Opportunistische Wireless-Verschlüsselung

Inhalt

Einleitung

Dieses Dokument beschreibt den OWE-Übergangsablauf und dessen Funktionsweise auf dem Catalyst 9800 Wireless LAN Controller (WLC).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfigurieren des 9800 WLC, des Access Points (AP) für den Basisbetrieb
- Konfigurieren von WLAN- und Richtlinienprofilen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C9800-80, Cisco IOS® XE 17.12.4 und getestet in Cisco IOS® XE 17.9.6
- AP-Modell: C9136I, sowohl im lokalen als auch im Flex-Connect-Modus geprüft

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Beschreibung

- OWE (Opportunistic Wireless Encryption) ist eine Erweiterung von IEEE 802.11, die eine Verschlüsselung für das Wireless-Medium bereitstellt. Der Zweck der OWE-basierten Authentifizierung besteht darin, offene, ungesicherte Wireless-Verbindungen zwischen den APs und Clients zu vermeiden.
- Das OWE verwendet die auf dem Diffie-Hellman-Algorithmus basierende Verschlüsselung, um die Wireless-Verschlüsselung einzurichten.
- Mit OWE führen der Client und der AP während des Zugriffsvorgangs einen Diffie-Hellman-Schlüsselaustausch durch und verwenden das resultierende paarweise Geheimnis mit dem 4-Wege-Handshake.
- Die Verwendung von OWE erhöht die Sicherheit von Wireless-Netzwerken in Bereitstellungen, in denen offene oder gemeinsam genutzte PSK-basierte Netzwerke bereitgestellt werden.

Schritte

1. Konfigurieren Sie ein OFFENES WLAN ohne Verschlüsselung/Sicherheit und aktivieren Sie Broadcast.
2. Konfigurieren Sie eine andere SSID mit OWE-Sicherheitseinstellungen, und ordnen Sie die OPEN WLAN-ID-Nummer in "sition-mode-wlan-id" zu. Deaktivieren Sie die Broadcast-SSID-Option in dieser OWE-Übergangs-SSID.
3. Ordnen Sie die OWE-Übergangs-WLAN-ID im Feld OPEN WLAN "sition-mode-wlan-id" zu.

Details zum Lab Repro

- Offener SSID-Name: OFFENER SCHULDNER

- SSID für OWE-Übergang: OWE-Übergang
- BSSID von OPEN-OWE: 40:ce:24:dd:2e:87
- BSSID des OWE-Übergangs: 40:ce:24:dd:2e:8f

SCHULDENFLUSS

1. Beacons können für OPEN SSID gesendet werden. Sie können sie anhand ihres SSID-Namens in AIR PCAP sehen.
2. In AIR PCAP wird auch die SSID mit aktivierter Sicherheitsfunktion und dem Namen "Wildcard" anstelle ihres eigenen SSID-Namens angezeigt.
3. Sobald die Clients den Beacon-Frame für die OPEN SSID empfangen haben, kann sie, wenn sie OWE hat oder unterstützt, eine Anfrage an die OWE-Übergangs-SSID senden (d. h., wenn die Sicherheit die SSID aktiviert hat, anstatt die OPEN SSID zu öffnen).
4. OWE-unterstützte Clients können die Antwort auf die Anfrage von der Übergangs-SSID erhalten.
5. Die OPEN-Authentifizierung kann zwischen Client und AP erfolgen.
6. Der Client kann eine Zuordnungsanforderung mit DH-Schlüsselaustauschdetails an den AP senden und den resultierenden paarweisen Schlüssel für einen 4-Wege-Handshake verwenden.
7. Der WAP kann eine Zuordnungsantwort senden.
8. Ein Vier-Wege-Handshake kann zwischen AP und Client-Gerät erfolgen.
9. Nach erfolgreicher Schlüsselverwaltung kann L2 PSK erfolgreich sein.
10. Der Client kann die IP von DHCP, ARP usw. erhalten.
11. Der Client kann in den Status "RUN" wechseln.
12. Wenn Client-Geräte OWE nicht unterstützen, kann es eine Anfrage an die OPEN SSID senden und direkt eine IP-Adresse erhalten, als sie in den RUN-Status wechseln kann.

Original Beacon-Rahmen

- Hier, AIR PCAP zeigt, dass, die SSID "OPEN-OWE" Rundfunk (Beacon Frame). Diese enthält Einzelheiten zur SSID des Übergangs mit der Bezeichnung "OWE-Transition".

Bild-1: Beacon-Rahmen für OFFENE SSID

Versteckte SSID-Beacons

- Gemäß der WLAN-Konfiguration ist "Broadcasting" für diese "OWE-Transition" SSID deaktiviert, jedoch können Sie versteckte SSID Beacons in AIR PCAP sehen, die den SSID-Namen "Wildcard" enthalten. Wenn Sie dieses Paket jedoch überprüfen, enthält es OWE-Transition-Details.
- Rufen Sie die BSSID der versteckten SSID ab, indem Sie dieses Paket verwenden, z. B. "40:ce:24:dd:2e:8f", und suchen Sie in der Paketerfassung danach.
- In diesem Paket zeigt es, dass, SSID "Missing" und es enthält seinen Übergang SSID als "OPEN-OWE" und seine BSSID "40:ce:24:dd:2e:87".

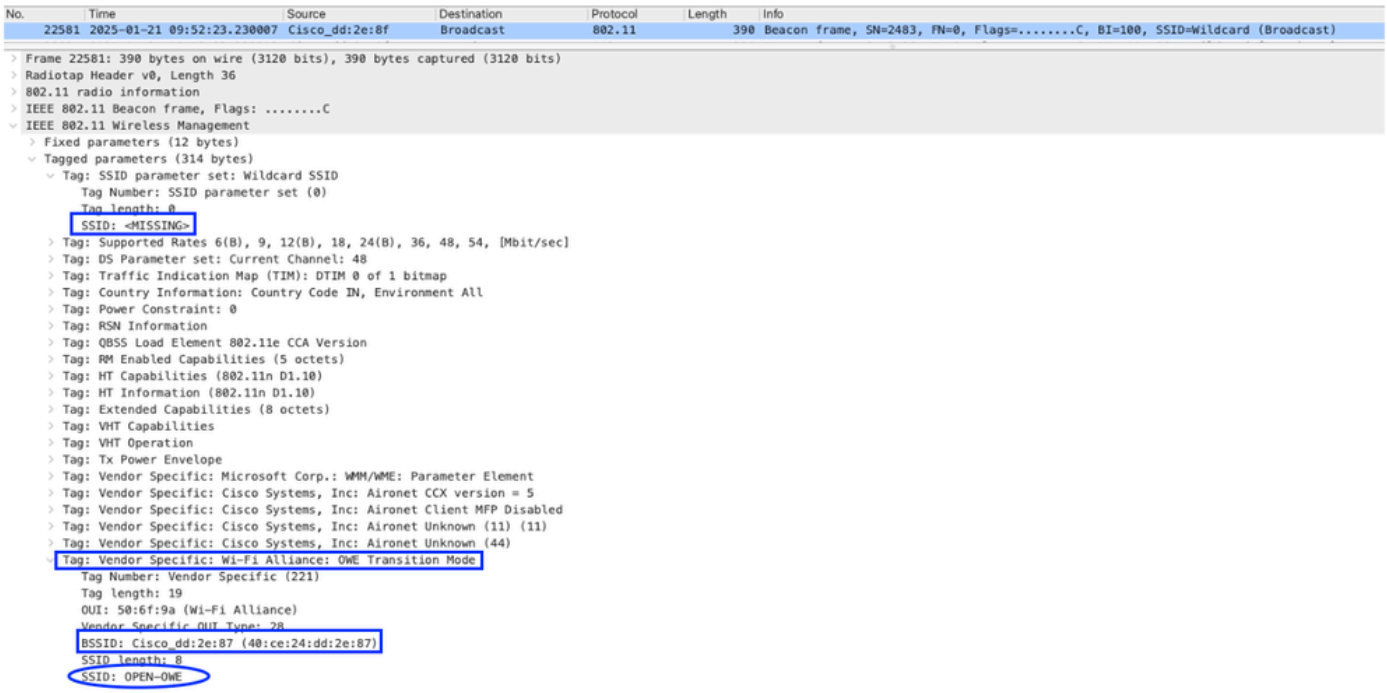

Bild-2: Versteckte SSID - OWE-Übergang

Anfrage zur Überprüfung vom Client an OWE-Transition-SSID gesendet

- Basierend auf dem Beacon-Frame "OPEN-OWE" SSID kennt der Client die anderen SSID-Details, die er verbinden muss, in diesem Szenario ist es "OWE-Transition". Wenn der Client die OWE-Verschlüsselung unterstützt, kann er die Anfrage an die OWE-Transition-SSID senden und eine Antwort erhalten.
- Anfrage an OWE-Transition BSSID "40:ce:24:dd:2e:8f" gesendet und Antwort erhalten. In diesem Paket für die Antwort auf die Anfrage sind auch die OPEN-OWE SSID-Details zu sehen.

