Opportunistic Wireless Encryptionのフローについて

内容

はじめに

このドキュメントでは、LEAD移行のフローと、Catalyst 9800ワイヤレスLANコントローラ(WLC)での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。

- 9800 WLCの基本動作用のアクセスポイント(AP)の設定方法
- WLANおよびポリシープロファイルの設定方法

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。

- C9800-80、Cisco IOS® XE 17.12.4、Cisco IOS® XE 17.9.6でもテスト済み
- APモデル：C9136I。ローカル接続モードとフレックス接続モードの両方でチェックされます。

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。

説明

- LEAN(Opportunistic Wireless Encryption)はIEEE 802.11の拡張で、ワイヤレスメディアに暗号化を提供します。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アルゴリズムベースの暗号化を使用して、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、その結果得られたペアワイズシークレットを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。

手順

1. 暗号化/セキュリティなしで1つのオープンWLANを設定し、ブロードキャストを有効にします。
2. LEADセキュリティを設定した別のSSIDを設定し、transition-mode-wlan-idでOPEN WLAN ID番号をマッピングします。このLEAD移行SSIDでブロードキャストSSIDオプションを無効にします。
3. OPEN WLANの「transition-mode-wlan-id」フィールドにLEAN移行WLAN ID番号をマッピングします。

ラボ再現の詳細

- Open SSID Name (オープンSSID名) :OPEN-LEAN
- LEAD遷移SSID名： LEAD-Transition
- BSSID of OPEN-LEAN:40:ce:24:dd:2e:87
- BSSID of LEAD-Transition:40:ce:24:dd:2e:8f

貸しフロー

1. ビーコンはOPEN SSIDでブロードキャストできます。 AIR PCAPでは、SSID名で確認できます。
2. また、AIR PCAPで、隠しセキュリティが有効なSSIDに、独自のSSID名ではなく「Wildcard」という名前が付いていることも確認できます。
3. クライアントがOPEN SSIDのビーコンフレームを受信すると、LEANを持つ、またはサポートしている場合、LEAN遷移SSID (OPEN SSIDの代わりにセキュリティが有効になっているSSID) にプローブ要求の送信を開始できます。
4. LEANをサポートするクライアントは、遷移SSIDからプローブ応答を取得できます。
5. オープン認証は、クライアントとAPの間で実行できます。
6. クライアントはDHキー交換の詳細を含むアソシエーション要求をAPに送信し、生成されたペアワイズシークレットを4ウェイハンドシェイクに使用できます。
7. APはアソシエーション応答を送信できます。
8. APとクライアントデバイスの間で4ウェイハンドシェイクが発生する可能性があります。
9. キー管理に成功すると、L2 PSKに成功する可能性があります。
10. クライアントはDHCP、ARPなどからIPを取得できる
11. クライアントはRUN状態になることができます。
12. LEANをサポートしていないクライアントデバイスは、OPEN SSID自体にプローブ要求を送信でき、RUN状態に移行するよりも直接IPを取得できます。

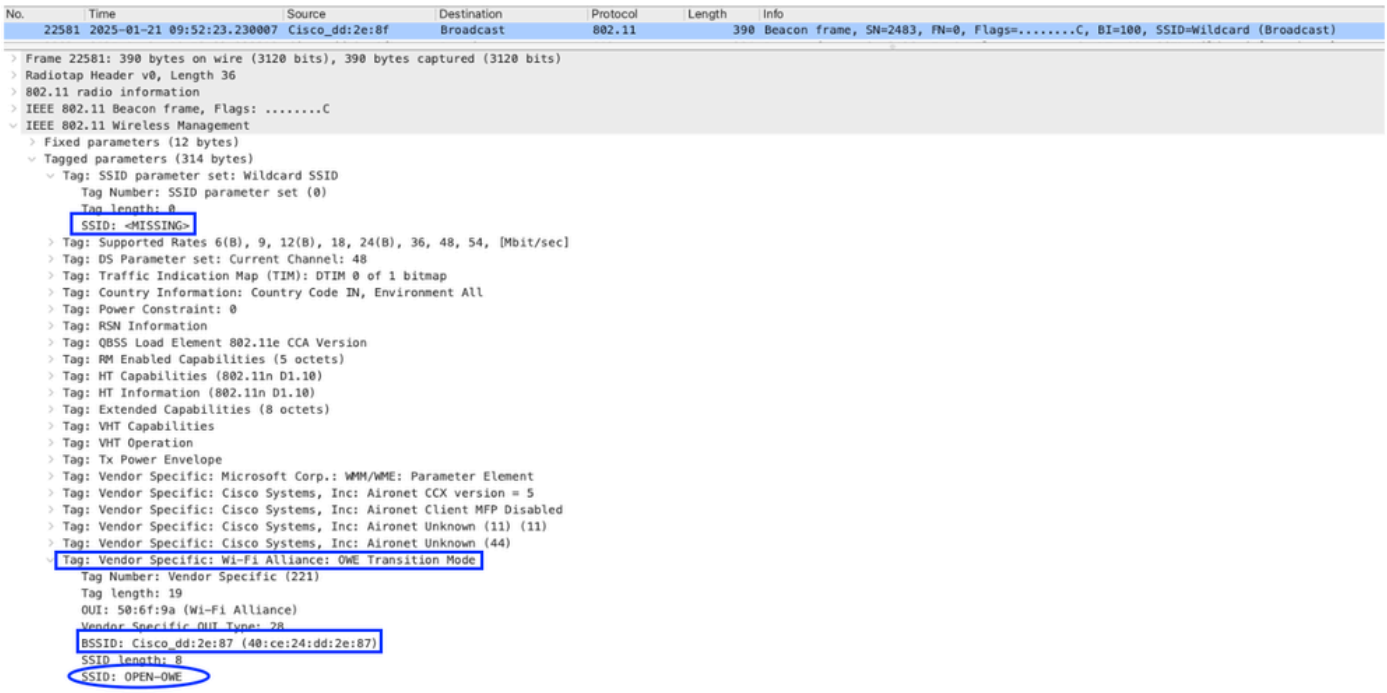
オリジナルビーコンフレーム

- ここで、AIR PCAPは、SSIDが「OPEN-LEAN」ブロードキャスト (ビーコンフレーム) であることを示しています。 移行SSIDの詳細を含み、「LEAR-Transition」と呼ばれます。

図1:OPEN SSIDのビーコンフレーム

隠しSSIDビーコン

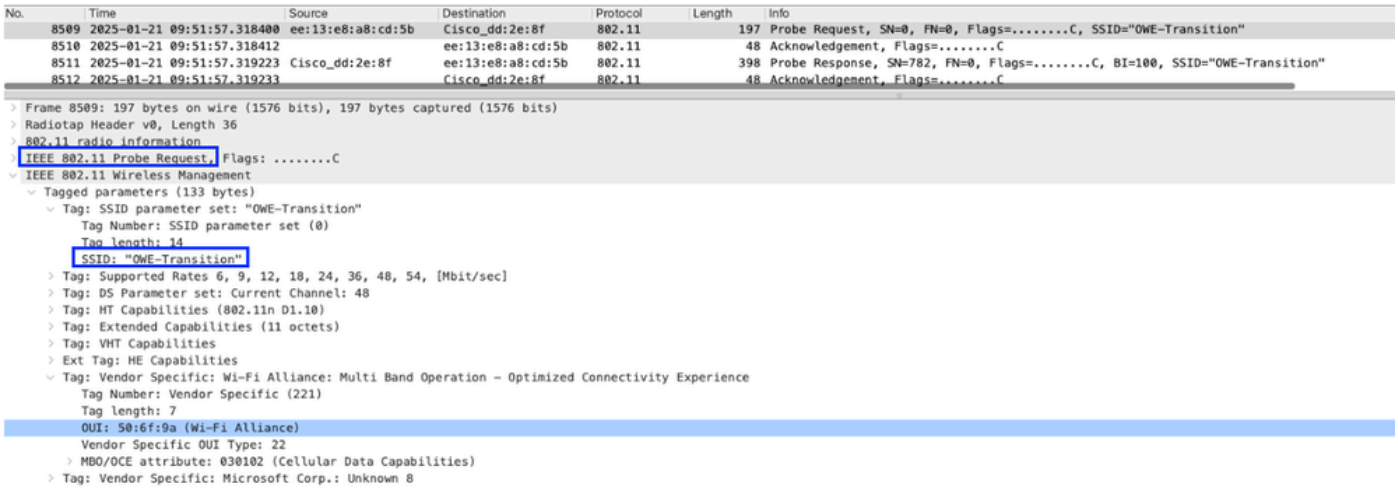
- WLANの設定により、「ブロードキャスト」はこの「LEAR-Transition」SSIDに対して無効になっていますが、AIR PCAPにはSSID名「Wildcard」を含む非表示のSSIDビーコンが表示される場合があります。 ただし、そのパケットを確認すると、LEAD-Transitionの詳細が含まれます。
- 「40:ce:24:dd:2e:8f」のように、このパケットを使用して隠しSSIDのBSSIDを取得し、パケットキャプチャで検索します。
- このパケットでは、SSID「Missing」が示され、このSSIDには「OPEN-LEAN」としての遷移SSIDと、そのBSSID「40:ce:24:dd:2e:87」が含まれています。



