Wi-Fi 6E WLANレイヤ2セキュリティの設定と確認

内容

はじめに

このドキュメントでは、Wi-Fi 6E WLANレイヤ2セキュリティを設定する方法と、さまざまなクライアントで想定される動作について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CiscoワイヤレスLanコントローラ(WLC)9800
- Wi-Fi 6Eをサポートするシスコアクセスポイント(AP)
- IEEE標準802.11ax。
- ツール：Wireshark v4.0.6

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- IOS® XE 17.9.3を搭載したWLC 9800-CL。
- AP C9136、CW9162、CW9164、およびCW9166。
- Wi-Fi 6Eクライアント：
  - Lenovo X1 Carbon Gen11(Intel AX211 Wi-Fi 6および6Eアダプタ、ドライババージョン22.200.2(1)搭載)
  - Netgear A8000 Wi-Fi 6および6Eアダプタ、ドライバv1(0.0.108)、
  - Android 13搭載の携帯電話Pixel 6a、
  - 携帯電話Samsung S23とAndroid 13。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ここで重要なのは、Wi-Fi 6Eは完全に新しい標準ではなく、拡張であるということです。 Wi-Fi 6Eは、Wi-Fi 6(802.11ax)無線規格を6 GHz無線周波数帯域に拡張したものです。

Wi-Fi 6Eは、最新世代のWi-Fi規格であるWi-Fi 6に基づいて構築されていますが、6 GHz帯域で動作できるのはWi-Fi 6Eデバイスとアプリケーションだけです。

Wi-Fi 6Eセキュリティ

Wi-Fi 6Eは、Wi-Fi Protected Access 3(WPA3)およびOpportunistic Wireless Encryption(LEAN)を使用してセキュリティを強化し、オープンおよびWPA2セキュリティとの下位互換性はありません。

WPA3とEnhanced Open Securityは現在、Wi-Fi 6E認定に必須であり、Wi-Fi 6EにはAPとクライアントの両方でProtected Management Frame(PMF)も必要です。

6 GHz SSIDを設定する場合、満たす必要がある特定のセキュリティ要件があります。

- LEAN、SAEまたは802.1x-SHA256を使用したWPA3 L2セキュリティ
- 保護された管理フレームが有効。
- 他のL2セキュリティ方式は許可されていません。つまり、混合モードは使用できません。

WPA3

WPA3は、WPA2での認証を向上させ、強力な暗号化機能を提供し、重要なネットワークの復元力を高めることで、Wi-Fiセキュリティを向上させるように設計されています。

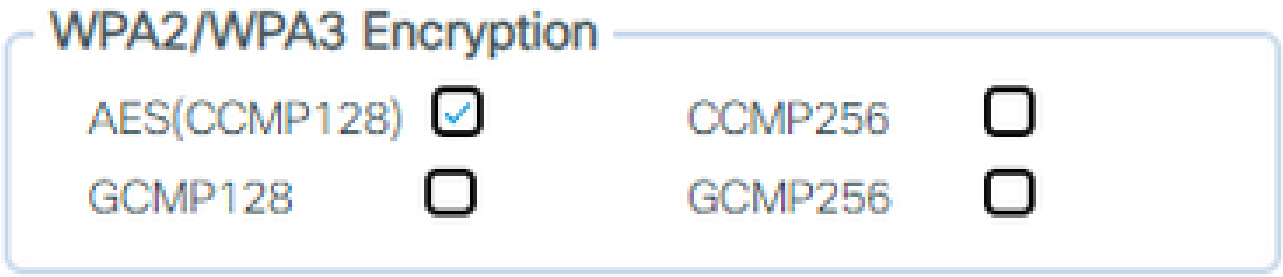
WPA3の主な機能は次のとおりです。

- Protected Management Frame(PMF)は、ユニキャストおよびブロードキャスト管理フレームを保護し、ユニキャスト管理フレームを暗号化します。つまり、ワイヤレス侵入検知システムとワイヤレス侵入防御システムでは、クライアントポリシーを適用するための総当たり的な方法が少なくなっています。
- SAE(Simultaneous Authentication of Equals)：パスワードベースの認証とキー承諾メカニズムを有効にします。これにより、総当たり攻撃から保護されます。
- 遷移モードは、WPA2を使用してWPA3をサポートしないクライアントに接続できるようにする混合モードです。

WPA3は、継続的なセキュリティの開発と準拠、および相互運用性に関するものです。WPA3（WPA2と同じ）を指定する情報要素(IE)はありません。WPA3は、AKM/暗号スイート/PMFの組み合わせによって定義されます。

9800 WLANの設定では、4つの異なるWPA3暗号化アルゴリズムを使用できます。

これらのプロトコルは、Galois/Counter Mode Protocol(GCMP)およびCounter Mode with Cipher Block Chaining Message Authentication Code Protocol(CCMP):AES(CCMP128)、CCMP256、GCMP128、GCMP256をベースにしています。