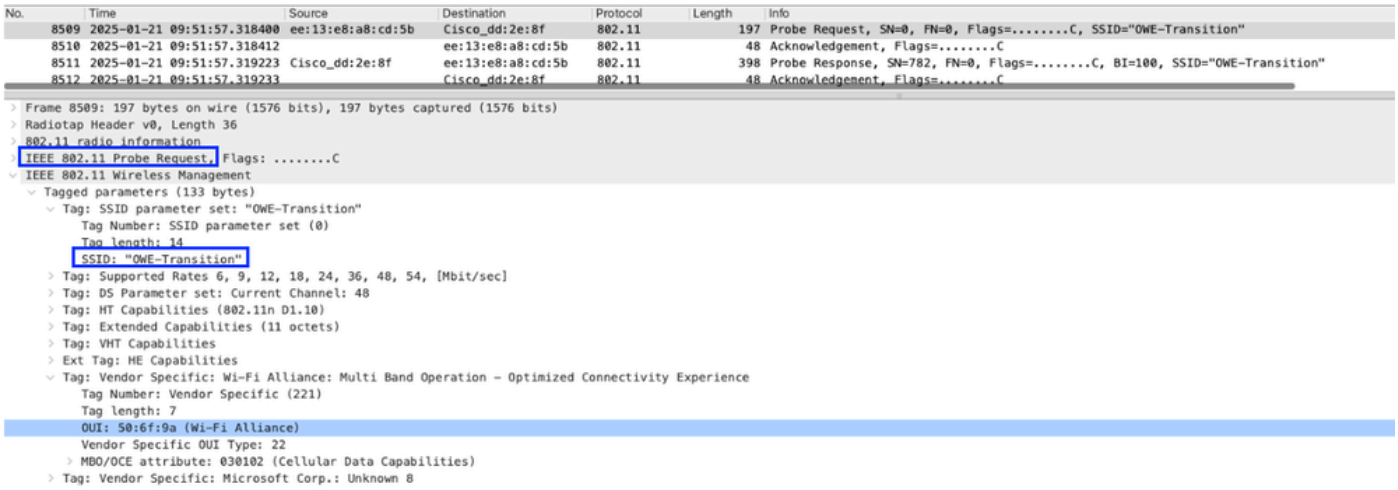

Bild-3: Anfrage senden

Testantwort vom AP an Client gesendet

- Der Client erhielt eine Anfrage für die SSID "OWE-Transition", hat jedoch seine ursprünglichen SSID-Details "OPEN-OWE" in der WiFi Alliance.

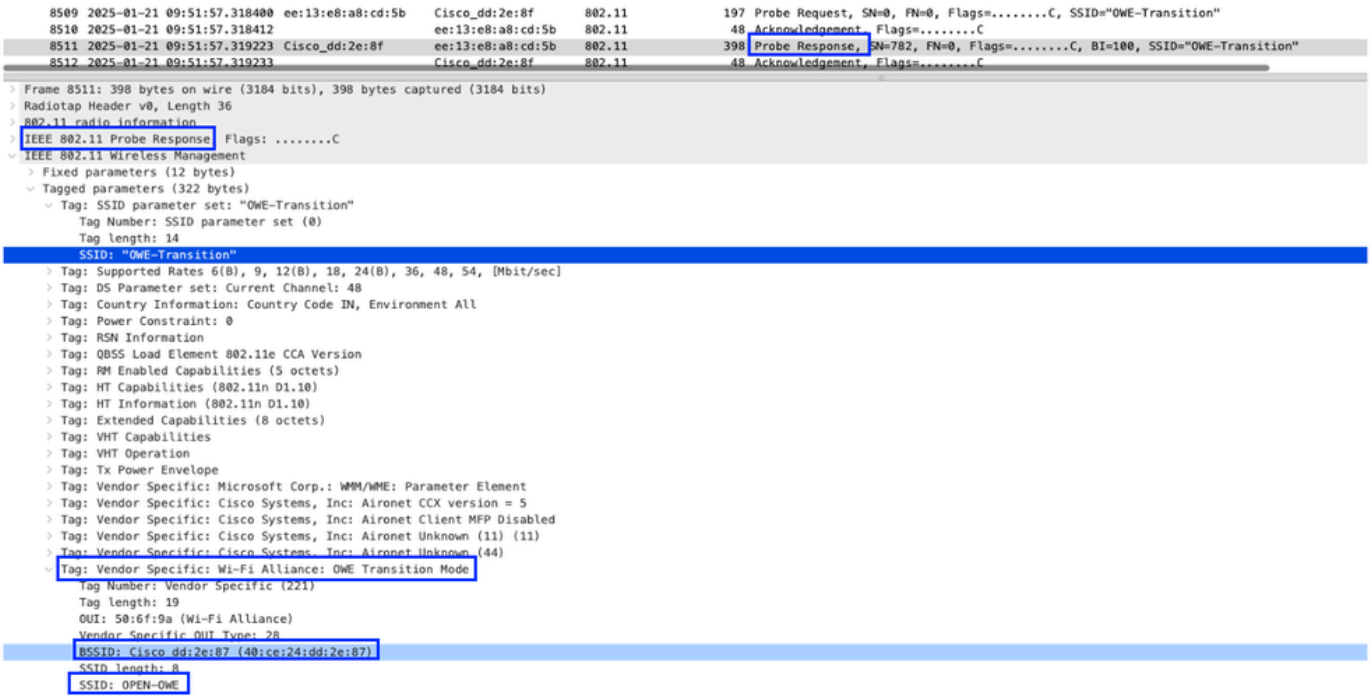

Bild-4: Antwort des Tests

OFFENE Authentifizierung

- Nach Erhalt der Antwort auf die Anfrage kann zwischen dem Client und dem Access Point eine OPEN-Authentifizierung erfolgen, um die Wi-Fi-Details und -Funktionen der Clients vor der Zuordnung zu überprüfen.

