSID 84:78:ac:f0:2a:90
!--- This is the Reassociation Request from the wireless client
     to the selected AP.

*apfMsConnTask_2: Jun 21 19:02:19.710: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:90
  (status 0) ApVapId 1 Slot 0
!--- This is the Reassociation Response from the AP to the client.
```

如圖所示，客戶端在向新AP傳送重新關聯請求後成功執行漫遊事件，並從AP接收重新關聯響應。由於客戶端已經具有IP地址，因此第一個資料幀用於ARP資料包。

如果您期望漫遊事件，但客戶端傳送關聯請求而不是重新關聯請求（您可以從某些影象和調試中確認該請求，如本文檔前面所述），則客戶端實際上並不漫遊。客戶端開始與WLAN進行新的關聯，就像斷開連線一樣，並嘗試從頭重新連線。發生這種情況的原因有多種，例如，當客戶端離開覆蓋區域並找到訊號品質足以啟動關聯的AP時，通常表示客戶端由於驅動程式、韌體或軟體問題而未啟動漫遊事件的客戶端問題。

**註**：您可以諮詢無線客戶端供應商以確定問題的原因。

# 具有更高級別安全性的漫遊

當在基本802.11開放系統身份驗證上為SSID配置了L2更高級別的安全時，初始關聯和漫遊時需要更多幀。本文檔中介紹了為802.11 WLAN標準化和實施的兩種最常見的安全方法：

- **WPA/WPA2-PSK（預共用金鑰）** — 使用預共用金鑰對客戶端進行身份驗證。
- **WPA/WPA2-EAP（可擴展身份驗證協定）** — 使用802.1X/EAP方法對客戶端進行身份驗證，以便通過使用身份驗證伺服器驗證更安全的憑據，例如證書、使用者名稱和密碼以及令牌。

需要注意的是，儘管這兩種方法（PSK和EAP）以不同的方式驗證/驗證客戶端，但兩種方法都使用基本相同的WPA/WPA2規則進行金鑰管理過程。無論安全性是WPA/WPA2-PSK還是WPA/WPA2-EAP，稱為WPA/WPA2 4路握手的流程都會在客戶端與主會話金鑰(MSK)作為原始金鑰材料的WLC/AP之間開始金鑰協商，一旦客戶端使用所用的特定驗證方法進行了驗證。

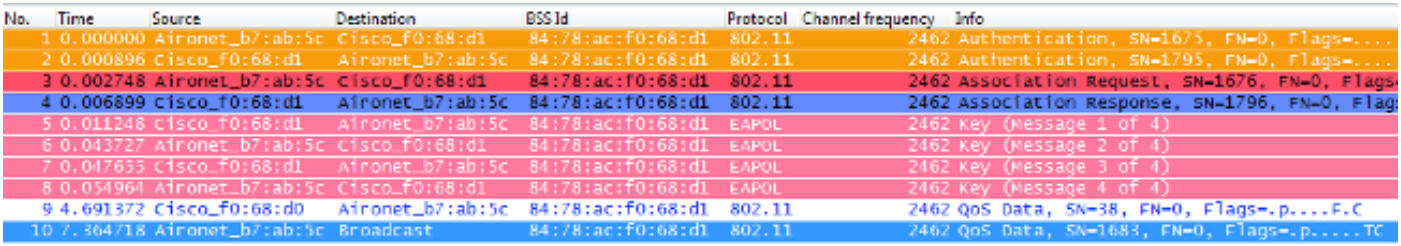
以下是流程摘要：

1. 當使用802.1X/EAP安全時，從EAP身份驗證階段派生MSK，或者當使用WPA/WPA2-PSK作為安全方法時，從PSK派生MSK。
2. 透過此MSK，使用者端和WLC/AP產生配對主金鑰(PMK),WLC/AP產生群組主金鑰(GMK)。
3. 一旦這兩個主金鑰準備就緒，客戶端和WLC/AP就會啟動WPA/WPA2 4次握手（本文檔稍後將介紹一些螢幕影象和調試），主金鑰作為實際加密金鑰協商的種子。
4. 這些最終的加密金鑰稱為成對瞬時金鑰(PTK)和組瞬時金鑰(GTK)。PTK從PMK派生，用於加密與客戶端的單點傳播幀。組臨時金鑰(GTK)從GMK派生，用於加密此特定SSID/AP上的組播/廣播。

## WPA/WPA2-PSK

當通過臨時金鑰完整性協定(TKIP)或高級加密標準(AES)執行用於加密的WPA-PSK或WPA2-PSK時，客戶端必須經過稱為WPA 4路握手的過程，用於初始關聯和漫遊時。如前所述，這基本上是用於WPA/WPA2派生加密金鑰的金鑰管理過程。但是當執行PSK時，也使用它來驗證使用者端是否有有

效的預先共用金鑰加入WLAN。此圖顯示了執行WPA或WPA2與PSK的初始關聯過程：



| No. | Time | Source | Destination | BSS Id | Protocol | Channel frequency | Info |
|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | Aironet_b7:ab:5c | Cisco_f0:68:d1 | 84:78:ac:f0:68:d1 | 802.11 | 2462 | Authentication, SN=1675, FN=0, Flags=.... |
| 2 | 0.000896 | Cisco_f0:68:d1 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d1 | 802.11 | 2462 | Authentication, SN=1795, FN=0, Flags=.... |
| 3 | 0.002748 | Aironet_b7:ab:5c | Cisco_f0:68:d1 | 84:78:ac:f0:68:d1 | 802.11 | 2462 | Association Request, SN=1676, FN=0, Flags |
| 4 | 0.006899 | Cisco_f0:68:d1 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d1 | 802.11 | 2462 | Association Response, SN=1796, FN=0, Flag |
| 5 | 0.011248 | Cisco_f0:68:d1 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d1 | EAPOL | 2462 | Key (Message 1 of 4) |
| 6 | 0.043727 | Aironet_b7:ab:5c | Cisco_f0:68:d1 | 84:78:ac:f0:68:d1 | EAPOL | 2462 | Key (Message 2 of 4) |
| 7 | 0.047655 | Cisco_f0:68:d1 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d1 | EAPOL | 2462 | Key (Message 3 of 4) |
| 8 | 0.054964 | Aironet_b7:ab:5c | Cisco_f0:68:d1 | 84:78:ac:f0:68:d1 | EAPOL | 2462 | Key (Message 4 of 4) |
| 9 | 4.691372 | Cisco_f0:68:d0 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d1 | 802.11 | 2462 | QoS Data, SN=38, FN=0, Flags=.p....F.C |
| 10 | 7.364718 | Aironet_b7:ab:5c | Broadcast | 84:78:ac:f0:68:d1 | 802.11 | 2462 | QoS Data, SN=1683, FN=0, Flags=.p.....TC |

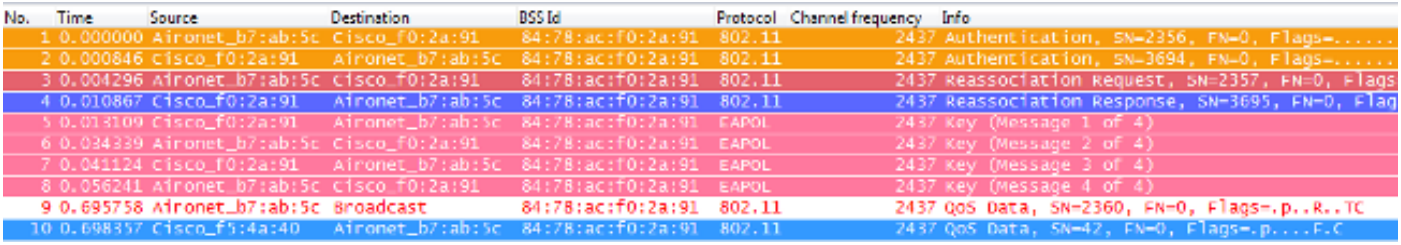
如圖所示，在802.11開放系統驗證和關聯過程之後，WPA 4向握手中有四個EAPOL幀，它們由AP用**message-1**發起，由客戶端用**message-4**結束。握手成功後，客戶端開始傳遞資料幀（如DHCP），在此情況下，資料幀使用衍生自4次握手的金鑰進行加密（這就是您看不到無線影象中的實際內容和流量型別的原因）。

> **註**:EAPOL幀用於在AP和客戶端之間傳輸所有金鑰管理幀和802.1X/EAP身份驗證幀；它們作為無線資料幀進行傳輸。

以下訊息會顯示在debug輸出中：

```
*apfMsConnTask_0: Jun 21 19:30:05.172: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID 84:78:ac:f0:68:d1
*apfMsConnTask_0: Jun 21 19:30:05.173: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d1
  (status 0) ApVapId 2 Slot 0
!--- The Association handshake is finished.

*dot1xMsgTask: Jun 21 19:30:05.178: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00
!--- Message-1 of the WPA/WPA2 4-Way handshake is sent
     from the WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.289: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.289: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2)
  from mobile 00:40:96:b7:ab:5c
!--- Message-2 of the WPA/WPA2 4-Way handshake is successfully
     received from the client.

*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.290: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- Message-3 of the WPA/WPA2 4-Way handshake is sent
     from the WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.309: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.310: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
!--- Message-4 (final message) of the WPA/WPA2 4-Way handshake
     is successfully received from the client, which confirms
     the installation of the derived keys. They can now be used in
     order to encrypt data frames with current AP.
```

漫遊時，客戶端基本上會跟蹤相同的幀交換，此時需要進行WPA 4次握手，以便使用新的AP獲取新的加密金鑰。這是因為標準確立的安全原因，以及新AP不知道原始金鑰的事實。唯一的區別是存在重新關聯幀而不是關聯幀，如下圖所示：



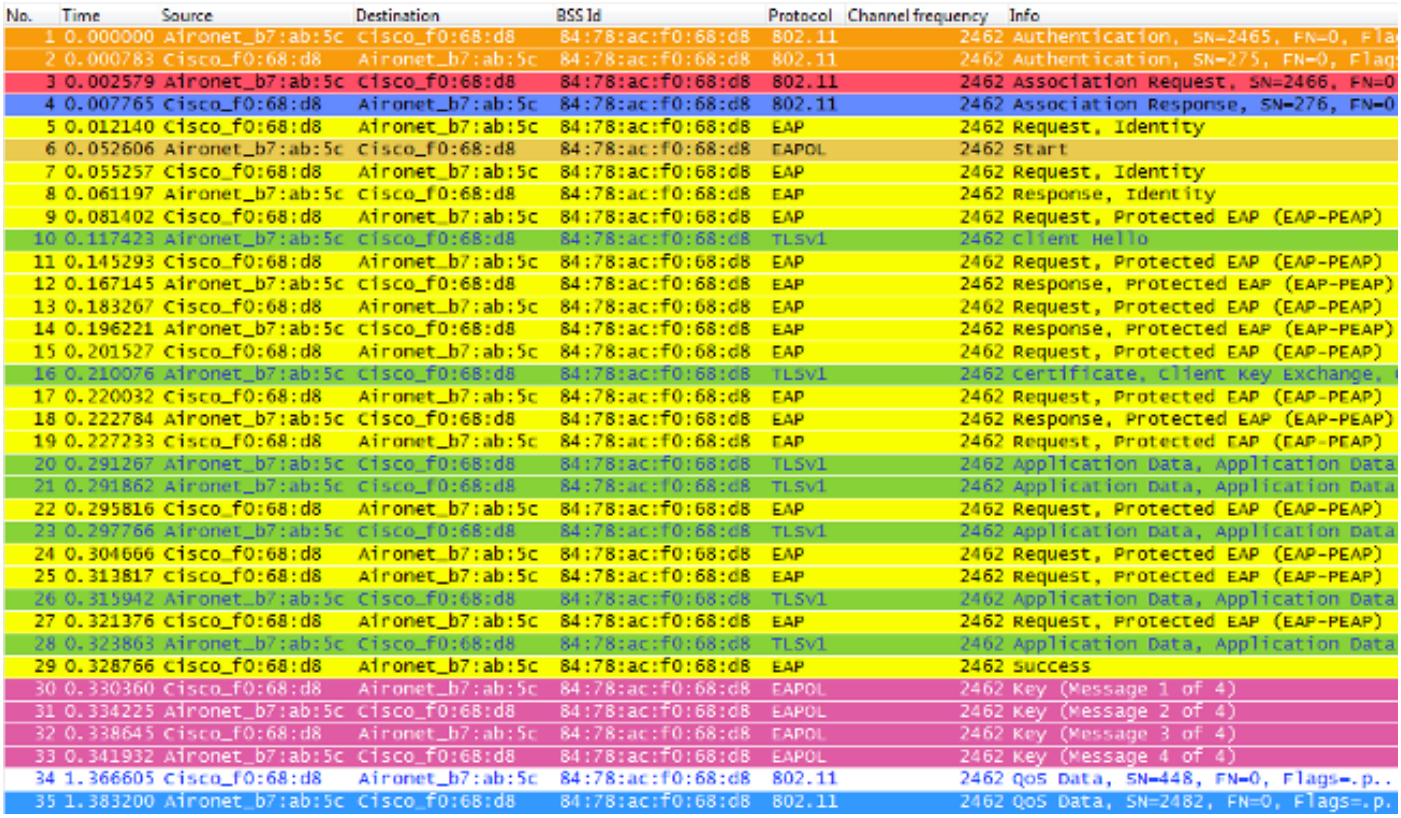
| No. | Time | Source | Destination | BSS Id | Protocol | Channel frequency | Info |
|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | Aironet_b7:ab:5c | Cisco_f0:2a:91 | 84:78:ac:f0:2a:91 | 802.11 | 2437 | Authentication, SN=2356, FN=0, Flags=..... |
| 2 | 0.000846 | Cisco_f0:2a:91 | Aironet_b7:ab:5c | 84:78:ac:f0:2a:91 | 802.11 | 2437 | Authentication, SN=3694, FN=0, Flags=..... |
| 3 | 0.004296 | Aironet_b7:ab:5c | Cisco_f0:2a:91 | 84:78:ac:f0:2a:91 | 802.11 | 2437 | Reassociation Request, SN=2357, FN=0, Flags |
| 4 | 0.010867 | Cisco_f0:2a:91 | Aironet_b7:ab:5c | 84:78:ac:f0:2a:91 | 802.11 | 2437 | Reassociation Response, SN=3695, FN=0, Flag |
| 5 | 0.013109 | Cisco_f0:2a:91 | Aironet_b7:ab:5c | 84:78:ac:f0:2a:91 | EAPOL | 2437 | Key (Message 1 of 4) |
| 6 | 0.034339 | Aironet_b7:ab:5c | Cisco_f0:2a:91 | 84:78:ac:f0:2a:91 | EAPOL | 2437 | Key (Message 2 of 4) |
| 7 | 0.041124 | Cisco_f0:2a:91 | Aironet_b7:ab:5c | 84:78:ac:f0:2a:91 | EAPOL | 2437 | Key (Message 3 of 4) |
| 8 | 0.056241 | Aironet_b7:ab:5c | Cisco_f0:2a:91 | 84:78:ac:f0:2a:91 | EAPOL | 2437 | Key (Message 4 of 4) |
| 9 | 0.695758 | Aironet_b7:ab:5c | Broadcast | 84:78:ac:f0:2a:91 | 802.11 | 2437 | QoS Data, SN=2360, FN=0, Flags=.p..R..TC |
| 10 | 0.698357 | Cisco_f5:4a:40 | Aironet_b7:ab:5c | 84:78:ac:f0:2a:91 | 802.11 | 2437 | QoS Data, SN=42, FN=0, Flags=.p....F.C |

您會在調試輸出中看到相同的消息，但來自客戶端的第一個資料包是Reassociation而不是Association，如前所述所示。

## WPA/WPA2-EAP

當使用802.1X/EAP方法驗證安全SSID上的客戶端時，在客戶端開始傳遞流量之前，需要更多的幀。這些額外幀用於驗證客戶端憑證，根據EAP方法，可以有四至二十個幀。這些是在關聯/重新關聯之後，但在WPA/WPA2 4次握手之前，因為身份驗證階段派生的MSK用作金鑰管理過程（4次握手）中最終加密金鑰生成的種子。

此圖顯示當執行具有PEAPv0/EAP-MSCHAPv2的WPA時，在初始關聯時在AP和無線客戶端之間通過空中交換的幀的示例：



| No. | Time | Source | Destination | BSS Id | Protocol | Channel frequency | Info |
|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | 802.11 | 2462 | Authentication, SN=2465, FN=0, Fla |
| 2 | 0.000783 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | 802.11 | 2462 | Authentication, SN=275, FN=0, Flag |
| 3 | 0.002579 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | 802.11 | 2462 | Association Request, SN=2466, FN=0 |
| 4 | 0.007765 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | 802.11 | 2462 | Association Response, SN=276, FN=0 |
| 5 | 0.012140 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAP | 2462 | Request, Identity |
| 6 | 0.052606 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | EAPOL | 2462 | Start |
| 7 | 0.055257 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAP | 2462 | Request, Identity |
| 8 | 0.061197 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | EAP | 2462 | Response, Identity |
| 9 | 0.081402 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 10 | 0.117423 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | TLSv1 | 2462 | Client Hello |
| 11 | 0.145293 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 12 | 0.167145 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | EAP | 2462 | Response, Protected EAP (EAP-PEAP) |
| 13 | 0.183267 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 14 | 0.196221 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | EAP | 2462 | Response, Protected EAP (EAP-PEAP) |
| 15 | 0.201527 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 16 | 0.210076 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | TLSv1 | 2462 | Certificate, Client Key Exchange, |
| 17 | 0.220032 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 18 | 0.222784 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | EAP | 2462 | Response, Protected EAP (EAP-PEAP) |
| 19 | 0.227233 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 20 | 0.291267 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | TLSv1 | 2462 | Application Data, Application Data |
| 21 | 0.291862 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | TLSv1 | 2462 | Application Data, Application Data |
| 22 | 0.295816 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 23 | 0.297766 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | TLSv1 | 2462 | Application Data, Application Data |
| 24 | 0.304666 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 25 | 0.313817 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 26 | 0.315942 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | TLSv1 | 2462 | Application Data, Application Data |
| 27 | 0.321376 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 28 | 0.323863 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | TLSv1 | 2462 | Application Data, Application Data |
| 29 | 0.328766 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAP | 2462 | Success |
| 30 | 0.330360 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAPOL | 2462 | Key (Message 1 of 4) |
| 31 | 0.334225 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | EAPOL | 2462 | Key (Message 2 of 4) |
| 32 | 0.338645 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | EAPOL | 2462 | Key (Message 3 of 4) |
| 33 | 0.341932 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | EAPOL | 2462 | Key (Message 4 of 4) |
| 34 | 1.366605 | Cisco_f0:68:d8 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d8 | 802.11 | 2462 | QoS Data, SN=448, FN=0, Flags=.p.. |
| 35 | 1.383200 | Aironet_b7:ab:5c | Cisco_f0:68:d8 | 84:78:ac:f0:68:d8 | 802.11 | 2462 | QoS Data, SN=2482, FN=0, Flags=.p. |

有時，此交換顯示或多或少幀，這取決於多種因素，如EAP方法、由於問題導致的重新傳輸、客戶端行為(如本示例中的兩個身份請求，因為客戶端在AP傳送第一個身份請求後傳送**EAPOL START)，或者客戶端已與伺服器交換證書。**只要為802.1X/EAP方法配置SSID，就會有更多幀（用於身份驗證），因此，客戶端開始傳送資料幀之前需要更多時間。

以下是偵錯訊息的摘要：

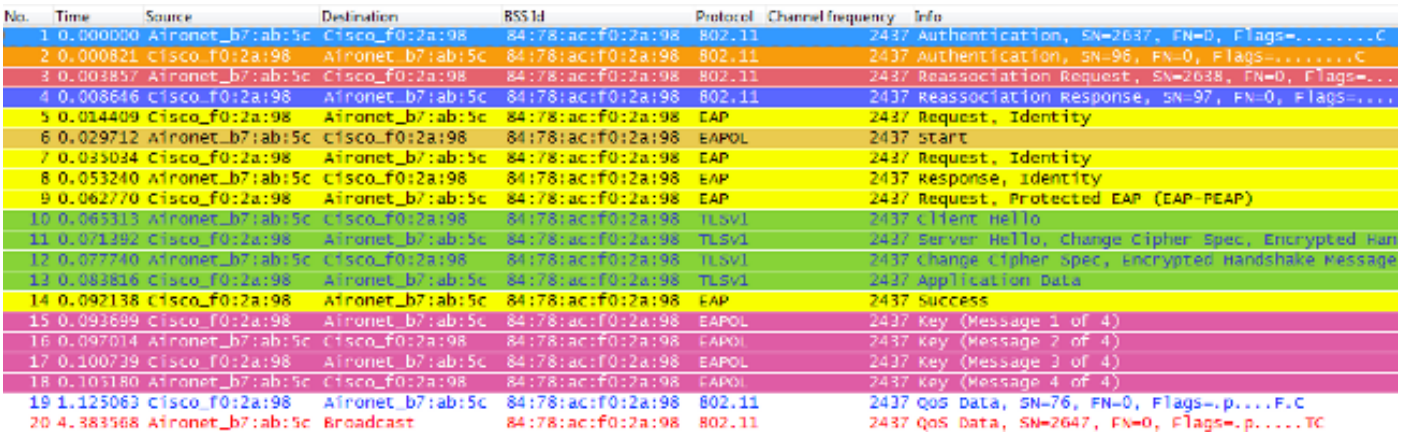
```
*apfMsConnTask_0: Jun 21 23:41:19.092: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID 84:78:ac:f0:68:d8
*apfMsConnTask_0: Jun 21 23:41:19.094: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d8
  (status 0) ApVapId 9 Slot 0
!--- The Association handshake is finished.