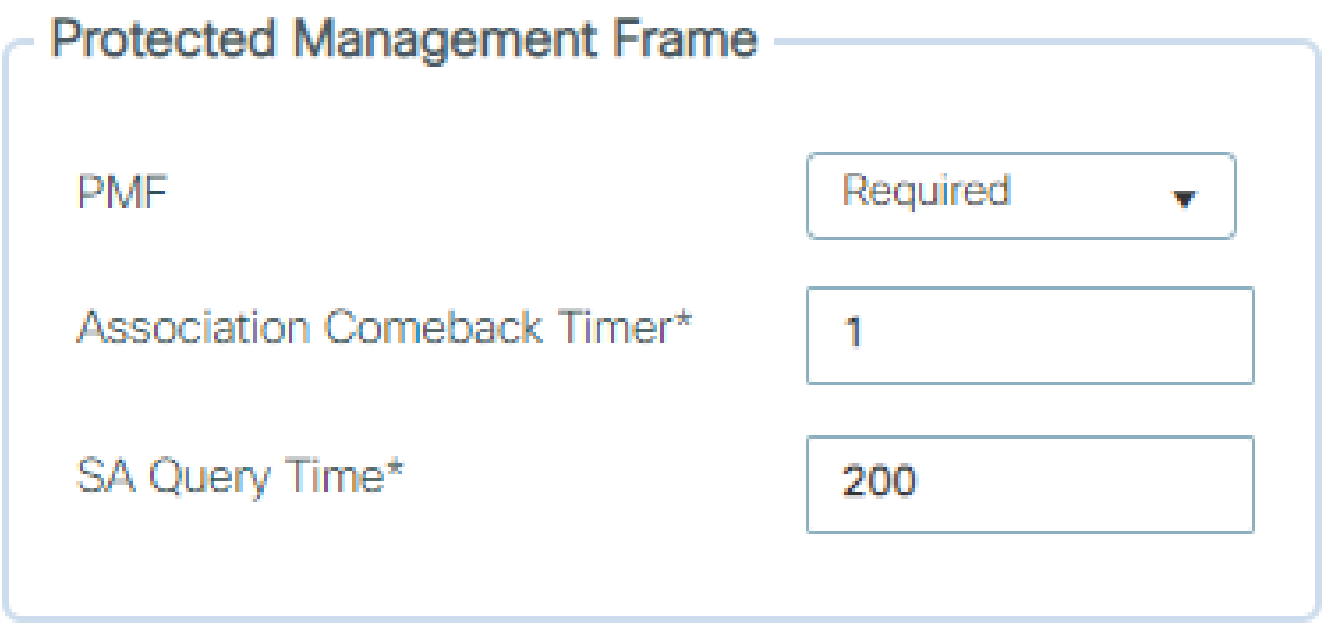


WPA2/3暗号化オプション

PMF

PMFを有効にすると、WLAN上でPMFがアクティブになります。

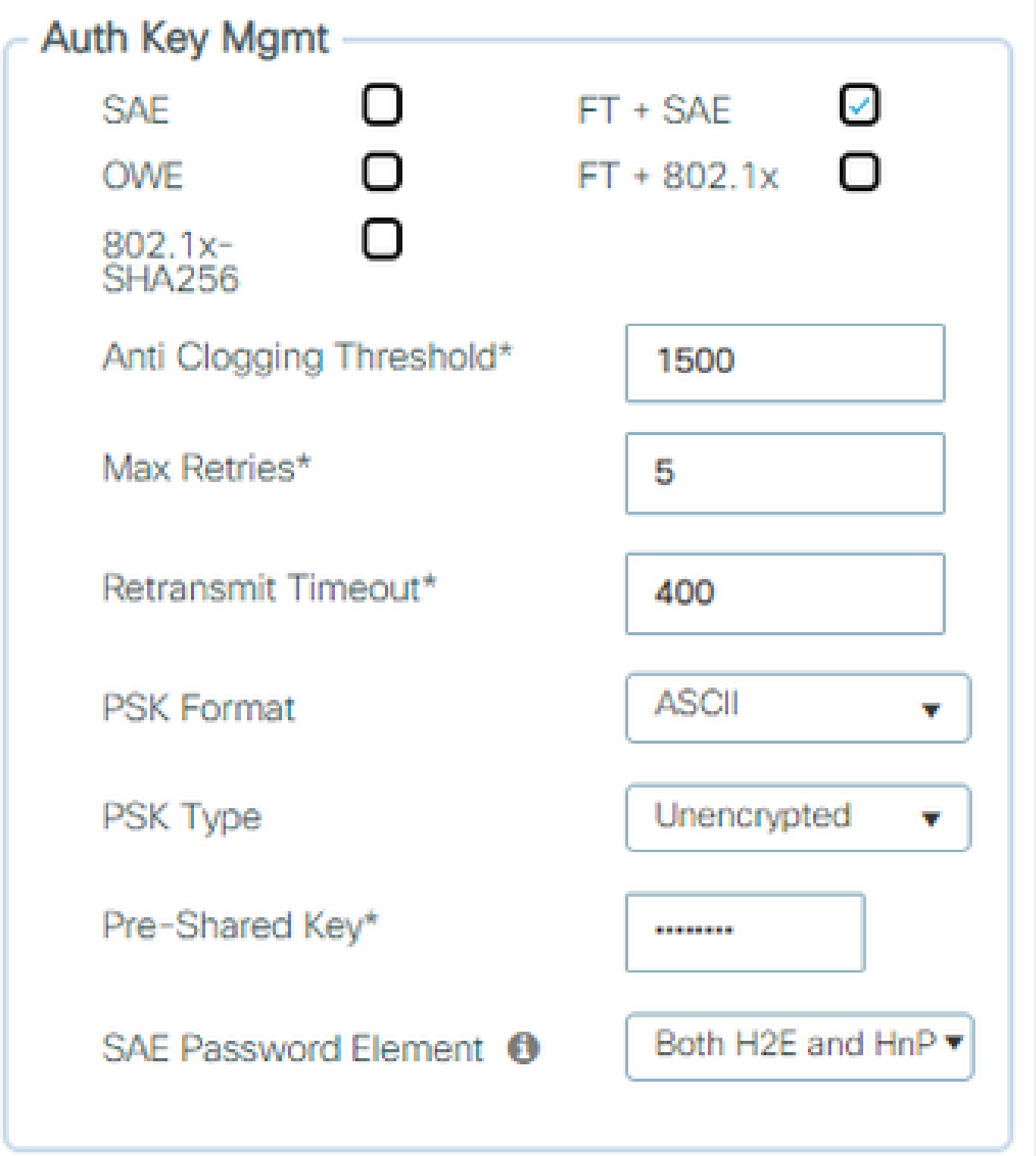
デフォルトでは、802.11管理フレームは認証されないため、スプーフィングから保護されません。Infrastructure Management Protection Frame(MFP)および802.11wで保護された管理フレーム(PMF)は、このような攻撃に対する保護を提供します。