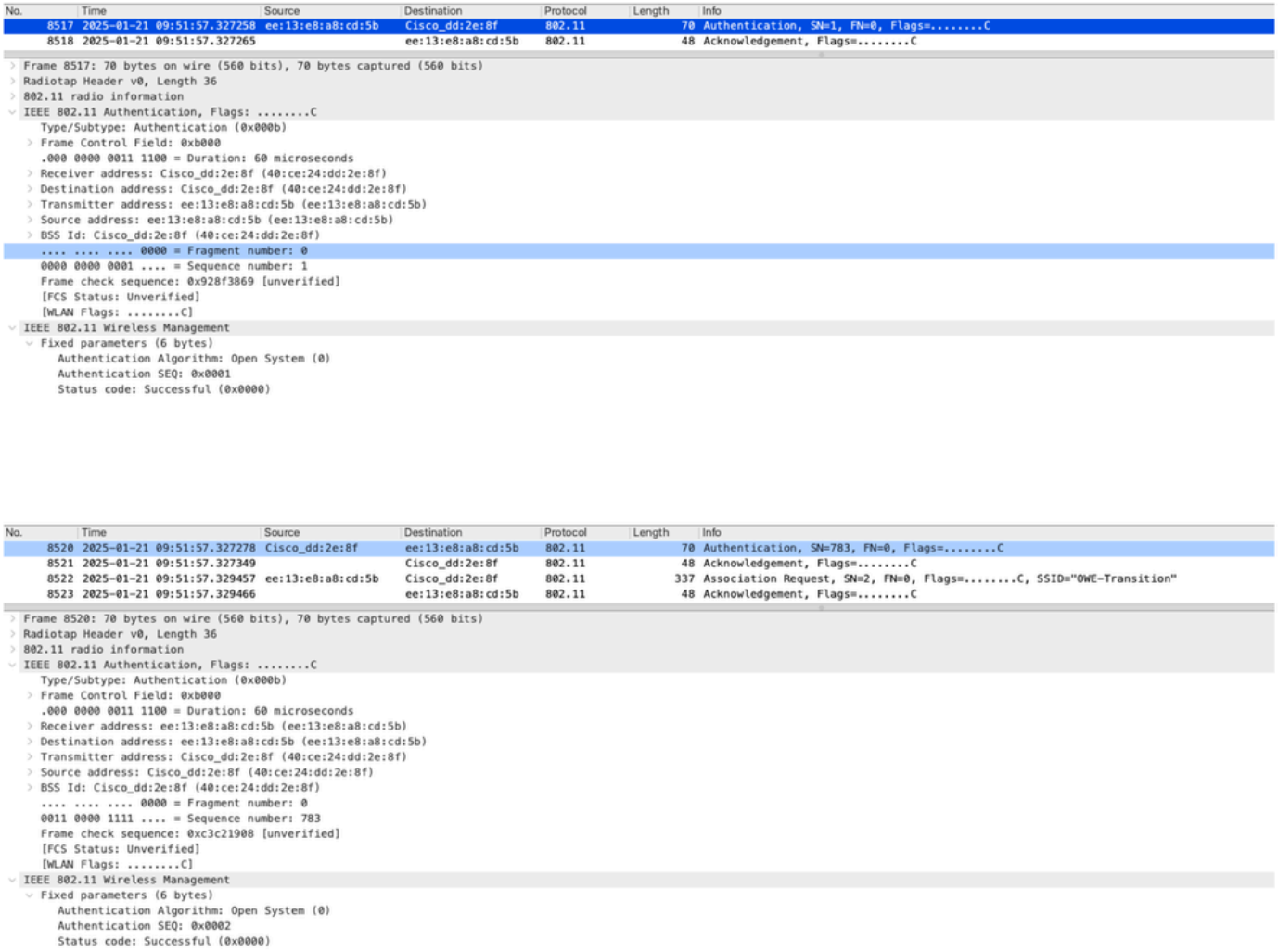

Bild-5: OPEN-Authentifizierung nach erfolgreicher Prüfung

Zuordnungsanforderung vom Client zum AP

- Beachten Sie, dass der Client für die Verschlüsselung einen Diffie-Hellman-Parameterwert anhängen kann.

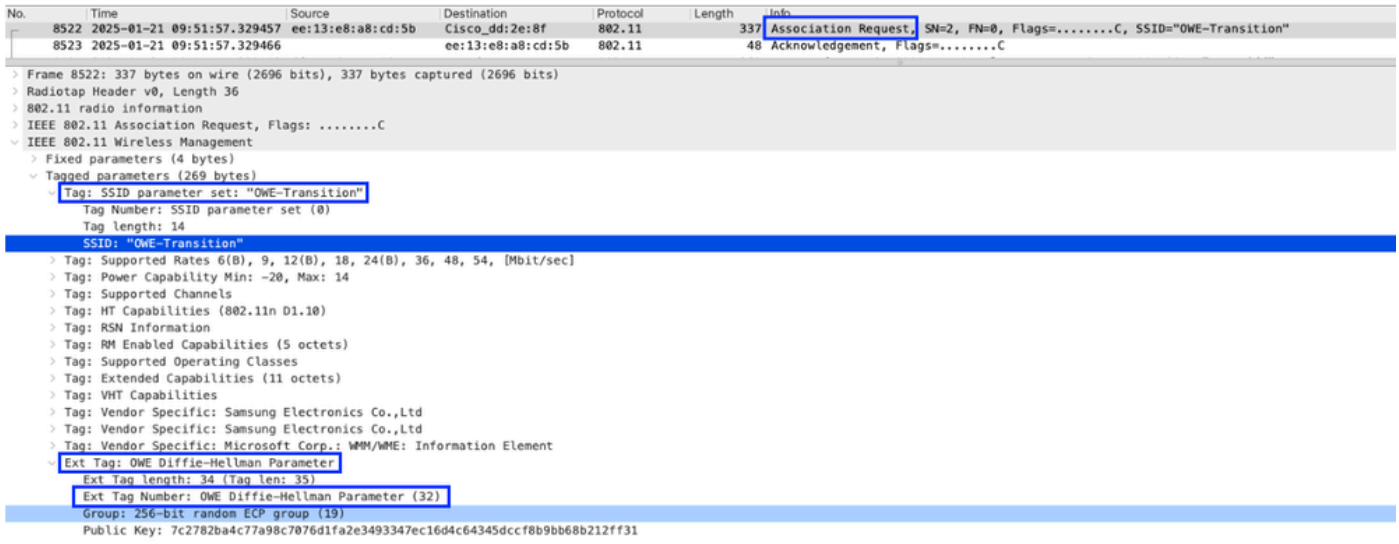

Bild-6: Zuordnungsanforderung

- In der RA-Ablaufverfolgung können Sie die Client-Protokolle der Zuordnungsphase anzeigen.

```
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
```

Zuordnungsantwort vom AP zum Client gesendet

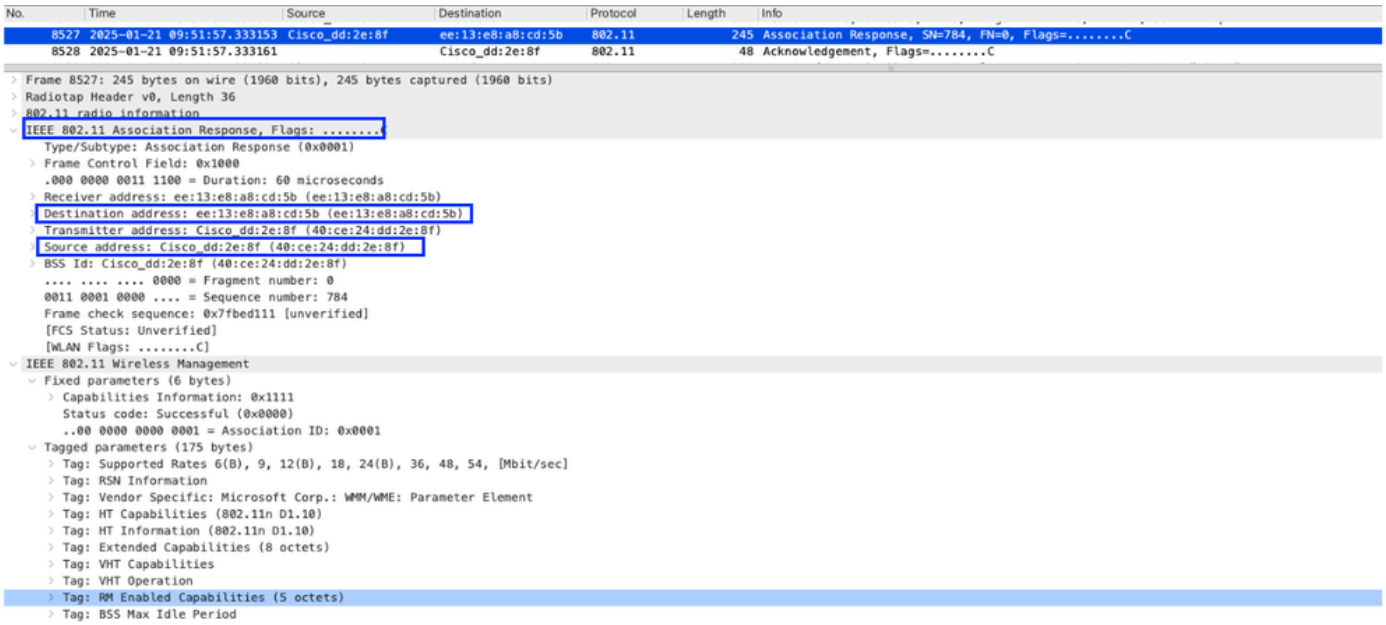

Bild-7: Assoziationsantwort

```
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
```

Schlüsselaustausch

Ein 4-Wege-Handshake kann zwischen dem AP und dem Client-Gerät erfolgen.

