配置并验证Wi-Fi 6E WLAN第2层安全性

目录

简介

本文档介绍如何配置Wi-Fi 6E WLAN第2层安全性，以及不同客户端上的要求。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科无线局域网控制器(WLC) 9800
- 支持Wi-Fi 6E的思科接入点(AP)。
- IEEE标准802.11ax。

- 工具：Wireshark v4.0.6

使用的组件

本文档中的信息基于以下软件和硬件版本：

- WLC 9800-CL，带IOS® XE 17.9.3。
- AP C9136、CW9162、CW9164和CW9166。
- Wi-Fi 6E客户端：
  - Lenovo X1 Carbon Gen11，带英特尔AX211 Wi-Fi 6和6E适配器，带驱动程序版本22.200.2(1)。
  - 带驱动程序v1(0.0.108)的Netgear A8000 Wi-Fi 6和6E适配器；
  - Android 13的手机Pixel 6a；
  - 装有安卓13的手机三星S23。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

需要了解的关键一点是，Wi-Fi 6E并不是一个全新的标准，而是一个扩展。 在其基本上，Wi-Fi 6E是Wi-Fi 6 (802.11ax)无线标准到6 GHz射频频段的扩展。

Wi-Fi 6E基于Wi-Fi 6（最新一代Wi-Fi标准）构建，但只有Wi-Fi 6E设备和应用可以在6-GHz频段运行。

Wi-Fi 6E安全

Wi-Fi 6E通过Wi-Fi Protected Access 3 (WPA3)和Opportunistic Wireless Encryption (OWE)提升安全性，并且不与Open和WPA2安全性向后兼容。

WPA3和增强型开放安全现在是Wi-Fi 6E认证的必要条件，并且Wi-Fi 6E还需要在AP和客户端中使用保护管理帧(PMF)。

配置6GHz SSID时，必须满足某些安全要求：

- WPA3 L2安全，带OWE、SAE或802.1x-SHA256
- 已启用受保护的管理帧；
- 不允许使用任何其他L2安全方法，即不能使用混合模式。

WPA3

WPA3旨在通过WPA2启用更好的身份验证，从而提高Wi-Fi安全性，提供更大的加密强度并提高关键网络的恢复能力。

WPA3的主要功能包括：

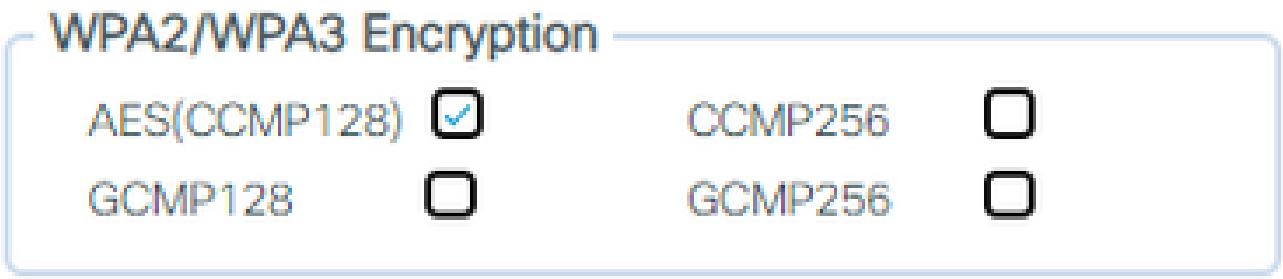
- 受保护的管理帧(PMF)保护单播和广播管理帧并加密单播管理帧。这意味着无线入侵检测和无

线入侵防御系统现在实施客户端策略的暴力方式更少。
- Simultaneous Authentication of Equals (SAE)启用基于密码的身份验证和密钥协商机制。这样可以防止暴力攻击。
- 过渡模式是一种混合模式，它允许使用WPA2连接不支持WPA3的客户端。

WPA3涉及持续的安全开发、一致性以及互操作性。
没有用于指定WPA3（与WPA2相同）的信息元素。WPA3由AKM/密码套件/PMF组合定义。

在9800 WLAN配置中，您可以使用四种不同的WPA3加密算法。

它们基于Galois/Counter Mode Protocol (GCMP)和Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)：AES (CCMP128)、CCMP256、GCMP128和GCMP256：