*dot1xMsgTask: Jun 21 23:41:19.098: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 1)
!--- The EAP Identity Request is sent to the client once it is
     associated in order to begin the higher-level authentication
     process. This informs the client that an identity to start
     this type of 802.1X/EAP authentication must be provided.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.226: 00:40:96:b7:ab:5c
  Received EAPOL START from mobile 00:40:96:b7:ab:5c
!--- The wireless client decides to start the EAP authentication
     process, and informs the AP with an EAPOL START data frame.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.227: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 2)
!--- WLC/AP sends another EAP Identity Request to the client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.235: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.235: 00:40:96:b7:ab:5c
  Received Identity Response (count=2) from mobile 00:40:96:b7:ab:5c
!--- The client responds with an EAP Identity Response on an EAPOL
     frame.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.301: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.301: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 3)
!--- Once the WLC/AP sends the client response to the Authentication
     Server on a RADIUS Access-Request packet, the server responds
     with a RADIUS Access-Challenge in order to officially start the
     EAP negotiation, handshake, and authentication with the client
     (sometimes with mutual authentication, dependent upon the EAP
     method). This response received by the WLC/AP is sent to the client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.344: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.344: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 3, EAP Type 25)
!--- The client responds with an EAP Response on an EAPOL frame, which
     is sent to the Authentication Server on a RADIUS Access-Request
     packet. The server responds with another RADIUS Access-Challenge.
     This process continues, dependent upon the EAP method (the exchange
     of certificates when used, the building of TLS tunnels, validation
     of client credentials, client validation of server identity when
     applicable). Hence, the next few messages are basically the same on
     the WLC/AP side, as this acts as a "proxy" between the client and
     the Authentication Server exchanges.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.347: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c
```

```
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.347: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 4)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.375: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.375: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 4, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.377: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.377: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 5)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.403: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.403: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 5, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.404: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.404: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 6)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.414: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.414: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 6, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.421: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.421: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 7)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.425: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.425: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 7, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.427: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.427: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 8)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.434: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.434: 00:40:96:b7:ab:5c
```

```
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 8, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.436: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.436: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 9)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.440: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.440: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 9, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.442: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.442: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 10)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.449: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.449: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 10, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.452: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.452: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 11)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.457: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.457: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 11, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.459: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.459: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 13)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.469: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.469: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 13, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.472: 00:40:96:b7:ab:5c
  Processing Access-Accept for mobile 00:40:96:b7:ab:5c
!--- The authentication finishes and is successful for this client,
     so the RADIUS Server sends a RADIUS Access-Accept to the WLC/AP.
     This RADIUS Access-Accept comes with the special attributes
```

```
     that are assigned to this client (if any are configured on the
     Authentication Server for this client). This Access-Accept also
     comes with the MSK derived with the client in the EAP
     authentication process, so the WLC/AP installs it in order to
     initiate the WPA/WPA2 4-Way handshake with the wireless client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.473: 00:40:96:b7:ab:5c
  Sending EAP-Success to mobile 00:40:96:b7:ab:5c
  (EAP Id 13)
!--- The accept/pass of the authentication is sent to the client as
     an EAP-Success message.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.473: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00
!--- Message-1 of the WPA/WPA2 4-Way handshake is sent from the
     WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.481: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.481: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2)
  from mobile 00:40:96:b7:ab:5c
!--- Message-2 of the WPA/WPA-2 4-Way handshake is successfully
     received from the client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.481: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- Message-3 of the WPA/WPA2 4-Way handshake is sent from the
     WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.487: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.487: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
!--- Message-4 (final message) of the WPA/WPA2 4-Way handshake
     is successfully received from the client, which confirms the
     installation of the derived keys. They can now be used in
     order to encrypt data frames with the current AP.
```

當無線客戶端在此處執行常規漫遊（正常行為，未實施快速安全漫遊方法）時，客戶端必須經過完全相同的過程並對身份驗證伺服器執行完全身份驗證，如圖所示。唯一的區別是客戶端使用重新關聯請求來通知新AP它實際上正在從另一個AP漫遊，但客戶端仍然必須經過完全驗證和新金鑰生成：



如圖所示，即使有比初始身份驗證中更少的幀（如前所述由多個因素引起），當客戶端漫遊到新AP時，也必須完成EAP身份驗證和WPA金鑰管理過程才能繼續傳遞資料幀（即使流量在漫遊前已主動傳送）。因此，如果客戶端有一個對延遲敏感的活動應用程式（如語音流量應用程式或對超時敏感的應用程式），則使用者可以在漫遊時發現問題，如音訊間隙或應用程式斷開。這取決於該過程花費多長時間才能使客戶端繼續傳送/接收資料幀。此延遲可能會更長，具體取決於：RF環境、客戶端數量、WLC和LAP之間的來回時間以及身份驗證伺服器的來回時間，以及其他原因。

以下是此漫遊事件的調試消息的摘要（與先前的消息基本相同，因此這些消息不會進行進一步說明）：

```
*apfMsConnTask_2: Jun 21 23:47:54.872: 00:40:96:b7:ab:5c
  Reassociation received from mobile on BSSID 84:78:ac:f0:2a:98

*apfMsConnTask_2: Jun 21 23:47:54.874: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:98
  (status 0) ApVapId 9 Slot 0

*dot1xMsgTask: Jun 21 23:47:54.879: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 1)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.895: 00:40:96:b7:ab:5c
  Received EAPOL START from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.895: 00:40:96:b7:ab:5c
  dot1x - moving mobile 00:40:96:b7:ab:5c into Connecting state

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.895: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 2)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.922: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.922: 00:40:96:b7:ab:5c
  Received Identity Response (count=2) from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.929: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.929: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 3)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.941: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.941: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 3, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.943: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.943: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 4)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.954: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c
```

```
*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.954: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 4, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.956: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.957: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 7)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.976: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.976: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 7, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.978: 00:40:96:b7:ab:5c
  Processing Access-Accept for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.978: 00:40:96:b7:ab:5c
  Sending EAP-Success to mobile 00:40:96:b7:ab:5c
  (EAP Id 7)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.978: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.995: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.995: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2)
  from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.995: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_4: Jun 21 23:47:55.005: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:55.005: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
```

這就是802.1X/EAP和WPA/WPA2安全框架的工作方式。為了防止應用程式/服務對常規漫遊事件延遲的影響，WiFi行業開發和實施了多種快速安全漫遊方法，以便在對WLAN/SSID使用安全時加快漫遊過程。當客戶端在AP之間漫遊時，通過在WLAN上部署高級安全功能，它們繼續傳遞流量時，會面臨一定的延遲。這是因為安全設定需要進行EAP身份驗證和金鑰管理幀交換，如前所述。

瞭解快速安全漫遊只是業界用來描述實施方法/方案的術語，當在WLAN上配置了安全時，該方法或方案可加速漫遊過程，瞭解這一點非常重要。 下一節將介紹可用於WLAN並由CUWN支援的各種快速安全漫遊方法/方案。

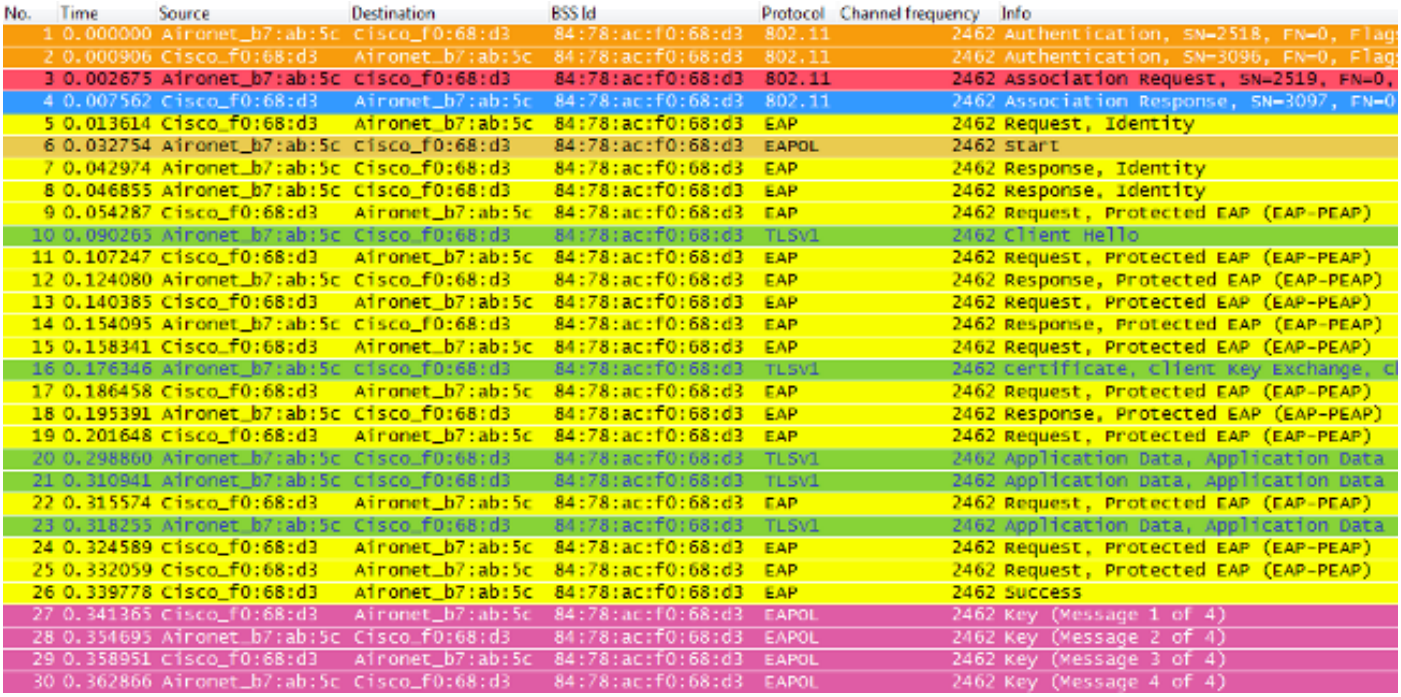
# 使用CCKM實現快速安全漫遊

Cisco Centralized Key Management(CCKM)是在企業WLAN上開發和實施的第一種快速安全漫遊方法，由Cisco建立，作為在WLAN上使用802.1X/EAP安全性時緩解迄今為止所解釋的延遲的解決方案。由於這是思科專有協定，因此只有思科WLAN基礎設施裝置和無線客戶端（來自多個供應商）支援，這些裝置與CCKM的思科相容擴展(CCX)相容。

CCKM可以使用適用於WLAN的所有不同加密方法實施，其中包括：WEP、TKIP和AES。大多數用於WLAN的802.1X/EAP身份驗證方法也支援該功能，具體取決於裝置支援的CCX版本。

> **註**：有關不同版本的CCX規範支援的功能內容（包括支援的EAP方法）的概述，請參考CCX版本和功能文檔，並驗證無線客戶端支援的精確CCX版本（如果它們與CCX相容），以便可以確認是否可實施您希望用於CCKM的安全方法。

此無線映像提供當您執行以TKIP作為加密，PEAPv0/EAP-MSCHAPv2作為802.1X/EAP方法的CCKM時，初始關聯時交換的幀的示例。這基本上與執行PEAPv0/EAP-MSCHAPv2的WPA/TKIP交換相同，但這次在客戶端和基礎結構之間協商了CCKM，以便它們使用不同的金鑰層次結構和快取方法，以便在客戶端必須漫遊時執行快速安全漫遊：



| No. | Time | Source | Destination | BSS Id | Protocol | Channel frequency | Info |
|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | 802.11 | 2462 | Authentication, SN=2518, FN=0, Flag |
| 2 | 0.000906 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | 802.11 | 2462 | Authentication, SN=3096, FN=0, Flag |
| 3 | 0.002675 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | 802.11 | 2462 | Association Request, SN=2519, FN=0, |
| 4 | 0.007562 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | 802.11 | 2462 | Association Response, SN=3097, FN=0 |
| 5 | 0.013614 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | EAP | 2462 | Request, Identity |
| 6 | 0.032754 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | EAPOL | 2462 | Start |
| 7 | 0.042974 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | EAP | 2462 | Response, Identity |
| 8 | 0.046855 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | EAP | 2462 | Response, Identity |
| 9 | 0.054287 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 10 | 0.090265 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | TLSv1 | 2462 | Client Hello |
| 11 | 0.107247 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 12 | 0.124080 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | EAP | 2462 | Response, Protected EAP (EAP-PEAP) |
| 13 | 0.140385 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 14 | 0.154095 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | EAP | 2462 | Response, Protected EAP (EAP-PEAP) |
| 15 | 0.158341 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 16 | 0.176346 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | TLSv1 | 2462 | Certificate, Client Key Exchange, C |
| 17 | 0.186458 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 18 | 0.195391 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | EAP | 2462 | Response, Protected EAP (EAP-PEAP) |
| 19 | 0.201648 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 20 | 0.298860 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | TLSv1 | 2462 | Application Data, Application Data |
| 21 | 0.310941 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | TLSv1 | 2462 | Application Data, Application Data |
| 22 | 0.315574 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 23 | 0.318255 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | TLSv1 | 2462 | Application Data, Application Data |
| 24 | 0.324589 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 25 | 0.332059 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 26 | 0.339778 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | EAP | 2462 | Success |
| 27 | 0.341365 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | EAPOL | 2462 | Key (Message 1 of 4) |
| 28 | 0.354695 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | EAPOL | 2462 | Key (Message 2 of 4) |
| 29 | 0.358951 | Cisco_f0:68:d3 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d3 | EAPOL | 2462 | Key (Message 3 of 4) |
| 30 | 0.362866 | Aironet_b7:ab:5c | Cisco_f0:68:d3 | 84:78:ac:f0:68:d3 | EAPOL | 2462 | Key (Message 4 of 4) |

以下是調試消息的摘要（為了減少輸出，刪除了某些EAP交換）：

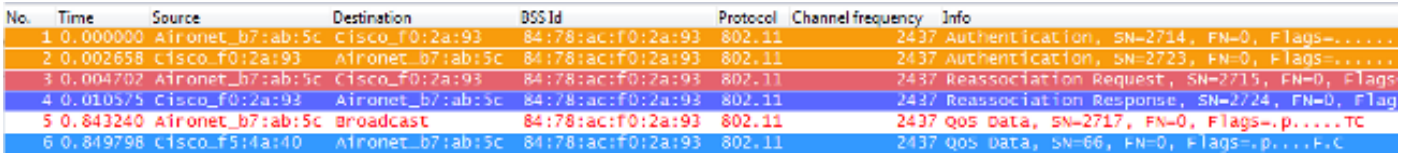
```
*apfMsConnTask_0: Jun 25 15:41:41.507: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID 84:78:ac:f0:68:d3
!--- This is the Association Request from the client.