Schlüssel-1 vom AP gesendet

Schlüssel-2 vom Client gesendet

Schlüssel-3 vom AP gesendet

Schlüssel-4 vom Client gesendet

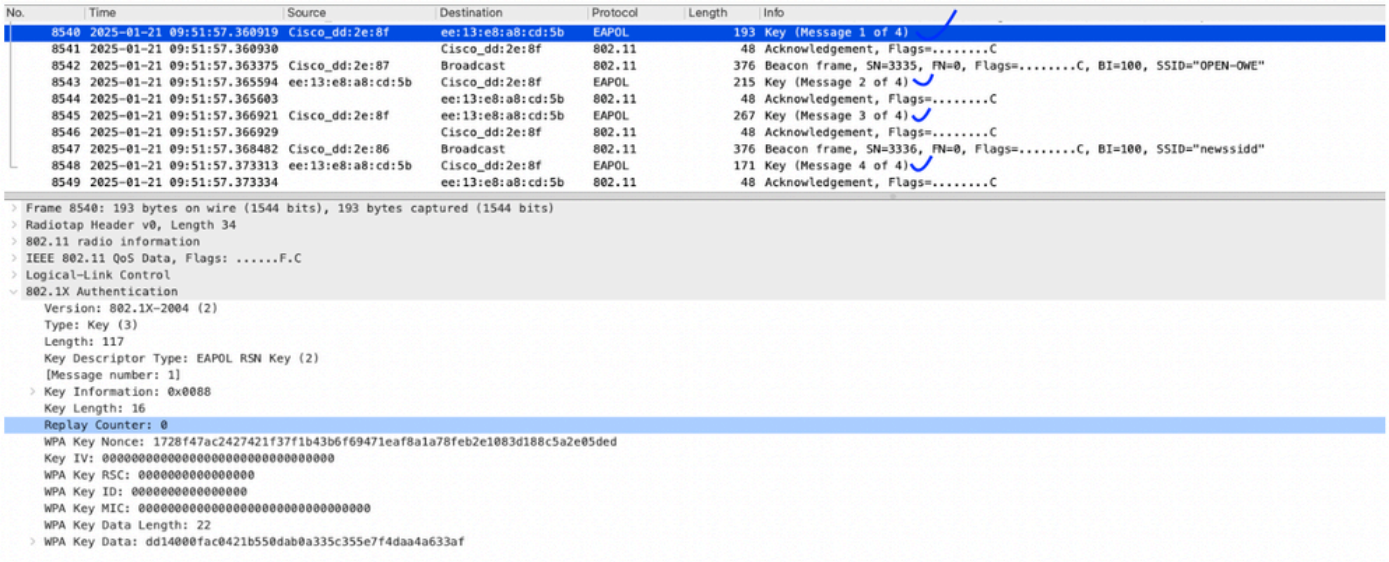

Bild-8: 4-Wege-Handshake

```
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-Authentifizierung erfolgreich

```
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-Lernstatus

```
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
```

Client im RUN-Status

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

Clients, die für OWE-Verschlüsselung nicht unterstützt werden

- Durch die Überprüfung eines Beacon-Frames an sich werden die Clients darauf aufmerksam, ob sie diese Verschlüsselungsmethode unterstützen können oder nicht. Wenn es nicht unterstützt wird, kann es einfach eine Anfrage senden, um SSID zu öffnen "OPEN-OWE" und eine normale offene Authentifizierung durchführen, IP-Adresse abrufen, dann kann es den RUN-Status gehen.

```
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
```

Informationen zur schnellen Umrüstung

- Wir können OWE nur in der OPEN Authentifizierung oder in Webauth (CWA/LWA/EWA) konfigurieren.
- FT wird bei der OWE-Umstellung nicht unterstützt.
- Wenn Sie FT aktivieren, erhalten Sie diese Fehlermeldung,

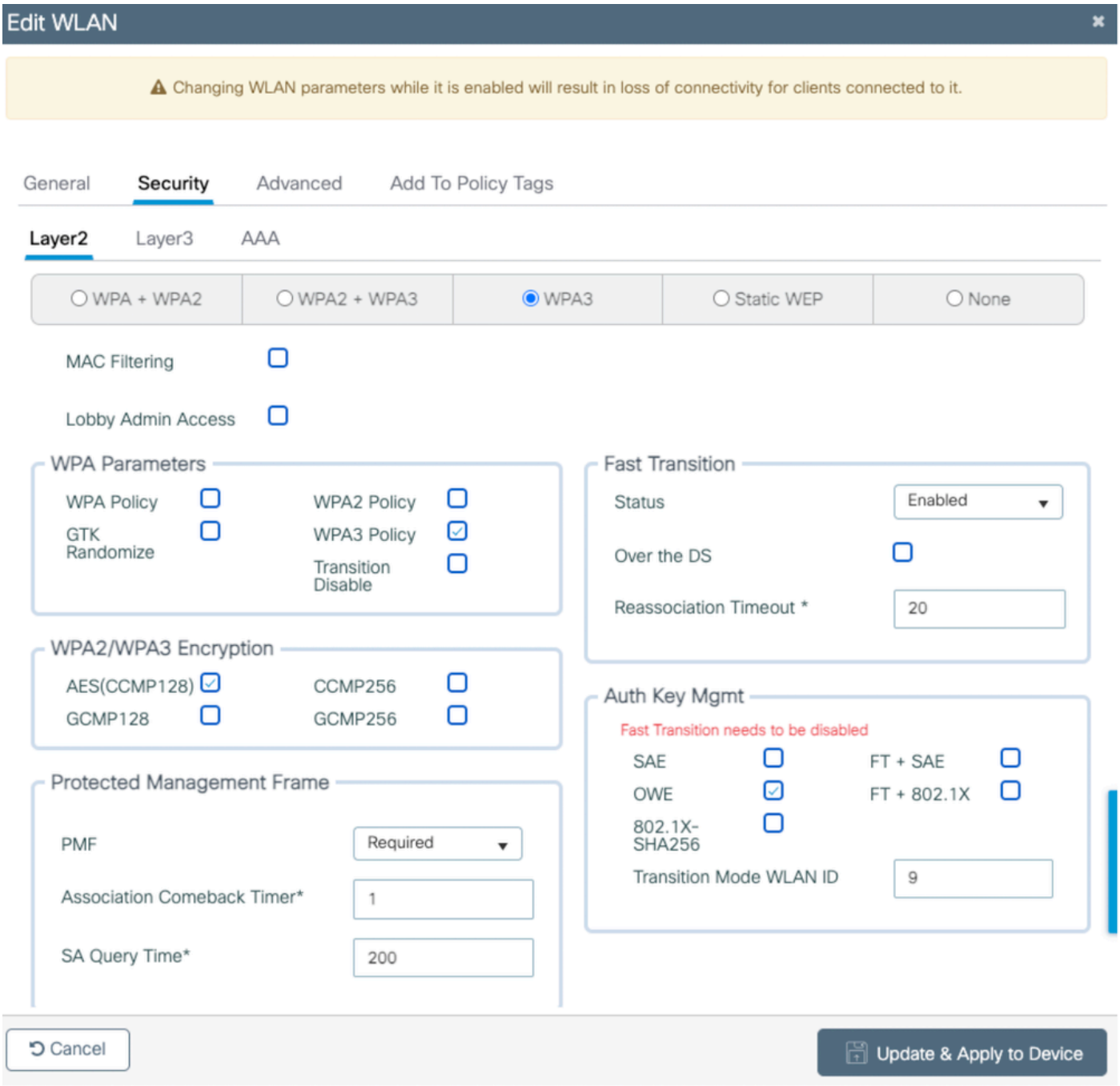

Bild-9: Fehlermeldung bei Aktivierung von FT in OWE Transition-SSID

OWE wird von PSK/dot1x nicht unterstützt

Wir können OWE in diesen Kombinationen nicht aktivieren.

