

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](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[Wi-Fi 6Eセキュリティ](#)

[WPA3](#)

[レベルセット：WPA3モード](#)

[Cisco Catalyst Wi-Fi 6E AP](#)

[クライアントでサポートされるセキュリティ設定](#)

[設定](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[基本設定](#)

[確認](#)

[セキュリティの検証](#)

[WPA3 - AES\(CCMP128\) + 使用料](#)

[WPA3 - AES\(CCMP128\) + 移行モード付き LEAN](#)

[WPA3 - パーソナル - AES\(CCMP128\) + SAE](#)

[WPA3 - パーソナル - AES\(CCMP128\) + SAE + FT](#)

[WPA3-Enterprise + AES\(CCMP128\) + 802.1x-SHA256 + FT](#)

[WPA3-Enterprise + GCMP128暗号+ SUITEB-1X](#)

[WPA3-Enterprise + GCMP256暗号+ SUITEB192-1X](#)

[セキュリティ結論](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、Wi-Fi 6E WLAN レイヤ 2 セキュリティの設定方法とさまざまなクライアントで予期される事柄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 Wireless Lan Controller(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は完全に新しい規格ではなく、拡張された規格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、Wi-Fi規格の最新世代である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(LEAP)により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を設定する際には、特定のセキュリティ要件を満たす必要があります。

- LEAP、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ません。つまり、混合モードは使用できません。

WPA3

WPA3は、WPA2を介した認証を強化し、強力な暗号化機能を提供して重要なネットワークの復元力を高めることで、Wi-Fiセキュリティを強化す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) : ユニキャストおよびブロードキャストの管理フレームを保護し、ユニキャストの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手段が少なくなっています。
- Simultaneous Authentication of Equals(SAE) : パスワードベースの認証とキー同意メカニズムを有効にします。これにより、ブルートフォース攻撃から保護されます。
- 移行モードは、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/Cipher Suite/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、およびGCMP256)に基づいています。

WPA2/WPA3 Encryption

AES(CCMP128)	☒	CCMP256	☐
GCMP128	☐	GCMP256	☐

WPA2/3暗号化オプション

PMF

PMFを有効にすると、WLAN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ていないため、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。

Protected Management Frame

PMF

Required ▼

Association Comeback Timer*

1

SA Query Time*

200

PMFオプション

認証キー管理

17.9.xバージョンで利用できるAKMオプションは次のとおりです。

Auth Key Mgmt

SAE	☐	FT + SAE	☒
OWE	☐	FT + 802.1x	☐
802.1x- SHA256	☐		

Anti Clogging Threshold*

1500

Max Retries*

5

Retransmit Timeout*

400

PSK Format

ASCII ▼

PSK Type

Unencrypted ▼

Pre-Shared Key*

SAE Password Element ⓘ

Both H2E and HnP ▼

AKMオプション

GUIには「FT + 802.1x-SHA256」がないことに注意してください。その理由は次のとおりです。

- 802.1XはAKM 1を指し、標準の802.1X - SHA1です。GUIでは、「WPA2」ポリシーまたは「WPA2+3」ポリシーについてののみ提示します。
- FT + 802.1xはAKM 3であり、実際には802.1X-SHA256上のFTです。これはWPA2ですすでに使用可能でしたが、すでにSHA256を使用しているため、WPA3準拠と見なされます。
- 802.1X:SHA256はAKM 5はWPA3に準拠しています。

FTクライアントだけをサポートする場合は、「FT+802.1x」だけを使用するWPA3 SSIDを設定できます。FTクライアントと非FTクライアントの両方をサポートする場合は、FT+802.1xおよび802.1x-SHA256を使用するWPA3 SSIDを設定できます。

