配置和驗證Wi-Fi 6E WLAN第2層安全性

目錄

簡介

本文檔介紹如何配置Wi-Fi 6E WLAN第2層安全性，以及在不同客戶端上預期會發生什麼。

必要條件

需求

思科建議您瞭解以下主題：

- 思科無線 LAN 控制器 (WLC) 9800
- 支援 Wi-Fi 6E 的思科存取點 (AP)
- IEEE 標準 802.11ax

- 工具：Wireshark v4.0.6

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 採用IOS® XE 17.9.3的WLC 9800-CL。
- 存取點C9136、CW9162、CW9164和CW9166。
- Wi-Fi 6E 用戶端：
  - Lenovo X1 Carbon Gen11 搭載 Intel AX211 Wi-Fi 6 和 6E 介面卡，並搭配 22.200.2(1) 版驅動程式
  - Netgear A8000 Wi-Fi 6 和 6E 介面卡搭配驅動程式 v1(0.0.108)
  - 搭載 Android 13 的手機 Pixel 6a
  - 搭載 Android 13 的手機 Samsung S23

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

請務必瞭解，Wi-Fi 6E 並非全新標準，而是原有標準的延伸。 Wi-Fi 6E是Wi-Fi 6 (802.11ax)無線標準在6 GHz射頻頻帶的延伸。

Wi-Fi 6E 的基礎是最新一代 Wi-Fi 標準 Wi-Fi 6，只不過 Wi-Fi 6E 裝置和應用程式可以在 6-GHz 頻帶中運作。

Wi-Fi 6E 安全性

Wi-Fi 6E 採用 Wi-Fi Protected Access 3 (WPA3) 及 Opportunistic Wireless Encryption (OWE) 有效提升網路安全，且不與開放網路及 WPA2 的安全性向下相容。

Wi-Fi 6E 認證現在強制使用 WPA3 和 Enhanced Open Security，且 Wi-Fi 6E 也要求 AP 和用戶端使用受保護的訊框管理 (PMF)。

設定 6 GHz SSID 時，必須符合以下幾項安全要求：

- 採用 OWE、SAE 或 802.1x-SHA256 的 WPA3 L2 安全防護
- 啟用受保護的訊框管理
- 不允許使用其他 L2 安全防護方法，亦即不接受混合模式

WPA3

WPA3的設計是為了提升Wi-Fi的安全性，因為它能在WPA2上啟用更好的驗證，提供增強的加密強度並增強重要網路的彈性。

WPA3的主要功能包括：

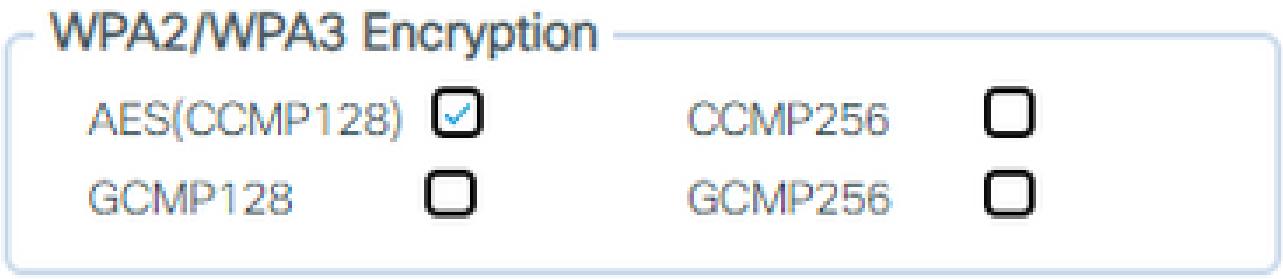
- 受保護的管理幀(PMF)保護單播和廣播管理幀並加密單播管理幀。這意味著無線入侵檢測和無

線入侵防禦系統現在使用更少的暴力方法來實施客戶端策略。
- Simultaneous Authentication of Equals (SAE)啟用基於密碼的身份驗證和金鑰協定機制。這可以防止暴力攻擊。
- 過渡模式是一種混合模式，它允許使用WPA2連線不支援WPA3的客戶端。

WPA3涉及持續的安全開發、一致性以及互操作性。
沒有指定WPA3（與WPA2相同）的「資訊元素」。WPA3由AKM/Cipher Suite/PMF組合定義。

在9800 WLAN配置中，您有4種不同的WPA3加密演算法可以使用。

它們基於Galois/Counter Mode Protocol (GCMP)和帶密碼塊鏈結消息驗證碼協定(CCMP)的計數器模式：AES (CCMP128)、CCMP256、GCMP128和GCMP256：