1. 802.1x oder FT+802.1x

2. PSK oder FT+PSK oder PSK-SHA256

3. SAE oder FT+SAE

4. 802.1x-SHA256 oder FT+802.1x-SHA256

Wenn Sie eine dieser Methoden aktivieren, können Sie die Fehlermeldung

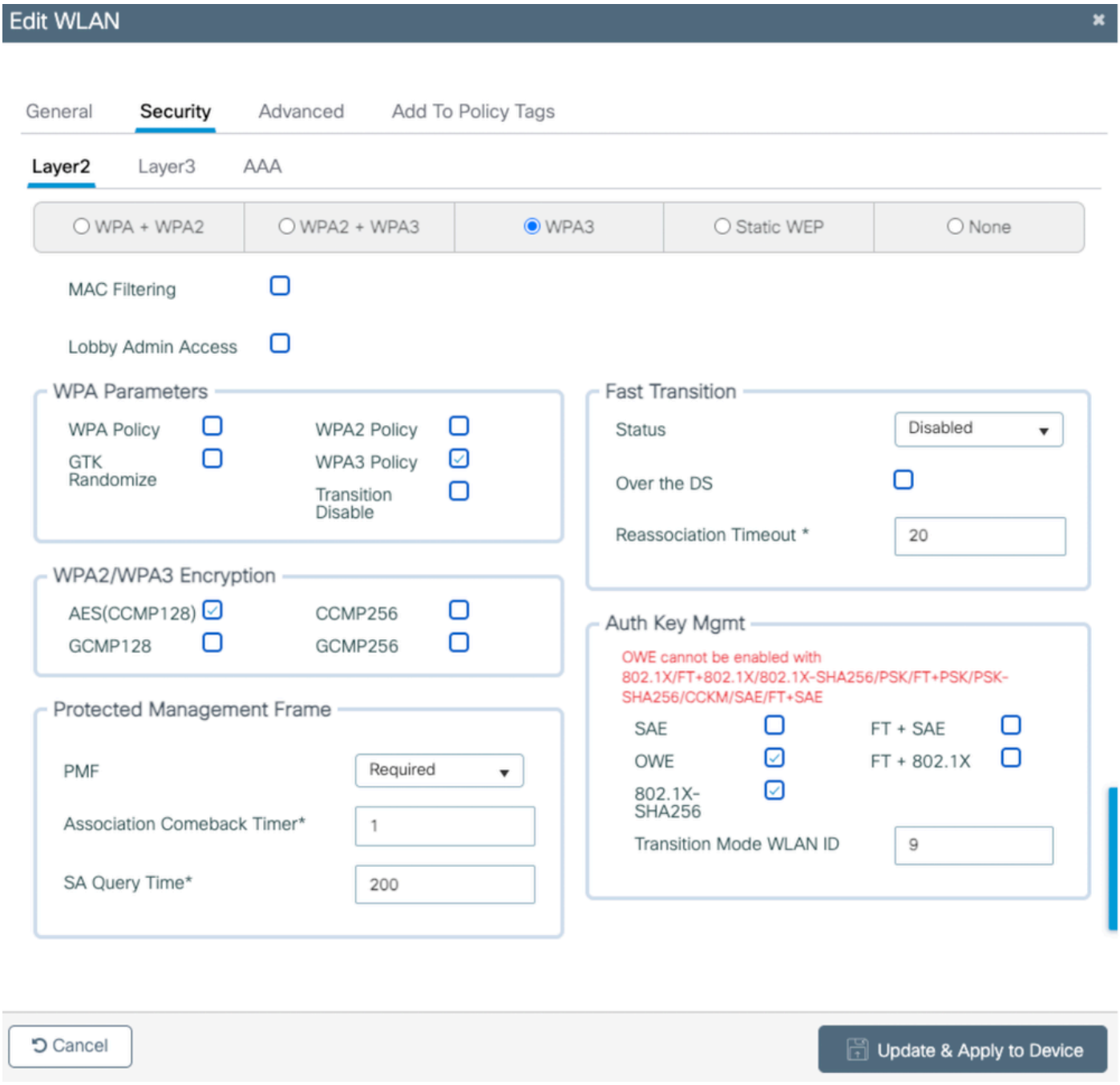

Bild-10: Fehlermeldung beim Abrufen der anderen Authentifizierungsmethoden in der OWE-SSID

