遷移モードを使用した拡張オープンSSIDの設定：LEAD

内容

はじめに

このドキュメントでは、Catalyst 9800ワイヤレスLANコントローラ(9800 WLC)で拡張オープン伝送モード(EOM)を設定およびトラブルシューティングする方法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
- WPA3をサポートするシスコアクセスポイント(AP)
- IEEE標準802.11ax。
- Wireshark.

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 C9130、C9136、CW9162、CW9164、およびCW9166

- Wi-Fi 6クライアント：
  - IOS 16上のiPhone SE第3世代
  - Mac OS 12のMacBook。
- Wi-Fi 6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。

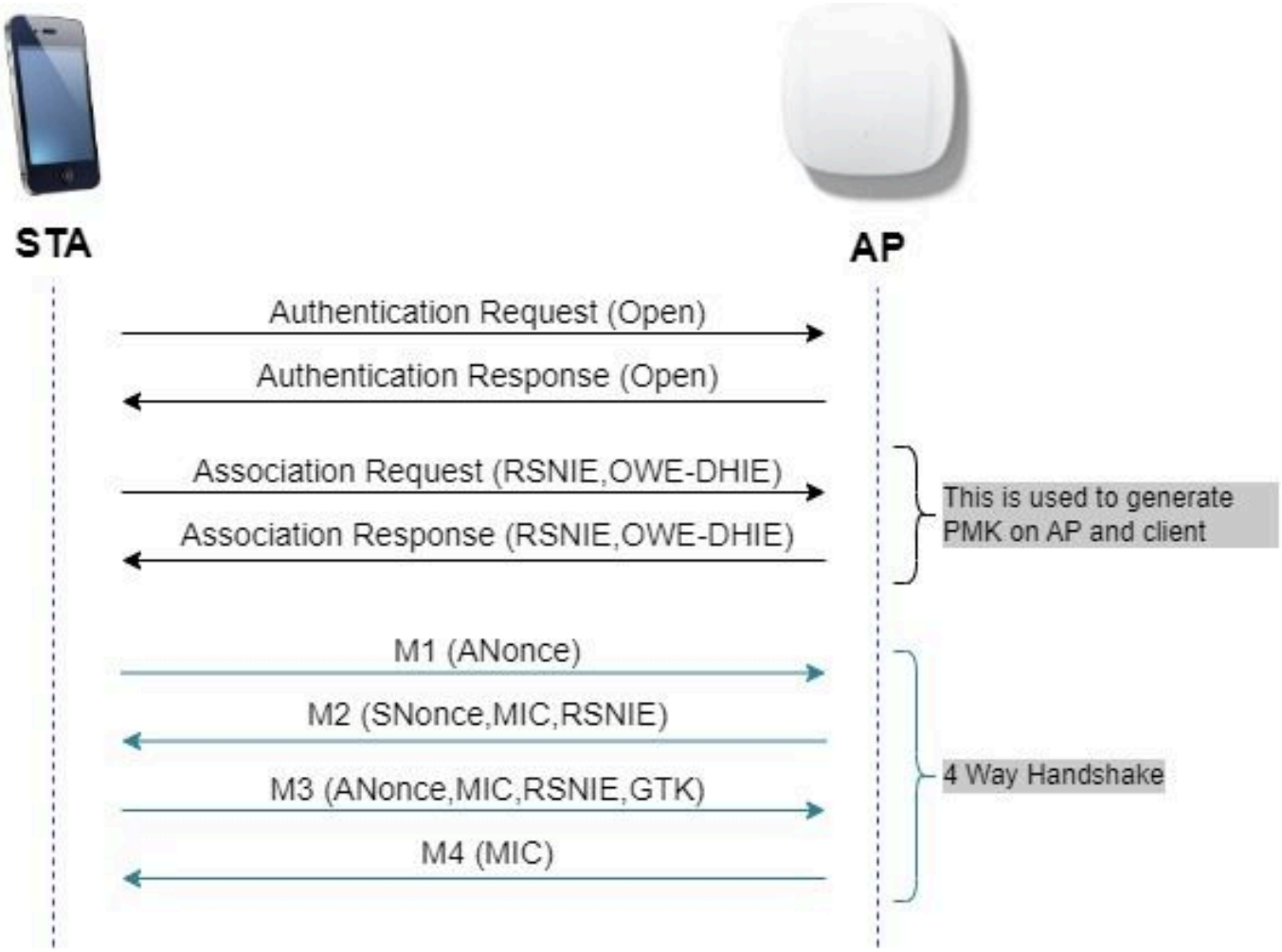
背景説明

Enhanced Openは、WPA3ワイヤレスセキュリティ規格の一部としてWiFi Allianceによって提供される認定です。オープン（未認証）ネットワークでOpportunistic Wireless Encryption(LEAN)を使用して、パッシブなスニフィングを防止し、パブリックPSKワイヤレスネットワークと比較して単純な攻撃を防止します。

Enhanced Openを使用すると、クライアントとWLC（中央認証の場合）またはAP（FlexConnectローカル認証の場合）は、関連付けプロセス中にDiffie-Hellman(DH)鍵交換を実行し、4ウェイハンドシェイクでPairwise Master Key Secret(PMK)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

移行モード

通常、エンタープライズネットワークには暗号化されていないゲストSSIDが1つだけあり、拡張オープンをサポートしない古いクライアントと、拡張オープン共存をサポートする新しいクライアントの両方を使用します。移行モードは、このシナリオに対応するために特別に導入されています。

これには2つのSSIDを設定する必要があります。1つはLEANをサポートする非表示SSIDで、もう1つはOpenでブロードキャストされるSSIDです。

Opportunistic Wireless Encryption(LEAD)移行モードでは、LEADおよび非LEAD STAが同じSSIDに同時に接続できます。すべてのLEAD STAがLEAD移行モードでSSIDを確認すると、LEADと接続します。

オープンWLANとLEAD WLANの両方がビーコンフレームを送信します。LEAD WLANからのビーコンおよびプローブ応答フレームには、オープンWLANのBSSIDおよびSSIDをカプセル化するためのWi-Fi AllianceベンダーIEが含まれており、同様に、オープンWLANにもLEAD WLAN用が含まれています。

Lean STAは、使用可能なネットワークのリスト内のユーザに対してのみ、LEAN Transition Modeで動作するLEAN APのOpen BSSのSSIDを表示し、そのLEAN APのLEAN BSS SSIDの表示

を抑制します。

ガイドラインおよび制限事項：

- 拡張オープンにはWPA3のみのポリシーが必要です。WPA3は、Cisco Wave 1(Cisco IOS®ベース)のAPではサポートされていません。
- Protected Management Frame(PMF)はRequiredに設定する必要があります。これは、WPA3のみのレイヤ2セキュリティでデフォルトで設定されています。
- Enhanced Openは、Enhanced Openをサポートする新しいバージョンを実行しているエンドクライアントでのみ動作します。
- Wi-Fi Enhanced Open Transition Modeは6 GHz帯域では許可されていません。WPA3™仕様 v3.4によると、6GHzおよびWi-Fi 7（EHT – 非常に高いスループット、またはMLO – マルチリンク動作）に関連する次の制約があります。
  - 「APが6 GHz帯域でBSSを運用している場合：[...] APのBSS設定は、Wi-Fi Enhanced Open Transition Mode（つまり、LEAD移行モード要素がビーコンとプローブ応答に含まれている場合）を許可しません。」
  - 「APがEHTまたはMLOが有効なBSSを運用している場合[...]:APのBSS設定は、Wi-Fi拡張オープン移行モード（つまり、ビーコンとプローブ応答にLEAD移行モード要素が含まれている場合）を許可しないものとする。