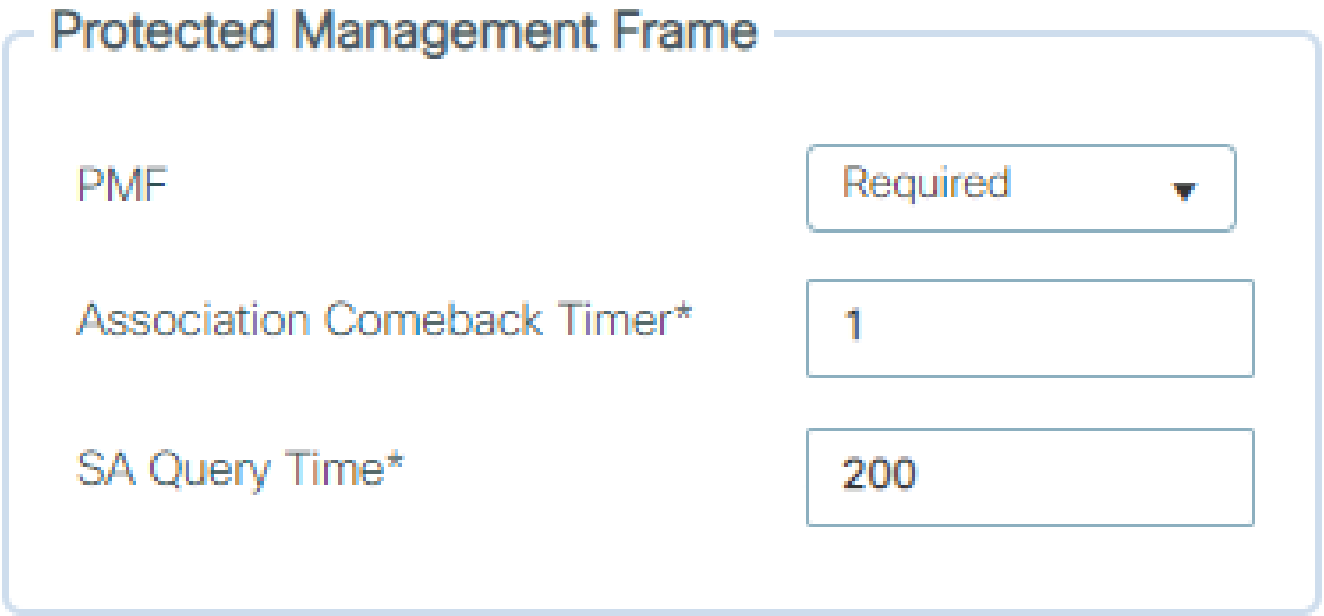


WPA2/3加密选项

PMF

启用PMF时，PMF在WLAN上激活。

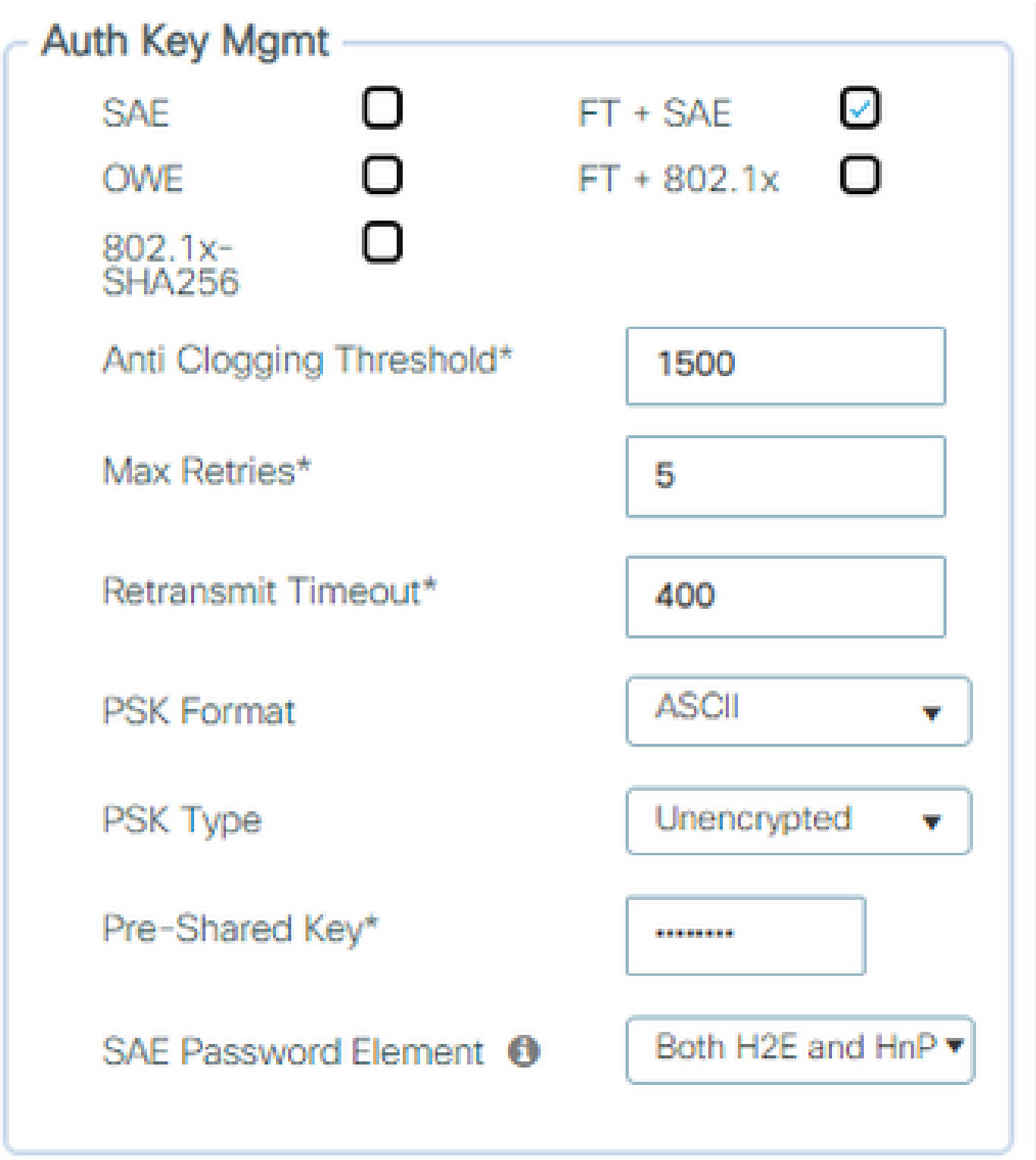
默认情况下，802.11管理帧未经身份验证，因此不能防范欺骗。基础设施管理保护帧(MFP)和802.11w保护管理帧(PMF)提供针对此类攻击的防护。