要約すると、既存のAKMはWPA3にすでに準拠しているため、WPA3用の802.1xではFT用の異なるAKMはありません。

次の表に、[IEEE Std 802.11™-2020](#)ドキュメントで定義されているさまざまなAKM値を示します。

AKM 8および9はSAEで使用され、AKM 1、3、5、11はWPA3-EnterpriseのみまたはWPA3-Enterpriseの移行で使用され、AKM 12、13は192ビットを使用するWPA3-Enterpriseで、AKM 18はEnhanced Open(LEAN)で使用されることに注意してください。

<u>OUI</u>	<u>スイート タイプ</u>	<u>認証タイプ</u>	<u>説明</u>
00-0F-AC	0	Reserved	Reserved
00-0F-AC	1	標準802.1x - SHA1	SHA1をサポートするIEEE標準802.1Xでネゴシエートされた認証
00-0F-AC	2	PSK - SHA-1	SHA1をサポートする事前共有キー
00-0F-AC	3	802.1x上のFT - SHA256	SHA256をサポートするIEEE Std 802.1X上でネゴシエートされた高速移行認証
00-0F-AC	4	FT over PSK - SHA256	SHA-256をサポートするPSKを使用した高速移行認証
00-0F-AC	5	標準802.1x - SHA256	IEEE Std 802.1X上でネゴシエートされた認証
00-0F-AC	6	PSK - SHA256	SHA256をサポートする事前共有キー
00-0F-AC	7	TDL	SHA256をサポートするTPKハンドシェイク

00-0F-AC	8	SAE - SHA256	SHA256を使用した等の同時認証
00-0F-AC	9	FT over SAE - SHA256	SHA256を使用した等の同時認証の高速移行
00-0F-AC	10	APPeerKey認証 – SHA256	SHA-256によるAPPeerKey認証
00-0F-AC	11	標準802.1x SuiteB - SHA256	SHA-256をサポートするSuite B準拠のEAP方式を使用してIEEE Std 802.1Xでネゴシエートされる認証
00-0F-AC	12	標準802.1x SuiteB - SHA384	SHA384をサポートするCNSA Suite準拠のEAP方式を使用してIEEE Std 802.1Xでネゴシエートされる認証
00-0F-AC	13	802.1x上のFT - SHA384	SHA384をサポートするIEEE Std 802.1X上でネゴシエートされた高速移行認証
00-0F-AC	14	SHA256およびAES-SIV-256によるファイル	SHA-256およびAES-SIV-256を使用したFILSでのキー管理、またはIEEE Std 802.1Xでの認証ネゴシエーション
00-0F-AC	15	SHA384およびAES-SIV-512によるファイル	SHA-384およびAES-SIV-512を使用したFILSでのキー管理、またはIEEE Std 802.1Xでの認証ネゴシエーション
00-0F-AC	16	FT over FILS (SHA256)	SHA-256およびAES-SIV-256によるFILS経由の高速移行認証、またはIEEE Std 802.1X経由でネゴシエートされた認証
00-0F-AC	17	FT over FILS (SHA384)	SHA-384およびAES-SIV-512を使用したFILS上での高速移行認証、またはIEEE Std 802.1X上でネゴシエートされた認証
00-0F-AC	18	Reserved	WiFi AllianceによるLEANに使用