PMFオプション

認証キー管理

17.9.xバージョンで使用可能なAKMオプションは次のとおりです。

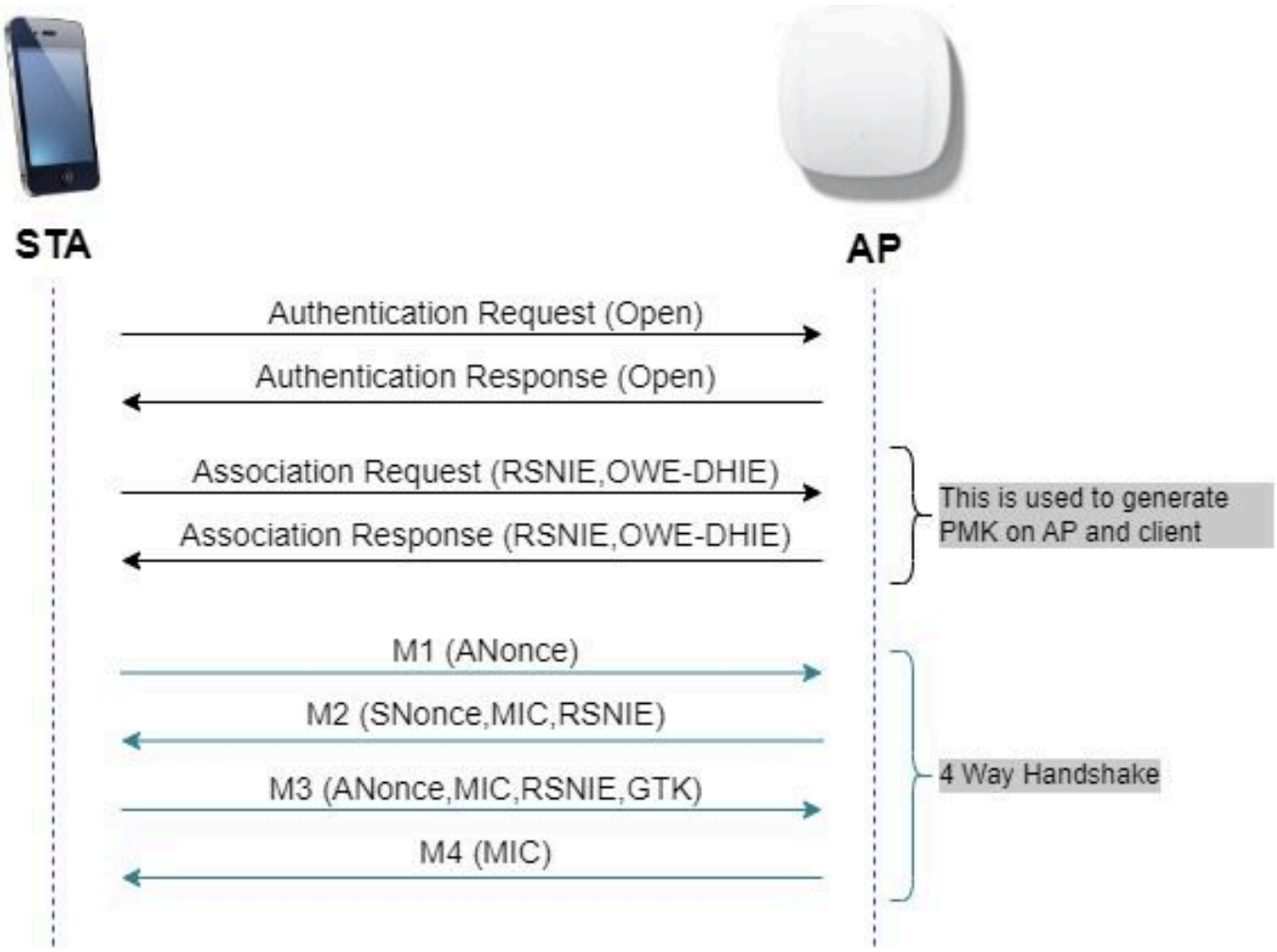


AKMオプション

負担

Opportunistic Wireless Encryption(LEAN)は、ワイヤレスメディアの暗号化を提供するIEEE 802.11の拡張です(IETF RFC 8110)。LEADベースの認証の目的は、APとクライアント間のオープンでセキュリティ保護されていないワイヤレス接続を回避することです。LEANは、暗号化に基づくDiffie-Hellmanアルゴリズムを使用して、無線暗号化を設定します。LEANを使用すると、クライアントとAPはアクセス処理中にDiffie-Hellman(DH)鍵交換を実行し、その結果得られたPairwise Master Key(PMK)秘密を4ウェイハンドシェイクで使用します。LEANを使用すると、オ

ープンまたは共有PSKベースのネットワークが展開される環境でワイヤレスネットワークセキュリティが強化されます。



LEANフレーム交換

SAE

WPA3では、Simultaneous Authentication of Equalsと呼ばれる新しい認証およびキー管理メカニズムを使用します。このメカニズムは、SAE Hash-to-Element(H2E)を使用することでさらに強化されます。