PMF选项

身份验证密钥管理

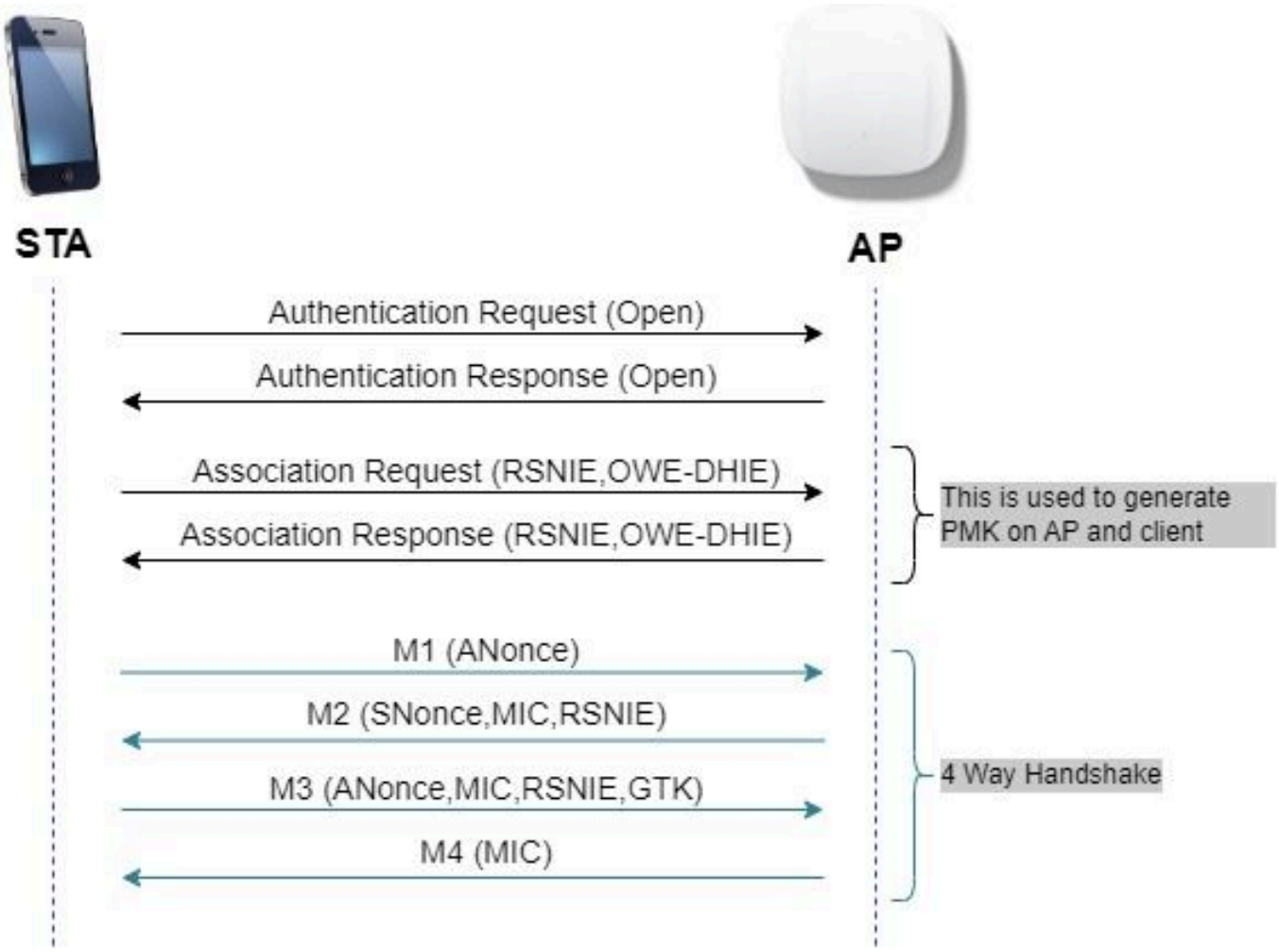
以下是17.9.x版本中可用的AKM选项：



AKM选项

OWE

机会无线加密(OWE)是对IEEE 802.11的扩展，提供无线介质加密(IETF RFC 8110)。基于OWE的身份验证的目的是避免AP和客户端之间的开放式非安全无线连接。OWE使用基于Diffie-Hellman算法的加密来设置无线加密。借助OWE，客户端和AP在访问过程中执行Diffie-Hellman密钥交换，并将生成的配对主密钥(PMK)密钥与4次握手配合使用。使用OWE可增强部署基于开放式或共享式PSK网络的无线网络的安全性。