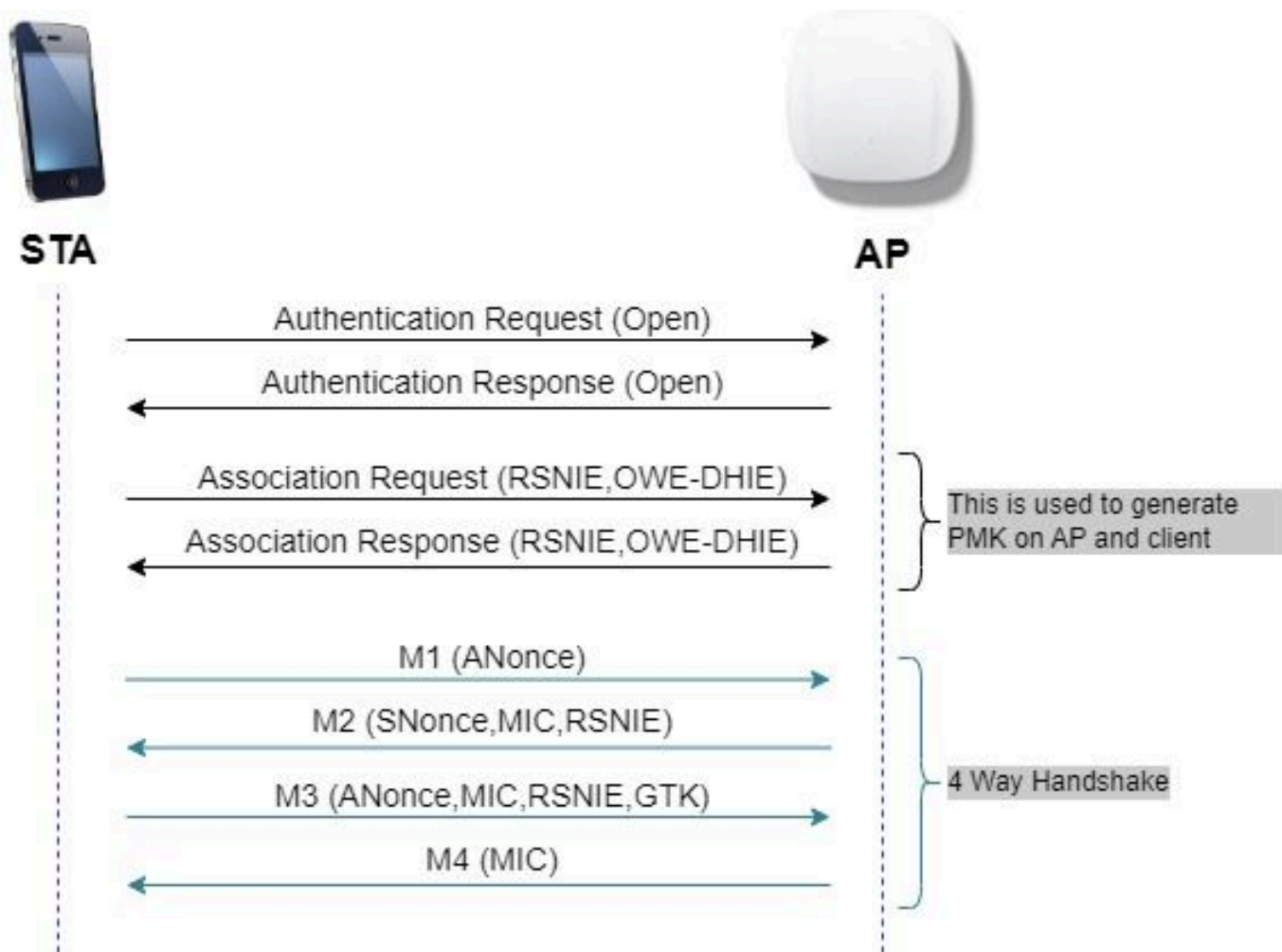
00-0F-AC	19	FT over PSK - SHA384	SHA384によるPSKを使用した高速移行認証
00-0F-AC	20	PSK-SHA384	SHA384をサポートする事前共有キー
00-0F-AC	21-255	Reserved	Reserved
00-0F-AC	[Any]	ベンダー固有	ベンダー固有

一部のAKMでは、(128ビットおよび192ビットのセキュリティ強度を提供する) 暗号化アルゴリズムのセットである「SuiteB」を参照しています。これは、2005年にNSA(National Security Agency)によって定義されました。2018年に、NSAはSuite B(Commercial National Security Algorithm Suite)をCNSA(Commercial National Security Algorithm Suite)に置き換え、最小192ビットセキュリティを提供しました。WPA3-Enterprise 192ビットモードはAES-256-GCMP暗号化を使用し、次に示すCNSA認証済み暗号スイートを使用します。