H2Eを使用したSAEは、WPA3とWi-Fi 6Eに必須です。

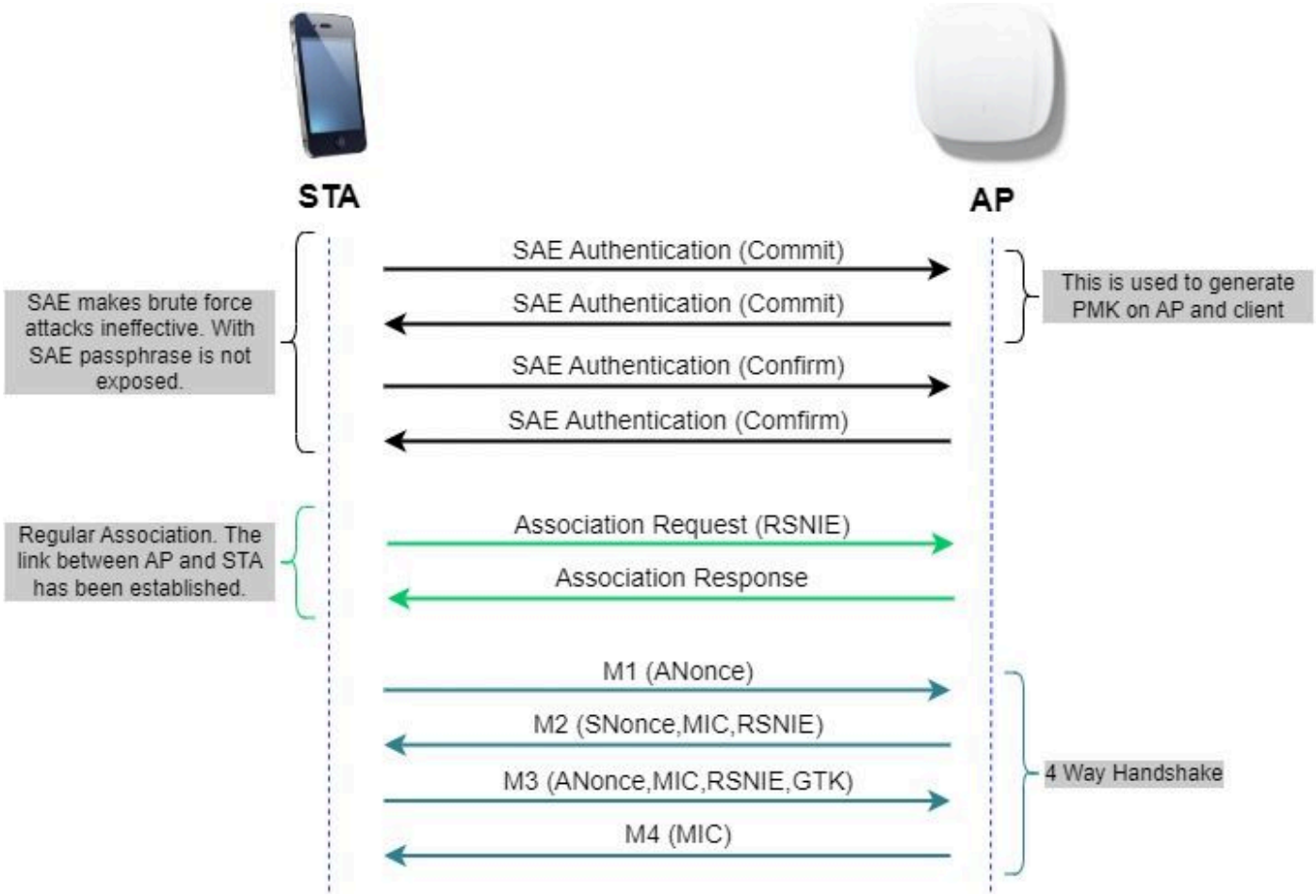
SAEは、オフライン辞書攻撃に対する耐性が高いと考えられるパスワードを使用して相互認証を実行する方法で効率的な交換を実行するために、離散対数暗号化を採用しています。

オフライン辞書攻撃とは、攻撃者がネットワークとのやり取りを行わずに可能なパスワードを試みることによってネットワークパスワードを決定しようとする攻撃です。

クライアントがアクセスポイントに接続すると、SAE交換が実行されます。成功した場合は、それぞれが暗号強度の高いキーを作成し、そこからセッションキーが取得されます。基本的に、クライアントとアクセスポイントはコミットのフェーズに入り、確認します。

確約が行われると、生成されるセッションキーがあるたびに、クライアントとアクセスポイント

はconfirm状態になります。この方法では、侵入者が単一のキーをクラックする可能性がありますが、他のすべてのキーをクラックする可能性はありません。



SAEフレーム交換

ハッシュから要素(H2E)