OWE帧交换

SAE

WPA3使用称为“等值的同时身份验证”的新身份验证和密钥管理机制。通过使用SAE散列到元素(H2E)，此机制得到了进一步增强。

WPA3和Wi-Fi 6E必须使用SAE和H2E。

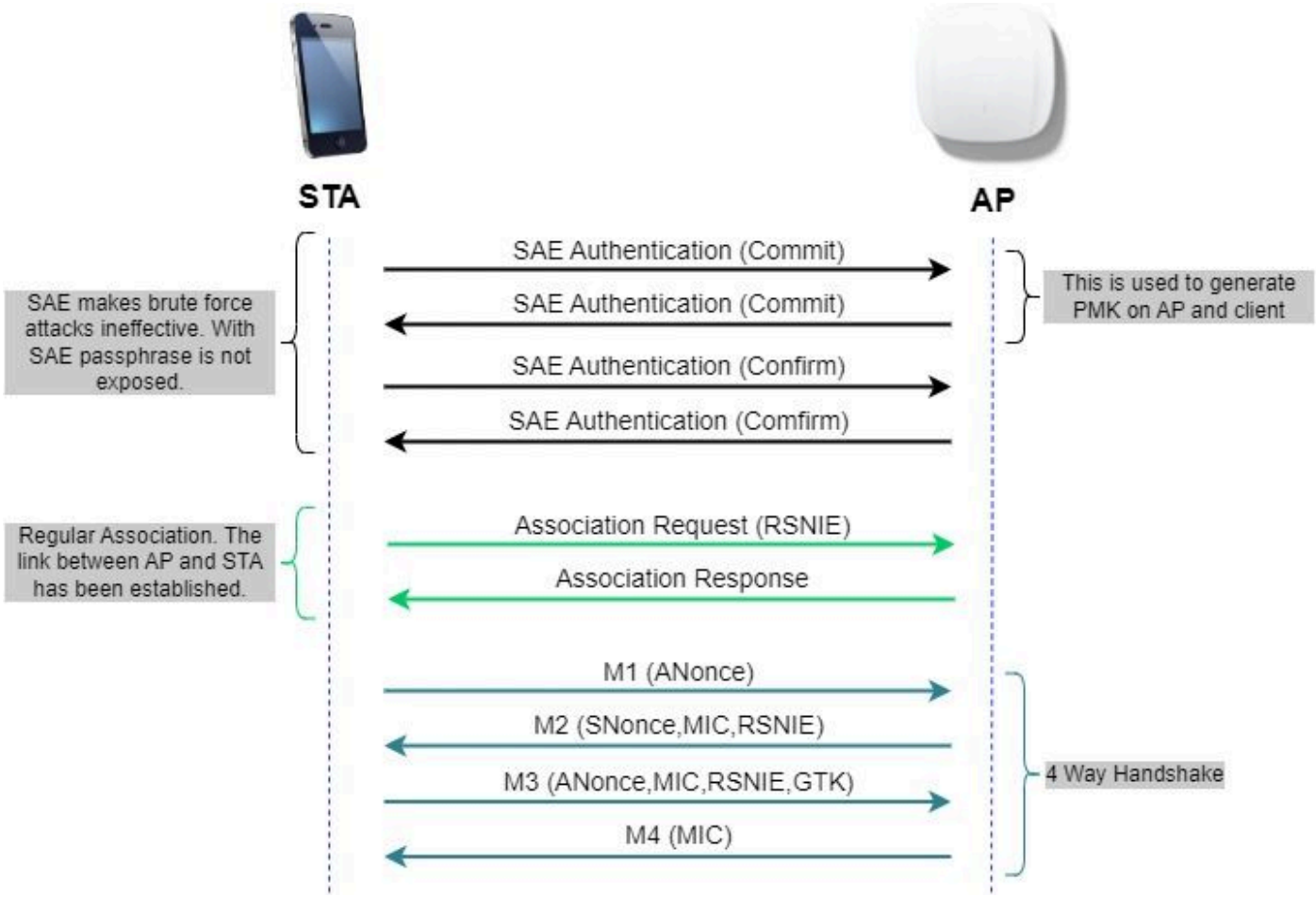
SAE采用离散对数密码执行有效交换，其方式是使用可能抵御离线字典攻击的密码执行相互身份验证。

离线字典攻击是指攻击者尝试通过尝试可能的密码来确定网络密码，而不进行进一步的网络交互。

当客户端连接到接入点时，它们会执行SAE交换。如果成功，它们会为每个会话密钥创建一个加密强密钥，会话密钥就是从该密钥派生的。基本上，客户端和接入点进入提交阶段，然后进行确认。

一旦有承诺，客户端和接入点就可以进入确认状态，每次有会话密钥需要生成。该方法使用前向保

密，即入侵者可以破解单个密钥，但不是所有其他密钥。



SAE帧交换

散列到元素(H2E)