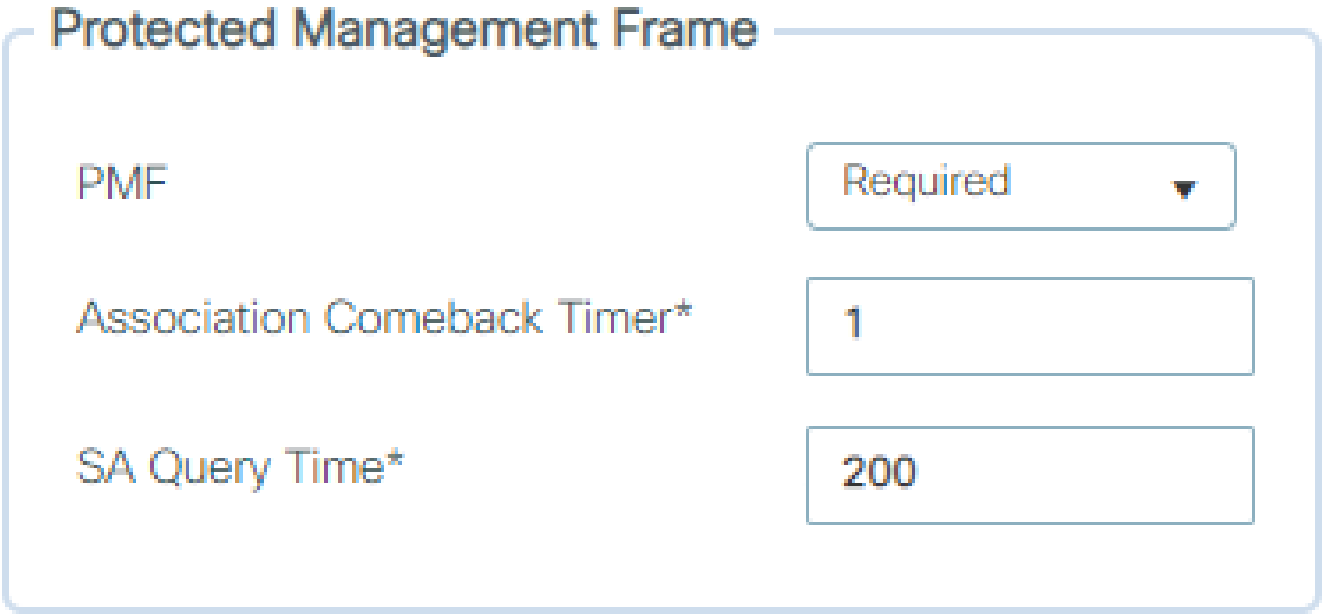


WPA2/3加密選項

PMF

啟用PMF時，PMF將在WLAN上啟用。

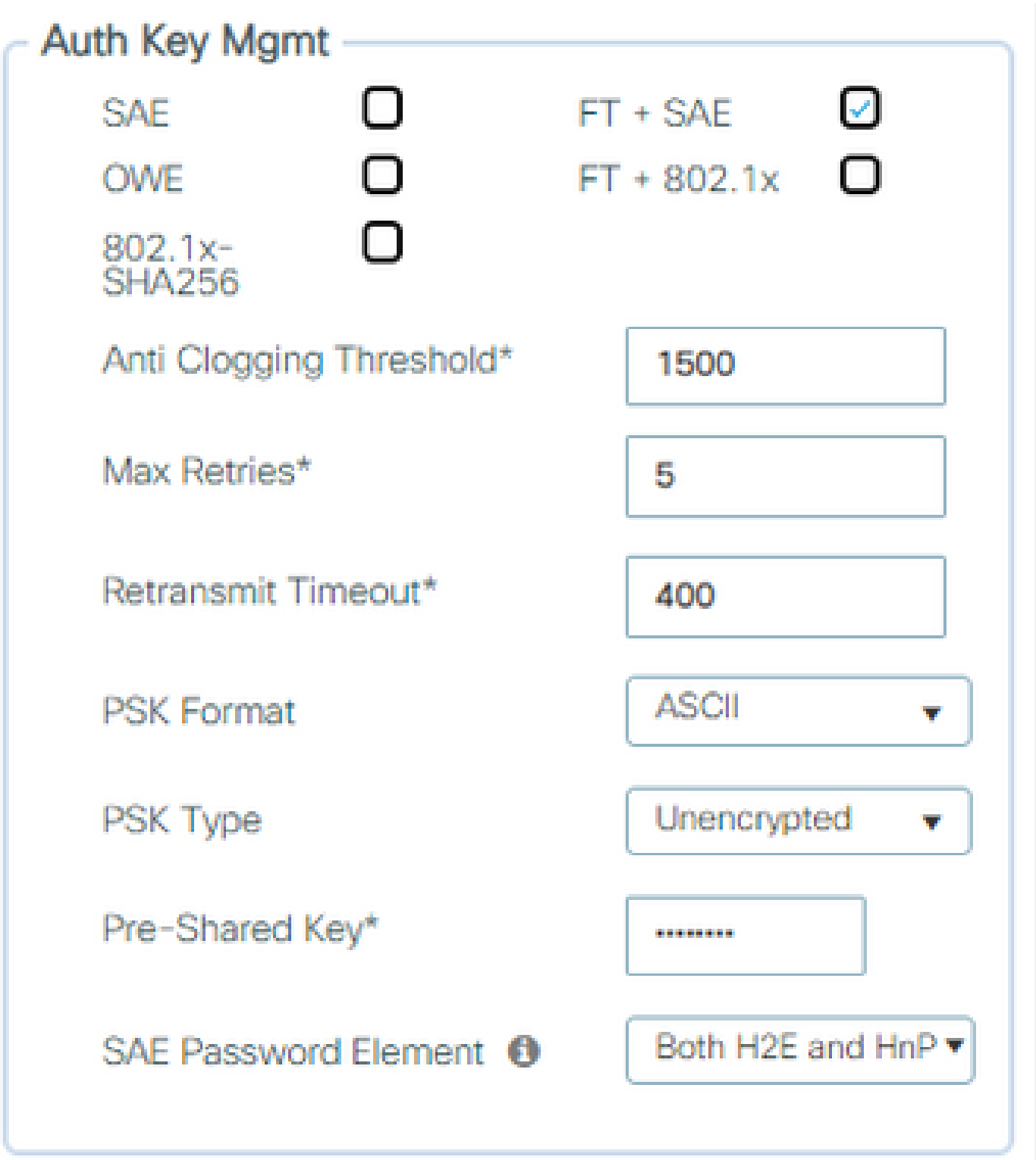
預設情況下，802.11管理幀未經身份驗證，因此不會受到防止欺騙的保護。基礎架構管理保護架構(MFP)和802.11w保護管理架構(PMF)提供針對此類攻擊的保護。