- AES-256-GCMP : 認証暗号化。
- HMAC-SHA-384」を参照してください。
- ECDHandECDSA : キーの確立と認証に384ビットの楕円曲線を使用します。

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とクライアントの間でセキュリティで保護されていないオープンなワイヤレス接続を回避することです。LEANでは、Diffie-Hellmanアルゴリズムに基づく暗号化を使用して、ワイヤレス暗号化を設定します。LEANを使用すると、クライアントとAPはアクセス手順の間にDiffie-Hellman(DH)キー交換を実行し、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。LEAD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導入されている環境のワイヤレスネットワークセキュリティが強化されます。



フレーム交換の負担

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。

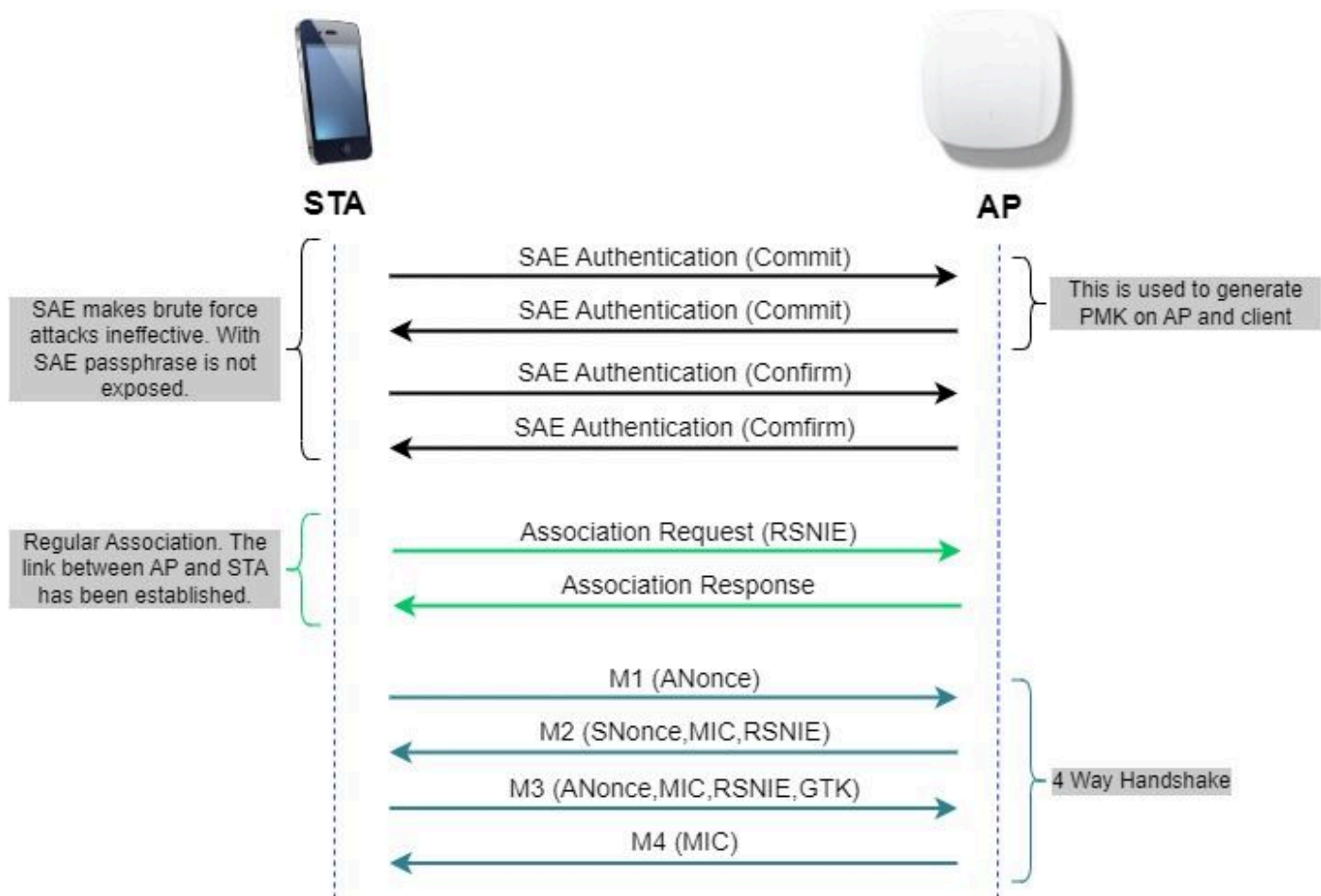