設定

管理者がEnhanced Openを設定する一方で、古いクライアントがゲストSSIDに接続できるようにする一般的な使用例です。

ネットワーク図

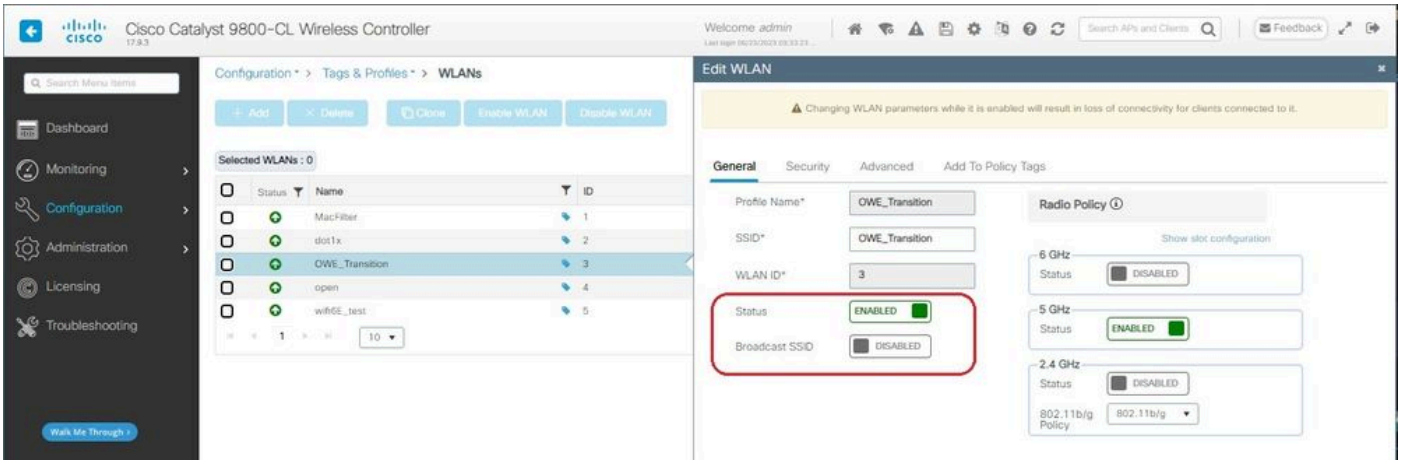
Network Topology

GUIの設定手順：

最初のSSIDを作成します。この名前は「LEAN_Transition」です。この例ではWLAN ID 3で、「Broadcast SSID」オプションを無効にして非表示になっていることを確認してください。

ステップ1 Configuration > Tags & Profiles > WLANsの順に選択して、WLANsページを開きます。

ステップ2 Addをクリックして新しいWLANを追加> add WLAN name "LEAR_Transition" > StatusをEnableに変更> Broadcast SSIDがDisabledになっていることを確認します。



LEAD移行の拡張オープンSSIDを非表示

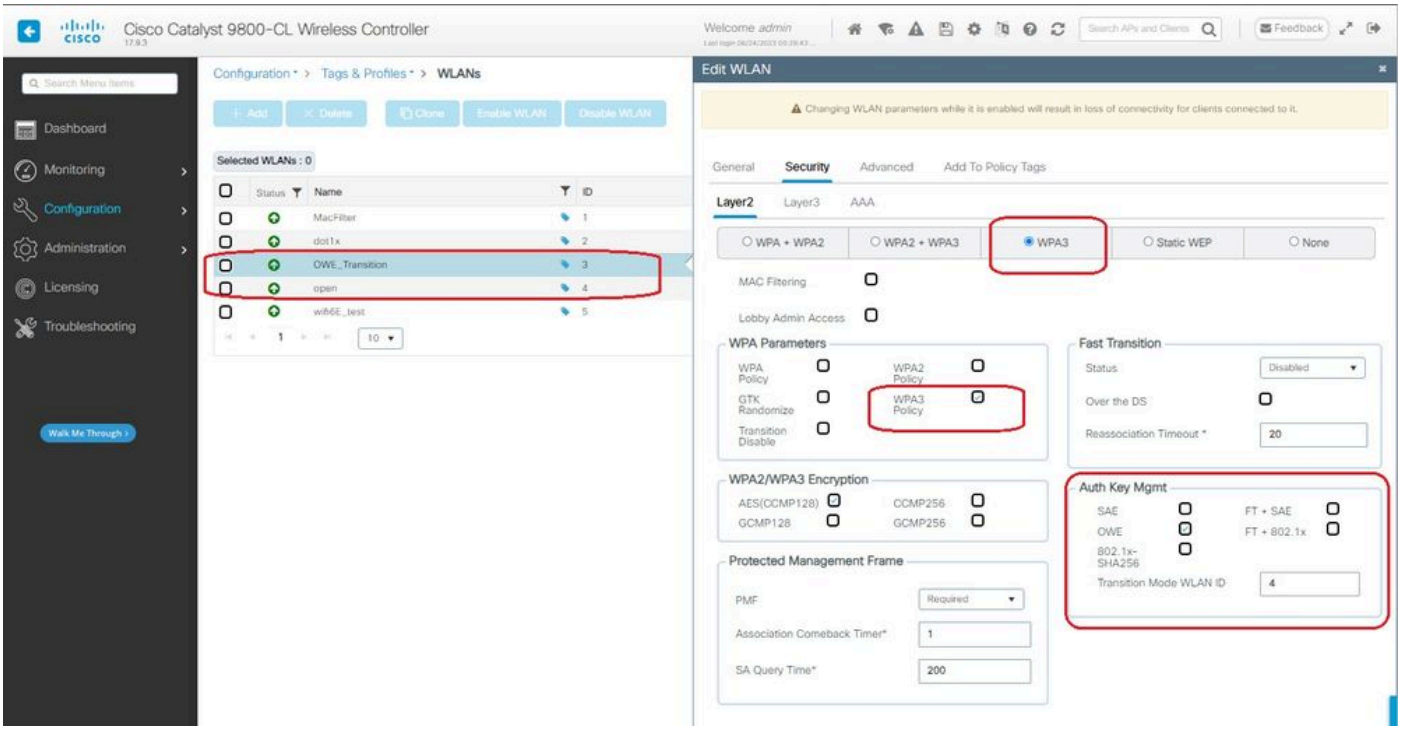
ステップ3 Security > Layer 2タブを選択> WPA3を選択します。

ステップ4:Protected Management Frame(PMF)(PMF)をRequiredに設定します。

ステップ5:WPA Parametersの下で、WPA3ポリシーを確認します。AES(CCMP128) Encryption and LEAD Auth Key Managementの順に選択します。