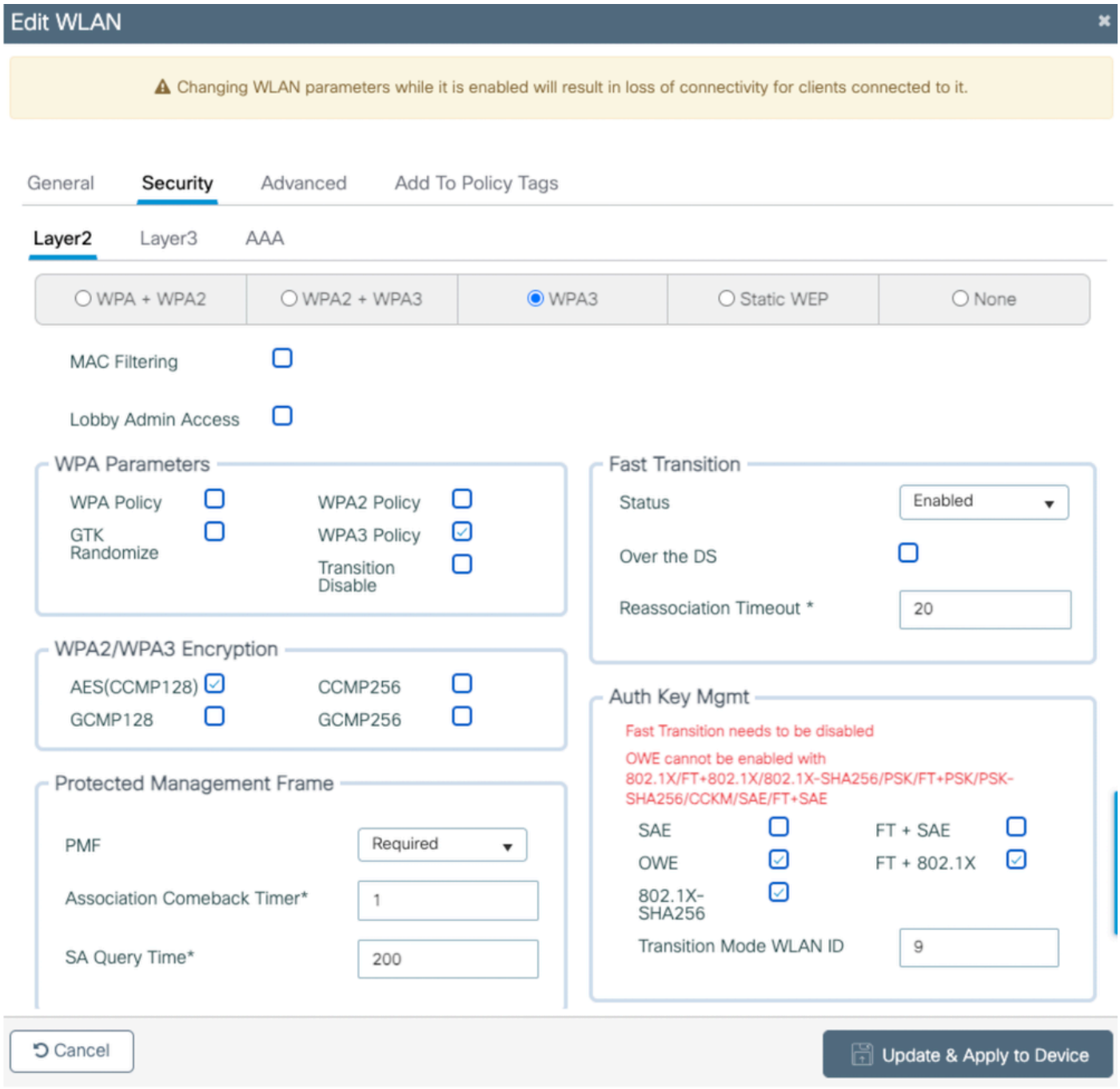

Bild-11: Fehlermeldung beim Aktivieren von AKM

- In der Cisco IOS® XE 17.9.6 IOS-Version können Sie die Option "OWE" unter AKM sehen, wenn Sie "WPA2+WPA3" auswählen. Sie können jedoch die Fehlermeldung erhalten, dass Sie OWE mit dieser Kombination nicht verwenden können.

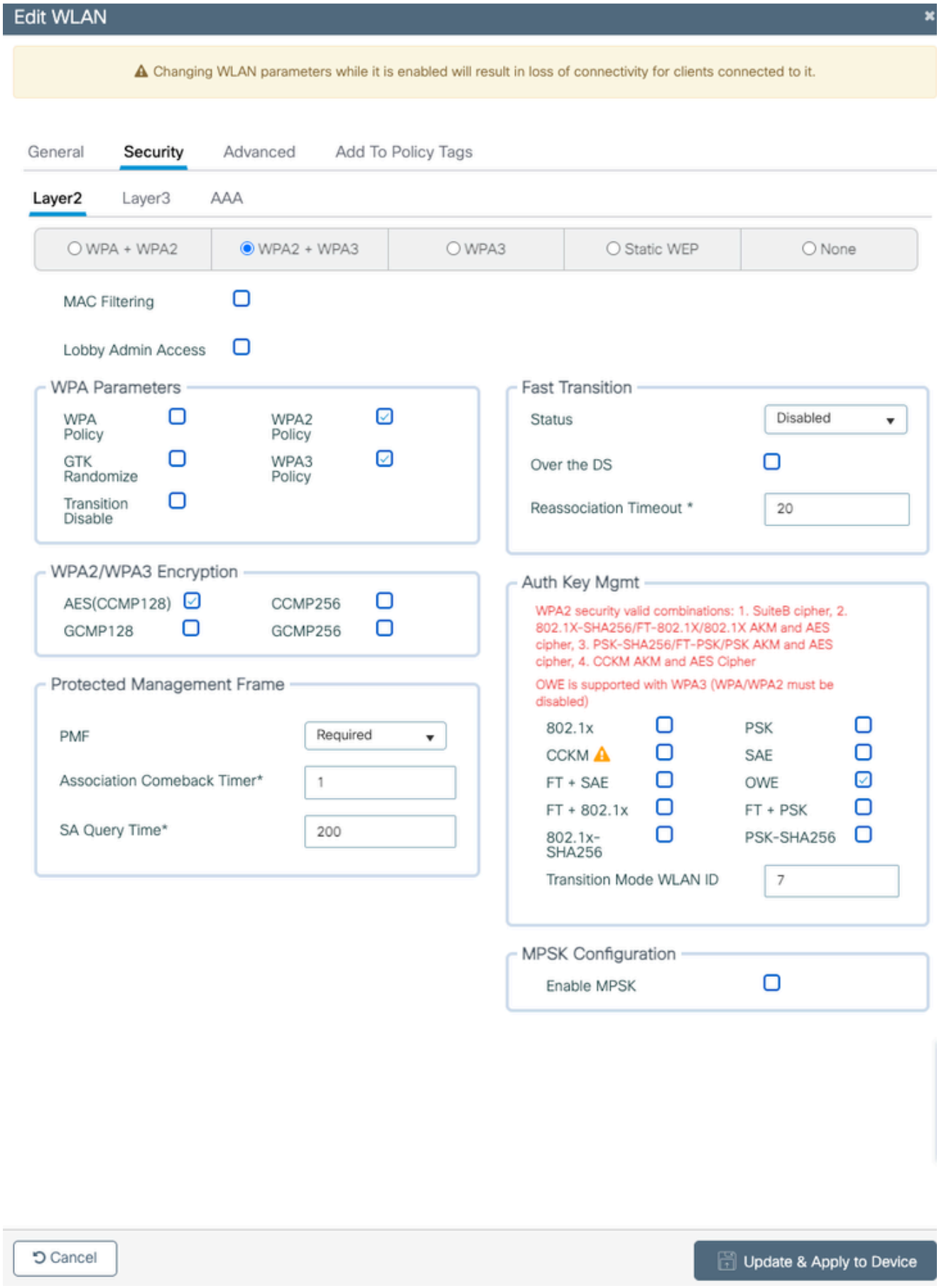

Bild-12: Fehlermeldung bei Auswahl von WPA2+WPA3

- Wenn Sie in der Version Cisco IOS® XE 17.12.4 "WPA2+WPA3" auswählen, wird die Option

"OWE" in AKM nicht angezeigt.