PMF選項

驗證金鑰管理

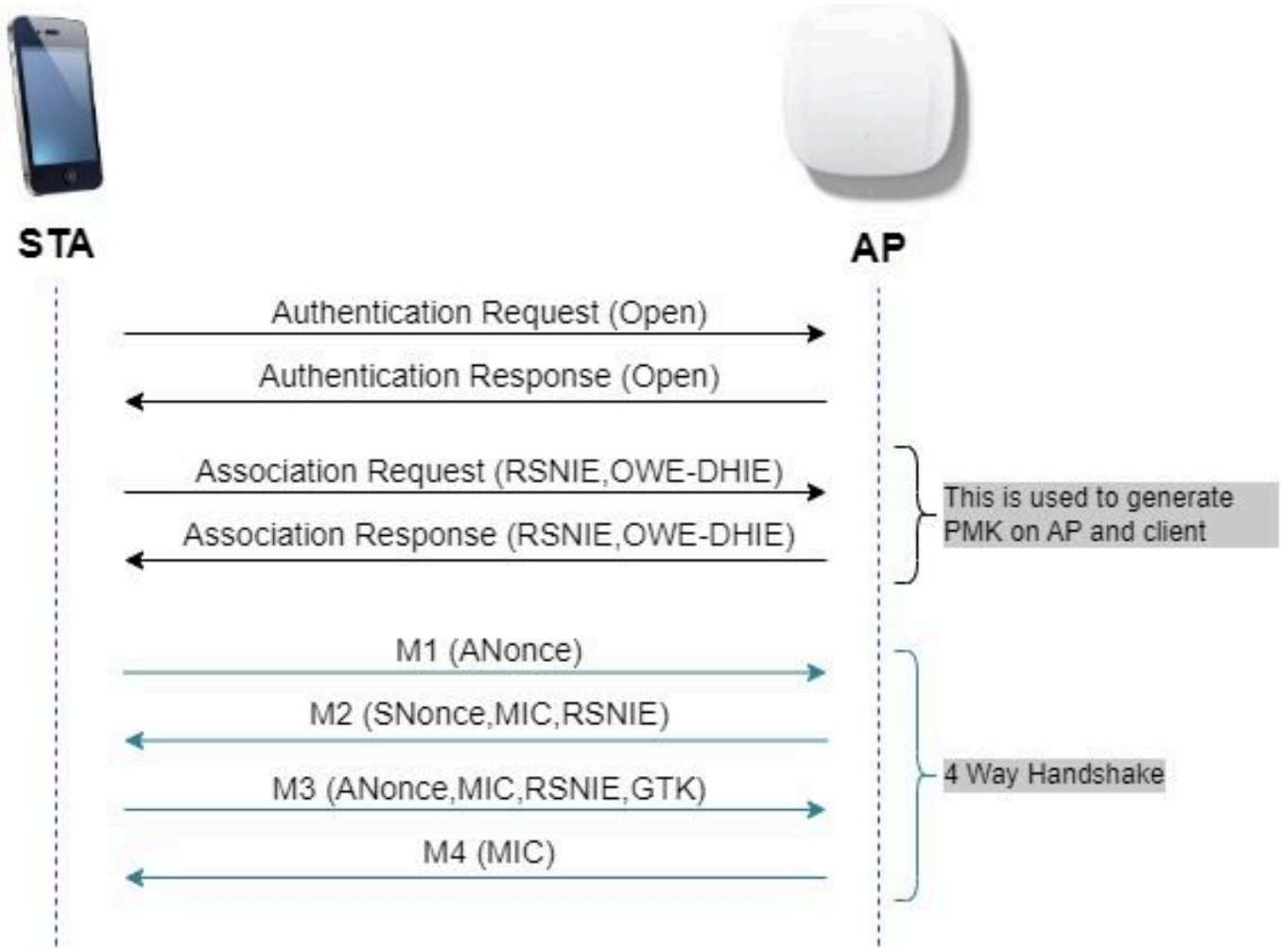
以下是17.9.x版中可用的AKM選項：



AKM選項

欠款

機會無線加密(OWE)是IEEE 802.11的擴展，提供無線介質的加密(IETF RFC 8110)。基於OWE的身份驗證的目的是避免AP和客戶端之間的開放非安全無線連線。OWE使用基於Diffie-Hellman演算法的加密來設定無線加密。使用OWE時，客戶端和AP在訪問過程中執行Diffie-Hellman金鑰交換，並使用生成的成對主金鑰(PMK)金鑰和4次握手。使用OWE可增強部署基於開放或共用PSK的網路的無線網路的安全性。