ステップ6 WLAN ID 4（オープンWLAN）を「Transition Mode WLAN ID」ボックスに追加します。

ステップ7 Apply to Deviceをクリックします。

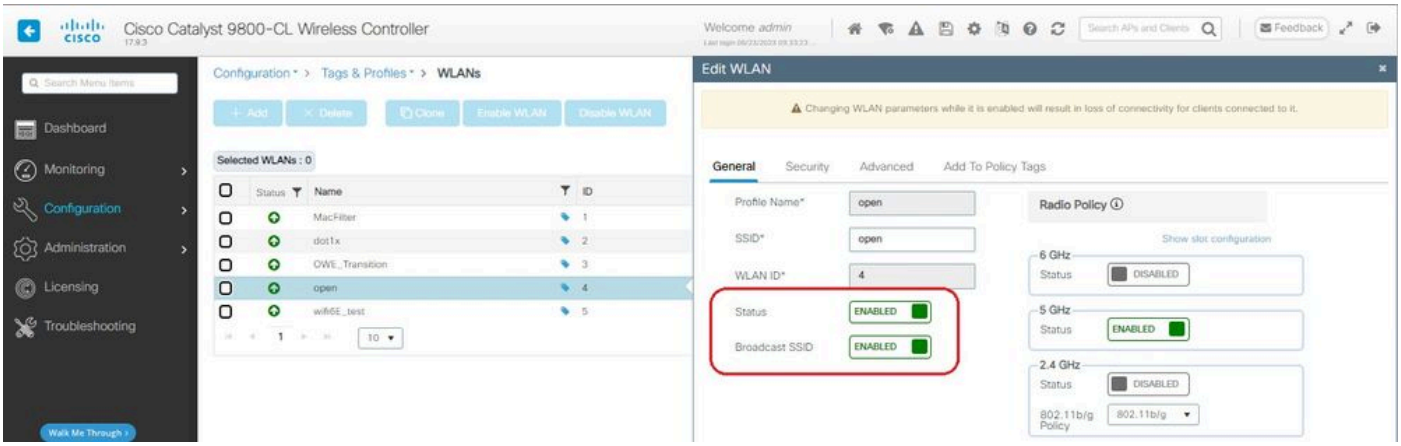


LEAD移行モード：LEAD SSID

2つ目のSSIDを作成し、この例では「open」という名前を付け、WLAN ID 4で「Broadcast SSID」が有効になっていることを確認します。

ステップ1 Configuration > Tags & Profiles > WLANsの順に選択して、WLANsページを開きます。

ステップ2 Addをクリックして新しいWLANを追加> add WLAN name "open" > change Status to Enable > Broadcast SSID is Enabledの順にクリックします。