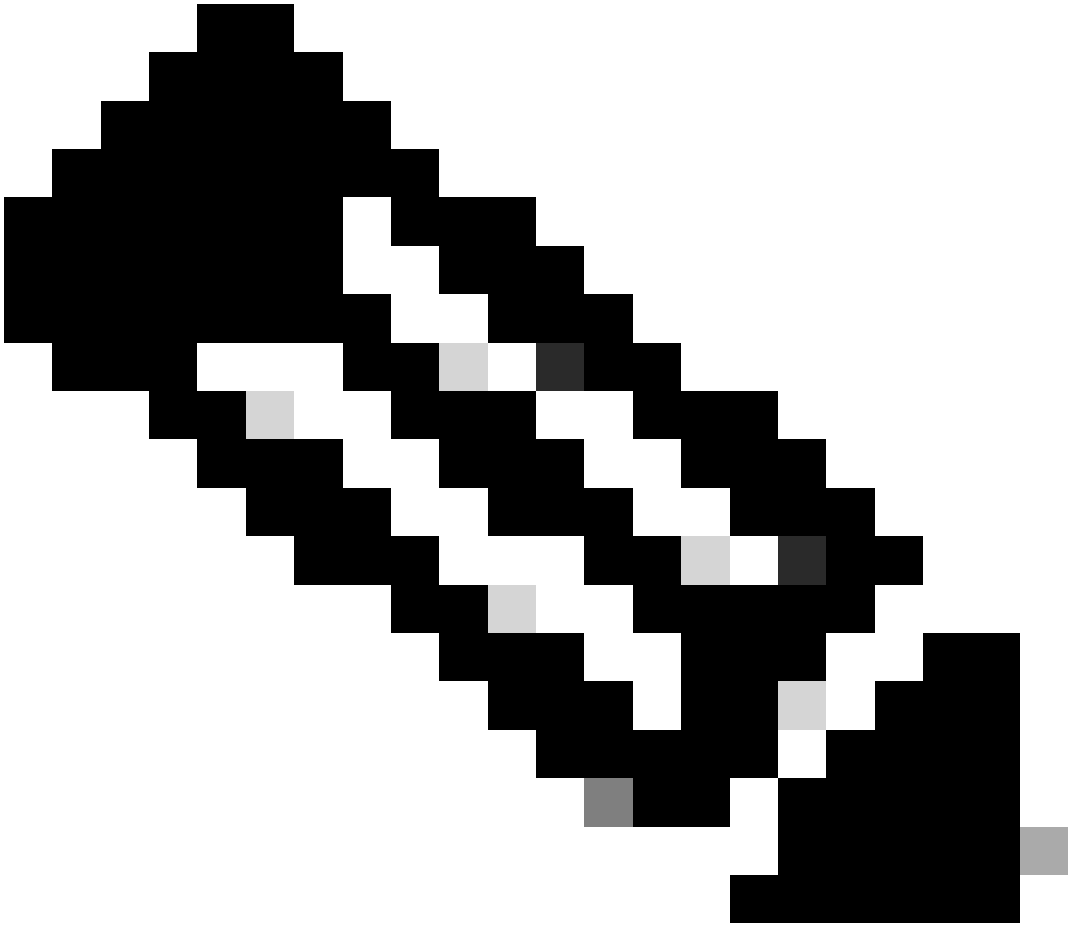
散列到元素(H2E)是一种新的SAE密码元素(PWE)方法。在此方法中，SAE协议中使用的密钥PWE从密码生成。

当支持H2E的站点(STA)向AP发起SAE时，它会检查AP是否支持H2E。如果是，则AP使用H2E，通过在SAE提交消息中使用新定义的状态代码值来获取PWE。

如果STA使用寻线寻址(HnP)，整个SAE交换将保持不变。

当使用H2E时，PWE衍生分为以下部分：

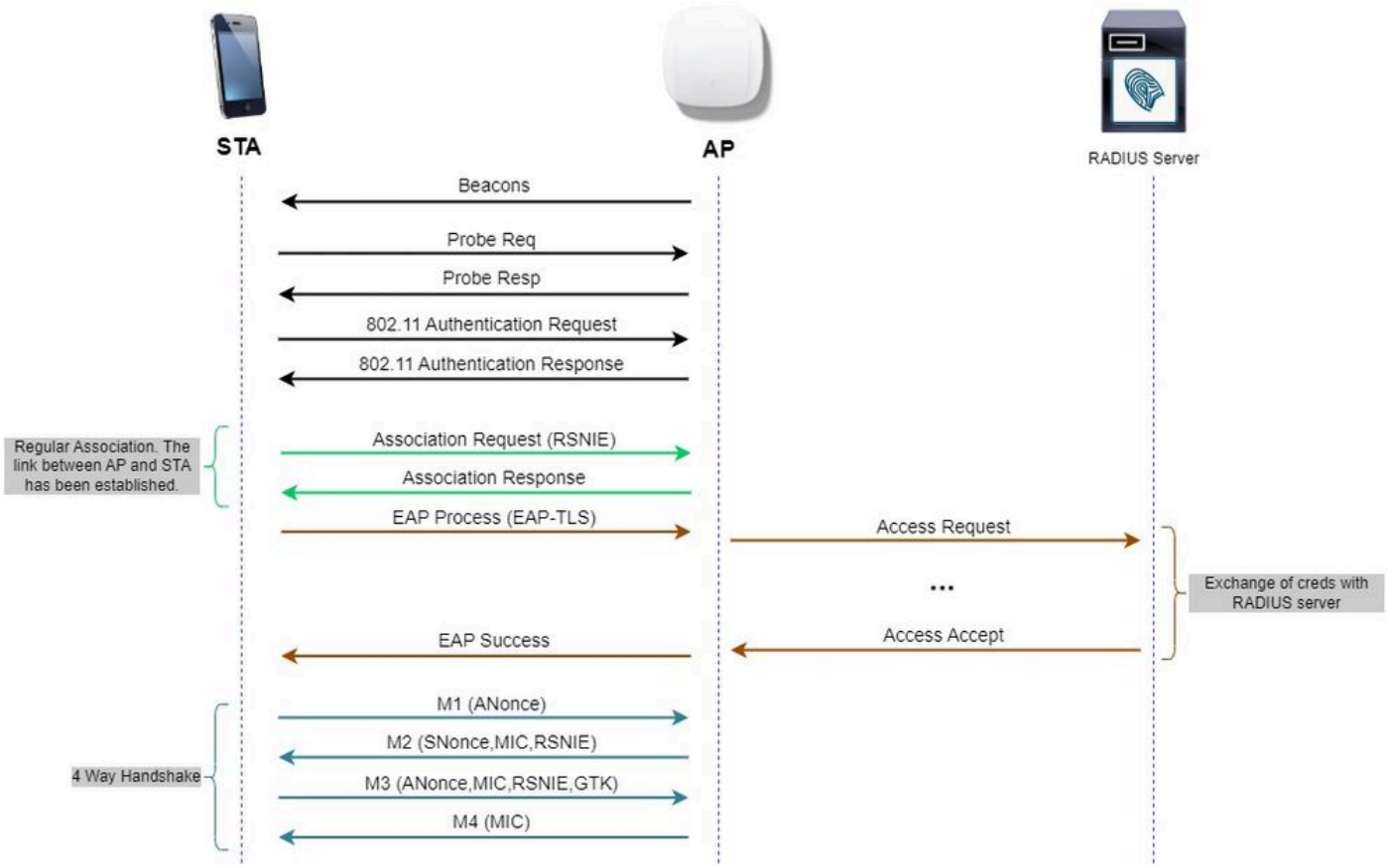
- 从密码派生秘密中间元素(PT)。在设备上为每个受支持的组初始配置密码时，可以脱机执行此任务。
- 从存储的PT派生PWE。这取决于对等体的协商组和MAC地址。在SAE交换期间实时执行该操作。