*apfMsConnTask_0: Jun 25 15:41:41.507: 00:40:96:b7:ab:5c
  Processing WPA IE type 221, length 22 for mobile
  00:40:96:b7:ab:5c
*apfMsConnTask_0: Jun 25 15:41:41.507: 00:40:96:b7:ab:5c
  CCKM: Mobile is using CCKM
!--- The WLC/AP finds an Information Element that claims CCKM
    support on the Association request that is sent from the client.
```

```
*apfMsConnTask_0: Jun 25 15:41:41.507: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8
!--- This is the key cache index for this client, which is set temporally.

*apfMsConnTask_0: Jun 25 15:41:41.508: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d3
  (status 0) ApVapId 4 Slot 0
!--- The Association Response is sent to the client.

*dot1xMsgTask: Jun 25 15:41:41.513: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 1)
!--- An EAP Identity Request is sent to the client once it is
     associated in order to begin the higher-level authentication
     process. This informs the client that an identity to start
     this type of 802.1X/EAP authentication must be provided.
     Further EAP messages are not described, as they are basically
     the same as the ones previously-explained.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.536: 00:40:96:b7:ab:5c
  Received EAPOL START from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.536: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 2)

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.546: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.546: 00:40:96:b7:ab:5c
  Received EAP Response packet with mismatching id
  (currentid=2, eapid=1) from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.550: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.550: 00:40:96:b7:ab:5c
  Received Identity Response (count=2) from mobile
  00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.555: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.555: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 3)

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.594: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.594: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 3, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.840: 00:40:96:b7:ab:5c
  Processing Access-Accept for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  Creating a PKC PMKID Cache entry for station 00:40:96:b7:ab:5c
  (RSN 0)<br/ >
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
```

```
  Setting active key cache index 8 ---> 0
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  CCKM: Create a global PMK cache entry
!--- WLC creates a global PMK cache entry for this client,
      which is for CCKM in this case.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  Sending EAP-Success to mobile 00:40:96:b7:ab:5c
  (EAP Id 13)
!--- The client is informed of the successful EAP authentication.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  INITPMK(message 1),replay counter 00.00.00.00.00.00.00.00
!--- Message-1 of the initial 4-Way handshake is sent from the
      WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2) from mobile
  00:40:96:b7:ab:5c
!--- Message-2 of the initial 4-Way handshake is received
      successfully from the client.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: 00:40:96:b7:ab:5c
  CCKM: Sending cache add
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: CCKM: Sending CCKM PMK
  (Version_1) information to mobility group
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: CCKM: Sending CCKM PMK
  (Version_2) information to mobility group
!--- The CCKM PMK cache entry for this client is shared with
      the WLCs on the mobility group.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- Message-3 of the initial 4-Way handshake is sent from the
      WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.866: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.866: 00:40:96:b7:ab:5c Received
  EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile
  00:40:96:b7:ab:5c
!--- Message-4 (final message) of this initial 4-Way handshake
      is received successfully from the client, which confirms the
      installation of the derived keys. They can now be used in order
      to encrypt data frames with the current AP.
```

使用CCKM時，與WLAN的初始關聯類似於常規WPA/WPA2，其中MSK(在此處也稱為網路作業階段金鑰(NSK))是與使用者端和RADIUS伺服器相互派生的。在成功進行身份驗證後，此主金鑰從伺服器傳送到WLC，並快取為派生所有後續金鑰的基礎，以便在客戶端與此WLAN關聯的生存期內使用。從這裡，WLC和使用者端取得用於基於CCKM的快速安全漫遊的種子資訊，這經過與WPA/WPA2類似的4次握手，以便取得具有第一個AP的單點傳送(PTK)和多點傳送/廣播(GTK)加密金鑰。

漫遊時注意到了大差異。在這種情況下，CCKM客戶端向AP/WLC傳送一個重新關聯請求幀（包括MIC和按順序遞增的隨機數），並提供足夠的資訊(包括新的AP MAC地址 — BSSID-)以派生新的PTK。有了這個重新關聯請求，WLC和新AP也有足夠的資訊來派生新的PTK，因此它們只是用重新關聯響應進行響應。使用者端現在可以繼續傳遞流量，如下圖所示：



| No. | Time | Source | Destination | BSS Id | Protocol | Channel frequency | Info |
|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | Aironet_b7:ab:5c | Cisco_f0:2a:93 | 84:78:ac:f0:2a:93 | 802.11 | 2437 | Authentication, SN=2714, FN=0, Flags=..... |
| 2 | 0.002658 | Cisco_f0:2a:93 | Aironet_b7:ab:5c | 84:78:ac:f0:2a:93 | 802.11 | 2437 | Authentication, SN=2723, FN=0, Flags=..... |
| 3 | 0.004702 | Aironet_b7:ab:5c | Cisco_f0:2a:93 | 84:78:ac:f0:2a:93 | 802.11 | 2437 | Reassociation Request, SN=2715, FN=0, Flags |
| 4 | 0.010575 | Cisco_f0:2a:93 | Aironet_b7:ab:5c | 84:78:ac:f0:2a:93 | 802.11 | 2437 | Reassociation Response, SN=2724, FN=0, Flag |
| 5 | 0.843240 | Aironet_b7:ab:5c | Broadcast | 84:78:ac:f0:2a:93 | 802.11 | 2437 | QoS Data, SN=2717, FN=0, Flags=.p.....TC |
| 6 | 0.849798 | Cisco_f5:4a:40 | Aironet_b7:ab:5c | 84:78:ac:f0:2a:93 | 802.11 | 2437 | QoS Data, SN=66, FN=0, Flags=.p....F.C |

以下是此漫遊事件的WLC偵錯摘要：

```
*apfMsConnTask_2: Jun 25 15:43:33.749: 00:40:96:b7:ab:5c
  CCKM: Received REASSOC REQ IE
*apfMsConnTask_2: Jun 25 15:43:33.749: 00:40:96:b7:ab:5c
  Reassociation received from mobile on BSSID
  84:78:ac:f0:2a:93
*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  Processing WPA IE type 221, length 22 for mobile
  00:40:96:b7:ab:5c
*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  CCKM: Mobile is using CCKM
!--- The Reassociation Request is received from the client,
     which provides the CCKM information needed in order to
     derive the new keys with a fast-secure roam.

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  Setting active key cache index 0 ---> 8

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  CCKM: Processing REASSOC REQ IE

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  CCKM: using HMAC MD5 to compute MIC
!--- WLC computes the MIC used for this CCKM fast-roaming
     exchange.

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  CCKM: Received a valid REASSOC REQ IE

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  CCKM: Initializing PMK cache entry with a new PTK
!--- The new PTK is derived.

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 0

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Creating a PKC PMKID Cache entry for station
  00:40:96:b7:ab:5c (RSN 0) on BSSID 84:78:ac:f0:2a:93
!--- The new PMKID cache entry is created for this new
     AP-to-client association.

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  CCKM: using HMAC MD5 to compute MIC
*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Including CCKM Response IE (length 62) in Assoc Resp to mobile
*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:93
```

```
  (status 0) ApVapId 4 Slot 0
!--- The Reassociation Response is sent from the WLC/AP to
     the client, which includes the CCKM information required
     in order to confirm the new fast-roam and key derivation.

*dot1xMsgTask: Jun 25 15:43:33.757: 00:40:96:b7:ab:5c
  Skipping EAP-Success to mobile 00:40:96:b7:ab:5c
!--- EAP is skipped due to the fast roaming, and CCKM does not
     require further key handshakes. The client is now ready to
     pass encrypted data frames on the new AP.
```

如圖所示，在避免EAP身份驗證幀和更多四向握手的同時，執行快速安全漫遊，因為新的加密金鑰仍然派生，但基於CCKM協商方案。這通過漫遊重新關聯幀以及客戶端和WLC以前快取的資訊來完成。

### 含CCKM的FlexConnect

- 支援集中身份驗證。這包括本地和中央資料交換。AP必須屬於同一個FlexConnect組。
- 支援Flex本地身份驗證。在連線模式下，快取可以從AP分發到控制器，然後分發到FlexConnect組中的其他AP。
- 支援獨立模式。如果AP上已經存在快取（由於以前的分發），則快速漫遊將起作用。獨立模式下的新身份驗證不支援快速安全漫遊。

### 使用CCKM的優勢

- CCKM是最快的快速安全漫遊方法，大多部署在企業WLAN上。 當在AP之間移動時，客戶端不需要通過金鑰管理握手來獲取新金鑰，並且不再需要在此WLAN上的客戶端生存期內對新AP執行完整的802.1X/EAP身份驗證。
- CCKM支援802.11標準中可用的所有加密方法（WEP、TKIP和AES），以及一些仍在舊版客戶端上使用的舊版思科專有方法。

### 使用CCKM時的缺點

- CCKM是Cisco專有的一種方法，它限制對Cisco WLAN基礎設施和CCX無線客戶端的實施和支援。
- CCX第5版並未被廣泛採用，因此許多CCX無線客戶端都不支援使用WPA2/AES的CCKM（主要是因為大多數無線客戶端已經支援使用WPA/TKIP的CCKM，這仍非常安全）。

## 使用PMKID快取/粘滯金鑰快取進行快速安全漫遊

成對式思維金鑰ID(PMKID)快取(**Sticky Key Caching，簡稱SKC)**是IEEE 802.11標準在802.11i安全修正內建議的第一個快速安全漫遊方法，其主要用途是為WLAN標準化高水準的安全保護。此快速安全漫遊技術被新增為WPA2裝置的一種可選方法，以便在實施此安全時改進漫遊。

這是可能的，因為每次客戶端完全通過EAP驗證時，客戶端和驗證伺服器都會派生MSK，MSK用於派生PMK。它用作WPA2 4路握手的種子，以派生會話使用的最終單播加密金鑰(PTK)（直到客戶端漫遊到另一個AP或會話過期）；因此，此方法可防止漫遊時的EAP身份驗證階段，因為它會重新利用客戶端和AP快取的原始PMK。客戶端只需通過WPA2 4次握手即可獲取新的加密金鑰。

此方法沒有廣泛部署為推薦的802.11標準快速安全漫遊方法，主要是由於以下原因：

- 此方法是可選的，並非所有WPA2裝置都支援此方法，因為802.11i修正案的目的並不涉及快速安全漫遊，而IEEE已經著手進行另一項修正，以標準化WLAN的快速安全漫遊（802.11r，本文檔稍後將對此進行介紹）。
- 此方法在實施上有很大的限制：無線客戶端只有在漫遊回他們之前已驗證/連線的AP時才能執行快速安全漫遊。

使用此方法，與任何AP的初始關聯就像對WLAN的常規首次身份驗證，其中針對身份驗證伺服器的整個802.1X/EAP身份驗證和金鑰生成的4次握手必須在客戶端能夠傳送資料幀之前進行，如下螢幕影象所示：

| No. | Time | Source | Destination | BSS Id | Protocol | Channel frequency | Info |
|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | 802.11 | 2462 | Authentication, SN=2, FN=0, Flags=..... |
| 2 | 0.000814 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | 802.11 | 2462 | Authentication, SN=4052, FN=0, Flags=... |
| 3 | 0.002747 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | 802.11 | 2462 | Association Request, SN=3, FN=0, Flags=. |
| 4 | 0.007357 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | 802.11 | 2462 | Association Response, SN=4053, FN=0, Fla |
| 5 | 0.011957 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Identity |
| 6 | 0.022896 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | EAP | 2462 | Response, Identity |
| 7 | 0.044470 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 8 | 0.069885 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Client Hello |
| 9 | 0.093349 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 10 | 0.095916 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | EAP | 2462 | Response, Protected EAP (EAP-PEAP) |
| 11 | 0.112358 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 12 | 0.116114 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | EAP | 2462 | Response, Protected EAP (EAP-PEAP) |
| 13 | 0.120221 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 14 | 0.129519 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Certificate, Client Key Exchange, Change |
| 15 | 0.139156 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 16 | 0.162262 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | EAP | 2462 | Response, Protected EAP (EAP-PEAP) |
| 17 | 0.166459 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 18 | 0.171454 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Application Data |
| 19 | 0.175710 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 20 | 0.178181 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Application Data |
| 21 | 0.182858 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 22 | 0.187006 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Application Data |
| 23 | 0.192835 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 24 | 0.197049 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Application Data |
| 25 | 0.202860 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 26 | 0.205372 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Application Data |
| 27 | 0.210763 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAP | 2462 | Success |
| 28 | 0.212505 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAPOL | 2462 | Key (Message 1 of 4) |
| 29 | 0.215434 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | EAPOL | 2462 | Key (Message 2 of 4) |
| 30 | 0.219023 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAPOL | 2462 | Key (Message 3 of 4) |
| 31 | 0.221930 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | EAPOL | 2462 | Key (Message 4 of 4) |
| 32 | 0.224559 | Apple_15:39:32 | Cisco_f5:4a:40 | 84:78:ac:f0:68:d2 | 802.11 | 2462 | QoS Data, SN=0, FN=0, Flags=.p.....TC |

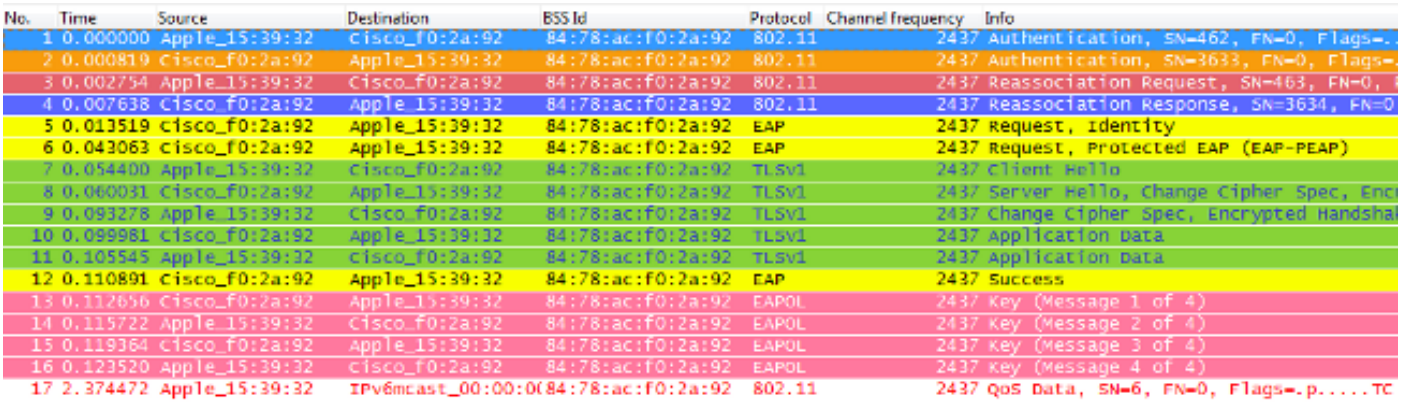
調試顯示與對WLAN進行初始身份驗證時其餘方法的EAP身份驗證幀交換相同，並新增了一些關於此處使用的金鑰快取技術的輸出。這些調試輸出被剪下，以便主要顯示新資訊，而不是整個EAP幀交換，因為每次交換基本相同的資訊用於客戶端對身份驗證伺服器的身份驗證。這一點目前已經過演示，並且與資料包影象中顯示的EAP身份驗證幀相關聯，因此為了簡便起見，大多數EAP消息都會從調試輸出中刪除：

```
*apfMsConnTask_0: Jun 22 00:23:15.097: ec:85:2f:15:39:32
  Association received from mobile on BSSID 84:78:ac:f0:68:d2
!--- This is the Association Request from the client.

*apfMsConnTask_0: Jun 22 00:23:15.098: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 20 for mobile ec:85:2f:15:39:32
!--- The WLC/AP finds an Information Element that claims PMKID
     Caching support on the Association request that is sent
     from the client.

*apfMsConnTask_0: Jun 22 00:23:15.098: ec:85:2f:15:39:32
  Received RSN IE with 0 PMKIDs from mobile ec:85:2f:15:39:32
!--- Since this is an initial association, the Association
     Request comes without any PMKID.

*apfMsConnTask_0: Jun 22 00:23:15.098: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 8
```

```
*apfMsConnTask_0: Jun 22 00:23:15.099: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d2
  (status 0) ApVapId 3 Slot 0
!--- The Association Response is sent to the client.