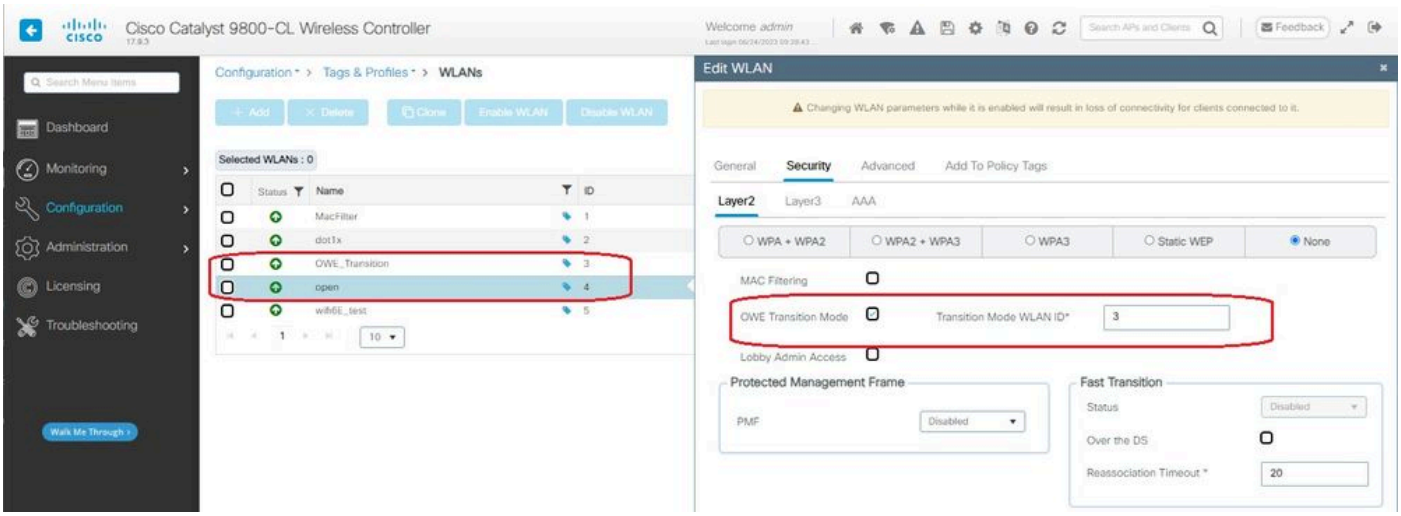


LEAD移行オープンSSID

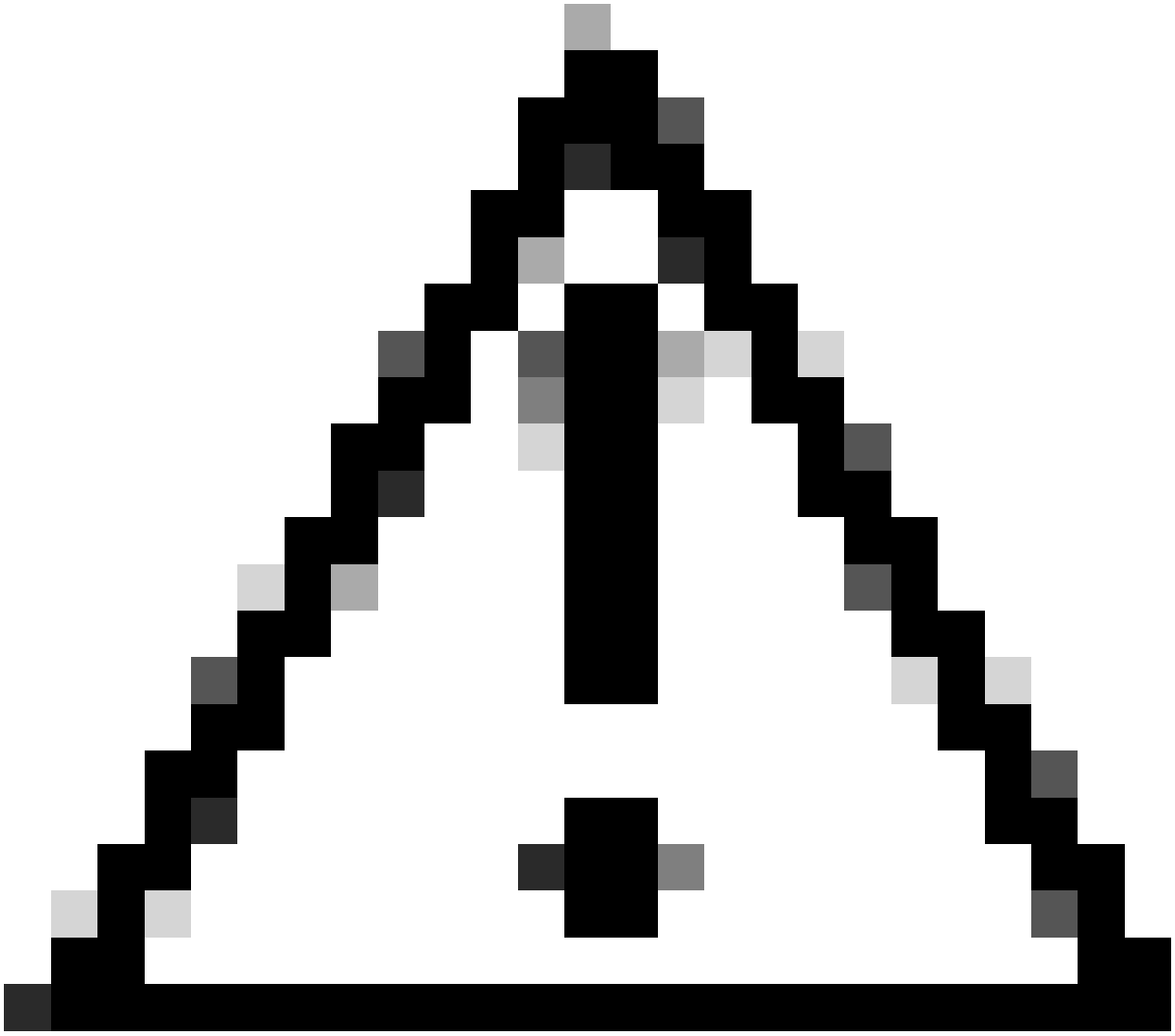
ステップ3:Security > Layer 2タブを選択> Noneを選択します。

ステップ4:「Transition Mode WLAN ID」ボックスにWLAN ID 3(LEAN_Transition)を追加します。

ステップ5 Apply to Deviceをクリックします。

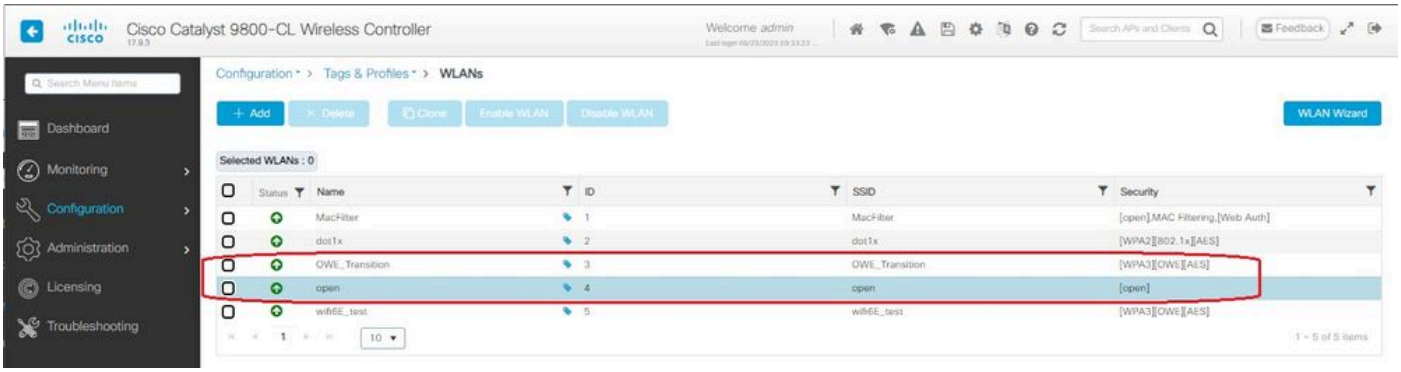


借用移行モードオープン*WLAN*セキュリティ



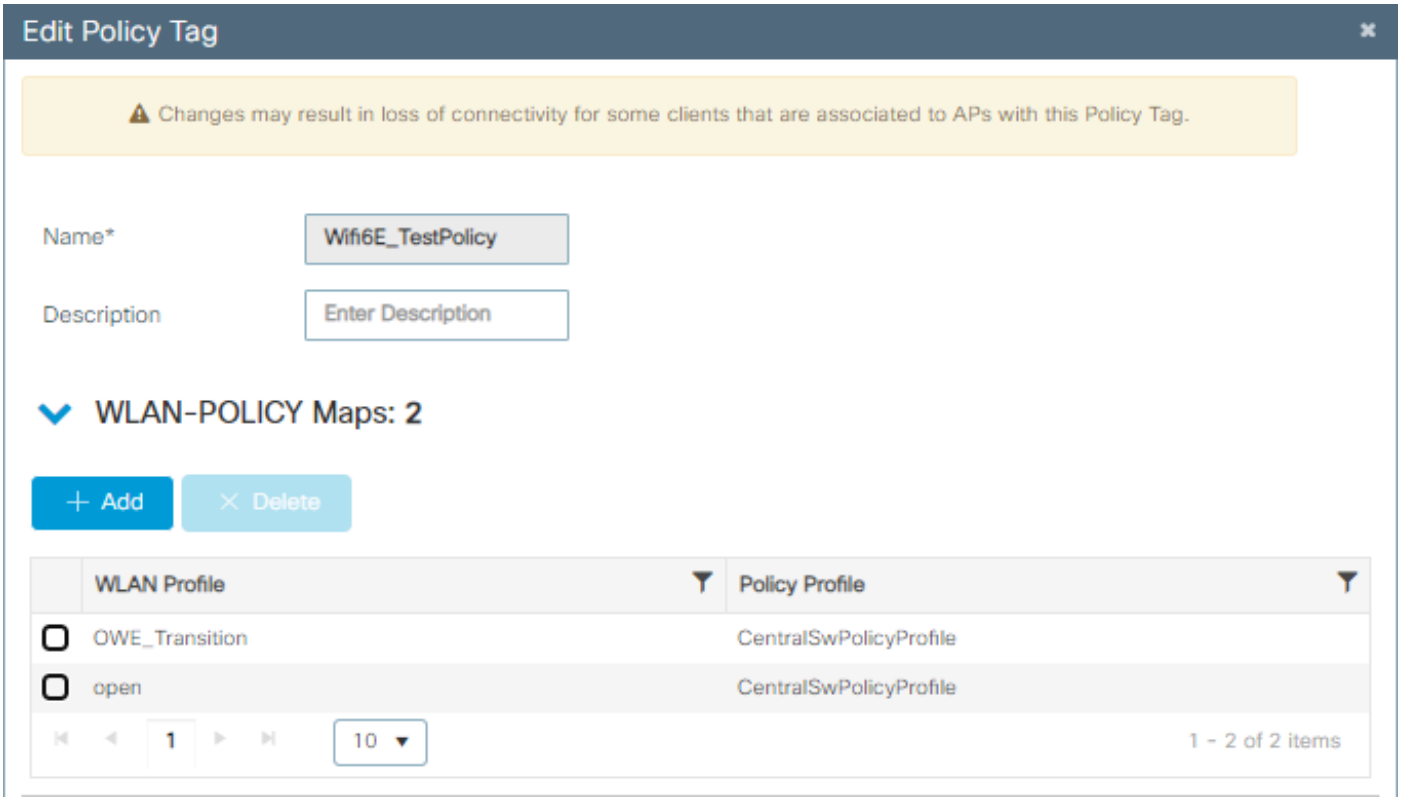
注意：以前にLEAD WLANと同じSSIDを使用してWLANを開いていた場合は、WindowsクライアントによってSSID名の後に「2」が追加されます。これを解決するには、「ネットワーク&インターネット> Wi-Fi > Manage known networks」に移動し、古い接続を削除します。