注意：6 GHz仅支持散列到元素SAE PWE方法。

WPA-企业aka 802.1x

WPA3-Enterprise是最安全的WPA3版本，它使用用户名加密码组合和802.1X来通过RADIUS服务器进行用户身份验证。默认情况下，WPA3使用128位加密，但它也引入了可选的可配置192位加密强度加密，为传输敏感数据的所有网络提供额外保护。



WPA3企业图流程

级别集：WPA3模式

- WPA3-个人
  - WPA3-仅个人模式
    - 需要PMF
  - WPA3-个人过渡模式
    - 配置规则：在AP上，每当启用WPA2-Personal时，默认情况下还必须启用WPA3-Personal过渡模式，除非管理员明确覆盖此模式才能在WPA2-Personal only模式下运行

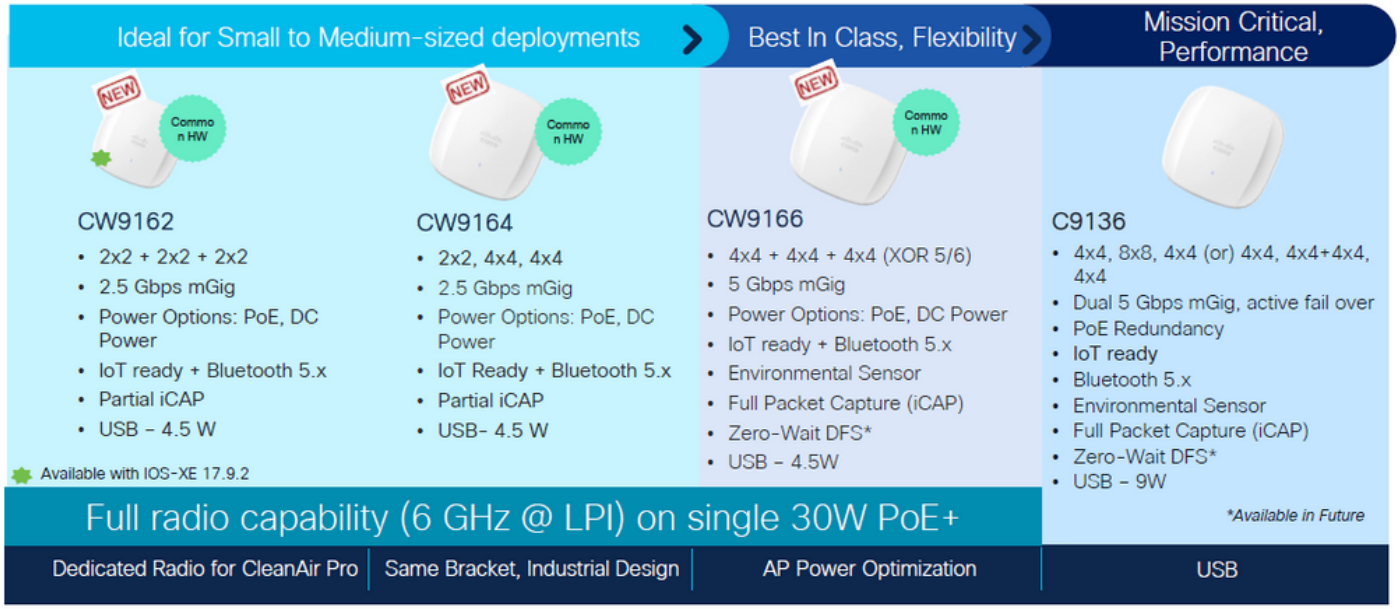
- WPA3-企业
  - 仅WPA3-企业模式
    - 应为所有WPA3连接协商PMF
  - WPA3-企业过渡模式
    - 应针对WPA3连接协商PMF
    - PMF对于WPA2连接是可选的
  - WPA3-Enterprise suite-B“192位”模式与商业国家安全算法(CNSA)一致
    - 不仅仅是联邦政府
    - 一致的加密密码套件以避免错误配置
    - 为加密和更好的哈希函数添加了GCMP和ECCP (SHA384)
    - 需要PMF