OWE幀交換

SAE

WPA3使用一種稱為「對等同時驗證」的新驗證和金鑰管理機制。透過使用SAE雜湊到元素(H2E)，此機製得到了進一步增強。

WPA3和Wi-Fi 6E必須使用H2E的SAE。

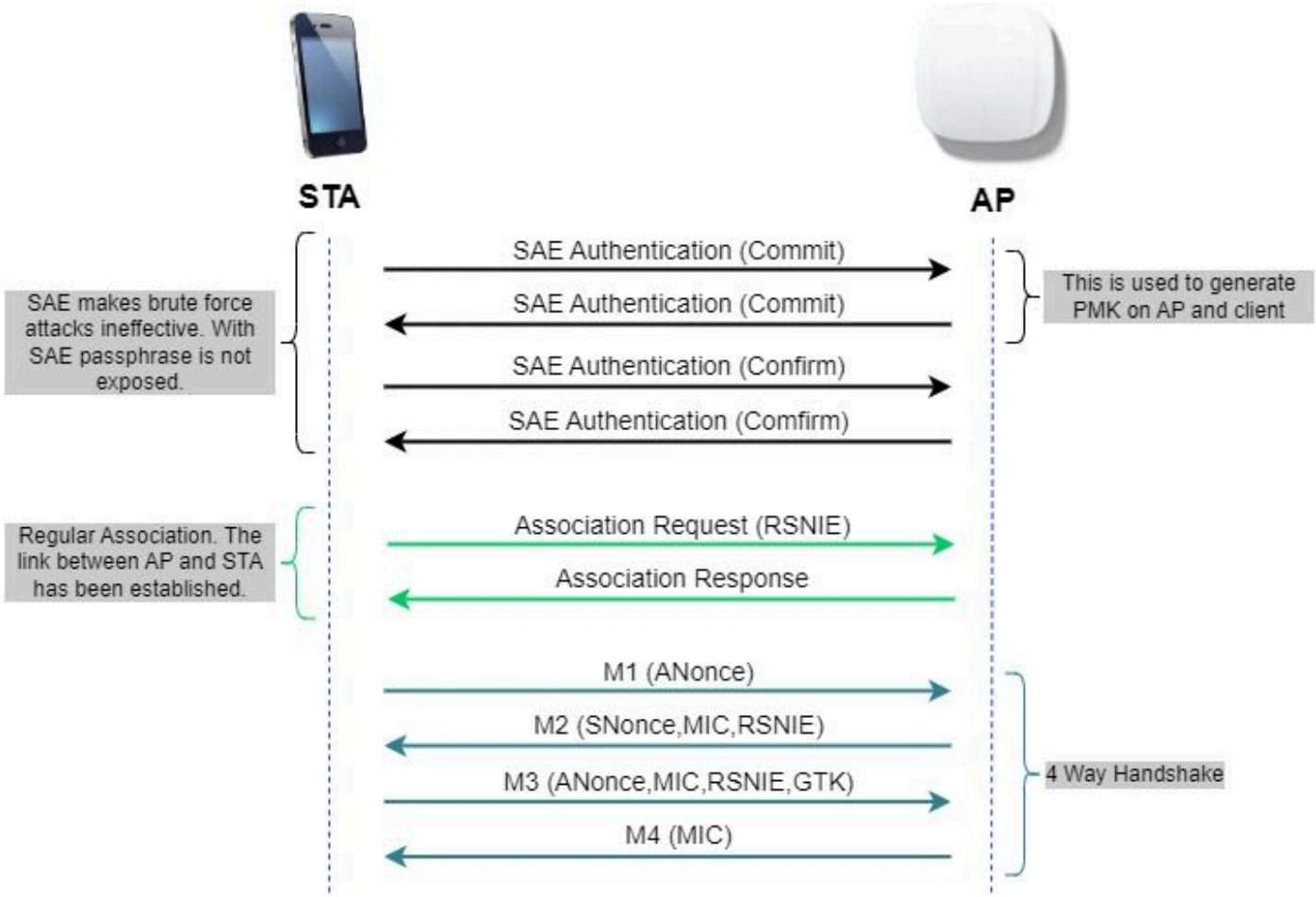
SAE採用離散對數密碼技術來執行有效交換，其方式是使用可能抵抗離線詞典攻擊的密碼執行相互身份驗證。

離線詞典攻擊是指攻擊者透過嘗試可能的密碼來確定網路密碼，而無需進一步進行網路互動。

當客戶端連線到存取點時，它們會執行SAE交換。如果成功，它們會為每個金鑰建立一個密碼強金鑰，從中派生會話金鑰。基本上，客戶端和存取點進入提交階段，然後進行確認。

一旦有承諾，則客戶端和存取點可以在每次生成會話金鑰時進入確認狀態。該方法使用前向保密

，入侵者可以破解單個金鑰，但不能破解所有其他金鑰。



SAE幀交換

雜湊到元素(H2E)

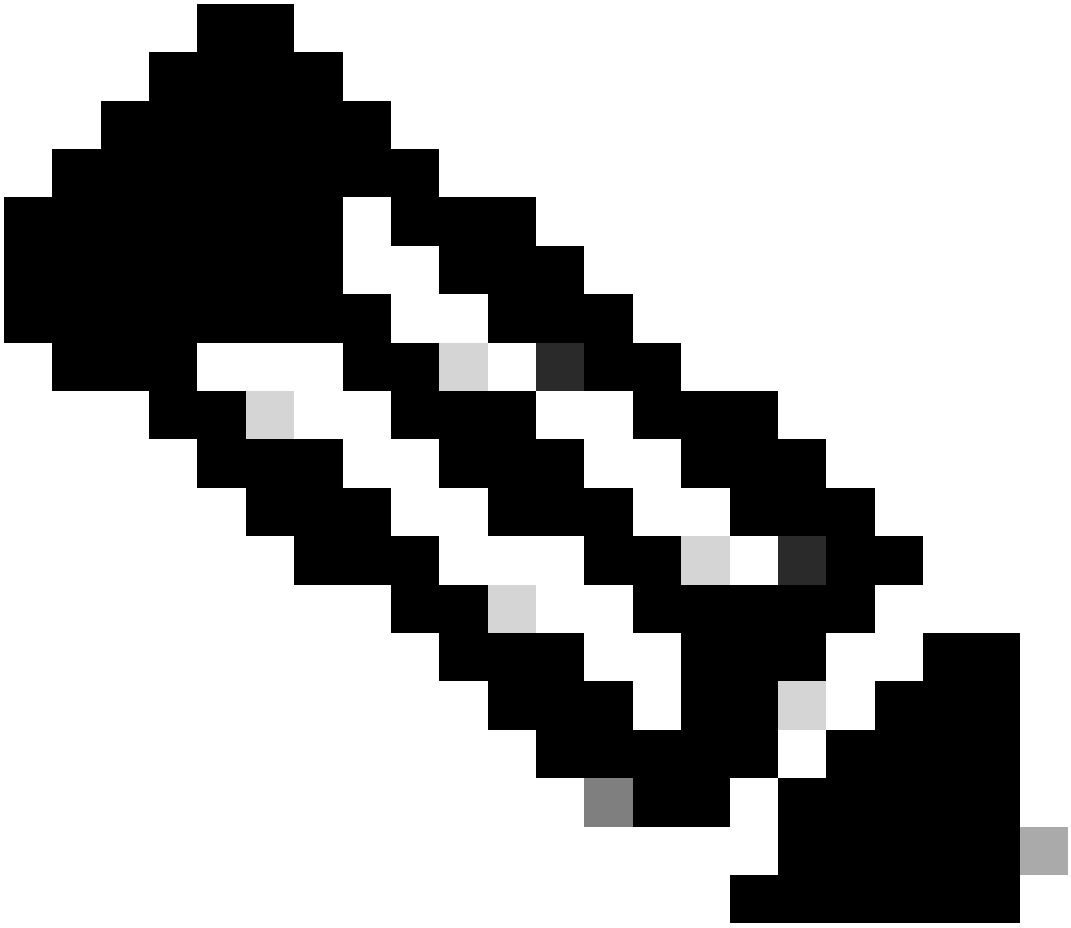
Hash-to-Element (H2E)是一種新的SAE密碼元素(PWE)方法。在此方法中，SAE協定中使用的密碼PWE從密碼生成。