次のスクリーンショットは、最終結果を示しています。1つのWLANは「LEAN_Transition」という名前のWPA3+LEAD+WPA3用に保護および設定され、もう1つは「open」という名前の完全にオープンなSSIDです。「open」と呼ばれる完全にオープンなSSIDだけがビーコンでSSIDをブロードキャストし、「LEAN_Transition」は非表示です。



借用移行モードのWLAN

手順6 作成したWLANを目的のポリシープロファイルにマッピングし、ポリシータグを作成してAPに適用します。



ポリシー タグ

CLI用の設定：

拡張オープンSSID:

```
Device# conf t
Device(config)# wlan OWE_Transition 3 OWE_Transition
Device(config)# no broadcast-ssid
Device(config)# no security ft adaptive
Device(config)# no security wpa wpa2
Device(config)# no security wpa akm dot1x
Device(config)# security wpa akm owe
Device(config)# security wpa transition-mode-wlan-id 4
Device(config)# security wpa wpa3
```

```
Device(config)# security pmf mandatory
Device(config)# no shutdown
```

オープンSSID:

```
Device# conf t
Device(config)# wlan open 4 open
Device(config)# no security ft adaptive
Device(config)# no security wpa
Device(config)# no security wpa wpa2
Device(config)# no security wpa wpa2 ciphers aes
Device(config)# no security wpa akm dot1x
Device(config)# security wpa transition-mode-wlan-id 3
Device(config)# no shutdown
```

ポリシープロファイル：

```
Device(config)# wireless tag policy Wifi6E_TestPolicy
Device(config-policy-tag)# wlan open policy CentralSwPolicyProfile
Device(config-policy-tag)# wlan OWE_Transition policy CentralSwPolicyProfile
```

確認

これは検証セクションです。

CLIでWLANの設定を確認します。

<#root>

```
Device#show wlan id 3
WLAN Profile Name : OWE_Transition
================================================

Identifier : 3

Description :

Network Name (SSID) : OWE_Transition

Status : Enabled

Broadcast SSID : Disabled

[...]
Security
```

802.11 Authentication : Open System

Static WEP Keys : Disabled

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Enabled

WPA (SSN IE) : Disabled
WPA2 (RSN IE) : Disabled

WPA3 (WPA3 IE) : Enabled

AES Cipher : Enabled

CCMP256 Cipher : Disabled
GCMP128 Cipher : Disabled
GCMP256 Cipher : Disabled
Auth Key Management
802.1x : Disabled
PSK : Disabled
CCKM : Disabled
FT dot1x : Disabled
FT PSK : Disabled
FT SAE : Disabled
Dot1x-SHA256 : Disabled
PSK-SHA256 : Disabled
SAE : Disabled

OWE : Enabled

SUITEB-1X : Disabled
SUITEB192-1X : Disabled
SAE PWE Method : Hash to Element, Hunting and Pecking(H2E-HNP)

Transition Disable : Disabled

CCKM TSF Tolerance (msecs) : 1000

OWE Transition Mode : Enabled

OWE Transition Mode WLAN ID : 4

OSEN : Disabled
FT Support : Disabled
FT Reassociation Timeout (secs) : 20
FT Over-The-DS mode : Disabled

PMF Support : Required

PMF Association Comeback Timeout (secs): 1
PMF SA Query Time (msecs) : 200
[...]
#show wlan id 4
WLAN Profile Name : open
==========

Identifier : 4

Description :

Network Name (SSID) : open

Status : Enabled

Broadcast SSID : Enabled

[...]
Security
802.11 Authentication : Open System
Static WEP Keys : Disabled

Wi-Fi Protected Access (WPA/WPA2/WPA3) : Disabled

OWE Transition Mode : Enabled

OWE Transition Mode WLAN ID : 3

OSEN : Disabled
FT Support : Disabled
FT Reassociation Timeout (secs) : 20
FT Over-The-DS mode : Disabled

PMF Support : Disabled

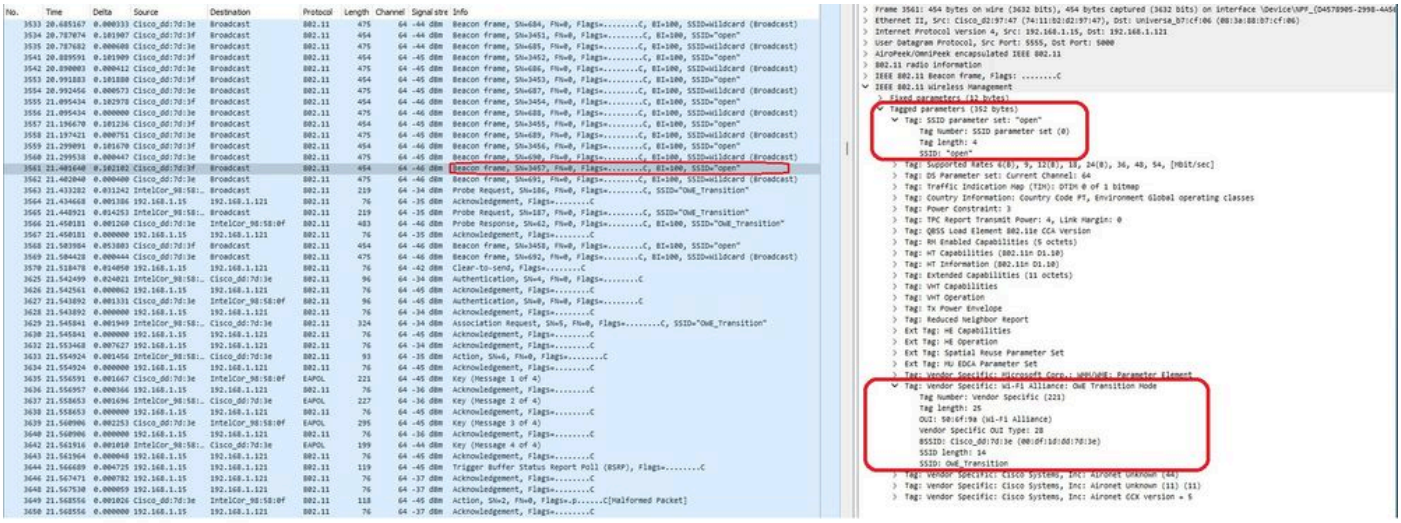
PMF Association Comeback Timeout (secs): 1
PMF SA Query Time (msecs) : 200
[...]