- WPA3 192位安全应专用于EAP-TLS，EAP-TLS需要请求方和RADIUS服务器上的证书。
- 要使用WPA3 192位企业版，RADIUS服务器必须使用允许的EAP密码之一：

  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

要了解有关Cisco WLAN中WPA3实施的详细信息（包括客户端安全兼容性列表），请随时查看WPA3部署指南。

思科Catalyst Wi-Fi 6E AP



Wi-Fi 6E接入点

客户端支持的安全设置

您可以使用WiFi联盟网页产品查找器查找支持WPA3-Enterprise的产品。

在windows设备上，您可以使用命令“netsh wlan show drivers”验证适配器支持的安全设置是什么。

在此，您可以看到英特尔AX211的输出：

```
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
```

客户端AX211的_netsh wlan show driver_的Windows输出

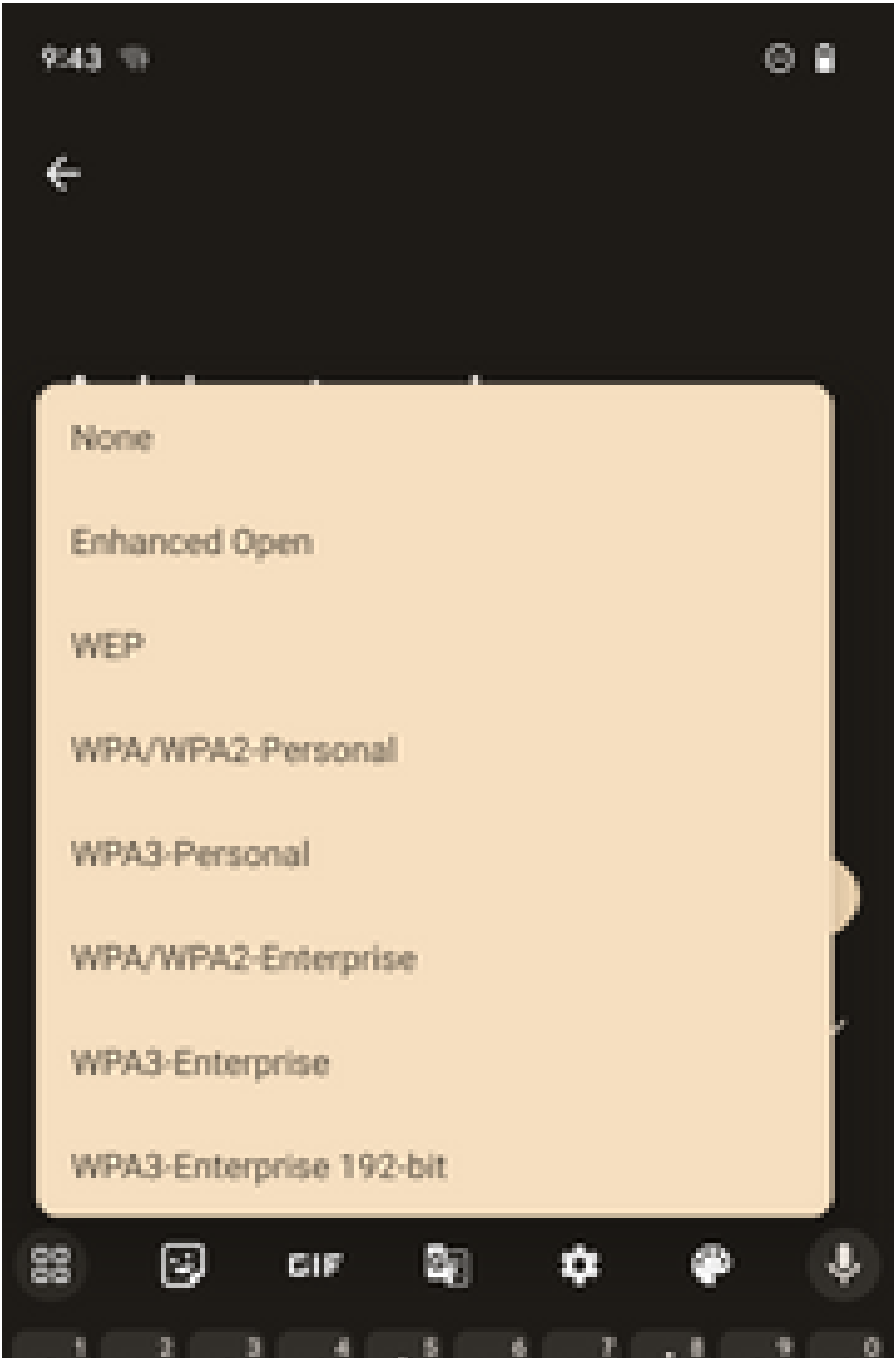
Netgear A8000：

```
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)
```