*dot1xMsgTask: Jun 22 00:23:15.103: ec:85:2f:15:39:32
  Sending EAP-Request/Identity to mobile ec:85:2f:15:39:32
  (EAP Id 1)

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.118: ec:85:2f:15:39:32
  Received EAPOL EAPPKT from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.118: ec:85:2f:15:39:32
  Received Identity Response (count=1) from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.126: ec:85:2f:15:39:32
  Processing Access-Challenge for mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.126: ec:85:2f:15:39:32
  Sending EAP Request from AAA to mobile ec:85:2f:15:39:32
  (EAP Id 2)

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.146: ec:85:2f:15:39:32
  Received EAPOL EAPPKT from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.146: ec:85:2f:15:39:32
  Received EAP Response from mobile ec:85:2f:15:39:32
  (EAP Id 2, EAP Type 25)

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Processing Access-Accept for mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Creating a PKC PMKID Cache entry for station ec:85:2f:15:39:32
  (RSN 2)
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 8
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 0
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Adding BSSID 84:78:ac:f0:68:d2 to PMKID cache at index 0
  for station ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274:
  New PMKID: (16)
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274:
  [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
!--- WLC creates a PMK cache entry for this client, which is
     used for SKC in this case, so the PMKID is computed with
     the AP MAC address (BSSID 84:78:ac:f0:68:d2).

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Sending EAP-Success to mobile ec:85:2f:15:39:32
  (EAP Id 12)

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.275:
  Including PMKID in M1  (16)
!--- The hashed PMKID is included on the Message-1 of the
     WPA/WPA2 4-Way handshake.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.275:
  [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
!--- This is the hashed PMKID.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.275: ec:85:2f:15:39:32
```

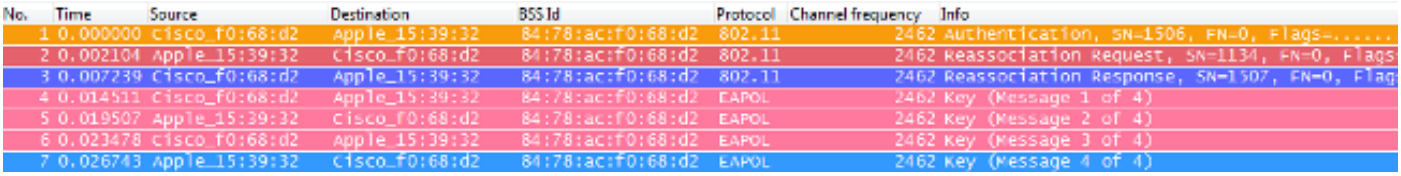
```
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00
!--- Message-1 of the WPA/WPA2 4-Way handshake is sent from
      the WLC/AP to the client.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.284: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.284: ec:85:2f:15:39:32
  Received EAPOL-key in PTK_START state (message 2) from mobile
  ec:85:2f:15:39:32
!--- Message-2 of the WPA/WPA-2 4-Way handshake is successfully
      received from the client.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.284: ec:85:2f:15:39:32
  PMK: Sending cache add

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.285: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- Message-3 of the WPA/WPA2 4-Way handshake is sent from
      the WLC/AP to the client.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.291: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.291: ec:85:2f:15:39:32
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile ec:85:2f:15:39:32
!--- Message-4 (final message) of this initial WPA/WPA2 4-Way
      handshake is successfully received from the client, which
      confirms the installation of the derived keys. They can
      now be used in order to encrypt data frames with the current AP.
```

通過此方法，AP和無線客戶端快取已建立的安全關聯的PMK。因此，如果無線客戶端漫遊到從未關聯的新AP，則客戶端必須再次執行完整的EAP身份驗證，如以下圖所示，客戶端漫遊到新AP:



| No. | Time | Source | Destination | BSS Id | Protocol | Channel frequency | Info |
|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | Apple_15:39:32 | Cisco_f0:2a:92 | 84:78:ac:f0:2a:92 | 802.11 | 2437 | Authentication, SN=462, FN=0, Flags=. |
| 2 | 0.000819 | Cisco_f0:2a:92 | Apple_15:39:32 | 84:78:ac:f0:2a:92 | 802.11 | 2437 | Authentication, SN=3633, FN=0, Flags= |
| 3 | 0.002754 | Apple_15:39:32 | Cisco_f0:2a:92 | 84:78:ac:f0:2a:92 | 802.11 | 2437 | Reassociation Request, SN=463, FN=0, |
| 4 | 0.007638 | Cisco_f0:2a:92 | Apple_15:39:32 | 84:78:ac:f0:2a:92 | 802.11 | 2437 | Reassociation Response, SN=3634, FN=0 |
| 5 | 0.013519 | Cisco_f0:2a:92 | Apple_15:39:32 | 84:78:ac:f0:2a:92 | EAP | 2437 | Request, Identity |
| 6 | 0.043063 | Cisco_f0:2a:92 | Apple_15:39:32 | 84:78:ac:f0:2a:92 | EAP | 2437 | Request, Protected EAP (EAP-PEAP) |
| 7 | 0.054400 | Apple_15:39:32 | Cisco_f0:2a:92 | 84:78:ac:f0:2a:92 | TLSv1 | 2437 | Client Hello |
| 8 | 0.060031 | Cisco_f0:2a:92 | Apple_15:39:32 | 84:78:ac:f0:2a:92 | TLSv1 | 2437 | Server Hello, Change Cipher Spec, Enc |
| 9 | 0.093278 | Apple_15:39:32 | Cisco_f0:2a:92 | 84:78:ac:f0:2a:92 | TLSv1 | 2437 | Change Cipher Spec, Encrypted Handsha |
| 10 | 0.099981 | Cisco_f0:2a:92 | Apple_15:39:32 | 84:78:ac:f0:2a:92 | TLSv1 | 2437 | Application Data |
| 11 | 0.105545 | Apple_15:39:32 | Cisco_f0:2a:92 | 84:78:ac:f0:2a:92 | TLSv1 | 2437 | Application Data |
| 12 | 0.110891 | Cisco_f0:2a:92 | Apple_15:39:32 | 84:78:ac:f0:2a:92 | EAP | 2437 | Success |
| 13 | 0.112656 | Cisco_f0:2a:92 | Apple_15:39:32 | 84:78:ac:f0:2a:92 | EAPOL | 2437 | Key (Message 1 of 4) |
| 14 | 0.115722 | Apple_15:39:32 | Cisco_f0:2a:92 | 84:78:ac:f0:2a:92 | EAPOL | 2437 | Key (Message 2 of 4) |
| 15 | 0.119364 | Cisco_f0:2a:92 | Apple_15:39:32 | 84:78:ac:f0:2a:92 | EAPOL | 2437 | Key (Message 3 of 4) |
| 16 | 0.123520 | Apple_15:39:32 | Cisco_f0:2a:92 | 84:78:ac:f0:2a:92 | EAPOL | 2437 | Key (Message 4 of 4) |
| 17 | 2.374472 | Apple_15:39:32 | IPv6mcast_00:00:0( | 84:78:ac:f0:2a:92 | 802.11 | 2437 | QoS Data, SN=6, FN=0, Flags=.p.....TC |

但是，如果無線客戶端漫遊回發生先前關聯/身份驗證的AP，則客戶端傳送重新關聯請求幀，該幀列出多個PMKID，從而通知AP從客戶端先前已進行身份驗證的所有AP中快取的PMK。因此，由於客戶端正在漫遊回也快取了此客戶端的PMK的AP，因此客戶端不需要通過EAP重新驗證以派生新的PMK。客戶端只需通過WPA2 4次握手，即可獲取新的臨時加密金鑰：



| No. | Time | Source | Destination | BSS Id | Protocol | Channel frequency | Info |
|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | 802.11 | 2462 | Authentication, SN=1506, FN=0, Flags=..... |
| 2 | 0.002104 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | 802.11 | 2462 | Reassociation Request, SN=1134, FN=0, Flags |
| 3 | 0.007239 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | 802.11 | 2462 | Reassociation Response, SN=1507, FN=0, Flag |
| 4 | 0.014511 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAPOL | 2462 | Key (Message 1 of 4) |
| 5 | 0.019507 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | EAPOL | 2462 | Key (Message 2 of 4) |
| 6 | 0.023478 | Cisco_f0:68:d2 | Apple_15:39:32 | 84:78:ac:f0:68:d2 | EAPOL | 2462 | Key (Message 3 of 4) |
| 7 | 0.026743 | Apple_15:39:32 | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | EAPOL | 2462 | Key (Message 4 of 4) |

**註**：此影象不顯示來自客戶端的第一個802.11開放系統身份驗證幀，但是這不是由於實現的方法所致，因為總是需要此幀。原因在於，此特定幀不是由介面卡或用於嗅探此示例的無線幀的無線資料包映像軟體進行映像的，而是出於教育目的，在此示例中保留為此類幀。請注意，執行無線資料包影象時可能會發生這種情況；影象可能會遺漏某些幀，但實際上這些幀是在客戶端和AP之間交換的。否則，漫遊不會在此示例中啟動。

以下是此快速安全漫遊方法的WLC偵錯摘要：

```
*apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32
  Reassociation received from mobile on BSSID
  84:78:ac:f0:68:d2
!--- This is the Reassociation Request from the client.

*apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 38 for mobile
  ec:85:2f:15:39:32
!--- The WLC/AP finds an Information Element that claims PMKID
     Caching support on the Association request that is sent
     from the client.

*apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32
  Received RSN IE with 1 PMKIDs from mobile
  ec:85:2f:15:39:32
!--- The Reassociation Request from the client comes with
     one PMKID.

*apfMsConnTask_0: Jun 22 00:26:40.787:
  Received PMKID:  (16)
*apfMsConnTask_0: Jun 22 00:26:40.788:
  [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
!--- This is the PMKID that is received.

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Searching for PMKID in MSCB PMKID cache for mobile
  ec:85:2f:15:39:32
!--- WLC searches for a matching PMKID on the database.

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Found an cache entry for BSSID 84:78:ac:f0:68:d2 in
  PMKID cache at index 0 of station ec:85:2f:15:39:32

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Found a valid PMKID in the MSCB PMKID cache for mobile
  ec:85:2f:15:39:32
!--- The WLC validates the PMKID provided by the client,
     and confirms that it has a valid PMK cache for this
     client-and-AP pair.

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Setting active key cache index 1 ---> 0

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID
  84:78:ac:f0:68:d2(status 0) ApVapId 3 Slot 0
!--- The Reassociation Response is sent to the client, which
     validates the fast-roam with SKC.
```

```
*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32
  Initiating RSN with existing PMK to mobile
  ec:85:2f:15:39:32
!--- WLC initiates a Robust Secure Network association with
     this client-and-AP pair based on the cached PMK found.
Hence, EAP is avoided as per the next message.

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32
  Skipping EAP-Success to mobile ec:85:2f:15:39:32

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32
  Found an cache entry for BSSID 84:78:ac:f0:68:d2 in
  PMKID cache at index 0 of station ec:85:2f:15:39:32

*dot1xMsgTask: Jun 22 00:26:40.795: Including PMKID in M1(16)
!--- The hashed PMKID is included on the Message-1 of the
     WPA/WPA2 4-Way handshake.

*dot1xMsgTask: Jun 22 00:26:40.795:
  [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
!--- The PMKID is hashed. The next messages are the same
     WPA/WPA2 4-Way handshake messages described thus far
     that are used in order to finish the encryption keys
     generation/installation.

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.811: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32
  Received EAPOL-key in PTK_START state (message 2) from mobile
  ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32
  PMK: Sending cache add

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.820: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.820: ec:85:2f:15:39:32
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile ec:85:2f:15:39:32
```

## 採用PMKID快取/粘滯金鑰快取的FlexConnect

- 在FlexConnect安裝上使用此方法時，如果向WLC使用中央身份驗證（通過中央或本地交換），則該方法可能會起作用，其行為看起來與先前解釋的類似；但是，FlexConnect不支援此SKC方法。
- 此方法僅在具有本地模式AP的CUWN上得到正式支援，在FlexConnect或其他模式下則不受支援。

## 採用PMKID快取/粘滯金鑰快取的PROS

此方法可以由自主獨立AP在本地實施，而無需集中裝置來管理快取的金鑰。

### 使用PMKID快取/粘滯金鑰快取的缺點

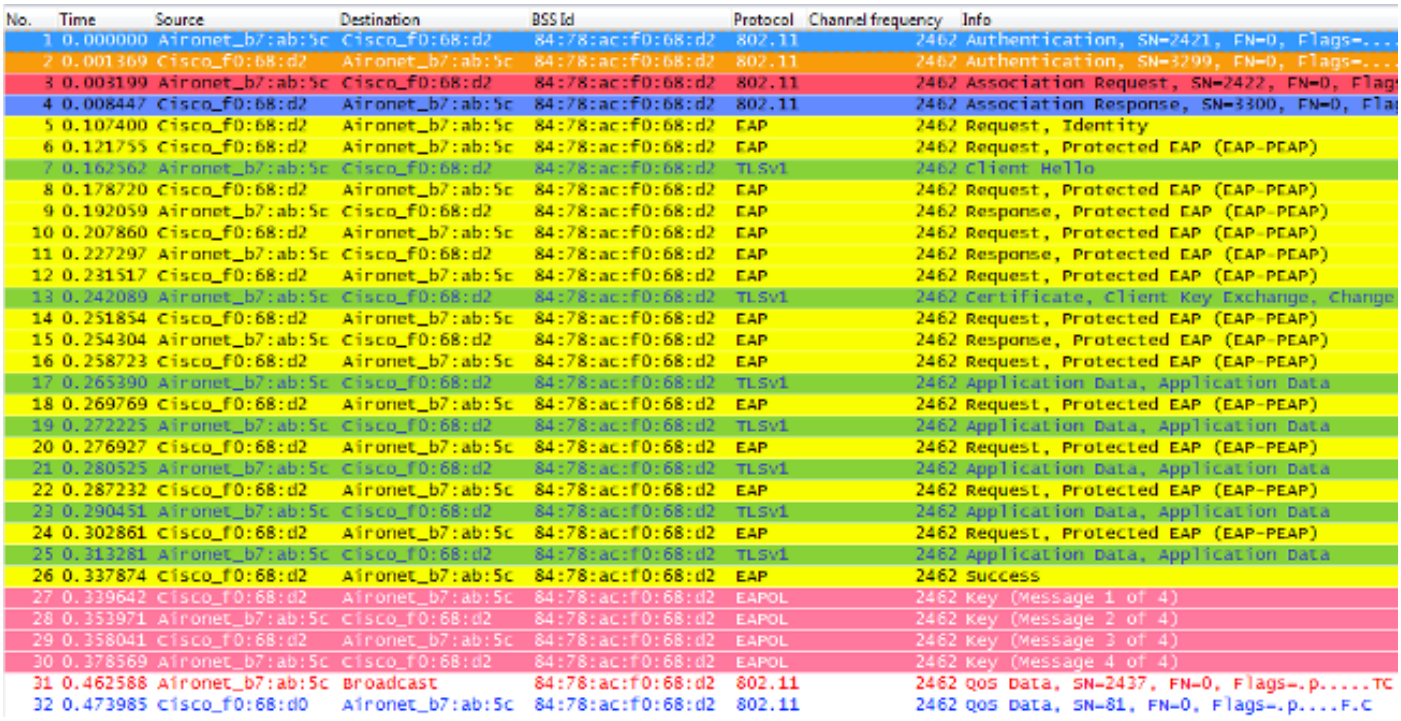
- 如本文檔前面所述，此方法的主要限制是客戶端在漫遊回其先前關聯/驗證的AP時只能執行快速安全漫遊。如果漫遊到新的AP，客戶端必須再次完成完整的EAP身份驗證。
- 無線客戶端和AP必須記住每次新身份驗證時派生的所有PMK，因此此功能通常限製為快取的一定數量的PMK。由於該標準未明確界定此限制，因此供應商可針對其SKC實施定義不同的限制。例如，思科WLAN控制器當前可以從客戶端快取最多8個AP的PMK。如果客戶端漫遊到每個會話中超過8個AP，則最早的AP將從快取清單中刪除，以便儲存新快取的條目。
- 此方法是可選的，但許多WPA2裝置仍不支援此方法，因此該方法並未被廣泛採用和部署。
- 執行控制器間漫遊時，不支援SKC。當在不同的WLC管理的AP之間移動時，即使這些AP位於同一個移動組上，也會發生這種情況。

## 使用機會式金鑰快取實現快速安全漫遊

機會式金鑰快取(OKC)，也稱為主動式金鑰快取(PKC)（本術語將在後面的說明中詳細解釋），基本上是對前面描述的WPA2 PMKID快取方法的增強，因此也稱為主動/機會PMKID快取。因此，必須注意的是，這不是由802.11標準定義的快速安全漫遊方法，且許多裝置不支援這種方法，但與PMKID快取一樣，它與WPA2-EAP一起使用。

即使在多個AP之間漫遊，該技術也允許無線客戶端和WLAN基礎設施在客戶端與此WLAN關聯的生存期內僅快取一個PMK（從與身份驗證伺服器進行初始802.1X/EAP身份驗證之後的MSK中匯出），因為它們都共用原始PMK，該原始PMK在所有WPA2 4次握手上用作種子。與SKC一樣，這仍然是必需的，以便每次客戶端與AP重新關聯時生成新的加密金鑰。要使AP共用來自客戶端會話的這個原始PMK，它們必須都處於某種管理控制之下，並配備一個集中式裝置，該裝置為所有AP快取並分發原始PMK。這類似於CUWN，其中WLC對其控制的所有LAP執行此作業，並使用移動組在多個WLC之間處理此PMK；因此，這是對自主AP環境的限制。

使用此方法(與PMKID快取(SKC)中的方法一樣，與任何AP的初始關聯都是對WLAN的常規首次身份驗證，在此過程中，您必須完成針對身份驗證伺服器的整個802.1X/EAP身份驗證以及金鑰生成的4次握手，然後才能傳送資料幀。以下是說明此問題的螢幕影象：



| No. | Time | Source | Destination | BSS Id | Protocol | Channel frequency | Info |
|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | 802.11 | 2462 | Authentication, SN=2421, FN=0, Flags=... |
| 2 | 0.001369 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | 802.11 | 2462 | Authentication, SN=3299, FN=0, Flags=... |
| 3 | 0.003199 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | 802.11 | 2462 | Association Request, SN=2422, FN=0, Flag |
| 4 | 0.008447 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | 802.11 | 2462 | Association Response, SN=3300, FN=0, Fla |
| 5 | 0.107400 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Identity |
| 6 | 0.121755 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 7 | 0.162562 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Client Hello |
| 8 | 0.178720 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 9 | 0.192059 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | EAP | 2462 | Response, Protected EAP (EAP-PEAP) |
| 10 | 0.207860 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 11 | 0.227297 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | EAP | 2462 | Response, Protected EAP (EAP-PEAP) |
| 12 | 0.231517 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 13 | 0.242089 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Certificate, Client Key Exchange, Change |
| 14 | 0.251854 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 15 | 0.254304 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | EAP | 2462 | Response, Protected EAP (EAP-PEAP) |
| 16 | 0.258723 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 17 | 0.265390 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Application Data, Application Data |
| 18 | 0.269769 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 19 | 0.272225 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Application Data, Application Data |
| 20 | 0.276927 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 21 | 0.280525 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Application Data, Application Data |
| 22 | 0.287232 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 23 | 0.290451 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Application Data, Application Data |
| 24 | 0.302861 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAP | 2462 | Request, Protected EAP (EAP-PEAP) |
| 25 | 0.313281 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | TLSv1 | 2462 | Application Data, Application Data |
| 26 | 0.337874 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAP | 2462 | Success |
| 27 | 0.339642 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAPOL | 2462 | Key (Message 1 of 4) |
| 28 | 0.353971 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | EAPOL | 2462 | Key (Message 2 of 4) |
| 29 | 0.358041 | Cisco_f0:68:d2 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | EAPOL | 2462 | Key (Message 3 of 4) |
| 30 | 0.378569 | Aironet_b7:ab:5c | Cisco_f0:68:d2 | 84:78:ac:f0:68:d2 | EAPOL | 2462 | Key (Message 4 of 4) |
| 31 | 0.462588 | Aironet_b7:ab:5c | Broadcast | 84:78:ac:f0:68:d2 | 802.11 | 2462 | QoS Data, SN=2437, FN=0, Flags=.p.....TC |
| 32 | 0.473985 | Cisco_f0:68:d0 | Aironet_b7:ab:5c | 84:78:ac:f0:68:d2 | 802.11 | 2462 | QoS Data, SN=81, FN=0, Flags=.p....F.C |

debug輸出顯示的EAP驗證訊框交換基本與對WLAN進行初始驗證時本文所述的其他方法相同（如圖所示），並新增了一些涉及WLC此處使用的關鍵快取技術的輸出。此偵錯輸出也會被剪下，以僅顯示相關資訊：