H2Eを使用したSAEは、WPA3およびWi-Fi 6Eに必須です。

SAEでは、離散型対数暗号化を使用して、オフライン辞書攻撃に対する耐性が高い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します。

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で、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、それぞれが暗号的に強力なキーを作成し、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が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るが、他のすべてのキーをクラックできるわけではない前方秘密が使用されます。



SAEフレーム交換

要素ハッシュ(H2E)

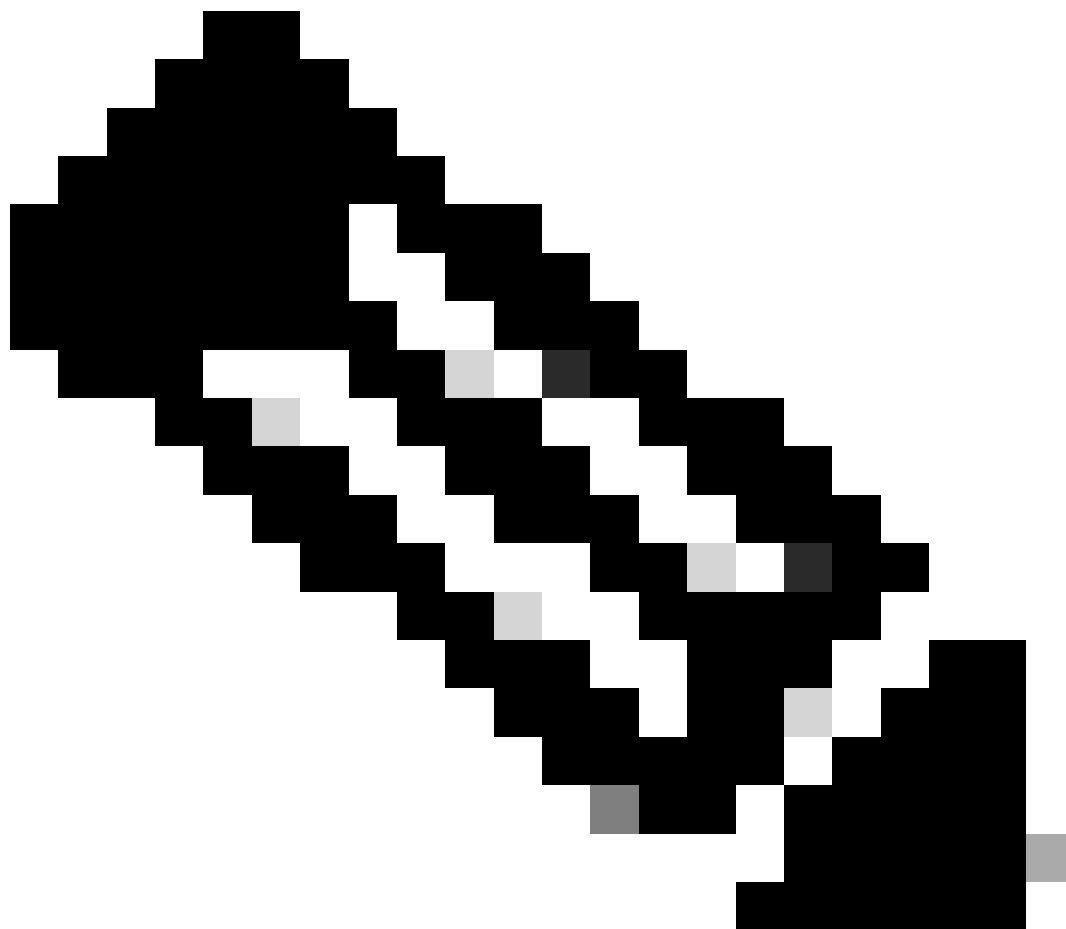
ハッシュから要素(H2E)は、新しいSAEパスワード要素(PWE)方式です。この方法では、SAEプロトコルで使用される秘密PWEがパスワードから生成されます。