支援H2E的站點(STA)向AP發起SAE時，會檢查AP是否支援H2E。如果是，則AP使用H2E在SAE提交消息中使用新定義的狀態代碼值來導出PWE。

如果STA使用「搜尋和啄食」(HnP)，則整個SAE交換保持不變。

使用H2E時，PWE派生分為以下元件：

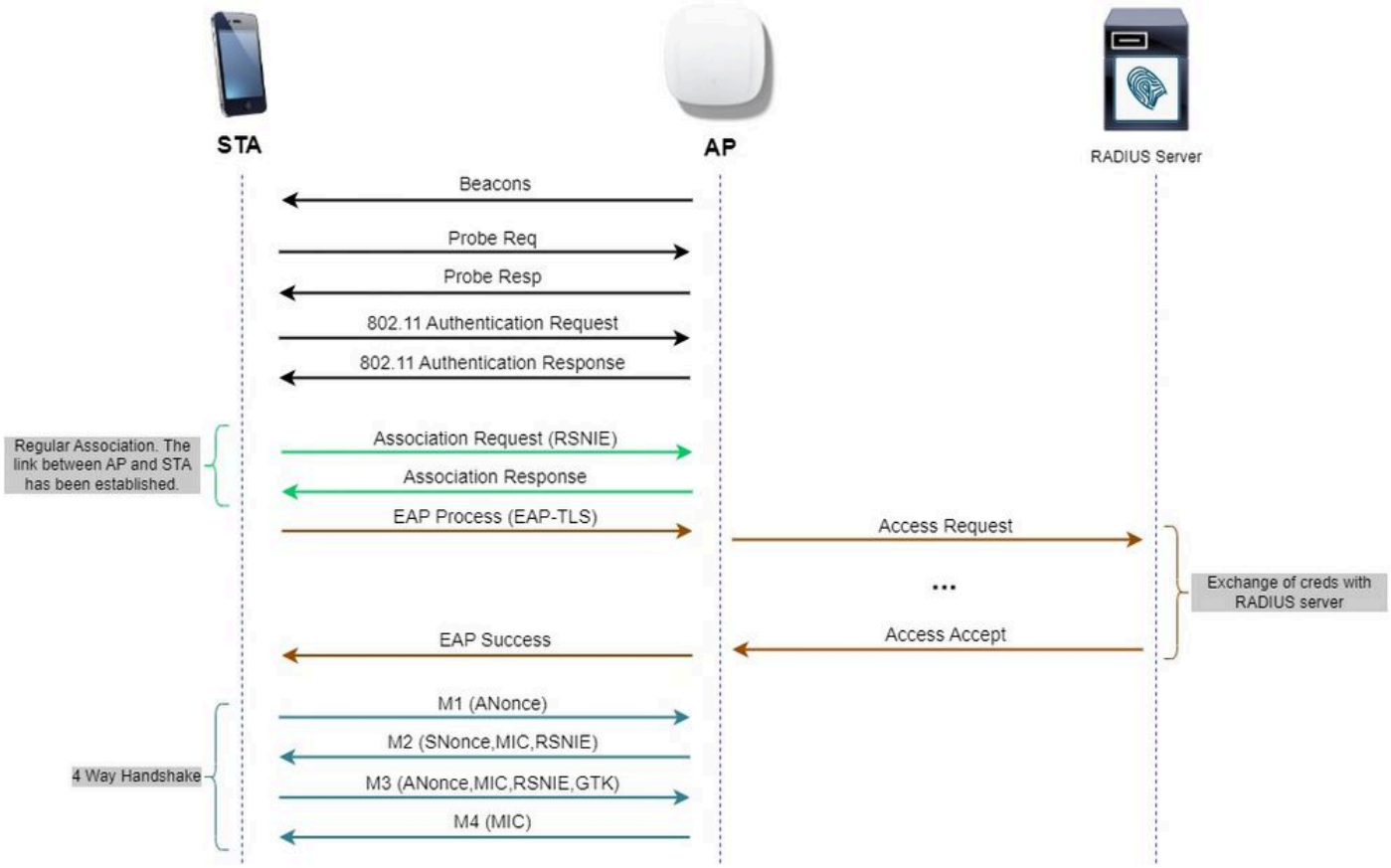
- 從密碼衍生秘密中間元素(PT)。當最初在裝置上為每個受支援的組配置密碼時，可以離線執行此操作。
- 從儲存的PT衍生PWE。這取決於對等體的協商組和MAC地址。這在SAE交換期間即時執行。



注意：6 GHz僅支援雜湊到元素SAE PWE方法。

WPA-企業aka 802.1x

WPA3-Enterprise是WPA3的最安全版本，它使用使用者名稱加密碼的組合與802.1X來使用RADIUS伺服器進行使用者驗證。預設情況下，WPA3使用128位加密，但它還引入了一個可選配置的192位加密強度加密，為傳輸敏感資料的任何網路提供額外的保護。