```
*apfMsConnTask_0: Jun 21 21:46:06.515: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID
  84:78:ac:f0:68:d2
!--- This is the Association Request from the client.

*apfMsConnTask_0: Jun 21 21:46:06.516: 00:40:96:b7:ab:5c
  Processing RSN IE type 48, length 20 for mobile
  00:40:96:b7:ab:5c
!--- The WLC/AP finds an Information Element that claims
     PMKID Caching support on the Association request that
     is sent from the client.

*apfMsConnTask_0: Jun 21 21:46:06.516: 00:40:96:b7:ab:5c
  Received RSN IE with 0 PMKIDs from mobile
  00:40:96:b7:ab:5c
!--- Since this is an initial association, the Association
     Request comes without any PMKID.

*apfMsConnTask_0: Jun 21 21:46:06.516: 00:40:96:b7:ab:5c
  Setting active key cache index 0 ---> 8

*apfMsConnTask_0: Jun 21 21:46:06.516: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID
  84:78:ac:f0:68:d2 (status 0) ApVapId 3 Slot
!--- The Association Response is sent to the client.

*dot1xMsgTask: Jun 21 21:46:06.522: 00:40:96:b7:ab:5
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 1)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.614: 00:40:96:b7:ab:5c
  Received EAPOL START from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.614: 00:40:96:b7:ab:5c
```

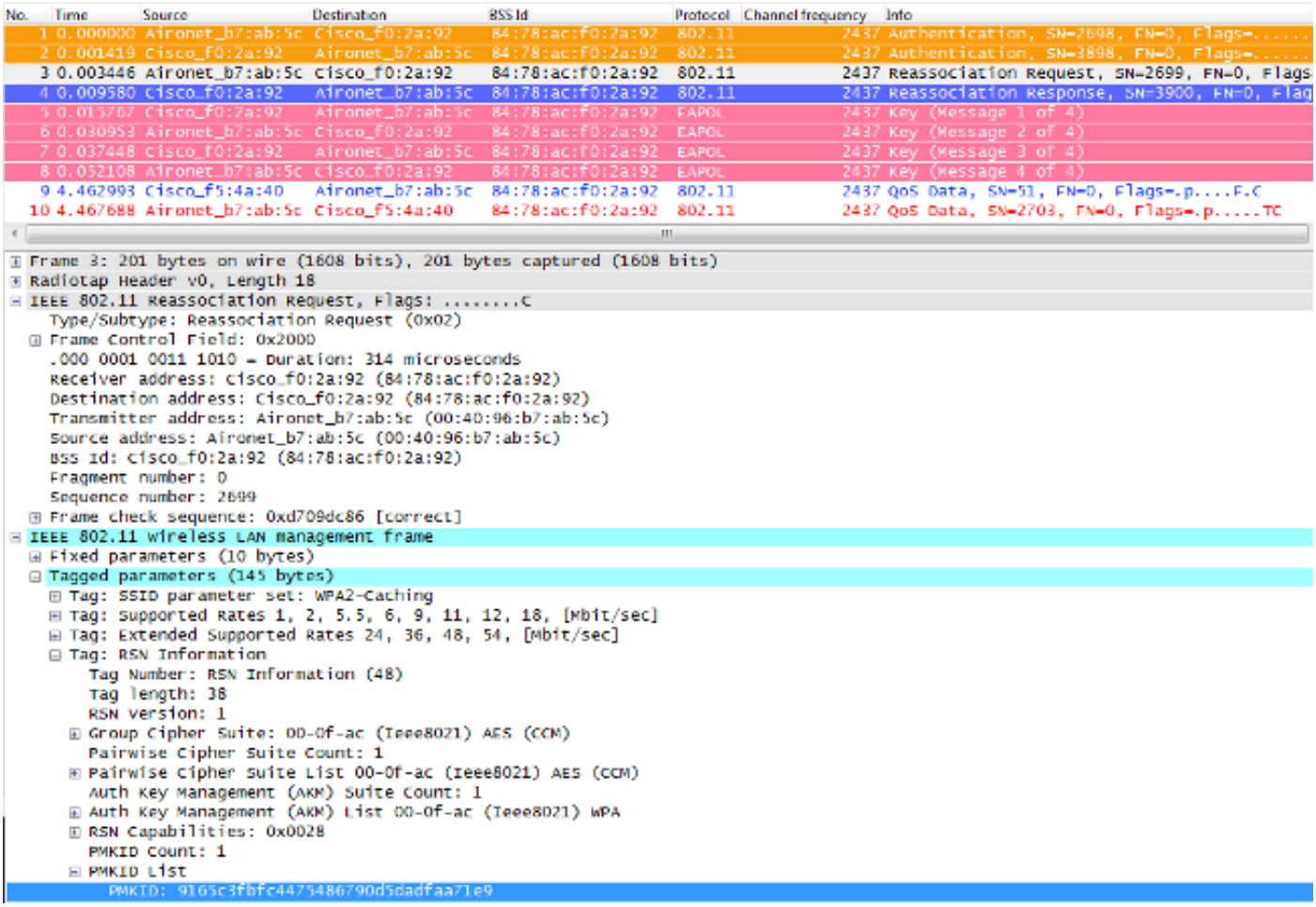
```
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 2)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.623: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.623: 00:40:96:b7:ab:5c
  Received Identity Response (count=2) from mobile
  00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.630: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.630: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 3)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.673: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.673: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 3, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.843: 00:40:96:b7:ab:5c
  Processing Access-Accept for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Creating a PKC PMKID Cache entry for station
  00:40:96:b7:ab:5c (RSN 2)
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 0
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Adding BSSID 84:78:ac:f0:68:d2 to PMKID cache at index 0
  for station 00:40:96:b7:ab:5
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: New PMKID: (16)
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844:
  [0000] 4e a1 7f 5a 75 48 9c f9 96 e3 a8 71 25 6f 11 d0
!--- WLC creates a PMK cache entry for this client, which is
     used for OKC in this case, so the PMKID is computed
     with the AP MAC address (BSSID 84:78:ac:f0:68:d2).

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  PMK sent to mobility group
!--- The PMK cache entry for this client is shared with the
     WLCs on the mobility group.

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Sending EAP-Success to mobile 00:40:96:b7:ab:5c (EAP Id 13)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Found an cache entry for BSSID 84:78:ac:f0:68:d2 in PMKID
  cache at index 0 of station 00:40:96:b7:ab:5

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: Including PMKID
  in M1  (16)
!--- The hashed PMKID is included on the Message-1 of the
     WPA/WPA2 4-Way handshake.

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844:
  [0000] 4e a1 7f 5a 75 48 9c f9 96 e3 a8 71 25 6f 11 d0
!--- This is the hashed PMKID. The next messages are the same
```

**WPA/WPA2 4-Way handshake messages described thus far that are used in order to finish the encryption keys generation/installation.**

```
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.865: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.865: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2)
  from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.865: 00:40:96:b7:ab:5c
  PMK: Sending cache add

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.865: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.889: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.890: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
```

使用此方法，無線客戶端和WLC（對於所有受管AP）快取最初建立的安全關聯的一個原始PMK。基本上，每次無線客戶端連線到特定AP時，都會根據以下條件對PMKID進行雜湊：客戶端MAC地址、AP MAC地址（WLAN的BSSID）以及該AP派生的PMK。因此，由於OKC為所有AP和特定客戶端快取相同的原始PMK，因此當此客戶端（重新）關聯到另一個AP時，為雜湊新PMKID而更改的唯一值是新的AP MAC地址。

當客戶端向新AP發起漫遊並傳送重新關聯請求幀時，如果它要通知AP快取的PMK用於快速安全漫遊，它將在WPA2 RSN資訊元素上新增PMKID。它知道漫遊位置的BSSID(AP)的MAC地址，然後客戶端只需雜湊此重新關聯請求上使用的新PMKID。當AP收到來自客戶端的此請求時，它還會使用已有的值（快取的PMK、客戶端MAC地址和自己的AP MAC地址）對PMKID進行雜湊，並使用成功的重新關聯響應進行響應，確認匹配的PMKID。快取的PMK可用作啟動WPA2 4次握手的種子，以便獲取新的加密金鑰（並跳過EAP）：




在此影象中，將選擇並展開來自客戶端的「重新關聯請求」幀，以便您可以看到該幀的更多詳細資訊。MAC地址資訊以及強大的安全網路（RSN，根據802.11i - WPA2）資訊元素，其中顯示了用於此關聯的WPA2設定的相關資訊（突出顯示的是從雜湊公式獲取的PMKID）。

以下是此使用OKC的快速安全漫遊方法的WLC偵錯摘要：

```
*apfMsConnTask_2: Jun 21 21:48:50.562: 00:40:96:b7:ab:5c
  Reassociation received from mobile on BSSID
  84:78:ac:f0:2a:92
!--- This is the Reassociation Request from the client.

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Processing RSN IE type 48, length 38 for mobile
  00:40:96:b7:ab:5c
!--- The WLC/AP finds and Information Element that claims
     PMKID Caching support on the Association request that
     is sent from the client.

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Received RSN IE with 1 PMKIDs from mobile
  00:40:96:b7:ab:5c
!--- The Reassociation Request from the client comes with
     one PMKID.

*apfMsConnTask_2: Jun 21 21:48:50.563:
  Received PMKID:  (16)

*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9
```

```
*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Searching for PMKID in MSCB PMKID cache for mobile
  00:40:96:b7:ab:5c
*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  No valid PMKID found in the MSCB PMKID cache for mobile
  00:40:96:b7:ab:5
!--- As the client has never authenticated with this new AP,
      the WLC cannot find a valid PMKID to match the one provided
      by the client. However, since the client performs OKC
      and not SKC (as per the following messages), the WLC computes
      a new PMKID based on the information gathered (the cached PMK,
      the client MAC address, and the new AP MAC address).

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Trying to compute a PMKID from MSCB PMK cache for mobile
  00:40:96:b7:ab:5c

*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: Find PMK in cache: BSSID =  (6)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 84 78 ac f0 2a 90
*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: Find PMK in cache: realAA =  (6)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 84 78 ac f0 2a 92
*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: Find PMK in cache: PMKID =  (16)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9
*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: AA (6)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 84 78 ac f0 2a 92
*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: SPA (6)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 00 40 96 b7 ab 5c
*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Adding BSSID 84:78:ac:f0:2a:92 to PMKID cache at
  index 0 for station 00:40:96:b7:ab:5c
*apfMsConnTask_2: Jun 21 21:48:50.563:
  New PMKID: (16)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9
*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Computed a valid PMKID from MSCB PMK cache for mobile
  00:40:96:b7:ab:5c
!--- The new PMKID is computed and validated to match the
      one provided by the client, which is also computed with
      the same information. Hence, the fast-secure roam is
      possible.

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Setting active key cache index 0 ---> 0

*apfMsConnTask_2: Jun 21 21:48:50.564: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:92
  (status 0) ApVapId 3 Slot
!--- The Reassociation response is sent to the client, which
      validates the fast-roam with OKC.

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c
  Initiating RSN with existing PMK to mobile
  00:40:96:b7:ab:5c
```

```
!--- WLC initiates a Robust Secure Network association with
     this client-and AP pair with the cached PMK found.
Hence, EAP is avoided, as per the the next message.

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c
  Skipping EAP-Success to mobile 00:40:96:b7:ab:5c

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c
  Found an cache entry for BSSID 84:78:ac:f0:2a:92 in
  PMKID cache at index 0 of station 00:40:96:b7:ab:5c

*dot1xMsgTask: Jun 21 21:48:50.570:
  Including PMKID in M1  (16)
!--- The hashed PMKID is included on the Message-1 of the
     WPA/WPA2 4-Way handshake.

*dot1xMsgTask: Jun 21 21:48:50.570:
  [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9
!--- The PMKID is hashed. The next messages are the same
     WPA/WPA2 4-Way handshake messages described thus far,
     which are used in order to finish the encryption keys
     generation/installation.

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2) from mobile
  00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5c
  PMK: Sending cache add