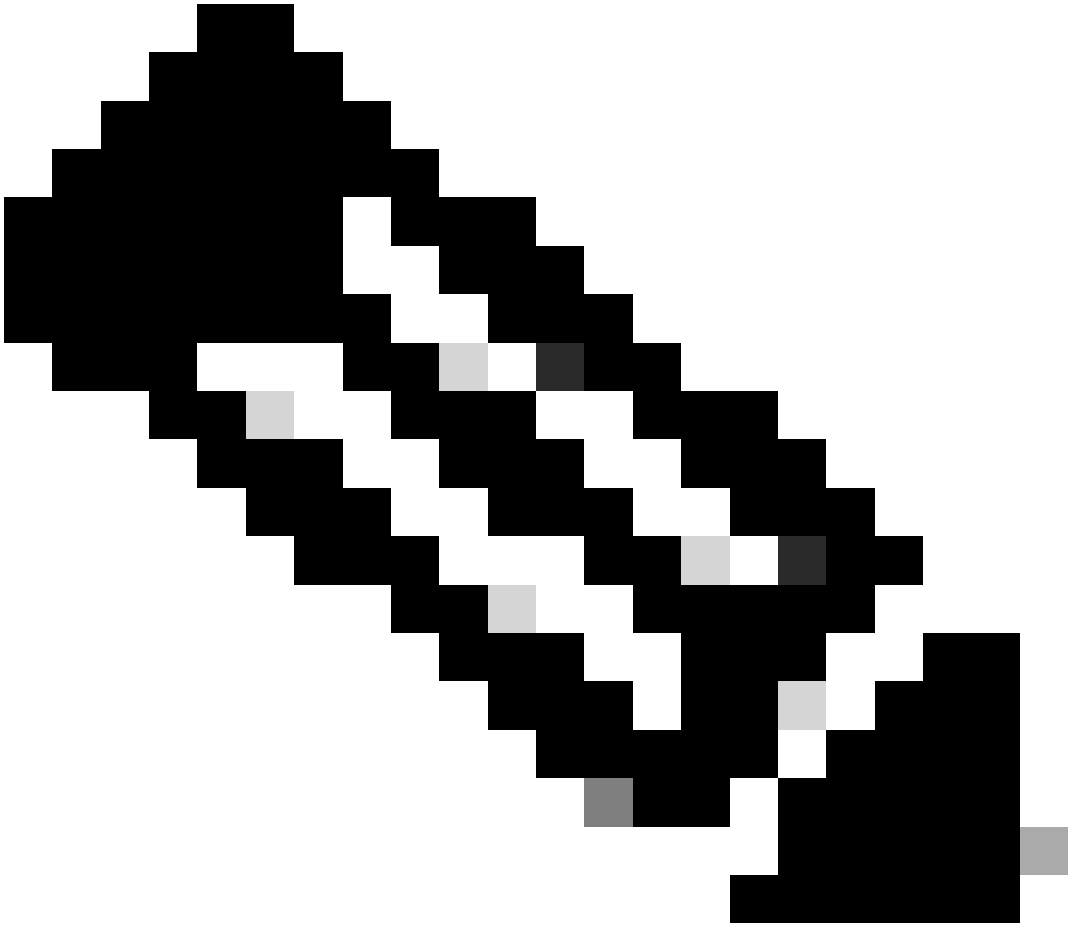
ハッシュから要素(H2E)は、新しいSAEパスワード要素(PWE)方式です。この方法では、SAEプロトコルで使用される秘密PWEがパスワードから生成されます。

H2Eをサポートするステーション(STA)は、APでSAEを開始するときに、APがH2Eをサポートしているかどうかを確認します。そうである場合、APはH2Eを使用し、SAEコミットメッセージで新しく定義されたステータスコード(SC)値を使用してPWEを取得します。

STAがハンティングアンドペッキング(HnP)を使用する場合、SAE交換全体は変更されません。

H2Eを使用する場合、PWE派生は次のコンポーネントに分割されます。

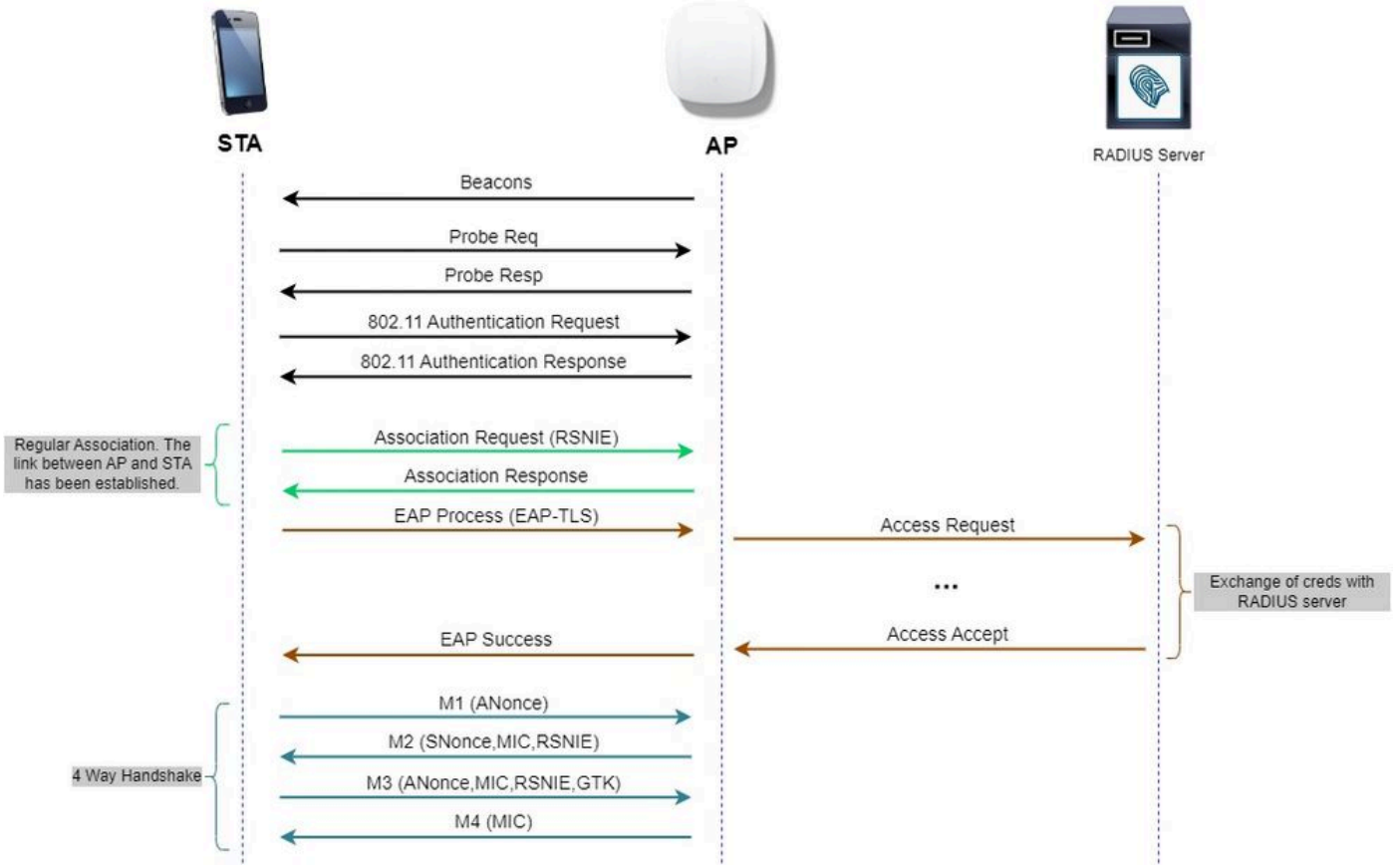
- パスワードから秘密中間要素(PT)を派生させます。この操作は、サポートされている各グループのデバイスでパスワードが最初に設定されたときにオフラインで実行できます。
- 保管されたPTからのPWEの導出これは、ピアのネゴシエートされたグループとMACアドレスによって異なります。これは、SAE交換中にリアルタイムで実行されます。