図–2：非表示のSSID – 使用期限の移行

クライアントからLEAD遷移SSIDにプローブ要求が送信されます。

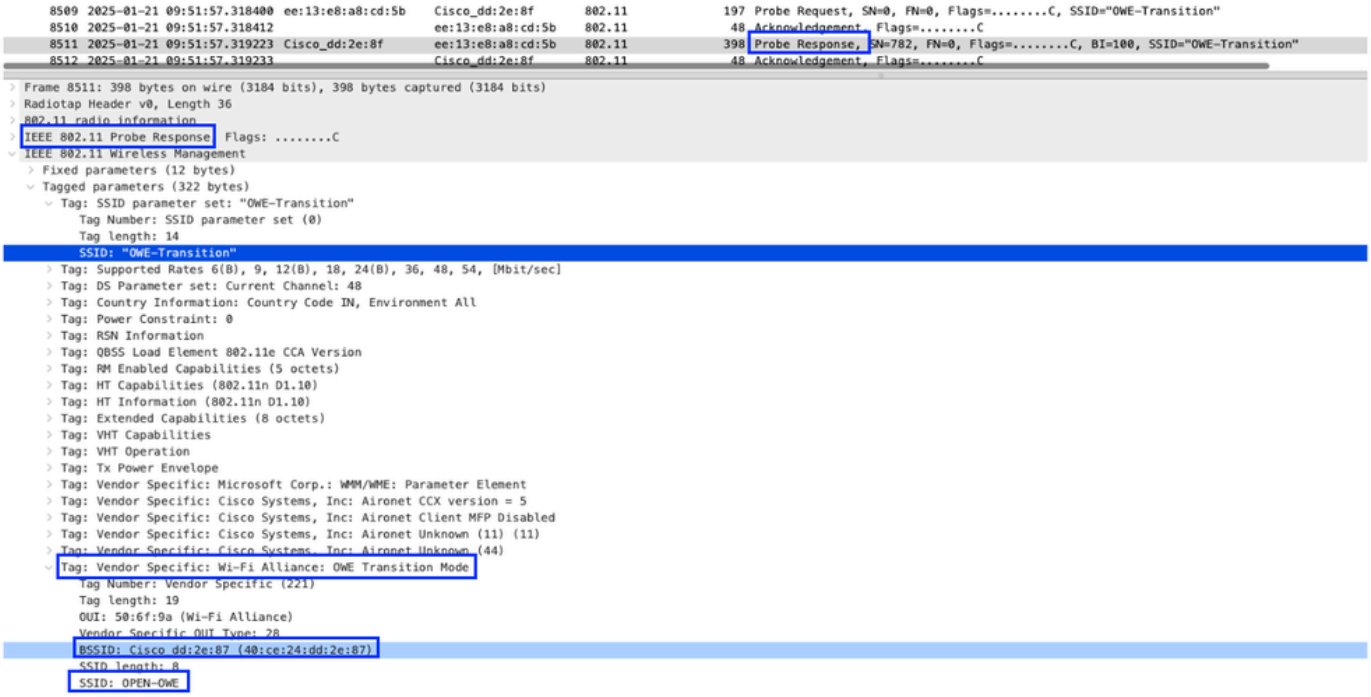
- ビーコンフレーム「OPEN-LEAN」SSIDに基づいて、クライアントは接続する必要がある他のSSIDの詳細を認識します。このシナリオでは、「LEAN-Transition」です。クライアントがLEAD暗号化をサポートできる場合、プローブ要求を「LEAD-Transition」SSIDに送信して応答を取得できます。
- プローブ要求がLEAN-Transition BSSID「40:ce:24:dd:2e:8f」に送信され、応答を受け取りました。このプローブ応答パケット内でも、OPEN-LEAD SSIDの詳細を確認できます。



図–3：プローブ要求

APからクライアントに送信されるプローブ応答

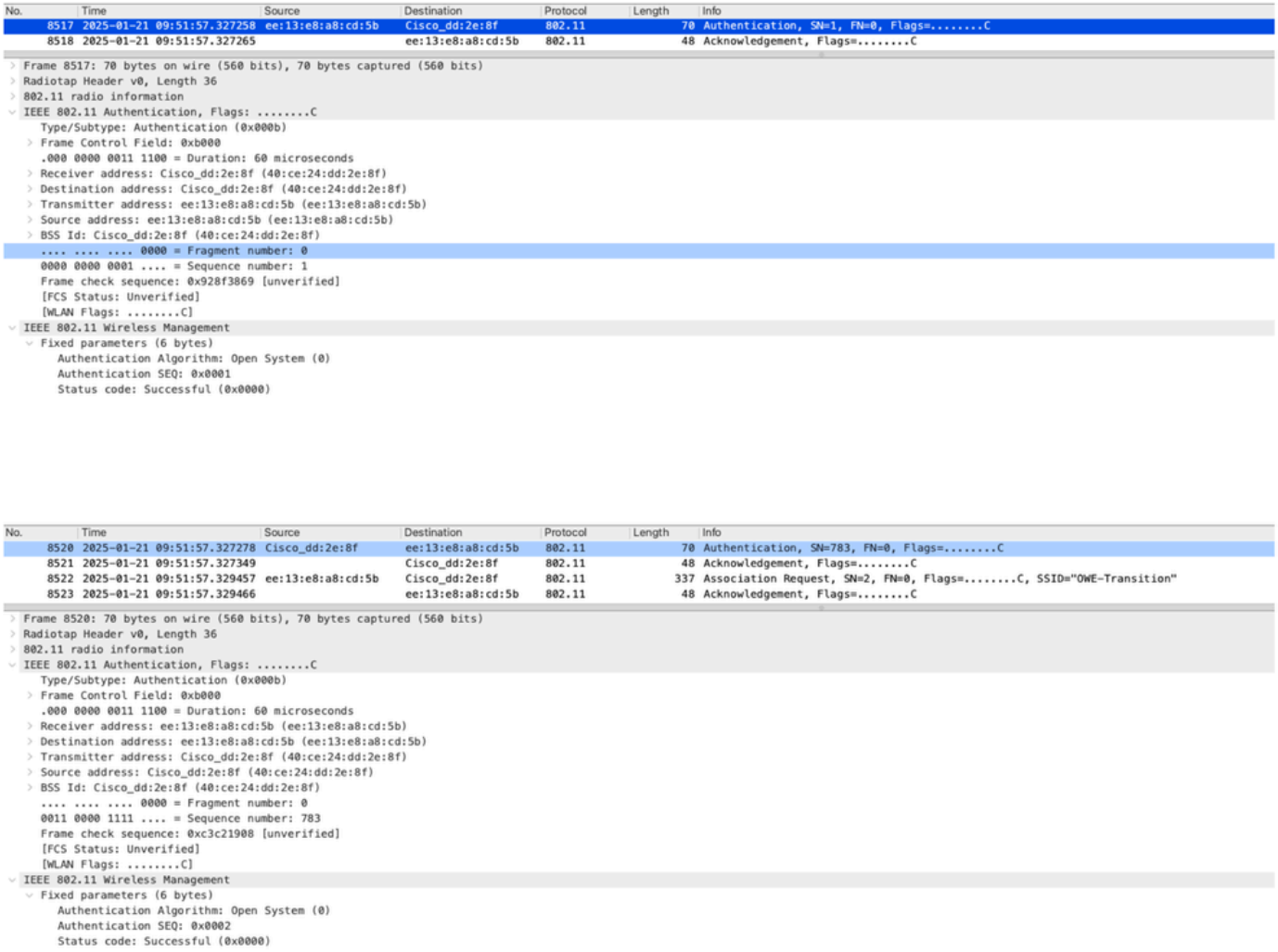
- クライアントはSSID「LEAN-Transition」のプローブ応答を受信しましたが、WiFi Allianceには元のSSIDの詳細「OPEN-LEAN」があります。