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.590: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.610: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.610: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
```

如調試的開頭所示，必須在收到來自客戶端的重新關聯請求之後計算PMKID。驗證PMKID並確認快取的PMK與WPA2 4次握手一起使用來獲取加密金鑰並完成快速安全漫遊時，需要執行此操作。請勿混淆調試中的CCKM條目；如前所述，這不是用於執行CCKM，而是OKC。這裡的CCKM只是WLC用於這些輸出的名稱，例如為計算PMKID而處理這些值的函式的名稱。

## 帶有機會式金鑰快取的FlexConnect

- 支援集中身份驗證。這包括本地和中央資料交換。如果AP屬於同一FlexConnect組，則快速安全漫遊由AP進行，否則快速安全漫遊由控制器進行。
  **注意**：如果AP不在同一FlexConnect組中，則此安裝程式可以運行，但這不是推薦的或支援的安裝程式。
- 支援Flex本地身份驗證。在連線模式下，快取可以從AP分發到控制器，然後分發到

FlexConnect組中的其他AP。
- 支援獨立模式。 如果AP上已經存在快取（由於以前的分發），則快速安全漫遊將起作用。獨立模式下的新身份驗證不支援快速安全漫遊。

### 使用機會式金鑰快取的優勢

- 無線使用者端和WLAN基礎架構不需要記住多個PMKID，只需將原始的PMK從初始驗證快取到WLAN即可。然後，您必須對每個AP安全關聯所需的正確PMKID（用於重新關聯請求）進行重新雜湊，以驗證快速安全漫遊。
- 在這裡，無線客戶端對同一WLAN/SSID上的新AP執行快速安全漫遊，即使它從未與該AP關聯（SKC的情況除外）。只要客戶端使用由集中部署管理的一個AP執行初始802.1X/EAP身份驗證，該集中部署為客戶端漫遊的所有AP處理PMK快取，則此WLAN上的其餘客戶端生存期不需要更多完全身份驗證。

### 使用機會式金鑰快取的缺點

- 此方法僅部署在一個集中式環境中，在該環境中，所有AP都處於某種管理控制之下（例如WLAN控制器），該管理控制負責快取和共用客戶端會話中的一個原始PMK。因此，這是對自治AP環境的限制。
- 802.11標準未建議或描述該方法中所使用的技術，因此不同裝置之間的支援差異很大。然而，這仍是等待802.11r時採用的方法。

### 有關「主動金鑰快取」術語的說明

主動金鑰快取（Proactive Key Caching，簡稱PKC）被稱為OKC（Opportational Key Caching，簡稱OKC），這兩個術語在描述此處介紹的相同方法時可以互換使用。但是，這只是Airspace在2001年使用的一個術語，用於舊的金鑰快取方法，然後被802.11i標準用作「預先驗證」的基礎（下面簡要介紹另一種快速安全漫遊方法）。PKC不是Preauthentication或OKC(Opportational Key Caching)，但當您聽到或讀到PKC時，參考基本上是OKC，而不是預先驗證。

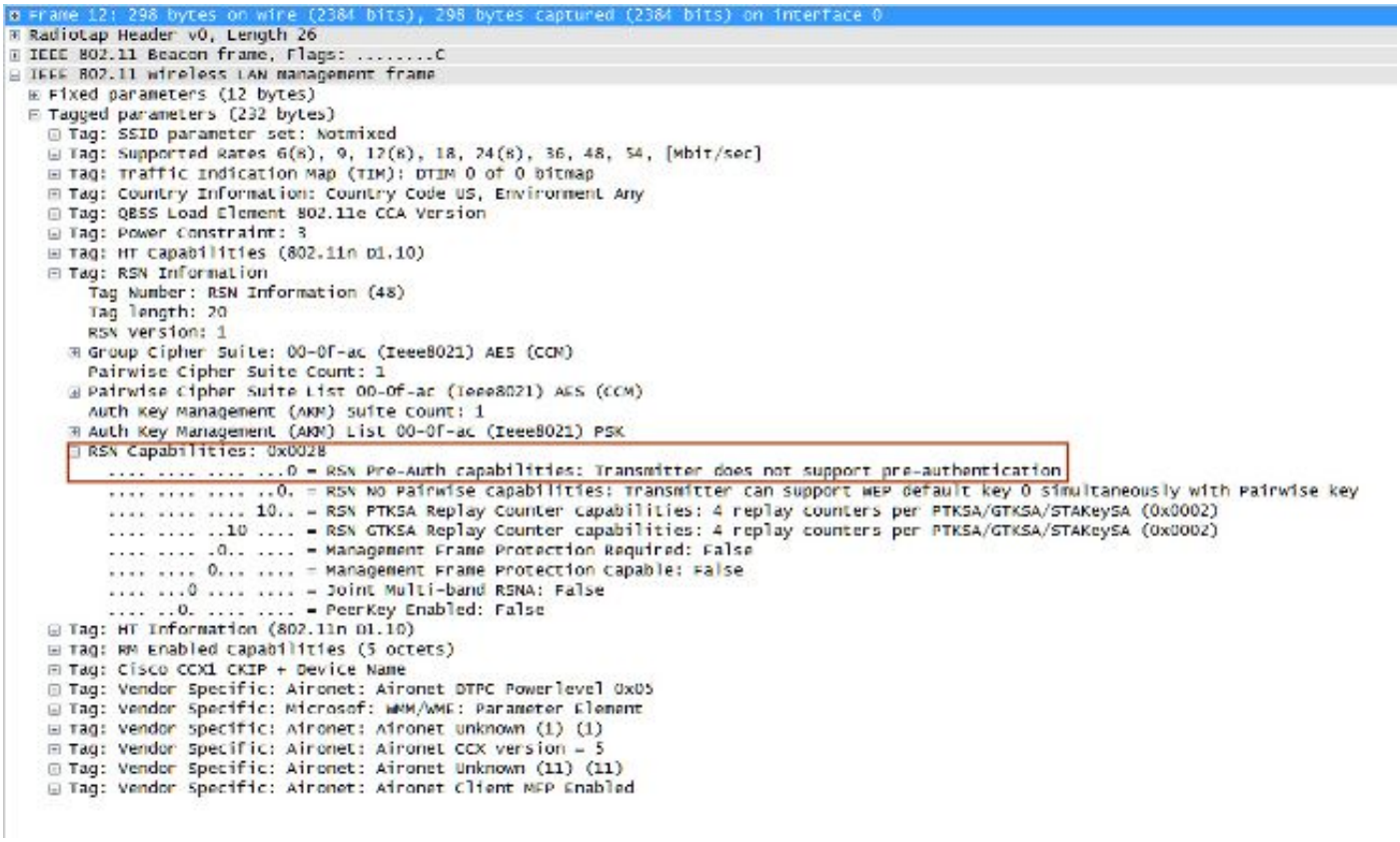
## 使用預先驗證的快速安全漫遊

802.11i安全修訂版中的IEEE 802.11標準也建議此方法，因此該方法也適用於WPA2，但它是唯一不受Cisco WLAN基礎設施支援的快速安全漫遊方法。因此，此處僅作簡要解釋，不作輸出。

使用預身份驗證，無線客戶端可以在與當前AP關聯的同時一次對多個AP進行身份驗證。發生這種情況時，客戶端將EAP身份驗證幀傳送到所連線的當前AP，但它將傳送到客戶端希望執行預先身份驗證的其他AP（鄰居AP可能是漫遊的候選對象）。當前AP通過分佈系統將這些幀傳送到目標AP。新AP對此客戶端的RADIUS伺服器執行完全身份驗證，因此整個新EAP身份驗證握手已完成，並且此新AP充當身份驗證器。

其思想是在客戶端實際漫遊到相鄰AP之前執行身份驗證並獲取PMK，因此，當需要漫遊時，客戶端已經通過身份驗證，並且已快取一個PMK，用於此新的AP到客戶端安全關聯，因此客戶端只需執行4次握手，並在客戶端傳送其初始Reassociation請求後體驗快速漫遊。

以下是來自AP信標的影象，其中顯示通告支援預身份驗證的RSN IE欄位（此欄位來自Cisco AP，其中確認不支援預身份驗證）：




### 預先驗證的Pros

每個AP到客戶端的安全關聯都有一個PMK，這可以被視為安全優勢，以防一個AP受到威脅且金鑰被盜（無法與其他AP一起使用）。但是，WLAN基礎架構在其他方法上以不同方式處理此安全優勢。

### 帶有預驗證的缺點

- 因為每個AP有一個PMK，所以客戶端對可以預先驗證的AP數量有限制。
- 每次客戶端使用新的AP執行預身份驗證時，都會有完整的EAP身份驗證交換，這意味著在網路上以及身份驗證伺服器上有更多負載。
- 大多數無線客戶端不支援此方法，因為它從未被高度採用（OKC更多地採用）。

## 802.11r快速安全漫遊

基於802.11r修正的快速安全漫遊技術(802.11標準正式命名為**Fast BSS Transition**，並稱為**FT**)是IEEE正式批准（2008年）的第一種802.11標準方法，它作為在AP（基本服務集或BSS）之間執行快速轉換的解決方案，明確定義了在WLAN上處理金鑰和快取金鑰時使用的金鑰層次結構。但是，它的採用一直很慢，這主要是因為在實際上需要快速轉換時已經提供了其他解決方案，例如與本文檔中前面介紹的方法之一一起使用時的VoWLAN實施。目前只有少數裝置支援英國《金融時報》的某些選項（到2013年）。

與其他方法相比，此技術解釋起來更為複雜，因為它引入了快取於不同裝置（每個裝置具有不同的角色）上的新概念和多層PMK，並且提供了更多快速安全漫遊選項。因此，簡要概述這種方法以及在每個可用的選項下實現的方法。

802.11r與SKC和OKC不同，主要是因為以下原因：

- 握手消息（例如PMKID、ANonce和SNonce交換）發生在802.11身份驗證幀或操作幀中，而不是重新關聯幀。與PMKID快取方法不同，避免了（重新）關聯消息交換之後進行的單獨的4次握手階段。與新AP的金鑰握手在客戶端完全漫遊或重新關聯此新AP之前開始。
- 它為快速漫遊握手提供了兩種方法：通過AIR和分散式系統(DS)。
- 802.11r具有更多金鑰層級。
- 由於此協定避免了客戶端漫遊時金鑰管理的4次握手（無需此握手即可生成新的加密金鑰 — PTK和GTK），因此它還可以應用於具有PSK的WPA2設定，而不僅僅是在使用802.1X/EAP進行身份驗證時。對於不發生EAP或4路握手交換的設定，這會進一步加快漫遊。

通過這種方法，當與第一AP建立連線時，無線客戶端僅對WLAN基礎設施執行一次初始認證，並且在相同FT移動域的AP之間漫遊時執行快速安全漫遊。

這是其中一個新概念，它主要是指使用同一SSID（稱為擴展服務集或ESS）並處理相同FT金鑰的AP。這與迄今為止解釋的其他方法類似。AP處理FT移動域金鑰的方式通常基於集中設定，例如WLC或移動組；但是，此方法也可以在自主AP環境中實施。

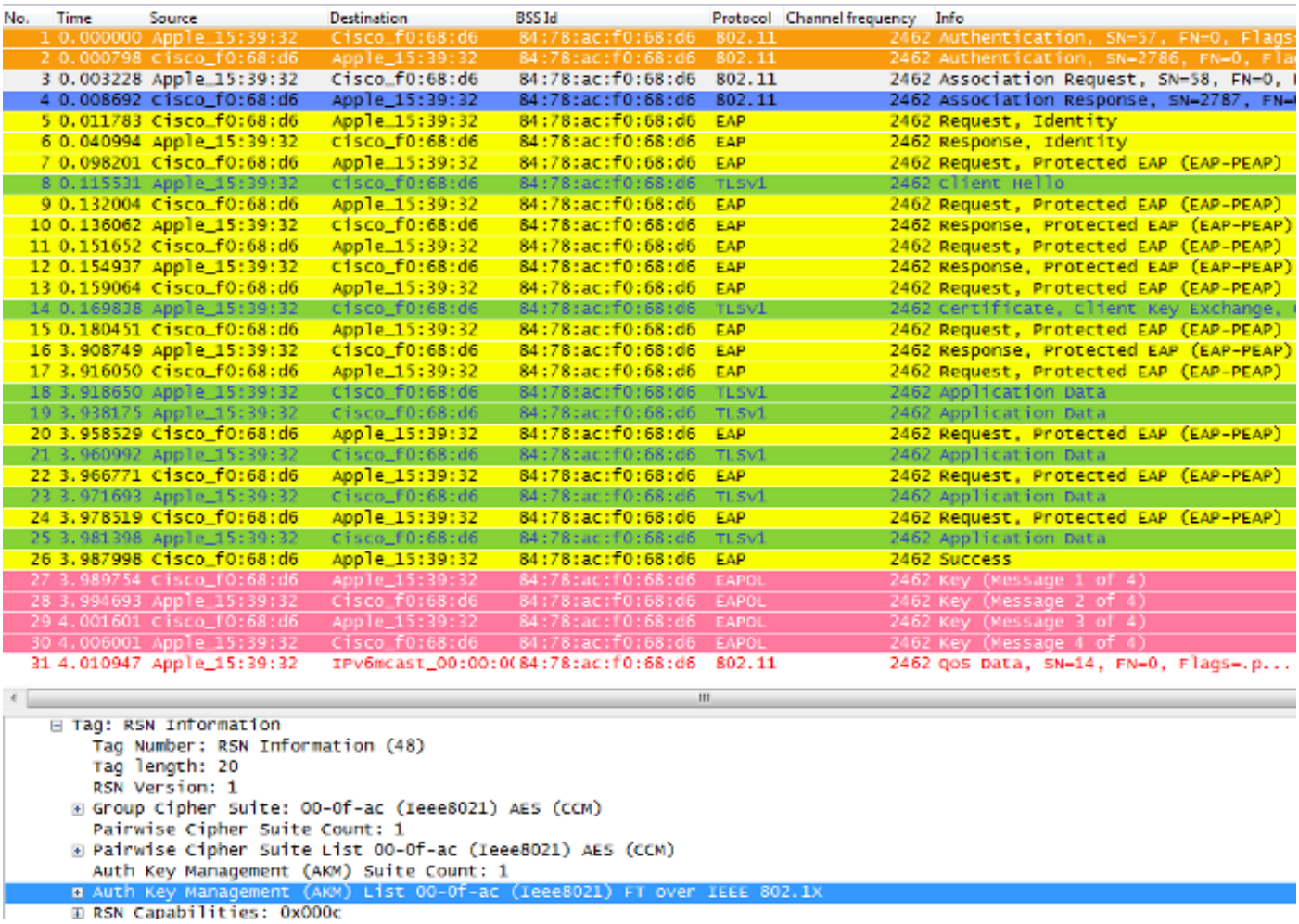
以下是關鍵層次結構的摘要：

- MSK仍然從初始802.1X/EAP身份驗證階段(身份驗證成功後，從身份驗證伺服器傳輸到身份驗證器(WLC))派生到客戶端請求方和身份驗證伺服器。與其它方法一樣，此MSK用作FT金鑰層次結構的種子。當您使用WPA2-PSK而不是EAP身份驗證方法時，PSK基本上是此MSK。
- 成對主金鑰R0(PMK-R0)從MSK匯出，MSK是FT金鑰層次的第一級金鑰。此PMK-R0的金鑰持有者是WLC和客戶端。
- 第二級金鑰稱為Pairwise主金鑰R1(PMK-R1)，從PMK-R0派生，金鑰持有者是客戶端和由WLC管理、持有PMK-R0的AP。
- FT金鑰層次結構的第三級也是最後一級金鑰是PTK，它是用於加密802.11單播資料幀的最終金鑰（類似於使用WPA/TKIP或WPA2/AES的其他方法）。此PTK在FT上從PMK-R1派生，金鑰持有者是客戶端和WLC管理的AP。

  **註**：根據WLAN供應商和實施設定（如自治AP、FlexConnect或網狀），WLAN基礎設施可以採用不同的方式傳輸和處理金鑰。它甚至可以更改金鑰持有者的角色，但由於這超出了本文檔的範圍，因此基於前面給出的金鑰層次結構彙總的示例將是下一個焦點。這些差異實際上與理解該過程無關，除非您實際上需要深入分析基礎設施裝置（及其代碼）以發現軟體問題。

## 空中BSS快速過渡

使用此方法，與任何AP的第一個關聯都是對WLAN的常規首次身份驗證，其中針對身份驗證伺服器的整個802.1X/EAP身份驗證和金鑰生成的4次握手必須在傳送資料幀之前進行，如下螢幕影象所示：




主要區別是：

- 身份驗證金鑰管理協商與常規WPA/WPA2略有不同，因此當與支援FT的WLAN基礎設施發生關聯時，會使用一些額外資訊來執行此協商。如圖所示，選擇來自客戶端的關聯請求幀，並突出顯示RNS資訊元素的AKM欄位，以便顯示此客戶端想要執行基於802.1X/EAP的FT。
- 還顯示了移動域資訊元素（FT的一部分），其中**FT Capability and Policy**欄位指示快速漫遊時是否通過空中或通過DS完成快速BSS過渡（在此圖中顯示通過空中）。
- 還新增另一個資訊元素（快速BSS轉換或FT IE，本文檔稍後將對此進行描述）在FT漫遊時執行FT身份驗證序列所需的資訊。
- 金鑰生成因金鑰層次結構而異，因此，即使FT四向握手看起來與WPA/WPA2四向握手類似，其內容實際上略有不同。

偵錯顯示基本與WLAN初始驗證時的其餘方法相同的EAP驗證幀交換（如圖所示），但新增了與WLC使用的關鍵快取技術有關的一些輸出；因此，剪下此調試輸出以僅顯示相關資訊：

```
*apfMsConnTask_0: Jun 27 19:25:23.426: ec:85:2f:15:39:32
  Association received from mobile on BSSID
  84:78:ac:f0:68:d6
!--- This is the Association request from the client.

*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Marking this mobile as TGr capable.
!--- WLC recognizes that the client is 802.11r-capable.