WPA3企業圖流程

級別集：WPA3模式

- WPA3-個人
  - WPA3-僅限個人模式
    - 需要PMF
  - WPA3-個人轉換模式
    - 配置規則：在AP上，每當啟用「WPA2個人」時，除非管理員明確覆寫為在「僅WPA2個人」模式下操作，否則預設也必須啟用「WPA3個人轉換」模式

- WPA3-企業
  - WPA3-僅限企業模式
    - 所有WPA3連線都應協商PMF
  - WPA3-企業轉換模式
    - WPA3連線應協商PMF
    - PMF對於WPA2連線是可選的
  - WPA3-Enterprise suite-B「192位元」模式符合商業國家安全演演算法(CNSA)
    - 不僅僅是聯邦政府
    - 一致的加密密碼套件以避免錯誤配置
    - GCMP與ECCP的加入，提供加密和更好的雜湊函式(SHA384)
    - 需要PMF

    - WPA3 192位元保全性必須專屬EAP-TLS，EAP-TLS在請求者和RADIUS伺服器上

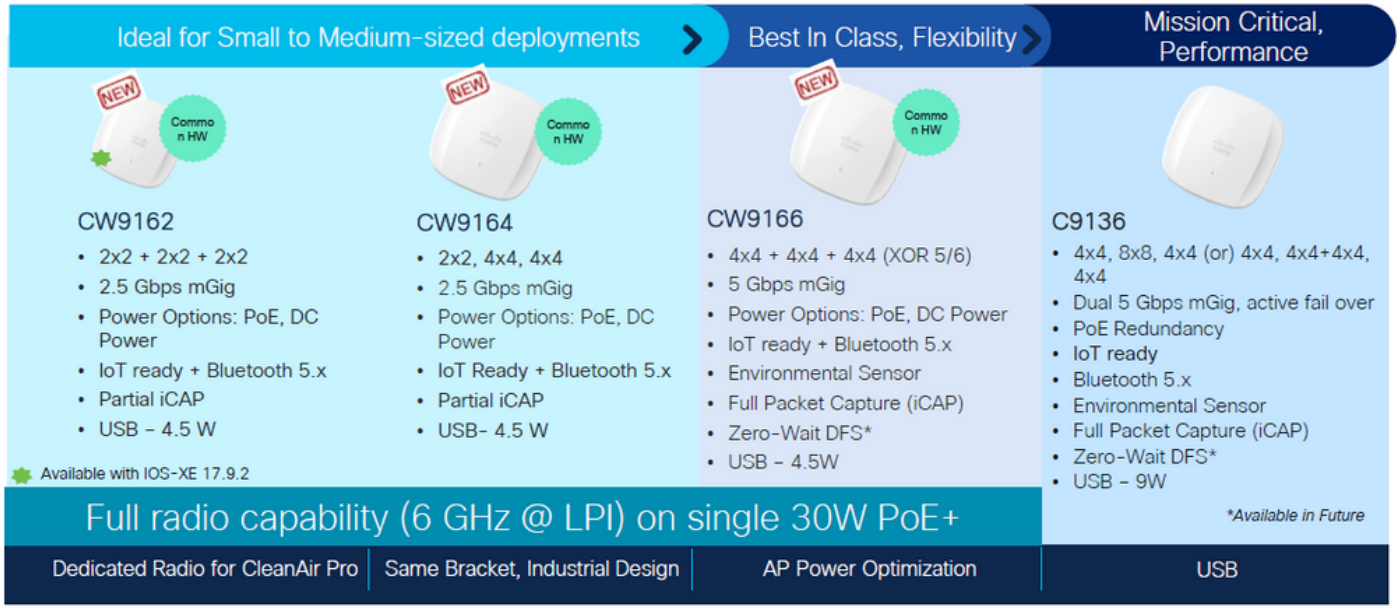
都需要憑證。

- 若要使用WPA3 192位元企業，RADIUS伺服器必須使用其中一個允許的EAP密碼：

  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

如需深入瞭解如何在 Cisco WLAN 實作 WPA3，包含用戶端安全相容對照表，請參閱 WPA3 部署指南。

Cisco Catalyst Wi-Fi 6E AP



Wi-Fi 6E 存取點

客戶端支援的安全設定

您可以使用WiFi聯盟網頁產品搜尋器找到支援WPA3-Enterprise的產品。

在windows裝置上，您可以使用命令「netsh wlan show drivers」驗證介面卡支援哪些安全設定。

您可以在這裡看到Intel AX211的輸出：

```
C:\Users\tantunes>netsh wlan show drivers

Interface name: Wi-Fi

    Driver                    : Intel(R) Wi-Fi 6E AX211 160MHz
    Vendor                    : Intel Corporation
    Provider                  : Intel
    Date                      : 3/9/2023
    Version                   : 22.200.2.1
    INF file                  : oem151.inf
    Type                      : Native Wi-Fi Driver
    Radio types supported     : 802.11b 802.11g 802.11n 802.11a 802.11ac 802.11ax
    FIPS 140-2 mode supported : Yes
    802.11w Management Frame Protection supported : Yes
    Hosted network supported  : No
    Authentication and cipher supported in infrastructure mode:
                                Open            None
                                Open            WEP-40bit
                                Open            WEP-104bit
                                Open            WEP
                                WPA-Enterprise  TKIP
                                WPA-Enterprise  CCMP
                                WPA-Personal    TKIP
                                WPA-Personal    CCMP
                                WPA2-Enterprise TKIP
                                WPA2-Enterprise CCMP
                                WPA2-Personal   TKIP
                                WPA2-Personal   CCMP
                                Open            Vendor defined
                                WPA3-Personal   CCMP
                                Vendor defined  Vendor defined
                                WPA3-Enterprise 192 Bits GCMP-256
                                OWE             CCMP
                                WPA3-Enterprise CCMP
                                WPA3-Enterprise TKIP
    Number of supported bands : 3
                                2.4 GHz [ 0 MHz - 0 MHz]
                                5 GHz   [ 0 MHz - 0 MHz]
                                6 GHz   [ 0 MHz - 0 MHz]
    IHV service present       : Yes
    IHV adapter OUI           : [00 00 00], type: [00]
    IHV extensibility DLL path: C:\WINDOWS\System32\DriverStore\FileRepository\netwtw6e.inf_amd64_eda979fbdedea064\IntelIHVRouter12.dll
```