H2Eをサポートするステーション(STA)がAPとのSAEを開始すると、APがH2Eをサポートするかどうかチェックされます。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/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。

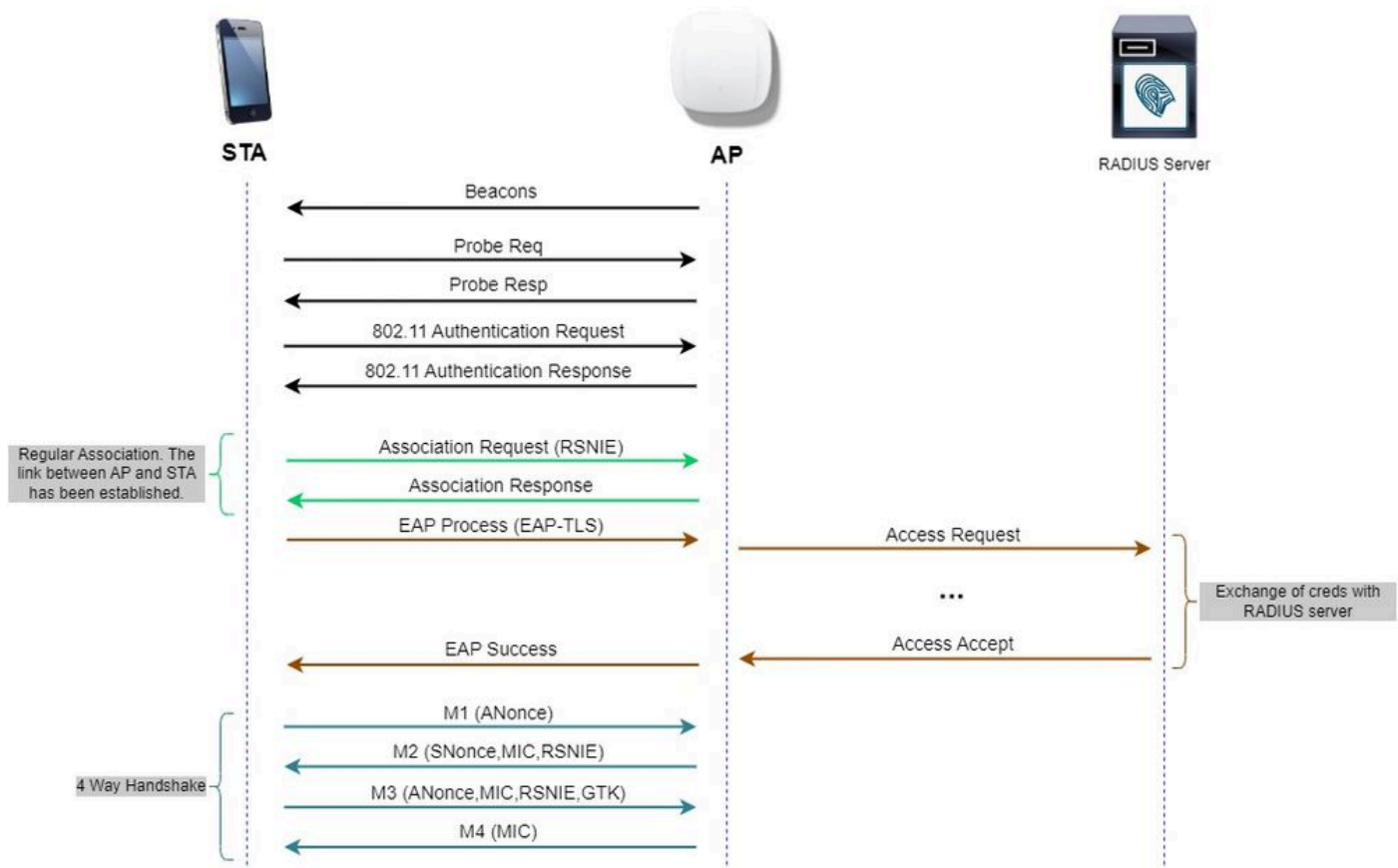
- パスワードからの秘密仲介要素(PT)の導出。これは、サポートされている各グループのパスワードがデバイスで最初に設定されたときにオフラインで実行できます。
- 格納されたPTからPWEを導出します。これは、ネゴシエートされたピアのグループとMACアドレスによって異なります。これは、SAE交換中にリアルタイムで実行されます。