図–4：プローブ応答

オープン認証

- プローブ応答を取得した後、クライアントとAPの間でオープン認証を実行し、関連付けの前にクライアントのWiFiの詳細と機能を確認できます。



図–5：プローブ成功後のオープン認証

クライアントからAPへのアソシエーション要求

- このパケットでは、クライアントが暗号化のためにDiffie-Hellmanパラメータ値を付加できることに注意してください。

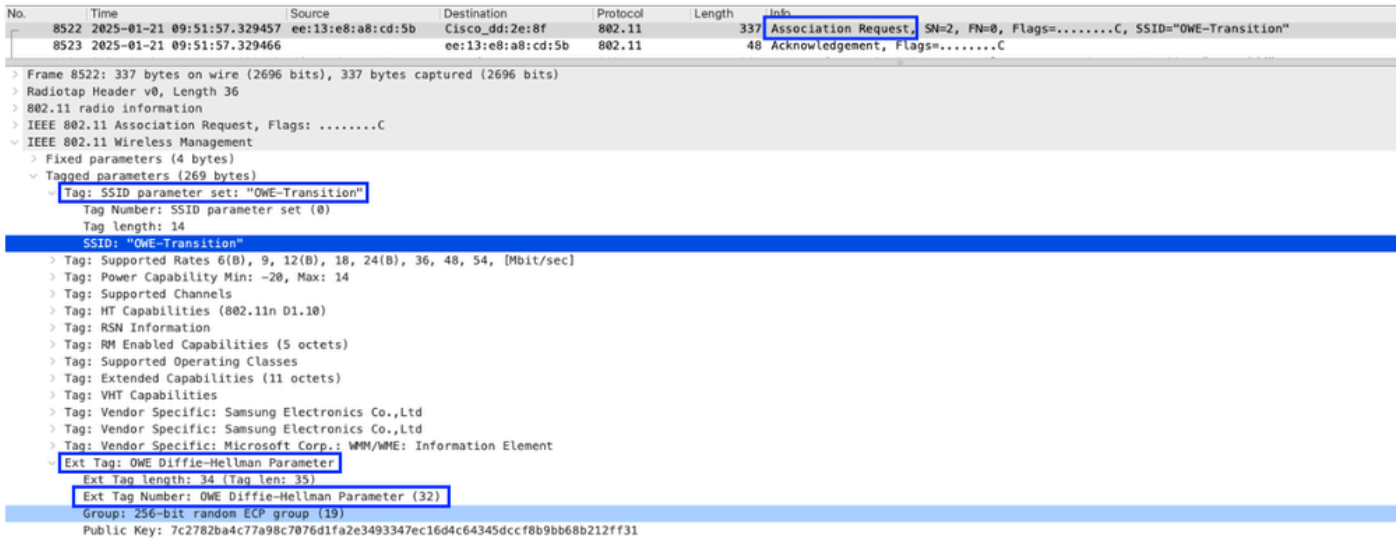


図6：関連付け要求

- RAトレースでは、アソシエーションフェーズからクライアントログの確認を開始できます。

```
2025/01/21 15:21:57.391071821 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (note): MAC: ee13.e8a8.cd5b  A
2025/01/21 15:21:57.391117645 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

APからクライアントに送信されるアソシエーション応答

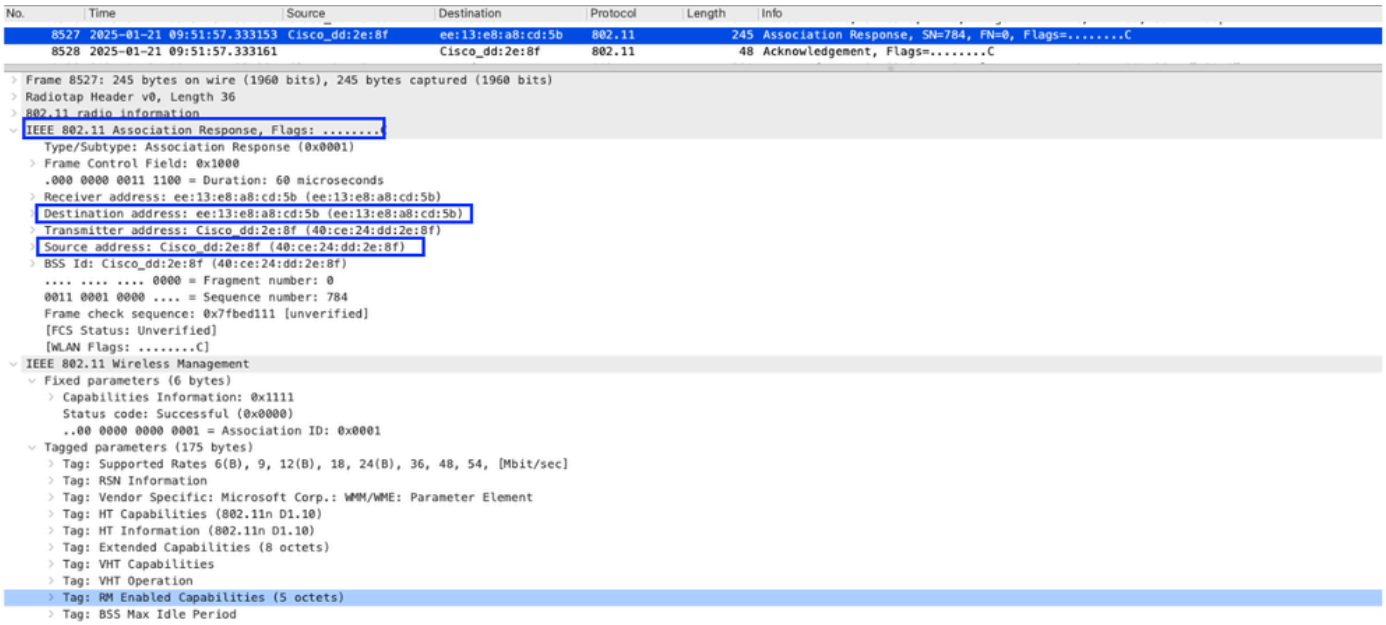


図7：アソシエーション応答

```
2025/01/21 15:21:57.391334260 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.392296819 {wncd_x_R0-0}{1}: [dot11] [21675]: (note): MAC: ee13.e8a8.cd5b  Associati
```

キー交換

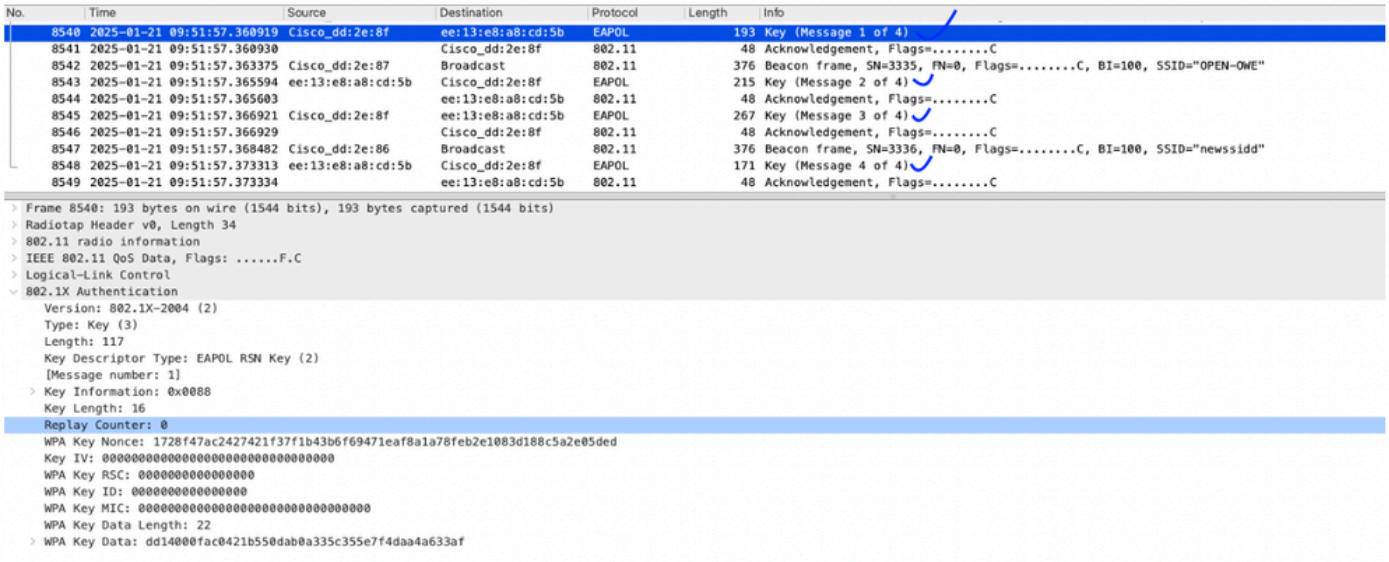
APとクライアントデバイスの間で4ウェイハンドシェイクが発生する可能性があります。

APによるキー1送信

クライアントによるキー2送信

APによるキー3の送信

クライアントによるキー4送信



イメージ8:4ウェイハンドシェイク