WLCでAP Configurationに移動し、両方のWLANがAP上でアクティブであることを確認できます。

LEAD移行モードAP動作設定ビューア

有効にすると、APはオープンSSIDを使用したビーコンのみを送信しますが、LEAD移行モード情報要素(IE)を伝送します。 拡張オープン機能を備えたクライアントがこのSSIDに接続すると、関連付け後にすべてのトラフィックを自動的に暗号化するLEADが使用されます。

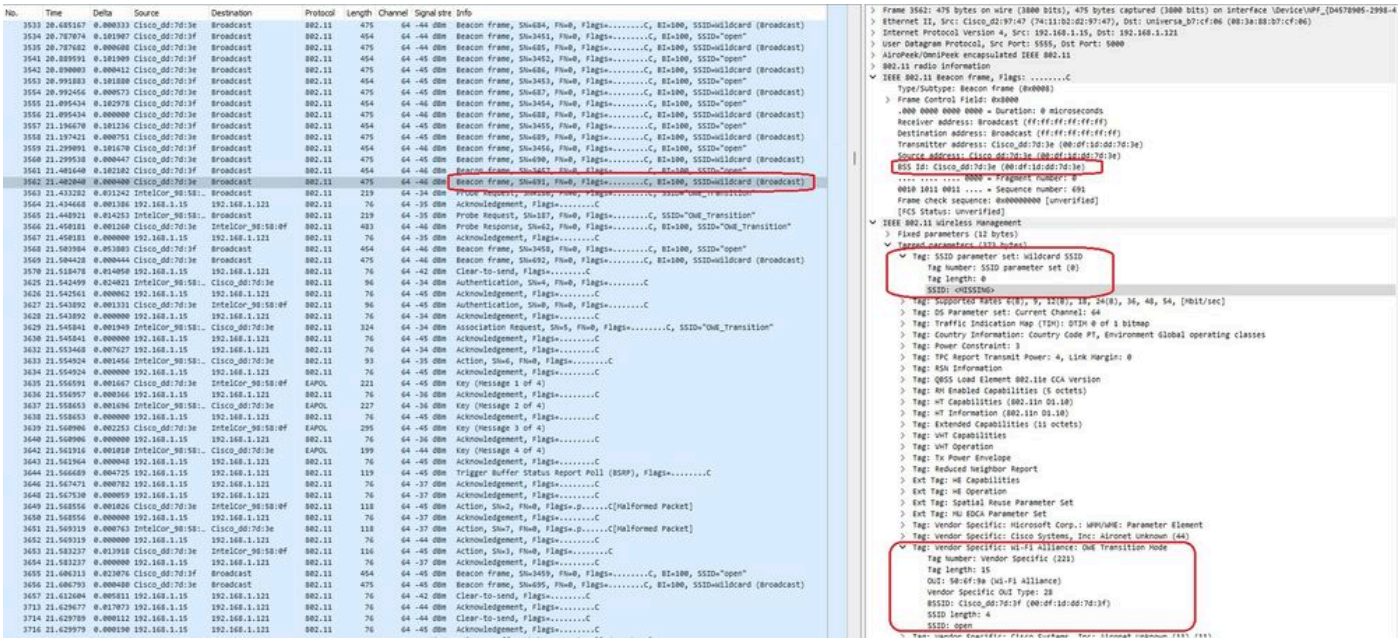
OTA(Over The Air)で確認できる内容は次のとおりです。



LEAD移行オープンSSIDビーコン

SSID「open」で送信されるビーコンには、BSSIDおよびSSID名「LEAN_Transition」などの拡張オープンSSIDの詳細を含むLEAD移行モードIEが含まれます。

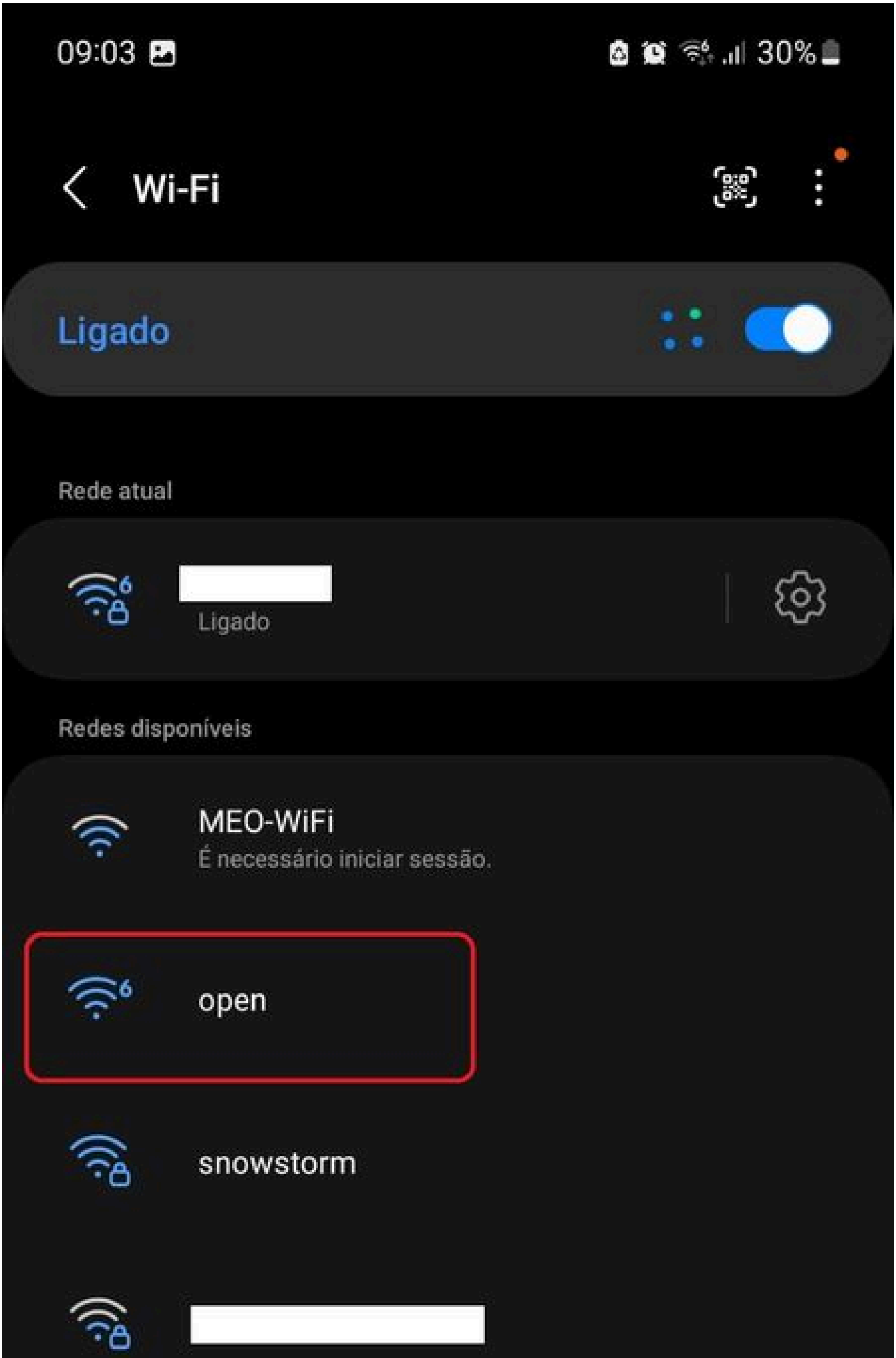
SSIDが非表示のビーコンOTAもあり、bssidでフィルタリングすると、フレームはBSSID 00:df:1d:dd:7d:3eに送信されます。このBSSIDはLEAD移行モードIE内のBSSIDです。