客户端Netgear A8000s的_netsh wlan show driver_的Windows输出

Android Pixel 6a：


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

OWE	AES-CCMP128	OWE	不适用.	不适用.	不适用	不适用	受支持	受支持	受支
SAE	AES-CCMP128	SAE（仅限H2E）	SHA256	不适用.	受支持	受支持	支持：仅H2E和FT-oTA	支持：仅限H2E。FT失败。FT-oDS失败。	受支仅限FT-FT-。
企业	AES-CCMP128	802.1x-SHA256	SHA256	PEAP/FAST/TLS	受支持	受支持	支持：SHA256和FT-oTA/oDS不支持：EAP-FAST	支持：SHA256和FT-oTA、FT-oDS (S23)不支持：EAP-FAST、FT-oDS (Pixel6a)	支持：SFT-不支：EFASoDS
企业	GCMP128	SuiteB-1x	SHA256-SuiteB	PEAP/FAST/TLS	Not Supported	Not Supported	Not Supported	Not Supported	Not Sup
企业	GCMP256	SuiteB-192	SHA384-SuiteB	TLS	Not Supported	Not Supported	不适用/待定	不适用/待定	Not Sup

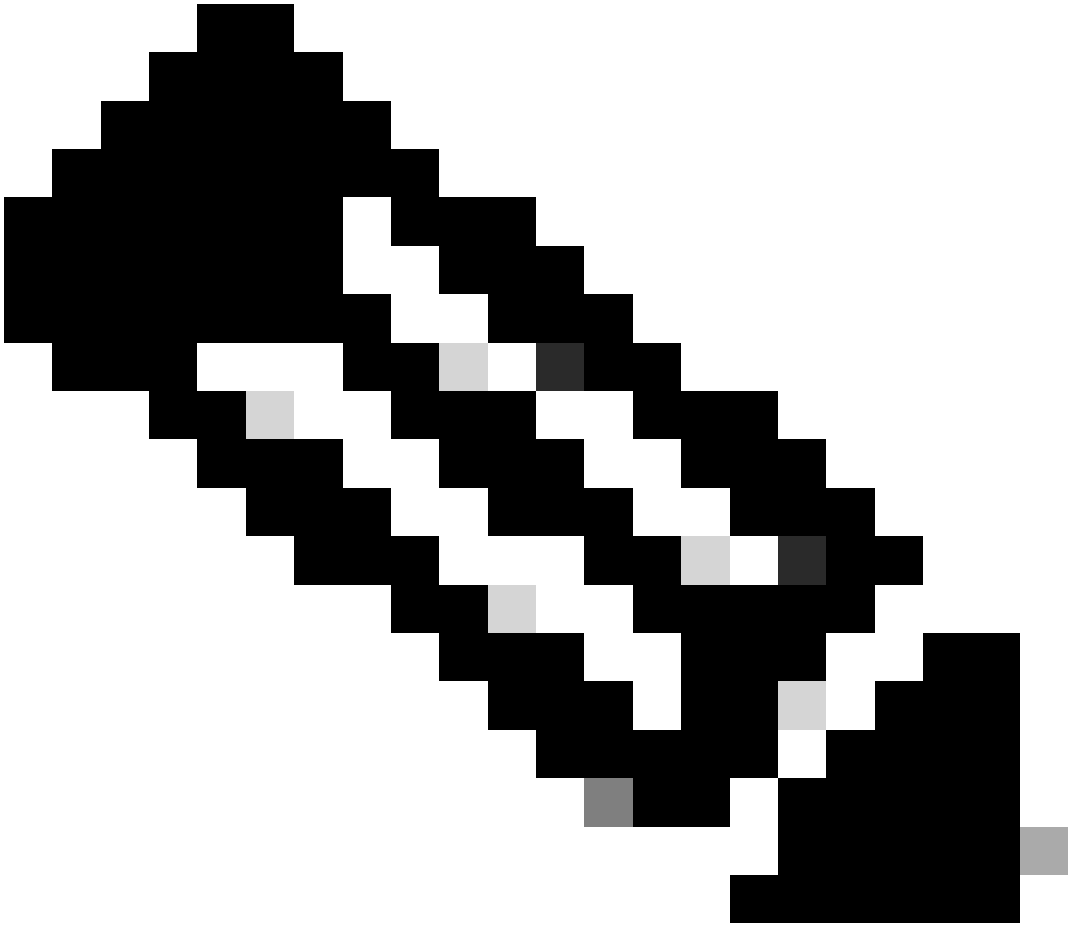
故障排除

本文档中使用的故障排除基于联机文档：

[排除COS AP故障]

故障排除的一般指导原则是使用客户端mac地址从WLC收集调试模式的RA跟踪，确保客户端使用设备mac而不是随机mac地址进行连接。

对于空中故障排除，建议使用嗅探器模式下的AP捕获客户端服务AP的信道上的流量。



注意：使用debug命令之前，请参阅有关Debug命令的重要信息。

相关信息

什么是Wi-Fi 6E？

什么是Wi-Fi 6与Wi-Fi 6E？

Wi-Fi 6E概览

Wi-Fi 6E：Wi-Fi下一重要章节（白皮书）

Cisco Live -使用Catalyst Wi-Fi 6E接入点构建下一代无线网络

Cisco Catalyst 9800系列无线控制器软件配置指南17.9.x

WPA3部署指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。