```
2025/01/21 15:21:57.392538716 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.392557538 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.392640494 {wncd_x_R0-0}{1}: [client-auth] [21675]: (note): MAC: ee13.e8a8.cd5b  L2
2025/01/21 15:21:57.394830551 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli
2025/01/21 15:21:57.395171903 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli
2025/01/21 15:21:57.420590731 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli

2025/01/21 15:21:57.420706435 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.420775720 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.426548998 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.426725965 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.426727805 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.434078994 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.434099154 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (note): MAC: ee13.e8a8.cd5b
```

L2認証の成功

```
2025/01/21 15:21:57.434111288 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.434250308 {wncd_x_R0-0}{1}: [client-auth] [21675]: (note): MAC: ee13.e8a8.cd5b  L2
2025/01/21 15:21:57.434286035 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli
2025/01/21 15:21:57.434308953 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

IPラーニングステート

```
2025/01/21 15:21:57.434789679 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.436611026 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.437239513 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.437508189 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.534166453 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interfac
2025/01/21 15:21:57.535325325 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.535874658 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interfac
2025/01/21 15:21:57.536500021 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

RUN状態のクライアント

```
2025/01/21 15:21:57.537017277 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
```

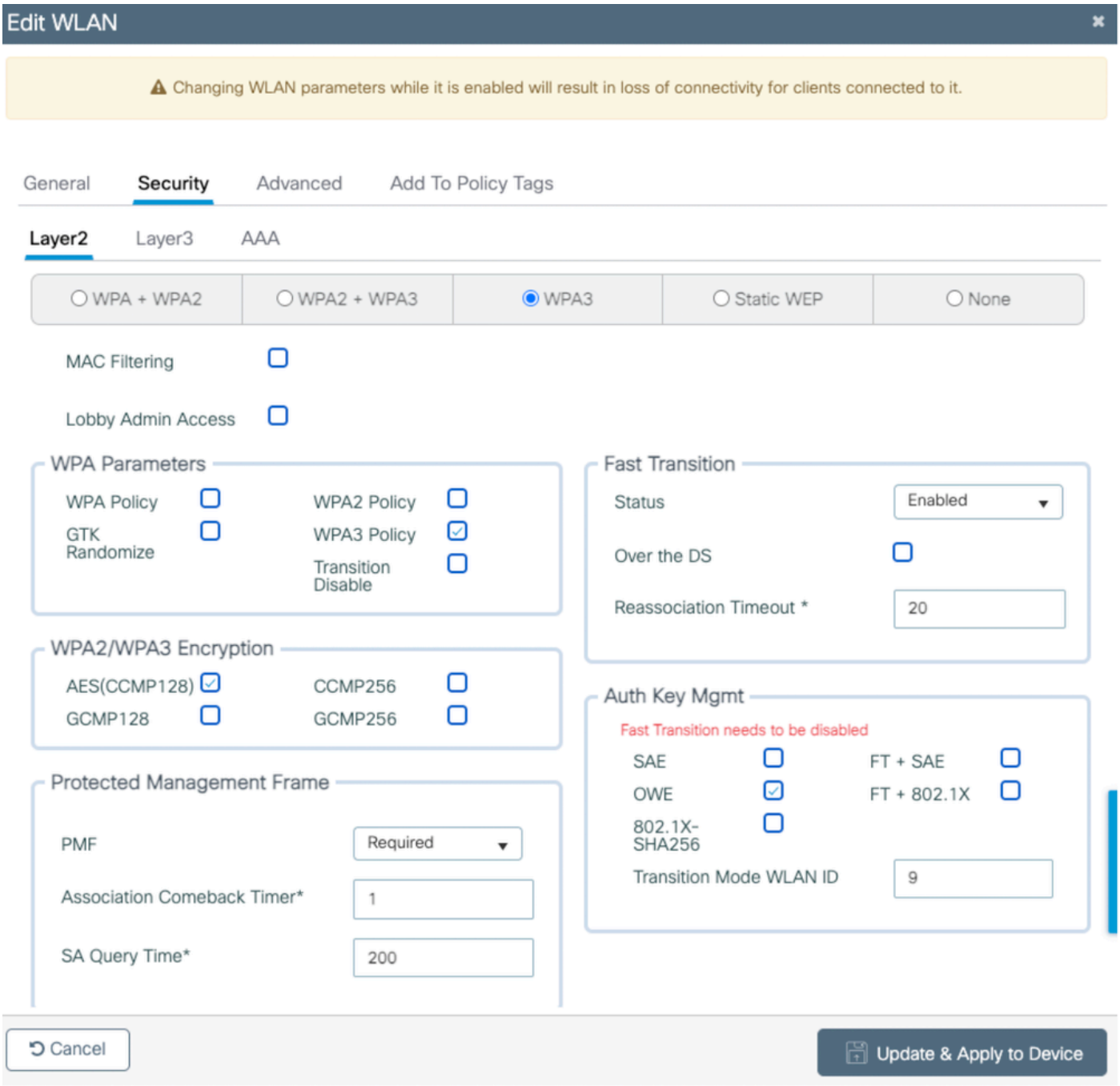
LEAD暗号化がサポートされていないクライアント

- ビーコンフレーム自体を確認することで、クライアントはこの暗号化方式をサポートできるかどうかを知ることができます。サポートされていない場合は、オープンSSID「OPEN-LEAN」にプローブ要求を送信するだけで、通常のオープン認証を実行し、IPアドレスを取得し、RUN状態に移行できます。