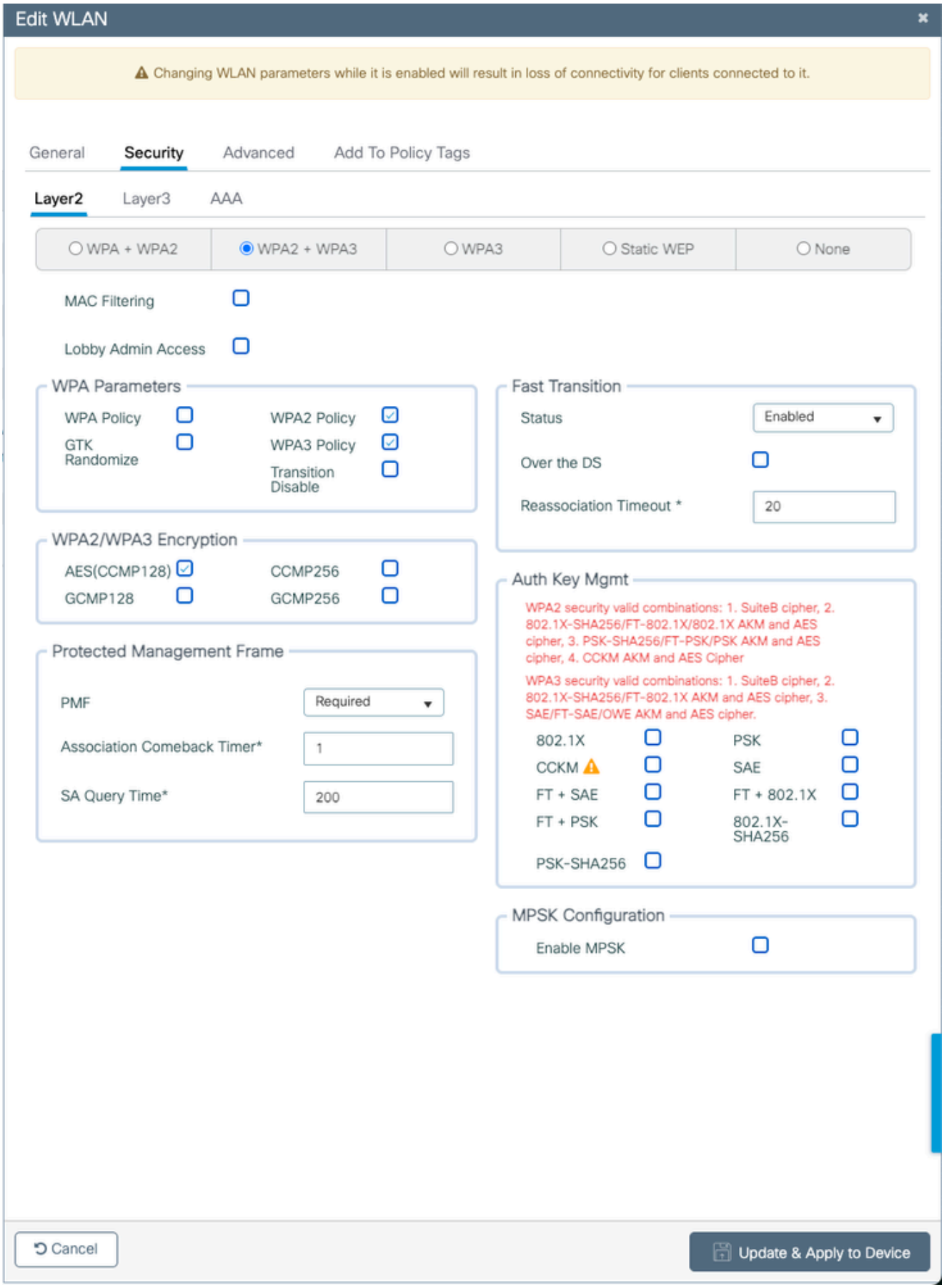

Bild-13: Fehlermeldung - OWE-Option wird in AKM nicht abgerufen

Fehlerbehebung

1. Überprüfen Sie, ob die Konfigurationen in beiden WLANs, in OPEN SSID und in OWE Transition SSID müssen Transition WLAN ID zugeordnet.
2. Die Broadcasting-Option muss in der OWE-Übergangs-SSID deaktiviert sein, sie darf nur in der OPEN-SSID aktiviert sein.
3. Überprüfen Sie die in diesem Artikel beschriebenen unterstützten Authentifizierungs-/Verschlüsselungs-/FT-Methoden.
4. Wenn die Konfigurationen von WLC-Ende an in Ordnung sind, erfassen Sie die erforderlichen Protokolle und Ausgaben, um das Problem einzugrenzen.

RA Trace und EPC (Embedded PAcket Capture)

Login to WLC GUI -> Troubleshooting -> Radioactive Trace -> Add client wifi MAC address -> Click that clients checkbox -> Start

Anmelden bei der WLC-GUI -> Fehlerbehebung -> Paketerfassung -> Neuen Dateinamen hinzufügen -> Wählen Sie die Uplink-Schnittstelle und WMI VLAN/Interface -> Start aus.

Vom Client-Computer: Wenn möglich, können Sie Wireshark-Anwendung installieren und die Paketerfassung sammeln, indem Sie WiFi-Schnittstelle auswählen.

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

LUFTKAPPE

Sie können es erfassen, indem Sie den MAC-Laptop verwenden oder einen der APs für den Sniffer-Modus konfigurieren. Weitere Informationen finden Sie unter diesen Links,

Von MAC-Laptop:

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

Von Sniffer AP:

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

Schließen Sie einen Laptop (Wireshark-Server) an den Switch-Port an, und es muss eine Wireshark-Anwendung installiert sein. Dieser Wireshark-Server muss über eine WLC WMI-Schnittstelle verfügen. Das Protokoll "5555 oder 5000 oder 5556" muss in der Firewall zugelassen werden, wenn es sich zwischen Ihrem WLC und dem Wireshark-Server befindet.

Markieren Sie, ob es irgendeinen "gscaler" in diesem PC installiert, wo wireshark installiert, wenn es als bitte "ausschalten" und versuchen, wenn es eine Firewall wie Windows Defender oder

etwas in ihm vorhanden ist, deaktivieren Sie diese und versuchen, PCAP zu sammeln.

Roaming

Wenn ein Client von einem Access Point zu einem anderen wechselt, muss er folgende Schritte ausführen:

- Erneute Zuordnung/Zuordnung erforderlich - Abhängig von der Kundenanforderung.
- Die DH-Daten (Diffie-Helman) müssen in der Zuordnungsanfrage gesendet werden.
- Der Client kann DH-Details in der Zuordnungsantwort vom Access Point abrufen, basierend auf diesen PMK-Informationen, die sowohl im Client als auch im Access Point generiert werden.
- Ein 4-Wege-Handshake kann zwischen AP und Client erfolgen.
- In OWE können Sie FT nicht aktivieren. 802.11r ist daher nicht möglich.
- Jedes Mal, wenn der Client Roaming, es muss 4-Wege-Handshake nach DH Austausch in Verbindung.
- Client und AP verwenden eine eigene PMKID, die für jeden AP und jeden Client eindeutig ist.
- Wenn der Client eine Verbindung mit demselben Access Point herstellt, kann dieselbe PMKID verwendet werden. Wenn der Client gelöscht wurde, als der Access Point eine neue PMKID generieren kann, verwendet der Client in einigen Szenarien dieselbe PMKID für den 4-Wege-Handshake.

Beispiel:

Wenn der Client eine Verbindung mit demselben Access Point herstellt, wird dieselbe PMKID sowohl in der Zuordnungsanforderung als auch in der Zuordnungsanforderung angezeigt. In der Zuordnungsantwort werden keine DH-Details angezeigt, wenn dieselbe PMKID verwendet wird.

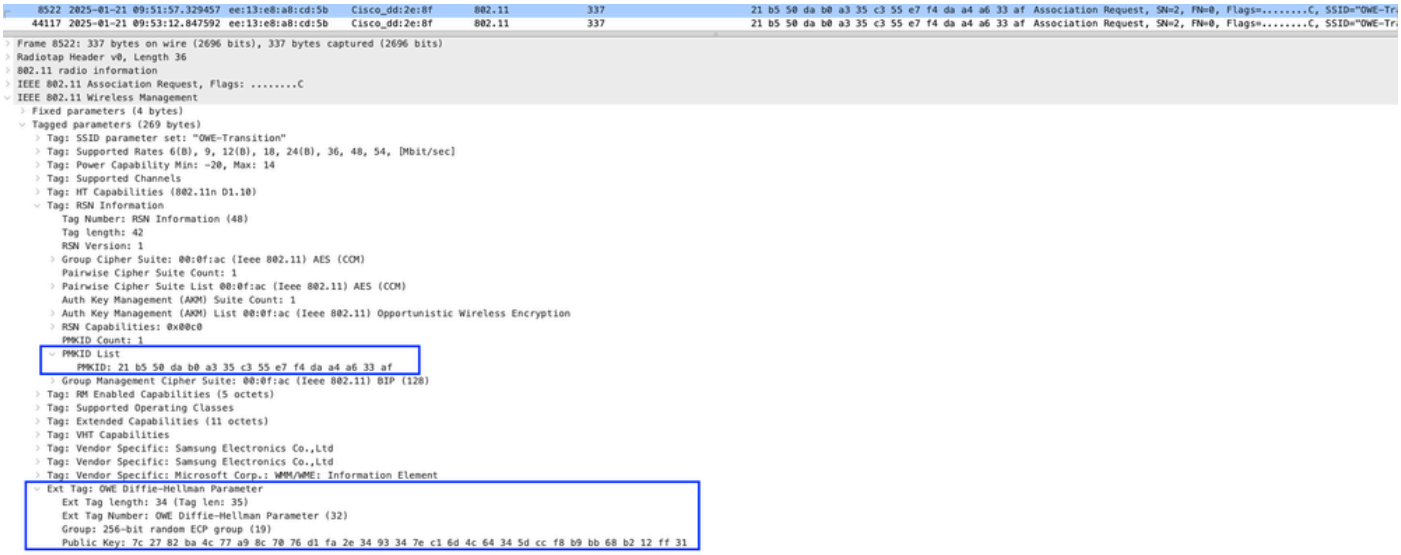

Bild-14: Verwendung derselben PMKID

Bild-15: Assoziationsantwort mit derselben PMKID

Zum Testen wurde dieser Client manuell vom WLC gelöscht und erneut mit demselben AP verknüpft. Zu diesem Zeitpunkt sendet der Client dieselbe PMKID, jedoch sendet der AP DH-Details als Antwort auf die Zuordnung.