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、RADIUSサーバでのユーザ認証に802.1Xを使用したユーザ名とパスワードの組み合わせを使用します。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のダイアグラムフロー

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 – パーソナル移行モード
 - 設定ルール：APでは、WPA2-Personalが有効である場合は常に、管理者が明示的にオーバーライドしてWPA2-Personal Only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 – エンタープライズ専用モード
 - すべてのWPA3接続でPMFがネゴシエートされます
 - WPA3 – エンタープライズ遷移モード
 - WPA3接続のためにPMFがネゴシエートされます
 - WPA2接続のPMFオプション
 - Commercial National Security Algorithm(CNSA)と連携するWPA3-Enterprise suite-B 「192ビット」モード
 - 単なる連邦政府に対してだけではなく –
 - 誤設定を回避するための一貫性のある暗号方式スイート
 - 暗号化および優れたハッシュ機能のためのGCMおよびECCPの追加(SHA384)
 - PMFが必要

- WPA3 192ビットセキュリティはEAP-TLSにのみ適用され、サブリカントとRADIUSサーバの両方で証明書が必要になります。
- 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互換性マトリクスを含む、Cisco WLANでのWPA3実装の詳細については、[WPA3 Deployment Guide](#)を参照してください。

Cisco Catalyst Wi-Fi 6E AP

Ideal for Small to Medium-sized deployments	Best In Class, Flexibility		Mission Critical, Performance
 CW9162 • 2x2 + 2x2 + 2x2 • 2.5 Gbps mGig • Power Options: PoE, DC Power • IoT ready + Bluetooth 5.x • Partial iCAP • USB - 4.5 W	 CW9164 • 2x2, 4x4, 4x4 • 2.5 Gbps mGig • Power Options: PoE, DC Power • IoT Ready + Bluetooth 5.x • Partial iCAP • USB - 4.5 W	 CW9166 • 4x4 + 4x4 + 4x4 (XOR 5/6) • 5 Gbps mGig • Power Options: PoE, DC Power • IoT ready + Bluetooth 5.x • Environmental Sensor • Full Packet Capture (iCAP) • Zero-Wait DFS* • USB - 4.5W	 C9136 • 4x4, 8x8, 4x4 (or) 4x4, 4x4+4x4, 4x4 • Dual 5 Gbps mGig, active fail over • PoE Redundancy • IoT ready • Bluetooth 5.x • Environmental Sensor • Full Packet Capture (iCAP) • Zero-Wait DFS* • USB - 9W
Available with IOS-XE 17.9.2 Full radio capability (6 GHz @ LPI) on single 30W PoE+			*Available in Future
Dedicated Radio for CleanAir Pro	Same Bracket, Industrial Design	AP Power Optimization	USB

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

WiFi Alliance Webページを使用して、WPA3-Enterpriseをサポートしている製品を確認できます
[製品の検索](#).