```
2025/01/16 15:36:06.178370757 {wncd_x_R0-2}{1}: [client-orch-sm] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:06.209288788 {wncd_x_R0-2}{1}: [dot11] [17332]: (note): MAC: d037.4587.8f35  Associati
2025/01/16 15:36:06.248651191 {wncd_x_R0-2}{1}: [client-auth] [17332]: (note): MAC: d037.4587.8f35  Ope
2025/01/16 15:36:06.248751507 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.281808554 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.303307756 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:10.305041414 {wncd_x_R0-2}{1}: [client-iplearn] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:10.305777492 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
```

高速移行情報

- LEANは、オープン認証(OAM)またはWebauth(CWA/LWA/EWA)でのみ設定できます。
- FTは借入移行ではサポートされていません。
- FTを有効にすると、



図–9:LEAD遷移SSIDでFTを有効にした場合のエラーメッセージ

LEANはPSK/dot1xではサポートされていません

これらの組み合わせではBORNを有効にできません

1. 802.1xまたはFT+802.1x

2. PSK、FT+PSKまたはPSK-SHA256

3. SAEまたはFT+SAE

4. 802.1x-SHA256またはFT+802.1x-SHA256

これらの方法のいずれかを有効にしようとすると、エラーメッセージ

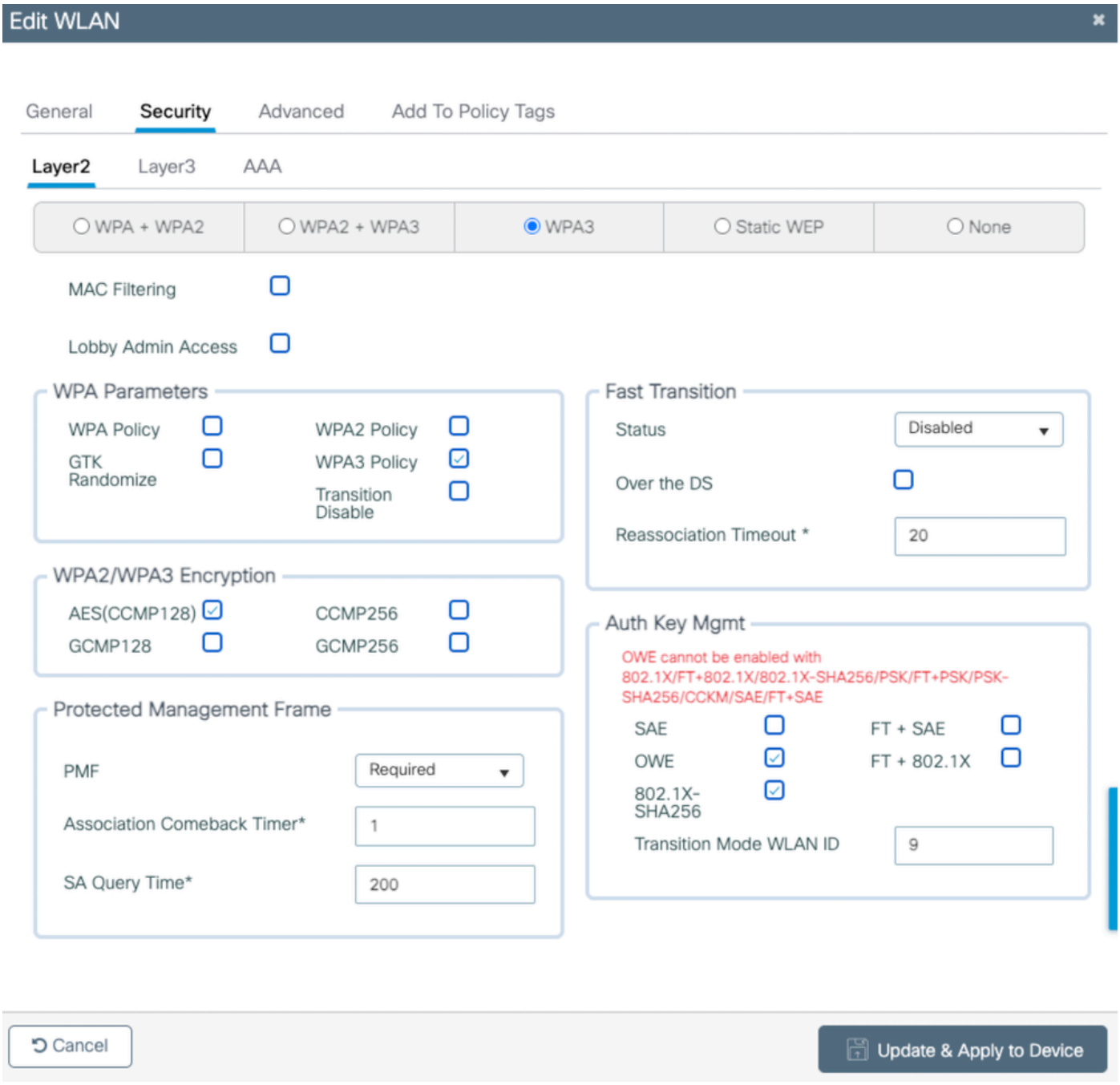
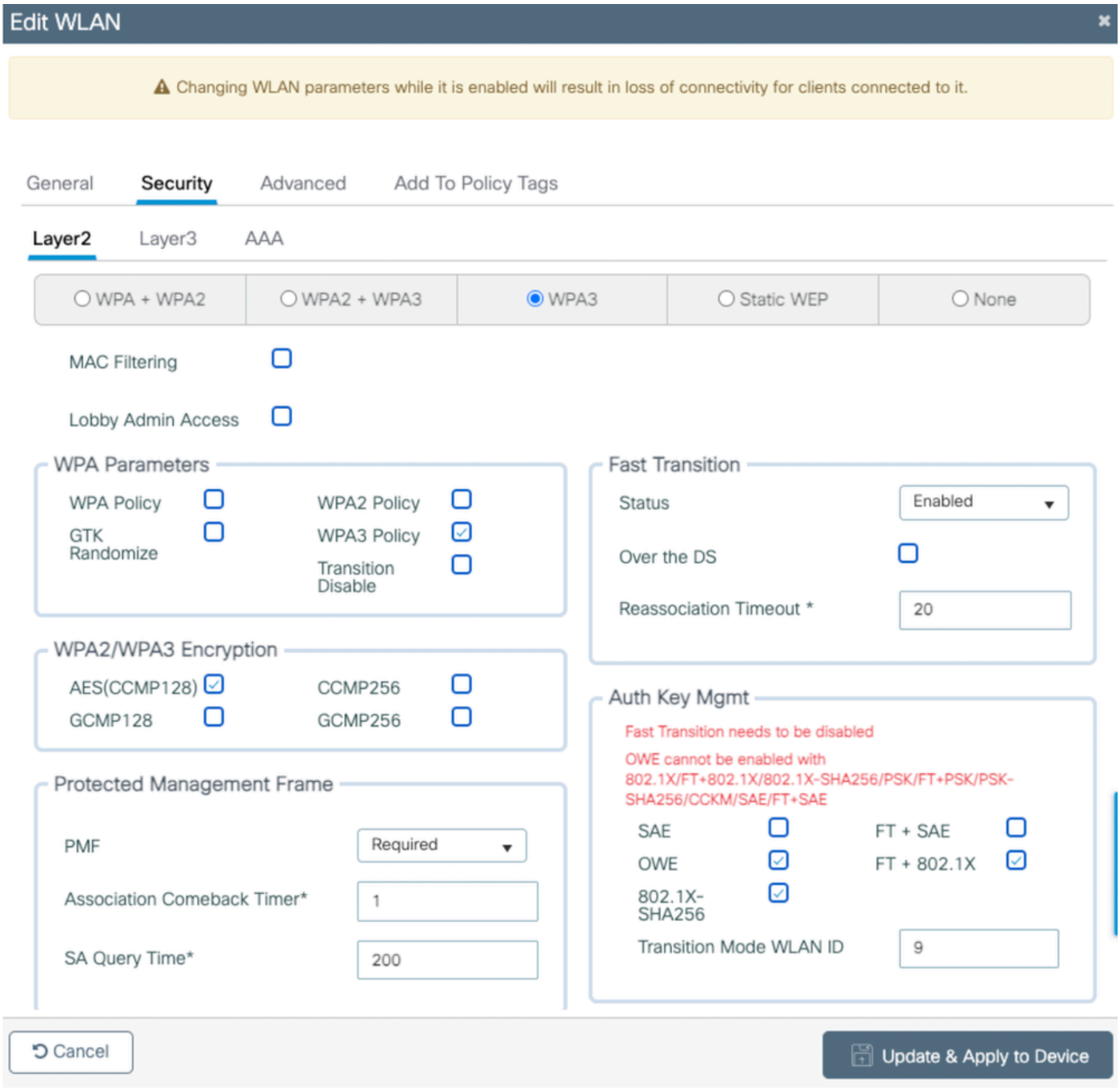
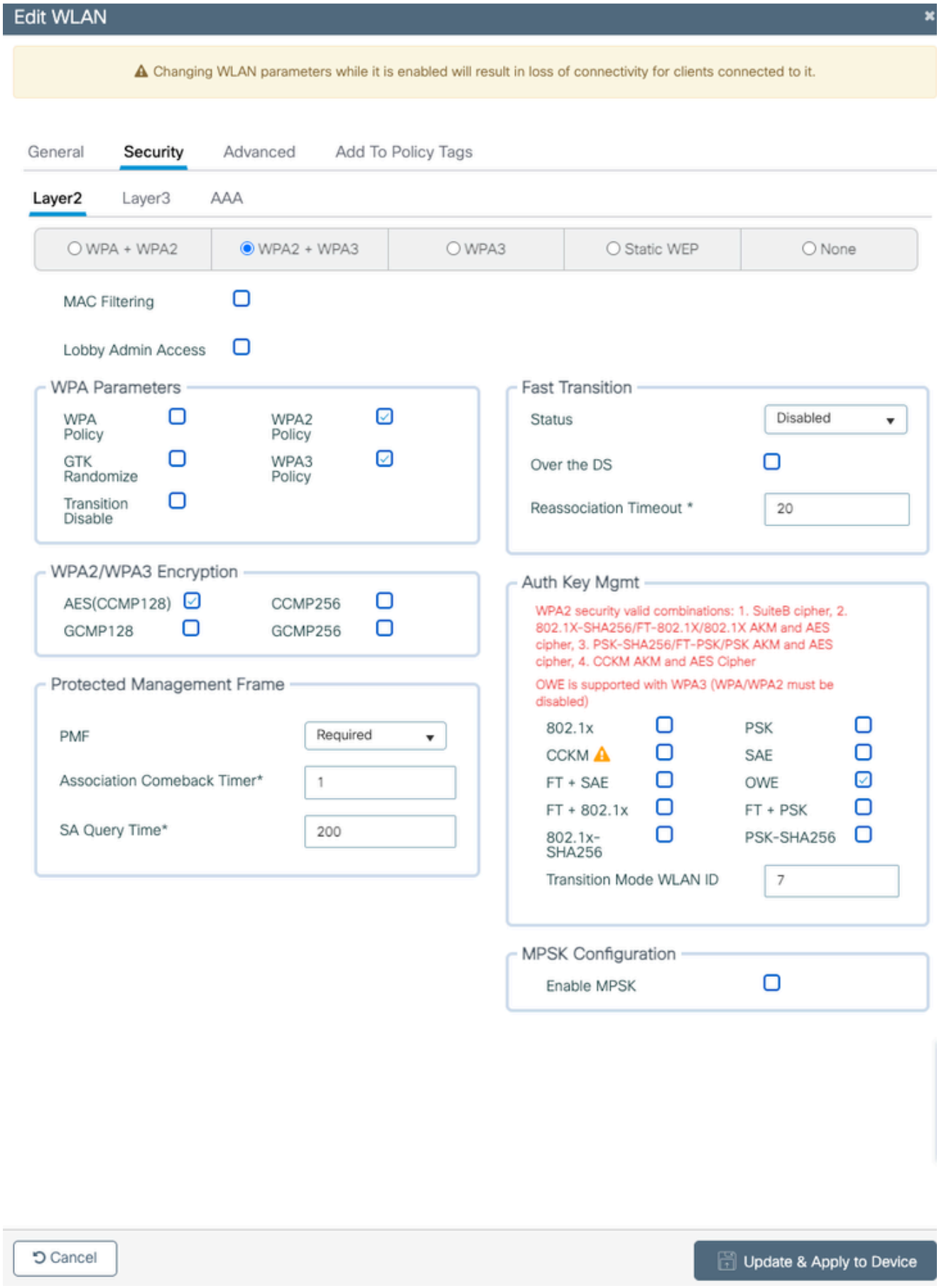


図10:LEAN SSIDで他の認証方式を有効にしているときにエラーメッセージが表示される



イメージ11:AKMを有効にしているときのエラーメッセージ

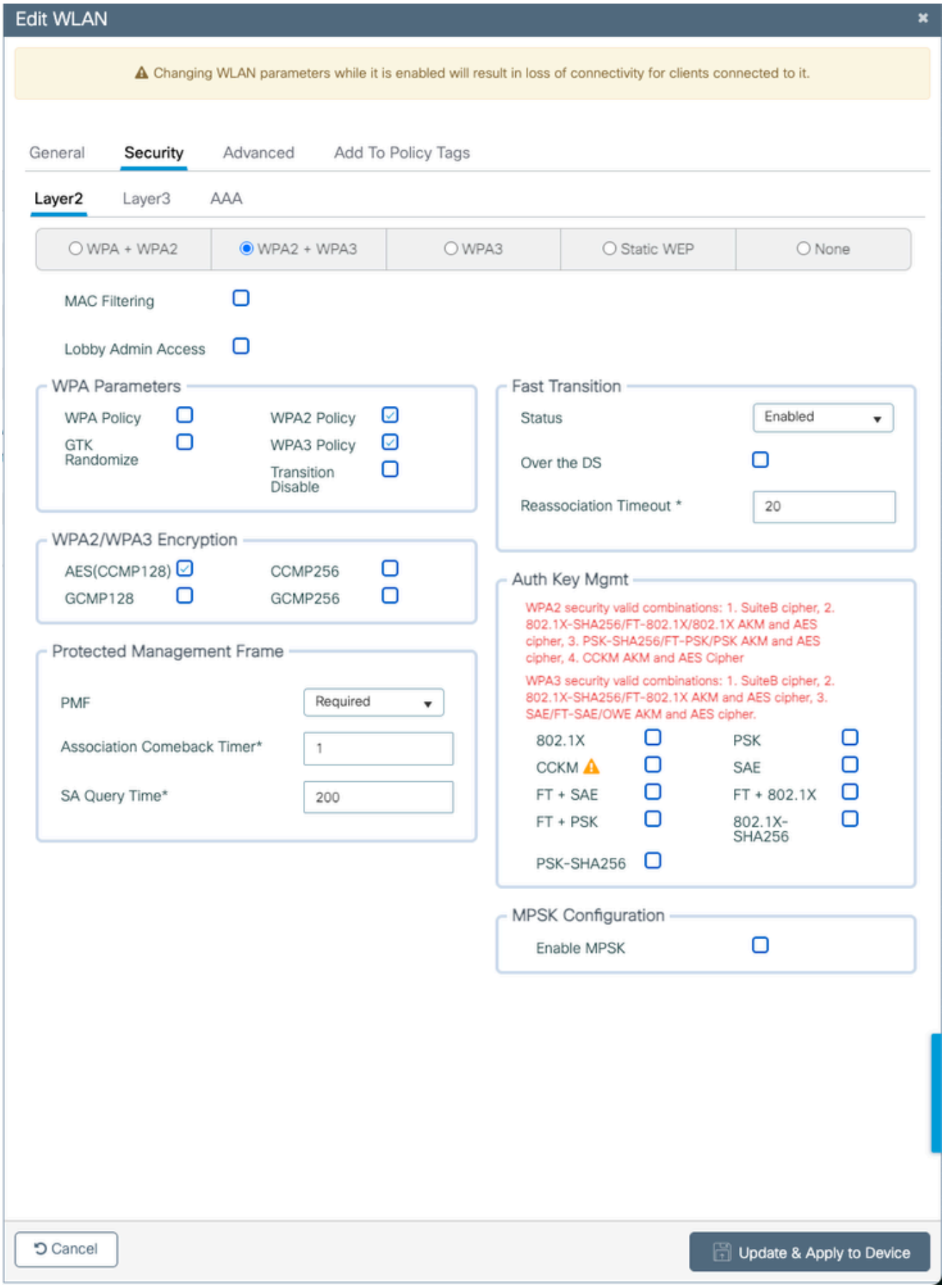