LEANビーコン

また、LEAD隠しビーコンには、オープンSSID BSSIDおよびSSID名「open」のLEAD移行モードIEが含まれていることも確認できます。

次のスクリーンショットは、拡張オープンをサポートするAndroidフォンを示しています。この画面には、ロックアイコンのないオープンSSIDのみが表示されます (ロックアイコンは、接続にパスワードが必要であるとユーザに思わせる可能性があります) 。ただし、接続されると、セキュリティには拡張オープンセキュリティが使用されていることが示されます。


09:03
30%
Wi-Fi
Ligado
Rede atual
Ligado
Redes disponíveis
MEO-WiFi
É necessário iniciar sessão.
open
snowstorm

```
Client MAC Address : 286b.3598.580f
[...]
AP Name: AP9136_5C.F524
AP slot : 1
Client State : Associated
Policy Profile : CentralSwPolicyProfile
Flex Profile : N/A
Wireless LAN Id: 3
```

WLAN Profile Name: OWE_Transition

Wireless LAN Network Name (SSID): OWE_Transition

```
BSSID : 00df.1ddd.7d3e
Connected For : 682 seconds
Protocol : 802.11ax - 5 GHz
Channel : 64
Client IIF-ID : 0xa0000003
Association Id : 2
```

Authentication Algorithm : Open System

```
Idle state timeout : N/A
[...]
```

Policy Type : WPA3

Encryption Cipher : CCMP (AES)

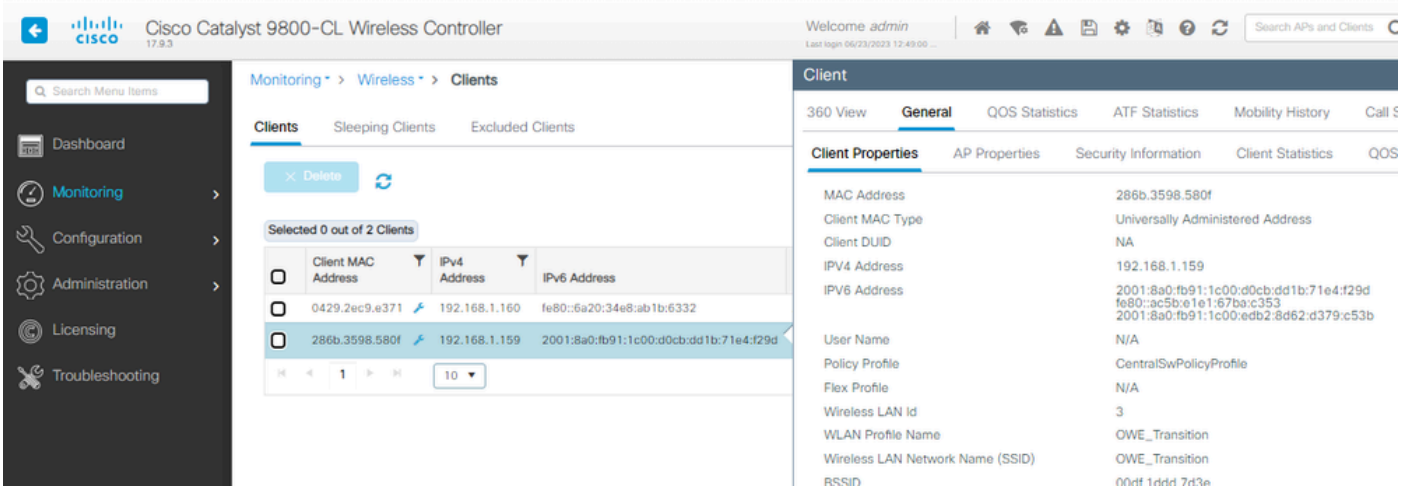
Authentication Key Management : OWE

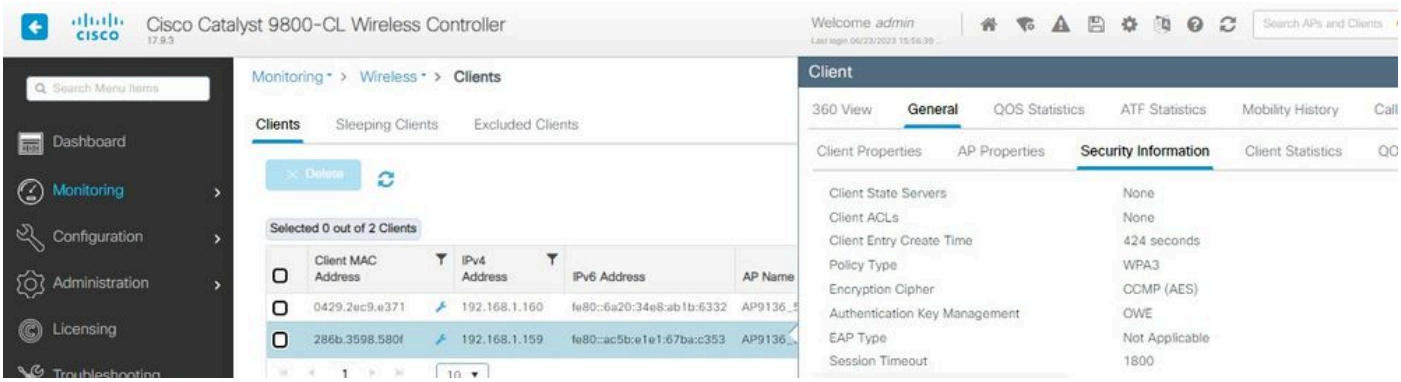
```
Transition Disable Bitmap : None
User Defined (Private) Network : Disabled
User Defined (Private) Network Drop Unicast : Disabled
Encrypted Traffic Analytics : No
```

Protected Management Frame - 802.11w : Yes

```
EAP Type : Not Applicable
```

WLC GUIでも同じことを確認できます。





Enhanced Openをサポートしていないクライアントは、暗号化なしで、オープンSSIDのみを表示して接続します。

ここに示すように、これらはEnhanced Open（それぞれIOS 15のiPhoneとMac OS 12のMacBook）をサポートせず、オープンなゲストSSIDのみを表示し、暗号化を使用しないクライアントです。


Proximus
17:04
Settings
Wi-Fi
Wi-Fi
open
Unsecured Network
MY NETWORKS
[redacted]
OTHER NETWORKS
apr0v0
[redacted]
Other...
Ask to Join Networks
Notify