注:6 GHzは、ハッシュから要素へのSAE PWE方式のみをサポートしています。

WPA – エンタープライズ（別名802.1x）

WPA3-Enterpriseは、WPA3の最も安全なバージョンであり、802.1Xとユーザ名およびパスワードの組み合わせを使用して、RADIUSサーバによるユーザ認証を行います。デフォルトでは、WPA3は128ビットの暗号化を使用しますが、オプションで設定可能な192ビットの暗号強度の暗号化も導入されています。これにより、機密データを送信するすべてのネットワークに対する保護が強化されます。



WPA3 Enterpriseの図のフロー

レベルセット：WPA3モード

- WPA3パーソナル
  - WPA3 – パーソナル専用モード
    - PMFが必要
  - WPA3-Personal移行モード
    - 設定ルール：APでは、WPA2-Personalが有効になっている場合は常に、管理者が明示的に上書きしてWPA2-Personal専用モードで動作しない限り、WPA3-Personal移行モードもデフォルトで有効にする必要があります

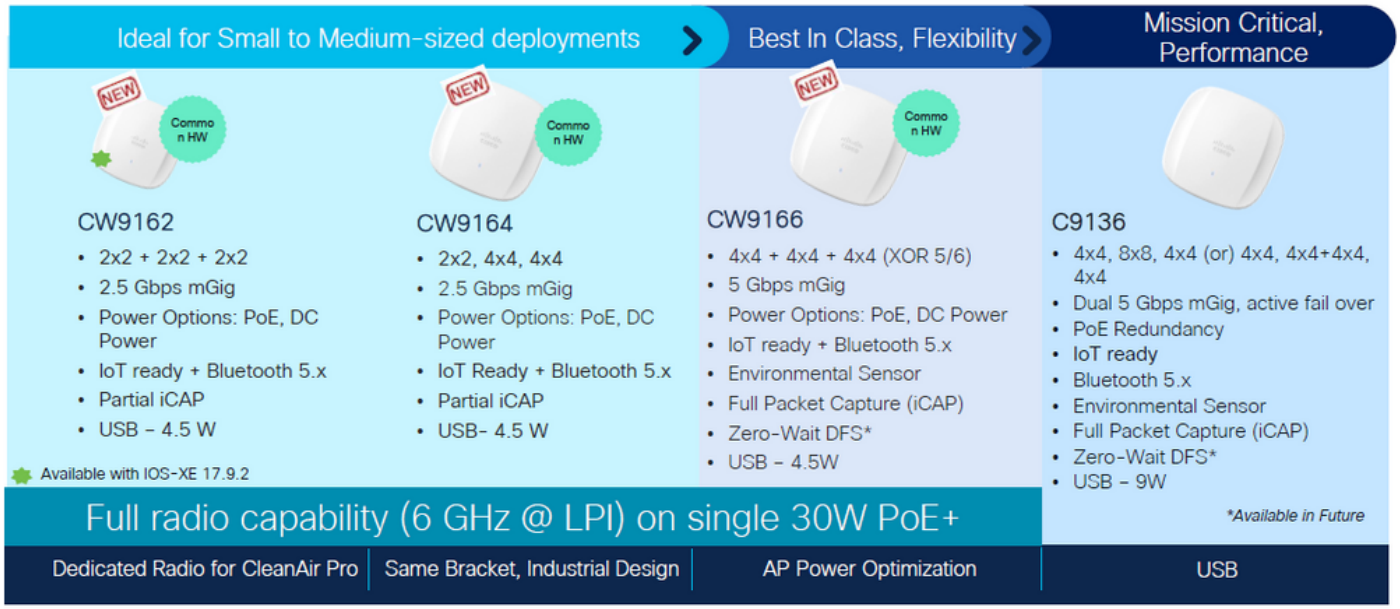
- WPA3 – エンタープライズ
  - WPA3-Enterprise専用モード
    - すべてのWPA3接続でPMFがネゴシエートされます
  - WPA3-Enterprise移行モード
    - WPA3接続ではPMFがネゴシエートされます
    - WPA2接続用のPMFオプション
  - Commercial National Security Algorithm(CNSA)に準拠したWPA3-Enterprise suite-B「192ビット」モード
    - 単なる連邦政府のためだけではない
    - 設定ミスを回避するための一貫性のある暗号暗号スイート
    - 暗号化やより良いハッシュ関数のためのGCMPとECCPの追加(SHA384)
    - PMFが必要