- Cisco IOS® XE 17.9.6 IOSバージョンでは、「WPA2+WPA3」を選択するとAKMの下に「LEAR」オプションが表示されますが、エラーメッセージが表示されることから、この組み合わせで「LEAD」を使用することはできません。



イメージ12:WPA2+WPA3を選択したときのエラーメッセージ

- Cisco IOS® XE 17.12.4バージョンで「WPA2+WPA3」を選択すると、AKMで「LEAN」オ

プションを取得できません。



画像–13：エラーメッセージ – AKMでLEANオプションが表示されない

トラブルシューティング

1. 両方のWLANの設定を確認します。OPEN SSIDとLEAD transition SSIDでは、移行WLAN IDがマッピングされている必要があります。
2. ブロードキャスティングオプションはLEAD移行SSIDで無効にする必要があります。OPEN SSIDでのみ有効にする必要があります。
3. この記事で説明されているサポートされている認証/暗号化/FT方式を確認します。
4. WLC側から設定に問題がない場合は、問題を絞り込むために必要なログと出力を収集してください。

RAトレースおよびEPC（組み込みパケットキャプチャ）

WLC GUIにログイン – > Troubleshooting -> Radioactive Trace -> Add client wifi MAC address -> Click that clients checkbox -> Start

WLC GUIへのログイン – >トラブルシューティング – >パケットキャプチャ – >新しいファイル名の追加 – >アップリンクインターフェイスおよびWMI VLAN/インターフェイスの選択 – >開始

クライアントマシンから：可能であれば、Wiresharkアプリケーションをインストールし、WiFiインターフェイスを選択してパケットキャプチャを収集できます。

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/213949-wireless-debugging-and-log-collection-on.html#anc12

エアーキャップ

MACラップトップを使用するか、APのいずれかをスニファモードに設定することで、この情報を収集できます。次のリンクを参照してください。

MACラップトップから：

https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-mobility/217042-collect-packet-captures-over-the-air-on.html

スニファAPから：

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217057-configure-access-point-in-sniffer-mode-o.html