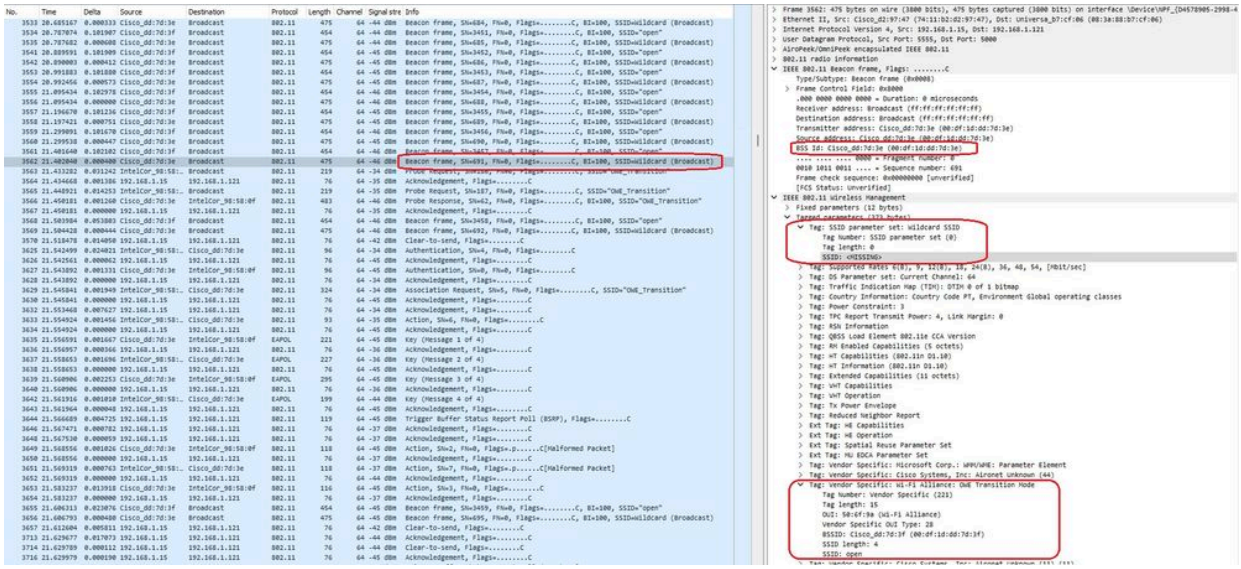
```
Client MAC Address : b44b.d623.a199
[...]
AP Name: AP9136_5C.F524
AP slot : 1
Client State : Associated
Policy Profile : CentralSwPolicyProfile
Flex Profile : N/A
Wireless LAN Id: 4


WLAN Profile Name: open


Wireless LAN Network Name (SSID): open


BSSID : 00df.1ddd.7d3f
[...]
Authentication Algorithm : Open System


[...]
Protected Management Frame - 802.11w : No


EAP Type : Not Applicable
```

トラブルシュート

1. すべてのクライアントがLEADをサポートしているわけではないので、クライアントがLEADをサポートしていることを確認します。クライアントベンダーのドキュメントを確認します。たとえば、Appleはデバイスのサポートについてここでドキュメント化しています。
2. 一部の古いクライアントは、LEAD移行モードIEが存在するためにオープンSSIDビーコンを受け入れず、範囲内のネットワークにSSIDを表示しない可能性があります。クライアントがOpen SSIDを認識できない場合は、WLAN設定からTransition VLAN（0に設定）を削除し、WLANが認識されるかどうかを確認します。
3. クライアントがオープンSSIDを確認し、LEADをサポートしているが、WPA3を使用せずに接続している場合は、遷移VLAN IDが正しく、両方のWLANのビーコンでブロードキャストされていることを確認します。APをスニファモードで使用して、OTAトラフィックをキャプチャできます。APをスニファモードで設定するには、次の手順を実行します。APs Catalyst 91xx in Sniffer Mode。
    - ビーコンはSSID「open」で送信され、BSSIDおよびSSID名「LEAN_Transition」などの拡張オープンSSIDの詳細を含むLEAD移行モードIEが含まれます。 

LEAD移行オープンSSIDビーコン

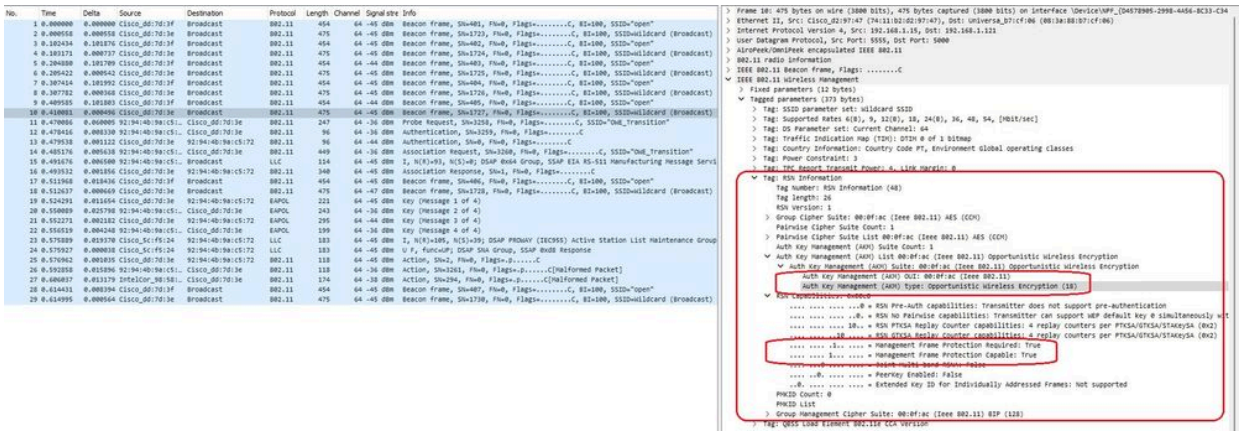
- SSIDが非表示のビーコンOTAもあり、bssidでフィルタリングすると、フレームはBSSID 00:df:1d:dd:7d:3eに送信されます。このBSSIDはLEAD移行モードIE内のBSSIDです。



LEANビーコン

また、LEAD隠しビーコンには、オープンSSID BSSIDおよびSSID名「open」のLEAD移行モードIEが含まれていることも確認できます。

- また、AKMの情報を表示して、MFPが必要かつ使用可能としてアドバタイズされていることを確認できます。



-

リーンビーコンAKM

4. クライアントのMACアドレスに基づいてRadioActiveトレースを収集すると、次のような口グが表示されます。

2023/06/23 15:08:58.567933 {wncd_x_R0-0}{1}: [client-keymgmt] [14854]: (note): MAC: xxxx.xxxx.xxxx EAP Key management successful. AKM:OWE Cipher:CCMP WPA Version: WPA3

2023/06/23 15:10:06.971651 {wncd_x_R0-0}{1}: [client-orch-state] [14854]: (note): MAC: xxxx.xxxx.xxxx Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN

参考資料

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

Wi-Fi Alliance® WPA3™仕様v3.4

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。