客戶端AX211的_netsh wlan show driver_的Windows輸出

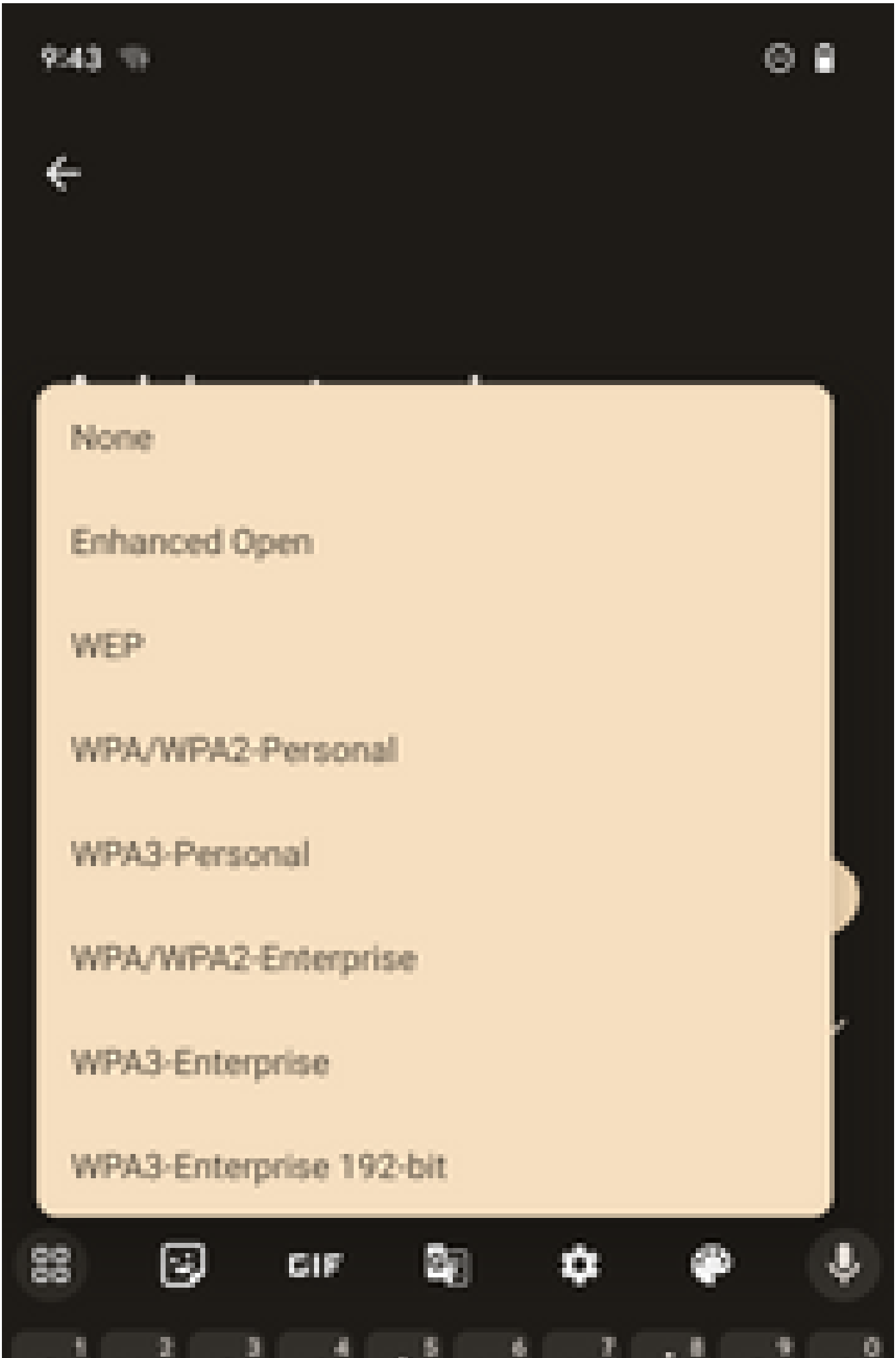
Netgear A8000：

```
Interface name: A8000_NETGEAR

    Driver                     : NETGEAR A8000 WiFi 6 & 6E Adapter
    Vendor                     : NETGEAR Inc.
    Provider                   : MediaTek, Inc.
    Date                       : 11/25/2022
    Version                    : 1.0.0.108
    INF file                   : oem9.inf
    Type                       : Native Wi-Fi Driver
    Radio types supported      : 802.11b 802.11a 802.11g 802.11n 802.11ac 802.11ax
    FIPS 140-2 mode supported : Yes
    802.11w Management Frame Protection supported : Yes
    Hosted network supported  : No
    Authentication and cipher supported in infrastructure mode:
                                Open             None
                                Open             WEP-40bit
                                Open             WEP-104bit
                                Open             WEP
                                WPA-Enterprise   TKIP
                                WPA-Enterprise   CCMP
                                WPA3-Personal    CCMP
                                OWE              CCMP
                                WPA-Personal     TKIP
                                WPA-Personal     CCMP
                                WPA2-Enterprise  TKIP
                                WPA2-Enterprise  CCMP
                                WPA2-Personal    TKIP
                                WPA2-Personal    CCMP
    Number of supported bands : 3
                                2.4 GHz [ 0 MHz - 0 MHz]
                                5 GHz   [ 0 MHz - 0 MHz]
                                6 GHz   [ 0 MHz - 0 MHz]
    IHV service present        : Yes
    IHV adapter OUI            : [00 00 00], type: [00]
    IHV extensibility DLL path: C:\WINDOWS\system32\mtkihvux.dll
    IHV UI extensibility ClSID: {00000000-0000-0000-0000-000000000000}
    IHV diagnostics CLSID      : {00000000-0000-0000-0000-000000000000}
    Wireless Display Supported: Yes (Graphics Driver: Yes, Wi-Fi Driver: Yes)
```