スイッチポートに1台のラップトップ（Wiresharkサーバ）を接続します。このラップトップにはWiresharkアプリケーションがインストールされている必要があり、このWiresharkサーバはWLC WMIインターフェイスに到達できる必要があります。WLCとWiresharkサーバの間にプロトコル「5555、5000、または5556」が存在する場合は、ファイアウォールでプロトコル「5555、5000、または5556」を許可する必要があります。

Wiresharkがインストールされているそのpcに「gscaler」がインストールされていることを確認します。それが「オフ」をオフにして試してください。Windows Defenderなどのファイアウォー

ルまたはその中に存在するものであれば、それらを無効にしてPCAPを収集してください。

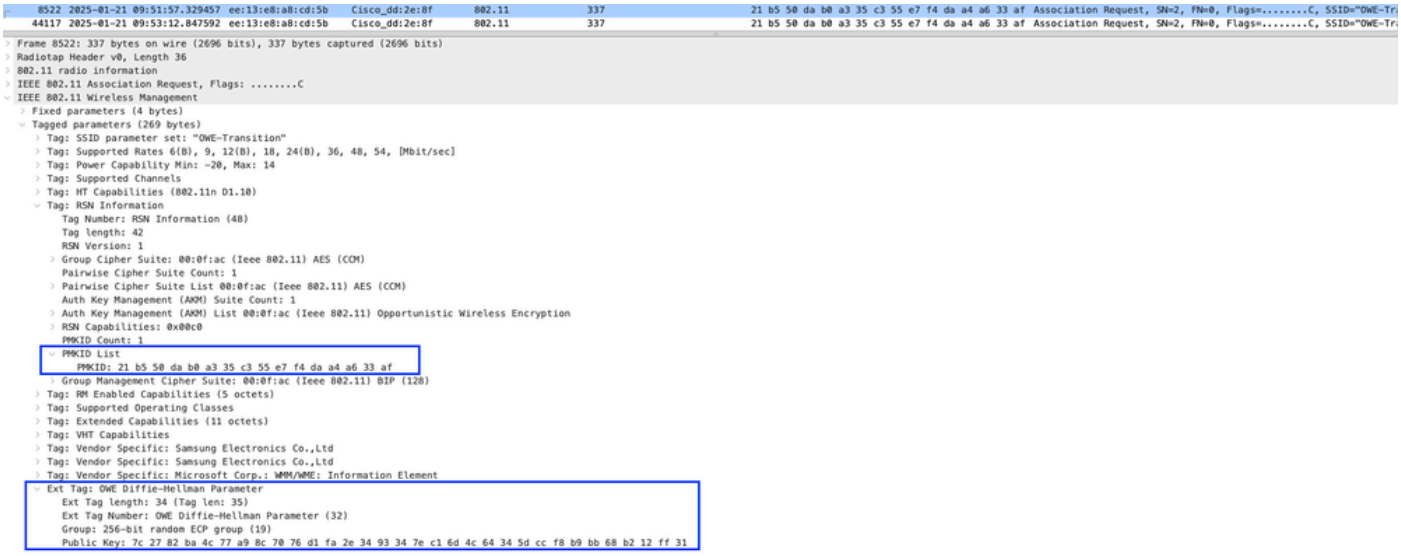
ローミング

クライアントがあるAPから別のAPにローミングする場合は、次の手順を実行する必要があります。

- 再関連付け/関連付けを送信する必要がある：クライアントの要求によって異なります。
- 関連付け要求でDH (Diffie-Helman)詳細を送信する必要があります。
- クライアントは、このPMKがクライアントとAPの両方で生成されることに基づいて、APからのアソシエーション応答でDHの詳細を取得できます。
- APとクライアントの間で4ウェイハンドシェイクが発生する可能性があります。
- LEANではFTを有効にできないため、802.11rは使用できません。
- クライアントがローミングするたびに、DH交換後に4ウェイハンドシェイクを関連付けて実行する必要があります。
- クライアントとAPは独自のPMKIDを使用し、APとクライアントごとに一意です。
- クライアントが同じAPに接続する場合、同じPMKIDを使用できます。場合によっては、クライアントが削除されると、APは新しいPMKIDを生成できますが、クライアントは4ウェイハンドシェイクに同じPMKIDを使用します。

例：

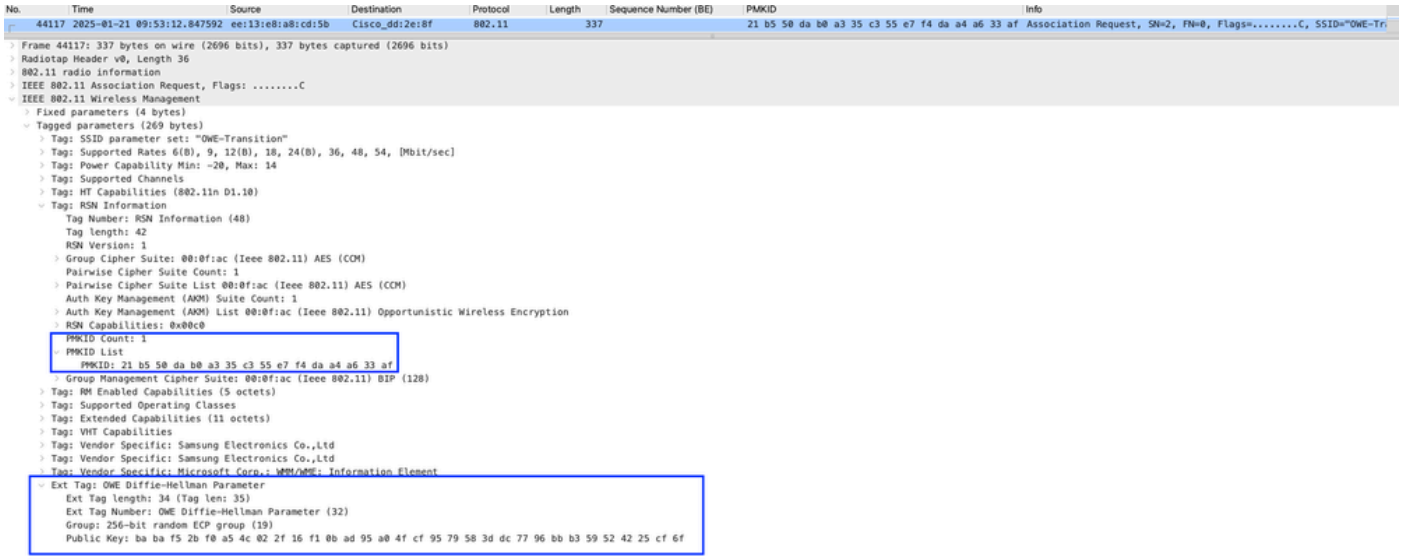
クライアントが同じAPに接続する場合、Association-RequestとAssociation-Responseの両方で同じPMKIDを確認できます。アソシエーション応答では、同じPMKIDを使用する場合はDHの詳細を表示できません。



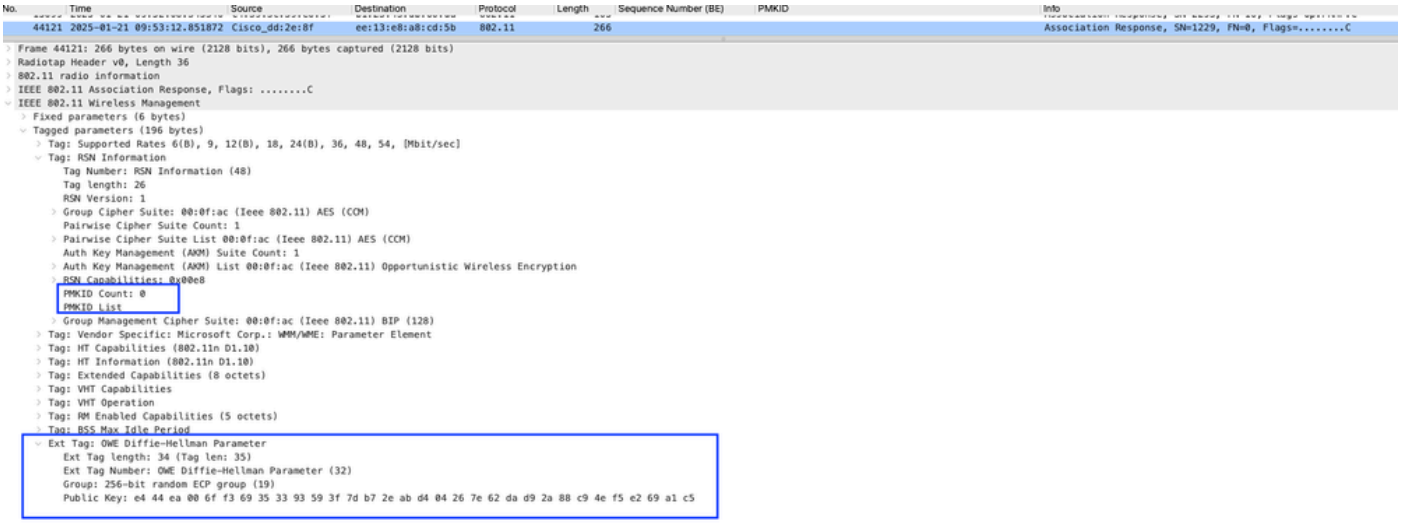
イメージ14：同じPMKIDの使用

画像–15：同じPMKIDを使用したアソシエーション応答

テストのために、このクライアントをWLCから手動で削除し、同じAPに再度関連付けました。この時点で、クライアントは同じPMKIDを送信しますが、APは関連付け応答でDHの詳細を送信します。