Windowsデバイスでは、「netsh wlan show drivers」コマンドを使用して、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\mtknhvux.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:



None

Enhanced Open

WEP

WPA/WPA2-Personal

WPA3-Personal

WPA/WPA2-Enterprise

WPA3-Enterprise

WPA3-Enterprise 192-bit



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 サポート対象外 : 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

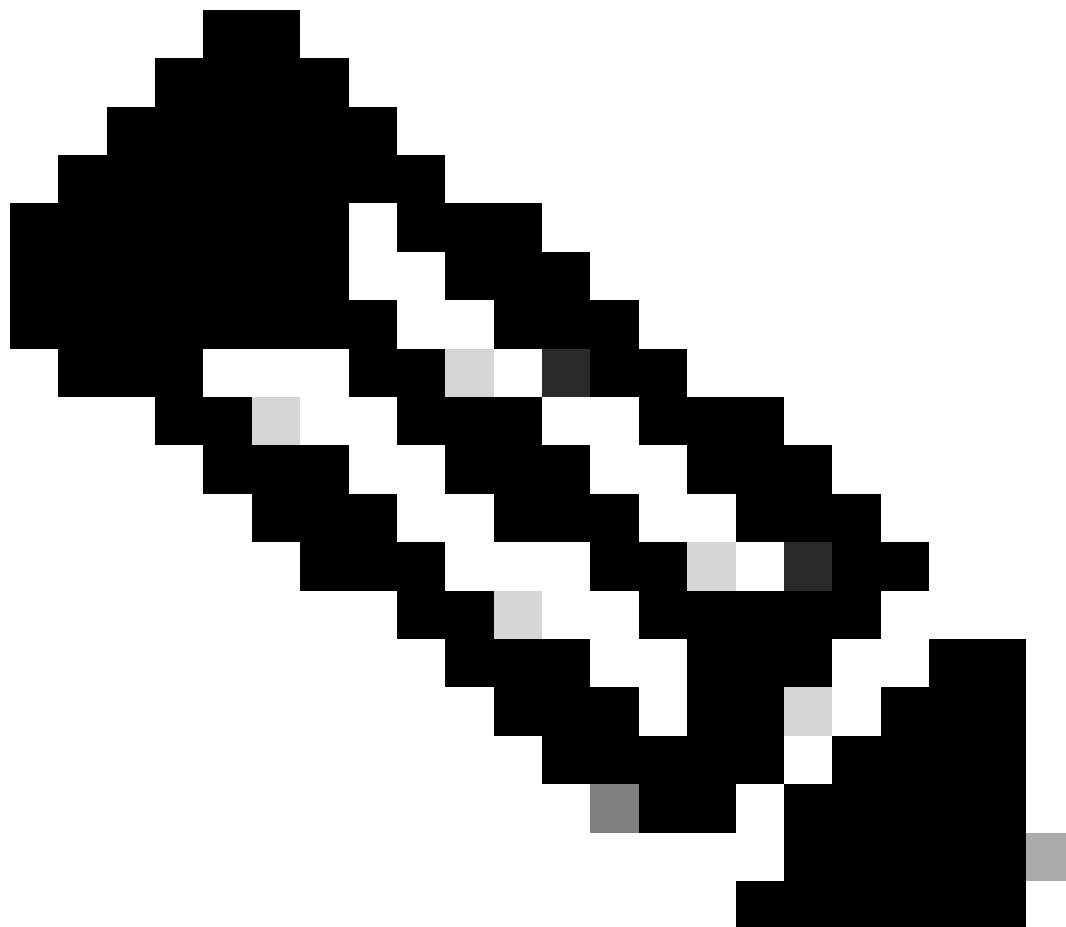
トラブルシューティング

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にサービスを提供するクライアントのチャンネルでトラフィックをキャプチャするスニファモードでAPを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の比較](#)

[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重要な章](#)

[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。