客戶端Netgear A8000s的_netsh wlan show driver_的Windows輸出

Android Pixel 6a：


9:43
None
Enhanced Open
WEP
WPA/WPA2-Personal
WPA3-Personal
WPA/WPA2-Enterprise
WPA3-Enterprise
WPA3-Enterprise 192-bit
GIF

欠款	AES-CCMP128	欠款	不。	不。	NA	NA	支援	支援	支援
SAE	AES-CCMP128	SAE（僅限H2E）	SHA256	不。	支援	支援	支援：僅H2E和FT-oTA	支援：僅H2E。FT失敗。FT-oDS失敗。	支援：僅限H2英國《金時報》。FT-oDS。
企業	AES-CCMP128	802.1x-SHA256	SHA256	PEAP/FAST/TLS	支援	支援	支援：SHA256和FT-oTA/oDS不支援：EAP-FAST	支援：SHA256和FT-oTA、FT-oDS (S23)不支援：EAP-FAST、FT-oDS (Pixel6a)	支援：SHA2FT-oTA不支援EAP-FAST、oDS。
企業	GCMP128	SuiteB-1x	SHA256-SuiteB	PEAP/FAST/TLS	不支援	不支援	不支援	不支援	不支援
企業	GCMP256	SuiteB-192	SHA384-SuiteB	TLS	不支援	不支援	不適用/待定	不適用/待定	不支援

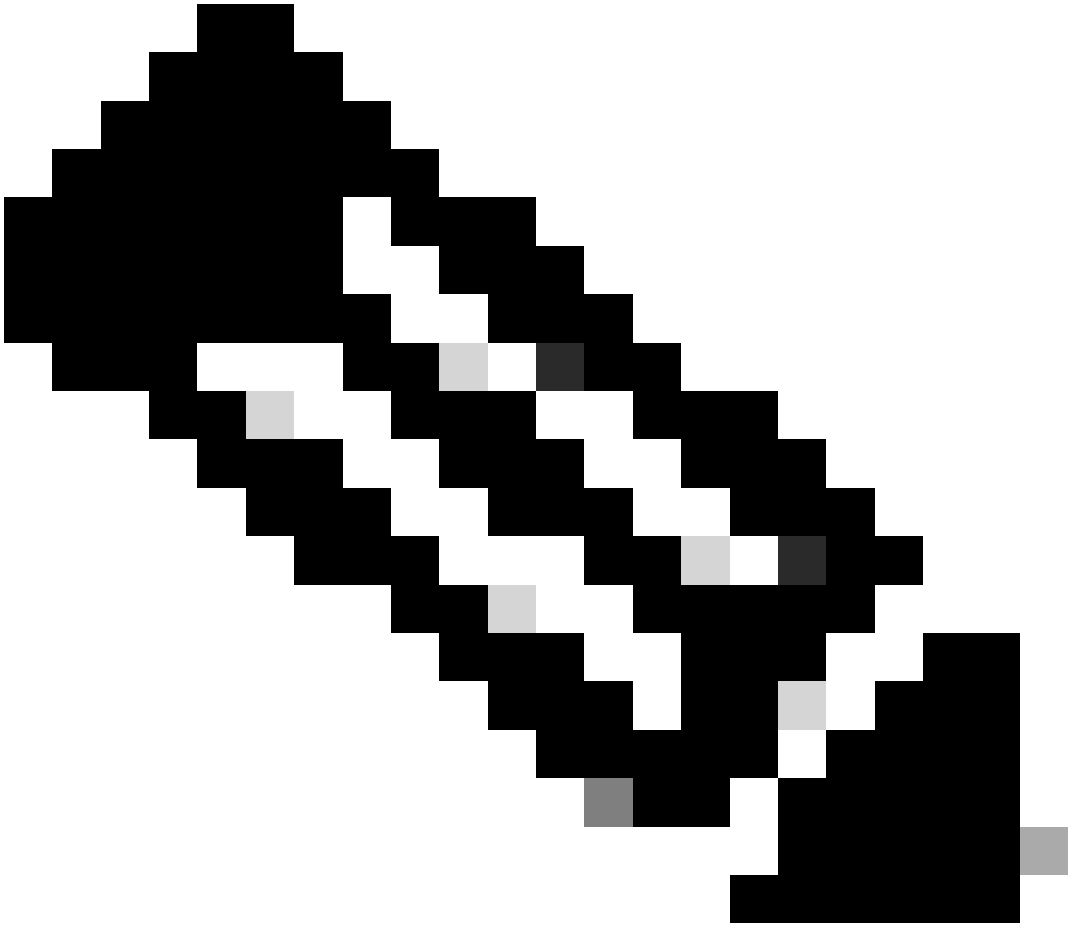
疑難排解

本文檔中使用的故障排除基於聯機文檔：

[疑難排解 COS AP]

故障排除的一般指南是使用客戶端mac地址從WLC收集調試模式下的RA跟蹤，以確保客戶端使用裝置mac而不是隨機mac地址進行連線。

對於無線故障排除，建議以嗅探器模式使用AP，捕獲客戶端服務AP的通道上的流量。



注意：使用debug命令之前，請參閱有關Debug命令的重要資訊。

相關資訊

什麼是 Wi-Fi 6E？

什麼是 Wi-Fi 6 與 Wi-Fi 6E？

Wi-Fi 6E 概覽

Wi-Fi 6E：Wi-Fi 白皮書重要新篇章

Cisco Live - 使用 Catalyst Wi-Fi 6E 存取點架構新世代無線網路

Cisco Catalyst 9800 系列無線控制器軟體設定指南 17.9.x

WPA3 部署指南

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）。