*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 20 for mobile
  ec:85:2f:15:39:32
```

**!--- The WLC/AP finds an Information Element that claims FT support on the Association request that is sent from the client.**

```
*apfMsConnTask_0: Jun 27 19:25:23.427:
  Sending assoc-resp station:ec:85:2f:15:39:32
  AP:84:78:ac:f0:68:d0-00 thread:144be808
*apfMsConnTask_0: Jun 27 19:25:23.427:
  Adding MDIE, ID is:0xaaf0
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Including FT Mobility Domain IE (length 5) in Initial
  assoc Resp to mobile
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Sending R0KH-ID as:-84.30.6.-3
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Sending R1KH-ID as 3c:ce:73:d8:02:00
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Including FT IE (length 98) in Initial Assoc Resp to mobile
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d6
  (status 0) ApVapId 7 Slot 0
```

**!--- The Association Response is sent to the client once the FT information is computed (as per the previous messages), so this is included in the response.**

```
*dot1xMsgTask: Jun 27 19:25:23.432: ec:85:2f:15:39:32
  Sending EAP-Request/Identity to mobile ec:85:2f:15:39:32
  (EAP Id 1)
```

**!--- EAP begins, and follows the same exchange explained so far.**

```
*apfMsConnTask_0: Jun 27 19:25:23.436: ec:85:2f:15:39:32
  Got action frame from this client.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.449: ec:85:2f:15:39:32
  Received EAPOL EAPPKT from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.449: ec:85:2f:15:39:32
  Received Identity Response (count=1) from mobile
  ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.456: ec:85:2f:15:39:32
  Processing Access-Challenge for mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.456: ec:85:2f:15:39:32
  Sending EAP Request from AAA to mobile ec:85:2f:15:39:32
  (EAP Id 2)

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.479: ec:85:2f:15:39:32
  Received EAPOL EAPPKT from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.479: ec:85:2f:15:39:32
  Received EAP Response from mobile ec:85:2f:15:39:32
  (EAP Id 2, EAP Type 25)

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.627: ec:85:2f:15:39:32
  Processing Access-Accept for mobile ec:85:2f:15:39:32
```

**!--- The client is validated/authenticated by the RADIUS Server.**

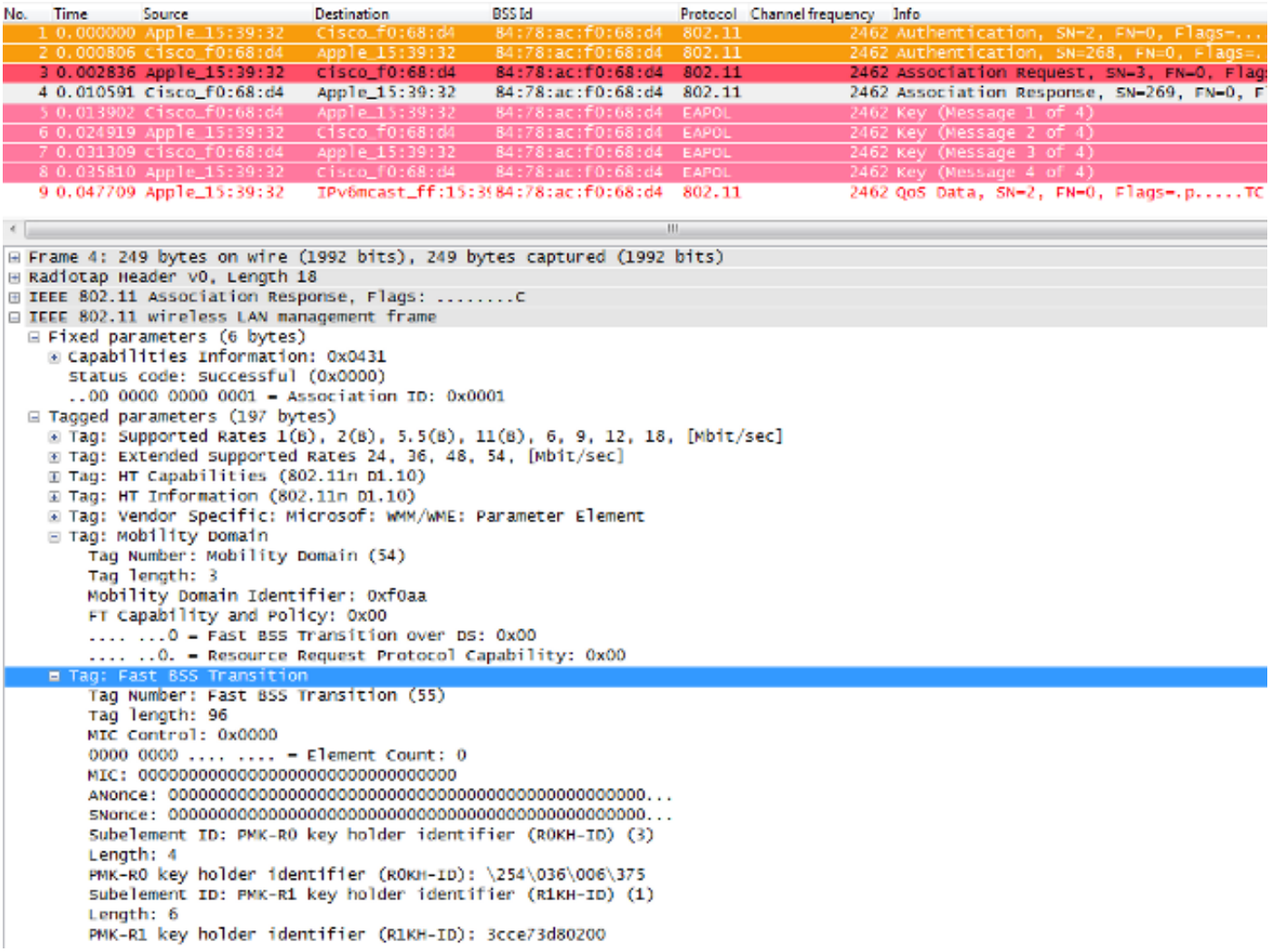
```
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.627: ec:85:2f:15:39:32
  Creating a PKC PMKID Cache entry for station
  ec:85:2f:15:39:32 (RSN 2)
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.627: ec:85:2f:15:39:32
  Resetting MSCB PMK Cache Entry 0 for station
  ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.627: ec:85:2f:15:39:32
```

```
  Setting active key cache index 8 ---> 8
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.628: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 0
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.628: ec:85:2f:15:39:32
  Adding BSSID 84:78:ac:f0:68:d6 to PMKID cache at index 0
  for station ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.628: New PMKID: (16)
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.628:
  [0000] 52 b8 8f cf 50 a7 90 98 2b ba d6 20 79 e4 cd f9
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.629: ec:85:2f:15:39:32
  Created PMK Cache Entry for TGr AKM:802.1x ec:85:2f:15:39:32
!--- WLC creates a PMK cache entry for this client, which is
      used for FT with 802.1X in this case, so the PMKID is
      computed with the AP MAC address (BSSID 84:78:ac:f0:68:d6).

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.629:
  ec:85:2f:15:39:32   R0KH-ID:172.30.6.253
  R1KH-ID:3c:ce:73:d8:02:00  MSK Len:48 pmkValidTime:1807
!--- The R0KH-ID and R1KH-ID are defined, as well as the PMK
      cache validity period.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: ec:85:2f:15:39:32
  PMK sent to mobility group
!--- The FT PMK cache entry for this client is shared with the
      WLCs on the mobility group.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: ec:85:2f:15:39:32
  Sending EAP-Success to mobile ec:85:2f:15:39:32 (EAP Id 12)

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: ec:85:2f:15:39:32
  Found an cache entry for BSSID 84:78:ac:f0:68:d6 in PMKID
  cache at index 0 of station ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: Including PMKID in
  M1  (16)
!--- The hashed PMKID is included on the Message-1 of the
      initial FT 4-Way handshake.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630:
  [0000] 52 b8 8f cf 50 a7 90 98 2b ba d6 20 79 e4 cd f9

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  INITPMK (message 1), replay counter 00.00.00.00.00.00.00.0
!--- Message-1 of the FT 4-Way handshake is sent from the
      WLC/AP to the client.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Received EAPOL-key in PTK_START state (message 2) from
  mobile ec:85:2f:15:39:32
!--- Message-2 of the FT 4-Way handshake is received
      successfully from the client.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Calculating PMKR0Name
!--- The PMKR0Name is calculated.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  DOT11R: Sending cache add

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: Adding MDIE,
  ID is:0xaaf0
```

```
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Adding TIE for reassociation deadtime:20000 milliseconds
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Adding TIE for R0Key-Data valid time :1807
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.640: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- After the MDIE, TIE for reassociation deadtime, and TIE
     for R0Key-Data valid time are calculated, the Message-3
     of this FT 4-Way handshake is sent from the WLC/AP to the
     client with this information.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.651: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.651: ec:85:2f:15:39:32
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile ec:85:2f:15:39:32
!--- Message-4 (final message) of this initial FT 4-Way handshake
     is received successfully from the client, which confirms the
     installation of the derived keys. They can now be used in order
     to encrypt data frames with the current AP.
```

**註**：為了調試此方法並達到此處顯示的額外802.11r/FT輸出，將啟用附加調試以及debug client(即debug ft events enable)。

以下是使用WPA2-PSK（而不是802.1X/EAP方法）執行FT時，與WLAN的初始關聯的映像和調試，其中選擇來自AP的關聯響應幀以顯示快速BSS轉換資訊元素（突出顯示）。執行FT四向握手所需的一些關鍵資訊也顯示出來：



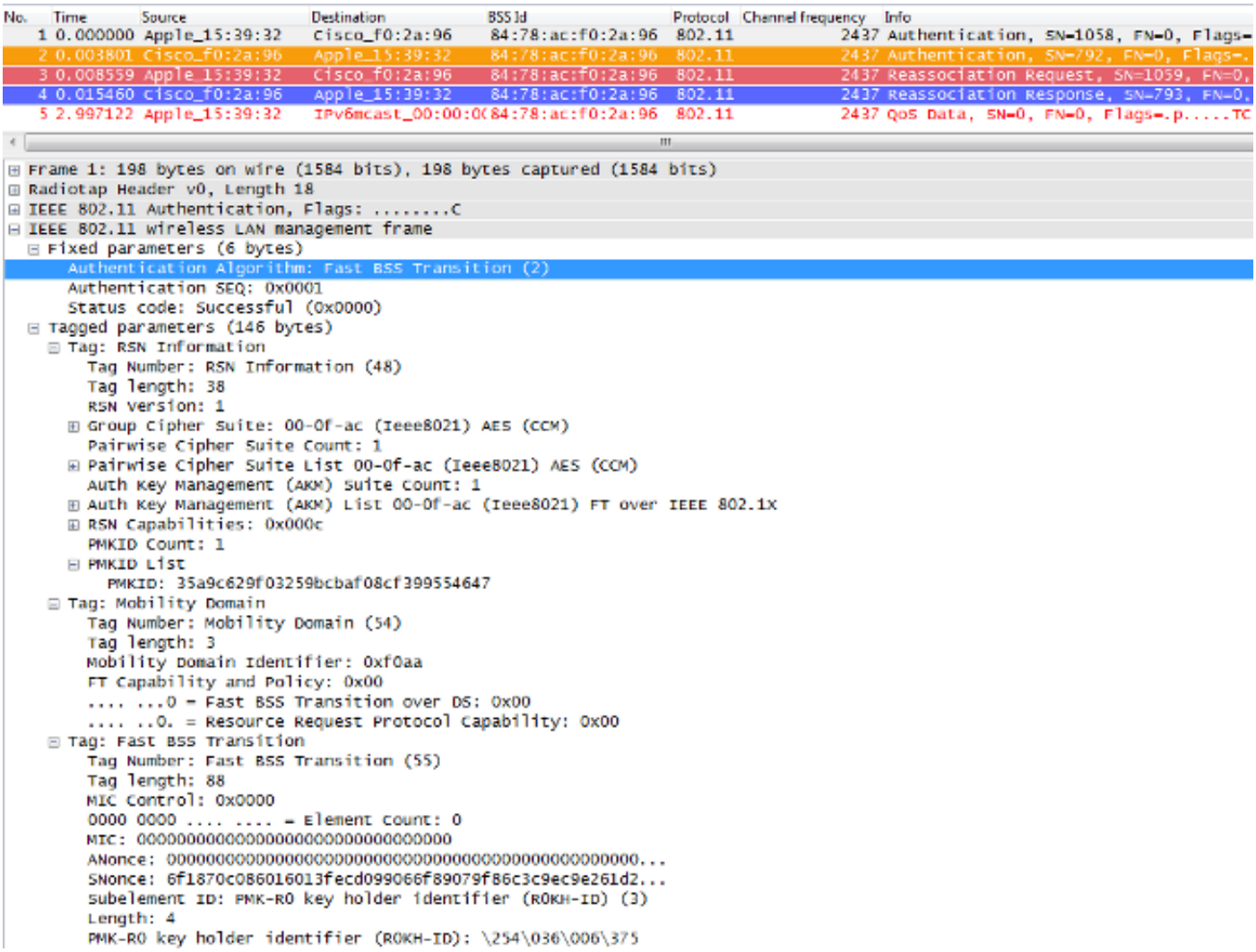

```
*apfMsConnTask_0: Jun 27 19:29:09.136: ec:85:2f:15:39:32
  Association received from mobile on BSSID
  84:78:ac:f0:68:d4

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Marking this mobile as TGr capable.

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 20 for mobile
  ec:85:2f:15:39:32

*apfMsConnTask_0: Jun 27 19:29:09.137: Sending assoc-resp
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:68:d0-00
  thread:144be808

*apfMsConnTask_0: Jun 27 19:29:09.137: Adding MDIE,
  ID is:0xaaf0

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Including FT Mobility Domain IE (length 5) in Initial
  assoc Resp to mobile

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Sending R0KH-ID as:-84.30.6.-3

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Sending R1KH-ID as 3c:ce:73:d8:02:00

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
```

```
  Including FT IE (length 98) in Initial Assoc Resp to mobile

*apfMsConnTask_0: Jun 27 19:29:09.138: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d4
  (status 0) ApVapId 5 Slot 0

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Creating a PKC PMKID Cache entry for station
  ec:85:2f:15:39:32 (RSN 2)

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Resetting MSCB PMK Cache Entry 0 for station
  ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 8

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 0

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Adding BSSID 84:78:ac:f0:68:d4 to PMKID cache at
  index 0 for station ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.142: New PMKID: (16)

*dot1xMsgTask: Jun 27 19:29:09.142:
  [0000] 17 4b 17 5c ed 5f c7 1d 66 39 e9 5d 3a 63 69 e7

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  Creating global PMK cache for this TGr client

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  Created PMK Cache Entry for TGr AKM:PSK
  ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  R0KH-ID:172.30.6.253   R1KH-ID:3c:ce:73:d8:02:00
  MSK Len:48 pmkValidTime:1813

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  Initiating RSN PSK to mobile ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  Found an cache entry for BSSID 84:78:ac:f0:68:d4 in
  PMKID cache at index 0 of station ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.142: Including PMKID
  in M1  (16)

*dot1xMsgTask: Jun 27 19:29:09.142:
  [0000] 17 4b 17 5c ed 5f c7 1d 66 39 e9 5d 3a 63 69 e7

*dot1xMsgTask: Jun 27 19:29:09.143: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00

*apfMsConnTask_0: Jun 27 19:29:09.144: ec:85:2f:15:39:32
  Got action frame from this client.

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.152: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32
```

```
*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: ec:85:2f:15:39:32
  Received EAPOL-key in PTK_START state (message 2) from
  mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: ec:85:2f:15:39:32
  Calculating PMKR0Name

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: Adding MDIE,
  ID is:0xaaf0

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: ec:85:2f:15:39:32
  Adding TIE for reassociation deadtime:20000 milliseconds

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: ec:85:2f:15:39:32
  Adding TIE for R0Key-Data valid time :1813

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.154: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.163: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.163: ec:85:2f:15:39:32
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile ec:85:2f:15:39:32
```

在802.11r中，與WLAN的初始關聯是衍生此技術使用的基本金鑰的基礎，就像其它快速安全漫遊方法一樣。主要區別在於客戶端開始漫遊時；FT不僅在使用時會避免802.1X/EAP，而且實際上會執行更高效的漫遊方法，將最初的802.11開放系統身份驗證和重新關聯幀（在AP之間漫遊時始終使用並且需要這些幀）結合起來以交換FT資訊並衍生新的動態加密金鑰來代替4次握手。

下一張圖顯示當執行具有802.1X/EAP安全的快速BSS空中轉換時交換的幀。選擇從客戶端到AP的開放式系統身份驗證幀，以便檢視開始FT金鑰協商所需的FT協定資訊元素。這用於使用新的AP（基於PMK-R1）派生新的PTK。突出顯示顯示身份驗證演算法的欄位，以顯示此客戶端不執行簡單的開放系統身份驗證，而是執行快速BSS轉換：

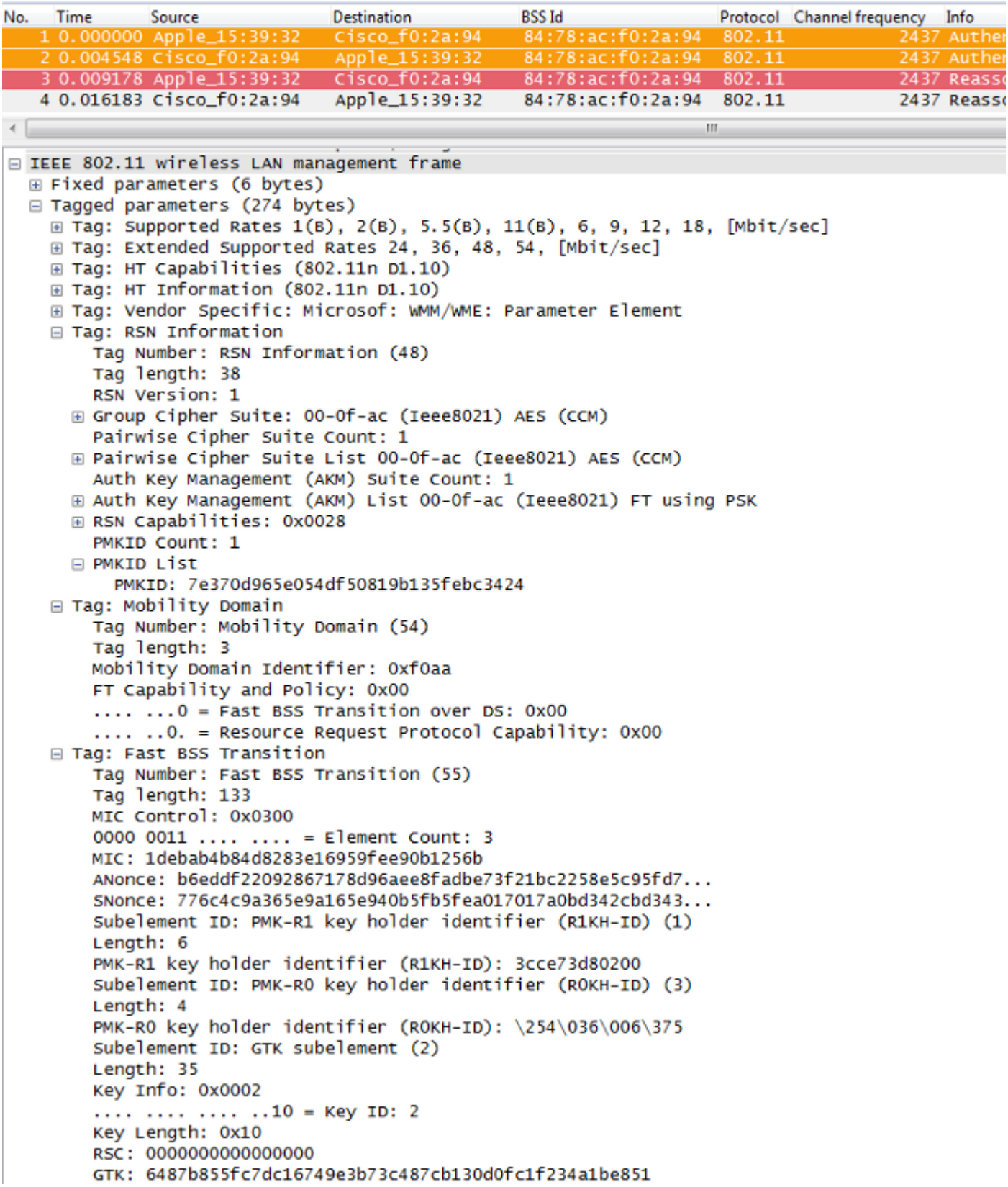



以下是在802.1X/EAP發生此FT漫遊事件時WLC的調試輸出：

```
*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  Doing preauth for this client over the Air
!--- WLC begins FT fast-secure roaming over-the-Air with
      this client and performs a type of preauthentication,
      because the client asks for this with FT on the Authentication
      frame that is sent to the new AP over-the-Air
      (before the Reassociation Request).