- WPA3 192ビットセキュリティは、サプリカントとRADIUSサーバの両方で証明書を必要とするEAP-TLSにのみ適用されます。
- WPA3 192ビットエンタープライズを使用するには、RADIUSサーバは許可されたEAP暗号のいずれかを使用する必要があります。

  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

クライアントセキュリティの互換性マトリクスを含む、Cisco WLANでのWPA3の実装に関する詳細については、WPA3導入ガイドを参照してください。

Cisco Catalyst Wi-Fi 6E AP



Wi-Fi 6Eアクセスポイント

クライアントでサポートされるセキュリティ設定

WPA3-Enterpriseをサポートしている製品は、WiFi Alliance Webページの製品ファインダを使用して確認できます。

Windowsデバイスでは、コマンド「netsh wlan show drivers」を使用して、アダプタによってサポートされているセキュリティ設定を確認できます。

Intel AX211の出力を次に示します。

```
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
```

クライアントAX211用の_netsh wlan show driver_のWindows出力

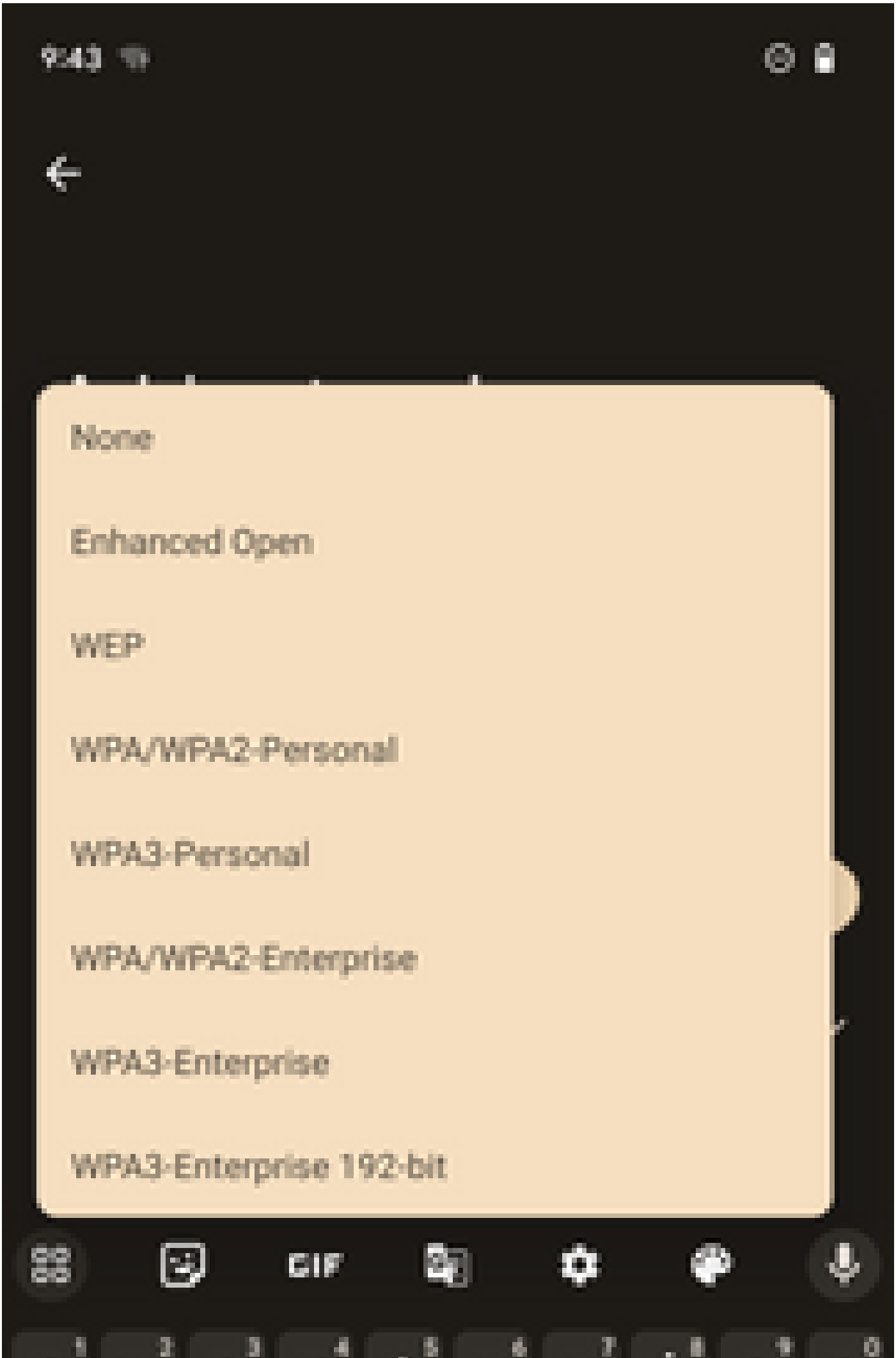
Netgear A8000:

```
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)
```