画像–16：削除後、クライアントは同じPMKIDをDH詳細とともに送信



画像–17:APはDH値を使用して新しいPMKIDを生成します

この例では、APとクライアントの両方が4ウェイハンドシェイクの実行中に同じPMKIDを使用し、「M1およびM2」メッセージを確認します。

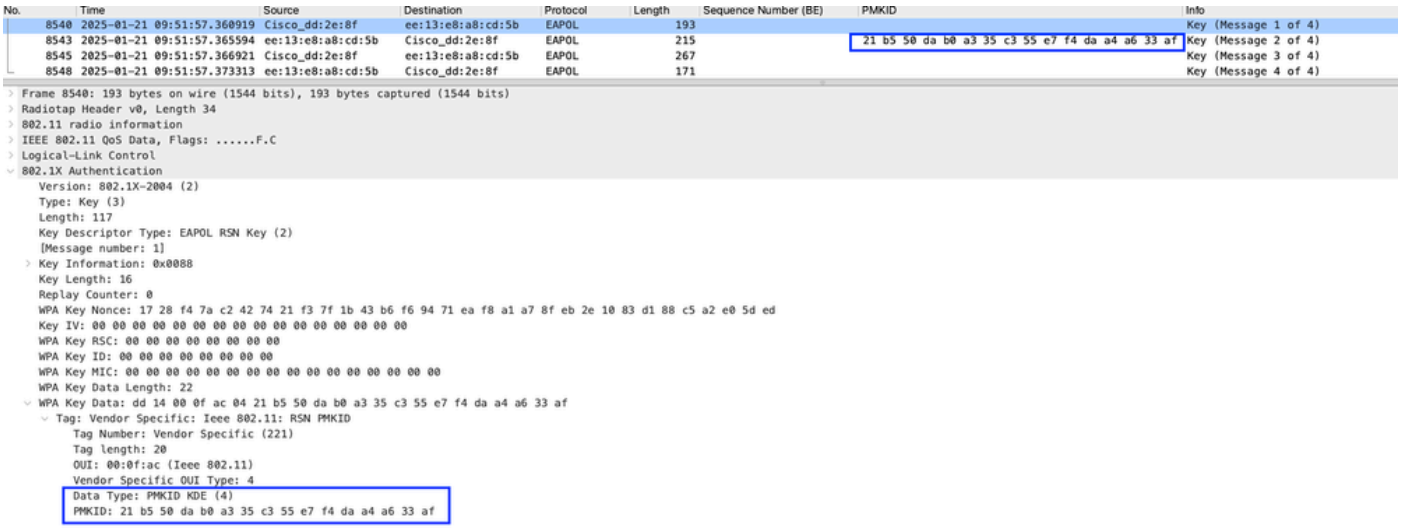


図18：同じPMKIDを使用するAPとクライアント

この例では、クライアントが同じPMKIDを使用しているが、クライアントの削除後に生成された異なるPMKIDをAPが使用している場合、「M1およびM2」メッセージを確認します。

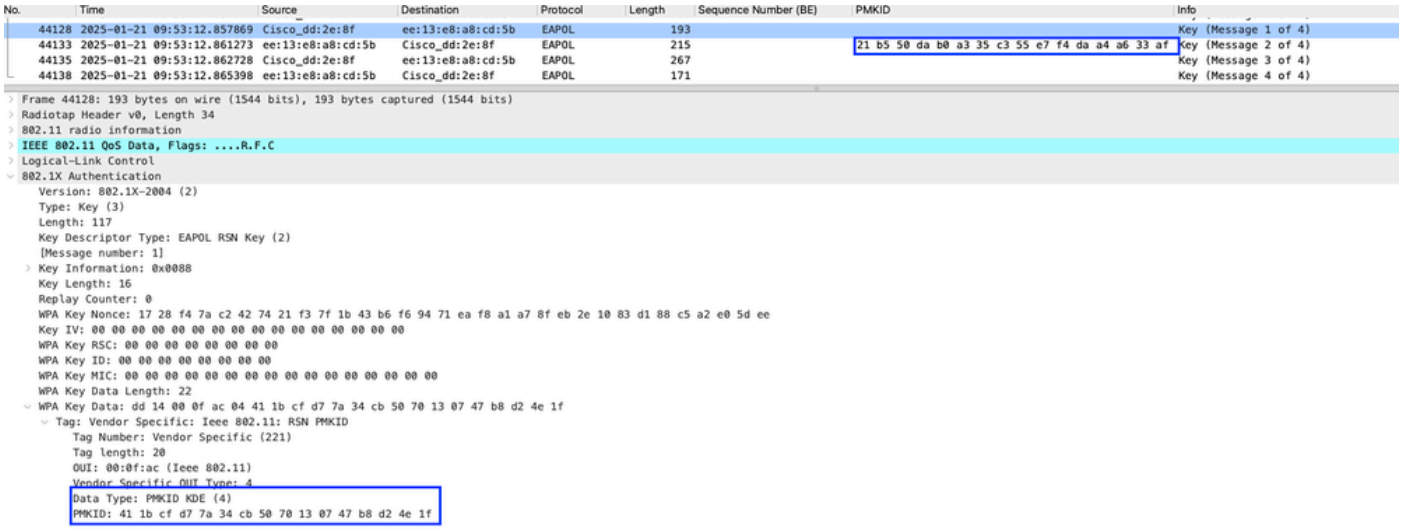


図19：異なるPMKIDを使用するAPとクライアント

内部RAトレースから：

次の例では、クライアントが関連付け要求でDHパラメータを送信し、APがPMKを生成したものよりも処理しています。

```
2025/01/21 15:18:50.157081690 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157082294 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157523328 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157531792 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532236 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532538 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157841380 {wncd_x_R0-0}{1}: [dot11-frame] [21675]: (debug): MAC: ee13.e8a8.cd5b  OW
```

その後、同じクライアントが同じAPに接続していますが、この時点では、APは新しいPMKIDを生成しませんでした。

```
2025/01/21 15:21:57.391898613 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391903915 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906073 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906329 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

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。