*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  Doing local roaming for destination address
  84:78:ac:f0:2a:96
!--- WLC performs the local roaming event with the new AP to
      which the client roams.

*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  Got 1 AKMs in RSNIE
*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  RSNIE AKM matches with PMK cache entry :0x3
!--- WLC receives one PMK from this client (known as AKM here),
      which matches the PMK cache entry hold for this client.

*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  Created a new preauth entry for AP:84:78:ac:f0:2a:96
*apfMsConnTask_2: Jun 27 19:25:48.751: Adding MDIE,
  ID is:0xaaf0
!--- WLC creates a new preauth entry for this AP-and-Client pair,
```

```
     and adds the MDIE information.

*apfMsConnTask_2: Jun 27 19:25:48.763: Processing assoc-req
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a:90-00
  thread:144bef38
*apfMsConnTask_2: Jun 27 19:25:48.763: ec:85:2f:15:39:32
  Reassociation received from mobile on BSSID
  84:78:ac:f0:2a:96
!--- Once the client receives the Authentication frame reply from the
     WLC/AP, the Reassociation request is sent, which is received at
     the new AP to which the client roams.

*apfMsConnTask_2: Jun 27 19:25:48.764: ec:85:2f:15:39:32
  Marking this mobile as TGr capable.

*apfMsConnTask_2: Jun 27 19:25:48.764: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 38 for mobile
  ec:85:2f:15:39:32

*apfMsConnTask_2: Jun 27 19:25:48.765: ec:85:2f:15:39:32
  Roaming succeed for this client.
!--- WLC confirms that the FT fast-secure roaming is successful
     for this client.

*apfMsConnTask_2: Jun 27 19:25:48.765: Sending assoc-resp
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a:90-00
  thread:144bef38
*apfMsConnTask_2: Jun 27 19:25:48.766: Adding MDIE,
  ID is:0xaaf0
*apfMsConnTask_2: Jun 27 19:25:48.766: ec:85:2f:15:39:32
  Including FT Mobility Domain IE (length 5) in
  reassociation assoc Resp to mobile
*apfMsConnTask_2: Jun 27 19:25:48.766: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:96
  (status 0) ApVapId 7 Slot 0
!--- The Reassociation response is sent to the client, which
     includes the FT Mobility Domain IE.

*dot1xMsgTask: Jun 27 19:25:48.769: ec:85:2f:15:39:32
  Finishing FT roaming for mobile ec:85:2f:15:39:32
!--- FT roaming finishes and EAP is skipped (as well as any
     other key management handshake), so the client is ready
     to pass encrypted data frames with the current AP.

*dot1xMsgTask: Jun 27 19:25:48.769: ec:85:2f:15:39:32
  Skipping EAP-Success to mobile ec:85:2f:15:39:32
```

此圖顯示了具有WPA2-PSK安全性的BSS空中快速過渡，其中選擇從AP到客戶端的最終「重新關聯響應」幀，以顯示有關FT交換的更多詳細資訊：




以下是使用PSK發生此FT漫遊事件時的調試輸出，與使用802.1X/EAP時的輸出類似：

```
*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  Doing preauth for this client over the Air

*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  Doing local roaming for destination address
  84:78:ac:f0:2a:94
```

```
*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  Got 1 AKMs in RSNIE

*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  RSNIE AKM matches with PMK cache entry :0x4

*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  Created a new preauth entry for AP:84:78:ac:f0:2a:94

*apfMsConnTask_2: Jun 27 19:29:29.854: Adding MDIE,
  ID is:0xaaf0

*apfMsConnTask_2: Jun 27 19:29:29.867: Processing assoc-req
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a:90-00
  thread:144bef38

*apfMsConnTask_2: Jun 27 19:29:29.867: ec:85:2f:15:39:32
  Reassociation received from mobile on BSSID
  84:78:ac:f0:2a:94

*apfMsConnTask_2: Jun 27 19:29:29.868: ec:85:2f:15:39:32
  Marking this mobile as TGr capable.

*apfMsConnTask_2: Jun 27 19:29:29.868: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 38 for mobile
  ec:85:2f:15:39:32

*apfMsConnTask_2: Jun 27 19:29:29.869: ec:85:2f:15:39:32
  Roaming succeed for this client.

*apfMsConnTask_2: Jun 27 19:29:29.869: Sending assoc-resp
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a:90-00
  thread:144bef38

*apfMsConnTask_2: Jun 27 19:29:29.869: Adding MDIE,
  ID is:0xaaf0

*apfMsConnTask_2: Jun 27 19:29:29.869: ec:85:2f:15:39:32
  Including FT Mobility Domain IE (length 5) in
  reassociation assoc Resp to mobile

*apfMsConnTask_2: Jun 27 19:29:29.870: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID
  84:78:ac:f0:2a:94 (status 0) ApVapId 5 Slot 0

*dot1xMsgTask: Jun 27 19:29:29.874: ec:85:2f:15:39:32
  Finishing FT roaming for mobile ec:85:2f:15:39:32
```

如圖所示，一旦在與WLAN的初始關聯時協商快速BSS轉換，漫遊時使用和所需的四個幀（來自客戶端的開放系統身份驗證、來自AP的開放系統身份驗證、重新關聯請求和重新關聯響應）基本上被用作FT四向握手，以便獲取新的PTK（單播加密金鑰）和GTK（組播/廣播加密金鑰）。

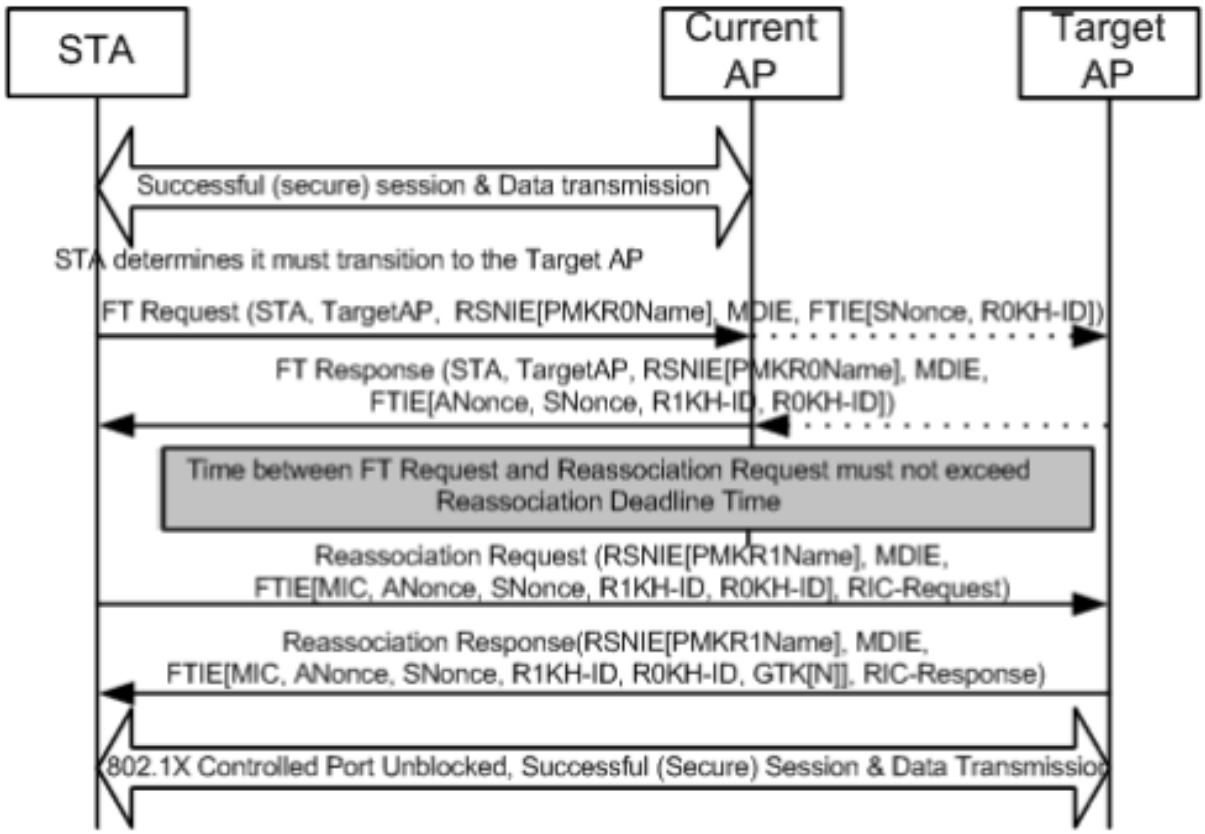
這替代了交換這些幀後通常發生的4次握手，並且無論您使用802.1X/EAP還是PSK作為安全方法，這些幀上的FT內容和金鑰協商基本相同。如圖所示，AKM欄位是主要區別，它確認客戶端是否使用PSK或802.1X執行FT。因此，必須注意的是，這四個幀通常沒有這種型別的用於金鑰協商的安全資訊，但是只有當客戶端FT漫遊時，才實施了802.11r，並且在初始關聯時在客戶端和WLAN基礎設施之間進行了協商。

## 通過DS實現快速BSS過渡

802.11r允許實施另一次快速BSS過渡，即由客戶端使用新的AP啟動FT漫遊，客戶端通過DS（分佈系統）進行漫遊，而不是通過無線進行。在這種情況下，使用FT Action幀來啟動金鑰協商，而不是使用開放式系統身份驗證幀。

基本上，一旦客戶端決定可以漫遊到更好的AP，客戶端會向當前連線的原始AP傳送FT操作請求幀，然後進行漫遊。客戶端指示它要漫遊的目標接入點的BSSID（MAC地址）。原始AP通過分佈系統（通常為有線基礎設施）將此FT操作請求幀轉發到目標AP，目標AP使用FT操作響應幀（也通過DS）響應客戶端，以便最終可以無線傳送到客戶端)。一旦此FT操作幀交換成功，客戶端完成FT漫遊；客戶端向目標AP傳送重新關聯請求（這次通過空中），並從新AP接收重新關聯響應，以確認漫遊和最終金鑰派生。

總之，有四個幀用於協商快速BSS轉換和匯出新的加密金鑰，但在這裡，開放系統身份驗證幀替換為FT操作請求/響應幀，這些幀通過分發系統用當前AP與目標AP交換。此方法也適用於安全方法802.1X/EAP和PSK，所有這些方法都受Cisco無線LAN控制器支援；但是，由於WiFi行業中的大多數無線客戶端不支援和實施此Over-the-DS轉換（並且由於幀交換和調試輸出基本上相同），因此本文檔中並未提供示例。相反，此影象用於直觀顯示Fast BSS Transition Over-the-DS:




## 採用802.11r的FlexConnect

- 支援集中身份驗證。這包括本地和中央資料交換。AP必須屬於同一個FlexConnect組。
- 不支援本地身份驗證。
- 不支援獨立模式。

## 802.11r的優勢

- 此方法首先使用IEEE在802.11標準上明確界定的關鍵層級作為修訂(802.11r)，因此這些FT技術的實施在供應商之間更相容，且沒有不同的解釋。

- 802.11r允許多種技術，根據您的需求有所幫助（空上和空中，適用於802.1x/EAP安全性和PSK安全性）。
- 無線客戶端對同一WLAN/SSID上的新AP執行快速安全漫遊，即使它從未與該AP關聯，也不需要儲存多個PMKID。
- 這是第一種快速安全漫遊方法，即使具有PSK安全性，也能實現更快的漫遊，並避免在使用WPA/WPA2 PSK的AP之間漫遊時所需的4次握手。快速安全漫遊方法的主要目的是在實現此安全方法時避免802.1X/EAP握手；但是，對於PSK安全，在避免4次握手時，使用802.11r可進一步加速漫遊事件。

### 802.11r的缺點

- 有一些無線客戶端裝置實際上支援快速BSS過渡，在大多數情況下，它們並不支援802.11r上提供的所有技術。
- 由於這些實施非常年輕，所以沒有足夠的測試結果或足夠的調試結果來解決可能出現的警告。
- 當您配置WLAN/SSID以使用任何FT方法時，只有支援802.11r的無線客戶端才能連線到此WLAN/SSID。FT設定對於客戶端不是可選的，因此那些不支援802.11r的無線客戶端必須連線到一個單獨的WLAN/SSID，其中FT完全未配置。

### 自適應802.11r

- 某些舊版客戶端無法與已啟用802.11r的WLAN/SSID關聯，即使對「混合模式」也是如此（您希望可以在支援和不支援802.11r的相同SSID客戶端上擁有該客戶端）。這表示負責解析強大的安全網路資訊元素(RSN IE)的客戶端請求方的驅動程式較舊，並且不知道IE中的其他AKM套件。由於此限制，客戶端無法向通告802.11r支援的WLAN傳送關聯請求，因此，您需要為802.11r客戶端配置一個WLAN/SSID，為不支援802.11r的客戶端配置一個單獨的WLAN/SSID。
- 為了解決此問題，思科無線區域網基礎架構引入了自適應802.11r功能。當FT模式在WLAN級別設定為Adaptive時，WLAN將在啟用802.11i的WLAN上通告802.11r移動域ID。有些Apple iOS10客戶端裝置識別80211i/WPA2 WLAN上存在MDIE，並執行專有握手來建立802.11r關聯。一旦客戶端成功完成802.11r關聯，它就可以像在正常啟用802.11r的WLAN中一樣進行FT漫遊。FT自適應僅適用於選定的Apple iOS10（及更高版本）裝置。所有其他使用者端可以在WLAN上繼續有802.11i/WPA2關聯，並執行支援的適用FSR方法。
- 有關為iOS10裝置在並未真正啟用802.11r（以便其他非802.11r客戶端可以成功連線）的WLAN/SSID上執行802.11r所引入的這一新功能的更多文檔，請參閱Cisco無線LAN上Cisco IOS裝置的企業最佳實踐。

## 結論

- 請記住，使用者端一律是決定漫遊到特定AP的客戶端，而WLC/AP無法決定該客戶端的流量。漫遊事件在無線客戶端認為必須漫遊時由無線客戶端啟動。
- WLC在同一個WLAN/SSID上同時支援大多數或所有FSR（快速安全漫遊）方法的組合。但是請注意，這通常無法運作，因為它非常依賴使用者端行為（在不同的行動裝置之間差異很大），以便支援或甚至瞭解WLC嘗試播發為支援的。通常問題比預期要修復的問題更多，而不是只在一個SSID中實現互操作性，因此不建議這樣做。如果確實需要使用，必須完成深入測試，測試此WLAN上可能使用的所有客戶端。
- 如果WLAN/SSID啟用了安全功能，瞭解開發快速安全漫遊方法是為了在您在AP之間移動時加速WLAN漫遊過程，這一點非常重要。如果沒有安全措施，則無需加速，因為客戶端AP只需在

傳送資料幀之前在AP之間漫遊時交換始終需要的無線管理幀（來自客戶端的開放系統身份驗證、來自AP的開放系統身份驗證、重新關聯請求和重新關聯響應）。因此，這不會移動得更快。如果您遇到沒有安全性的漫遊問題，則沒有快速漫遊的方法來改進漫遊，只有用於確認WLAN/SSID設定和設計是否適合無線客戶端站在AP覆蓋信元之間相應地漫遊。

- 802.11r/FT是使用WPA2-PSK實現的，以便利用此安全機制加速漫遊事件並避免4次握手，如802.11r一節所述。
- 所有方法都有各自的優缺點，但最後，您必須始終驗證無線客戶端站是否支援您要實施的特定方法，以及Cisco WLAN基礎設施是否支援所有可用的方法。因此，您必須選擇連線到特定WLAN/SSID的無線客戶端實際支援的最佳方法。例如，在某些部署中，您可以為Cisco無線IP電話（支援使用CCKM的WPA2/AES，但非802.11r）建立使用CCKM的WLAN/SSID，然後為支援此快速安全漫遊方法的無線使用者端，透過802.11r/FT建立另一個使用WPA2/SSID(或使用OKC（如果這是支援的））。
- 如果無線客戶端不支援任何可用的快速安全漫遊方法，那麼當具有802.1X/EAP安全的WLAN/SSID上的AP之間漫遊時（可能導致客戶端應用/服務中斷），這些客戶端始終可以嘗試本文檔中所述的延遲。
- 除了SKC（WPA2 PMKID快取）外，所有方法都支援由不同WLC管理的AP之間的快速安全漫遊（控制器間漫遊），只要它們位於同一個移動組上。
- 當802.1X/EAP身份驗證用於WPA/WPA2時，CUWN完全支援本文中介紹的所有不同快速安全漫遊方法。當使用PSK(WPA2-Personal)時，CUWN不支援在與WPA2-RSN一起使用的方法上進行快速安全漫遊（CCKM、PMKID快取/SKC、OKC/PKC），其中通常不需要快速漫遊方法。但是，在具有PSK的WPA2-FT(802.11r)的情況下，CUWN支援快速安全漫遊，如本文也說明。

# 相關資訊

- 802.11r BSS快速過渡部署指南
- 思科技術支援與下載

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）。