クライアントNetgear A8000sでの_netsh wlan show driver_のWindows出力

Androidピクセル6a:


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

負担	AES-CCMP128	負担	適用外.	適用外.	適用外	適用外	サポート	サポート
SAE	AES-CCMP128	SAE（H2Eのみ）	SHA256	適用外.	サポート	サポート	サポート：H2Eのみ、およびFT-oTA	サポート：H2Eのみ。FTが失敗しました。FT-oDSが失敗しました。
エンタープライズ	AES-CCMP128	802.1x-SHA256	SHA256	PEAP/FAST/TLS	サポート	サポート	サポート：SHA256およびFT-oTA/oDS 非サポート：EAP-FAST	サポート：SHA256およびFT-oTA、FT-oDS(S23) サポート対象外：EAP-FAST、FT-oDS(Pixel6a)
エンタープライズ	GCMP128	スイートB-1x	SHA256-SuiteB	PEAP/FAST/TLS	サポート対象外	サポート対象外	サポート対象外	サポート対象外
エンタープライズ	GCMP256	スイートB-192	SHA384-SuiteB	[TLS]	サポート対象外	サポート対象外	該当なし/未定	該当なし/未定

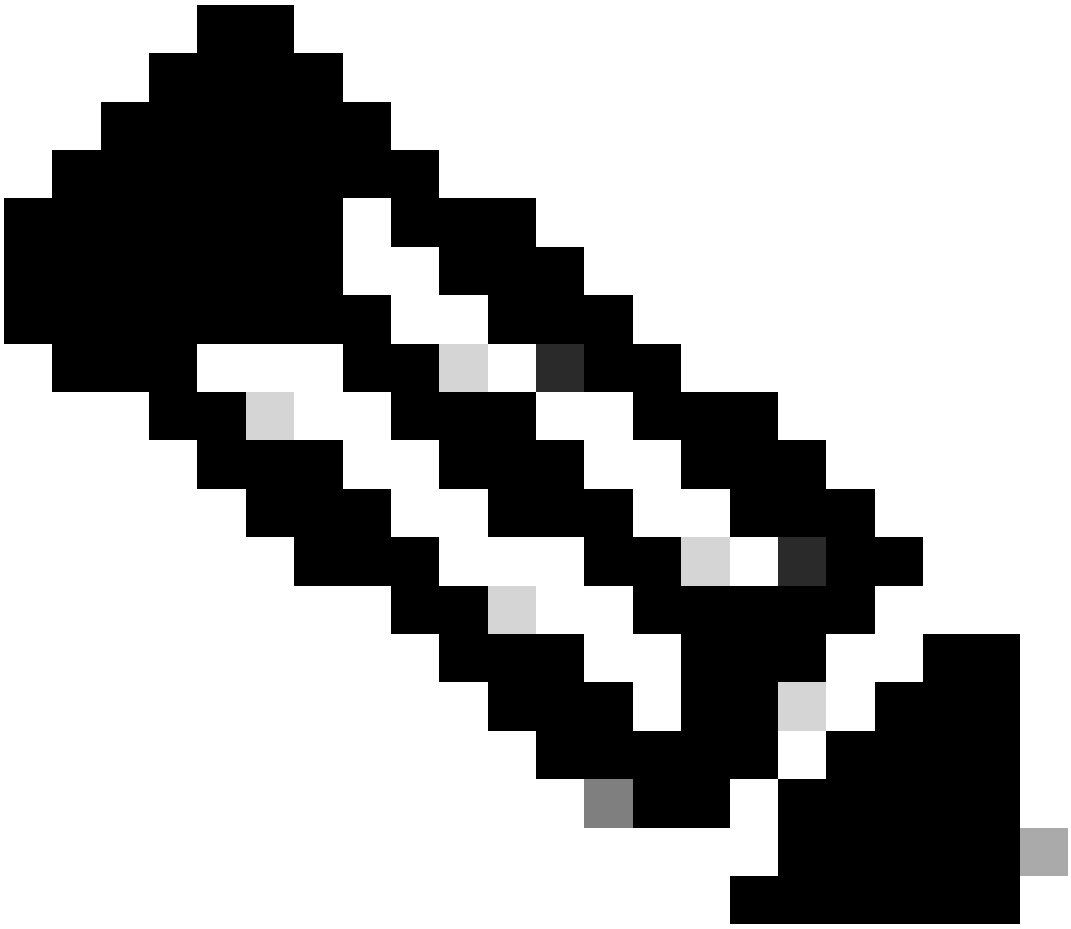
トラブルシュート

このドキュメントで使用するトラブルシューティングは、次のオンラインドキュメントに基づいています。

COS APのトラブルシューティング

トラブルシューティングの一般的なガイドラインは、クライアントがランダム化されたMACアドレスではなくデバイスMACを使用して接続していることを確認するために、クライアントMACアドレスを使用してWLCからデバッグモードでRAトレースを収集することです。

Over-the-Airのトラブルシューティングでは、APにサービスを提供しているクライアントのチャネルでトラフィックをキャプチャするAPをスニファモードで使用することを推奨します。



注：debugコマンドを使用する前に、『debugコマンドの重要な情報』を参照してください。

関連情報

Wi-Fi 6Eとは

Wi-Fi 6とWi-Fi 6Eについて

Wi-Fi 6E概要

Wi-Fi 6E:Wi-Fiに関するホワイトペーパーの次の章

Cisco Live - Catalyst Wi-Fi 6Eアクセスポイントによる次世代ワイヤレスネットワークの設計

Cisco Catalyst 9800シリーズワイヤレスコントローラソフトウェアコンフィギュレーションガイド17.9.x

WPA3導入ガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。