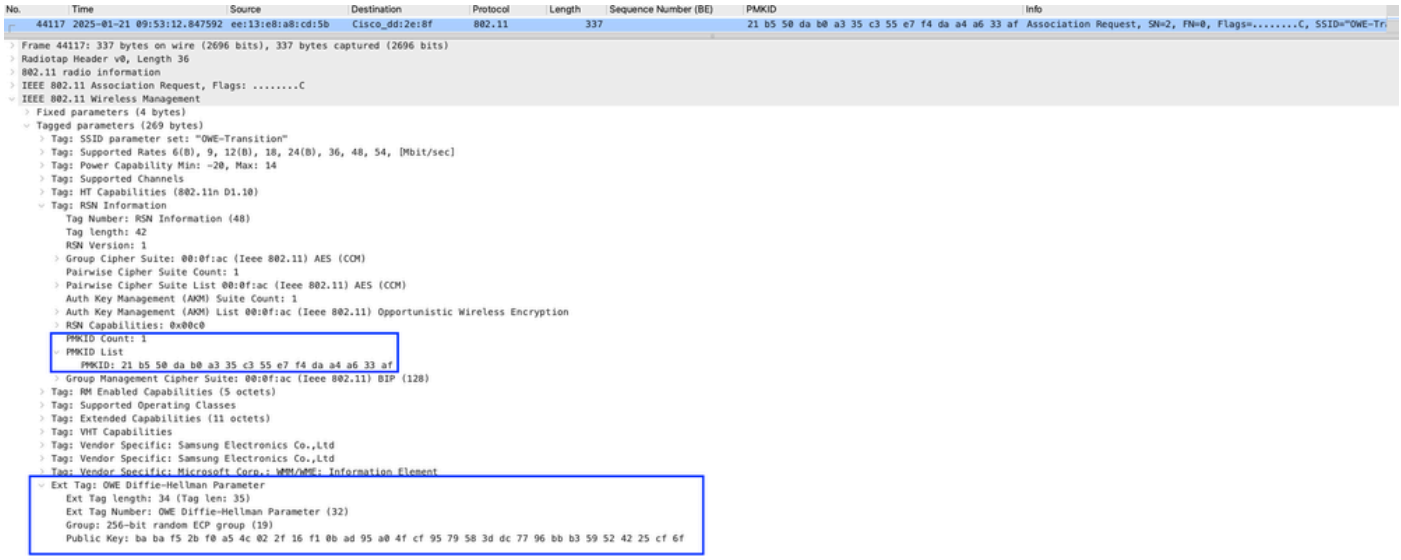

Bild-16: Nach dem Löschen hat der Client dieselbe PMKID mit DH-Details gesendet.

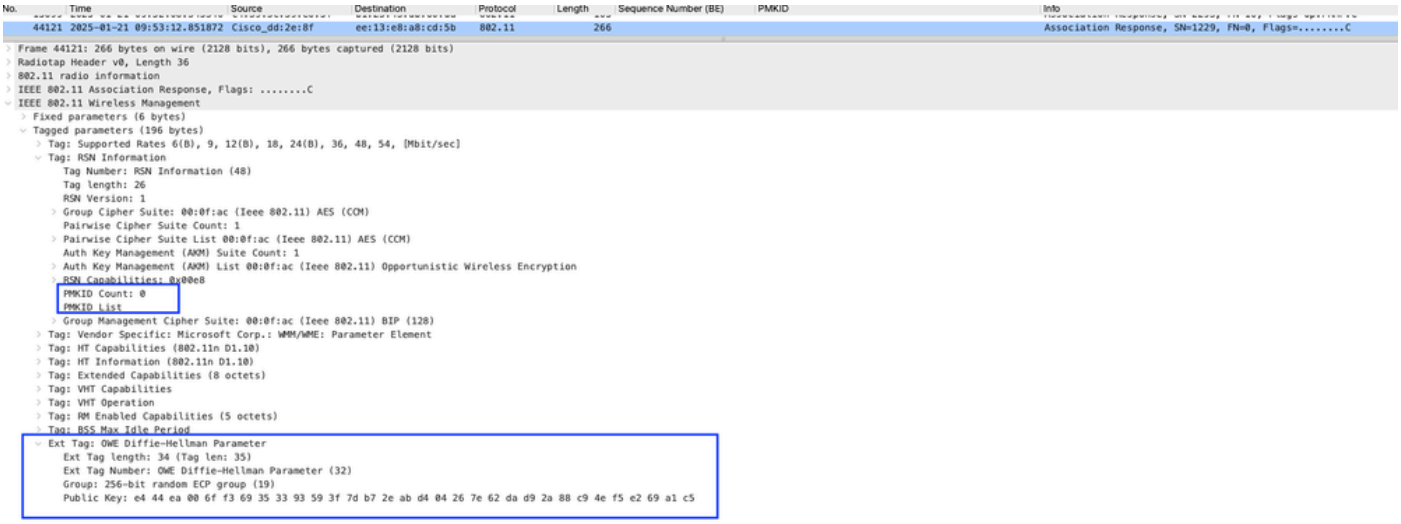

Bild-17: AP verwendet DH-Werte, um die neue PMKID zu generieren

In diesem Beispiel: AP und Client verwenden beim 4-Wege-Handshake dieselbe PMKID und checken M1- und M2-Nachrichten ein.

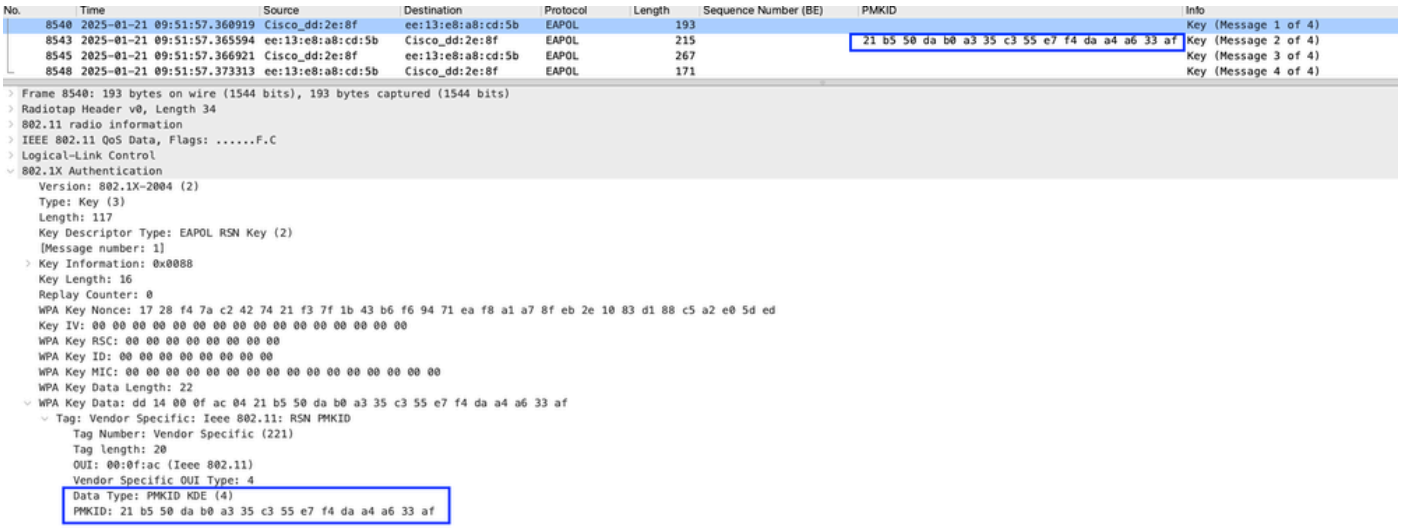

Bild 18: AP und Client mit derselben PMKID

In diesem Beispiel: Client, der dieselbe PMKID verwendet, aber AP, der eine andere PMKID verwendet, die er generiert hat, nachdem der Client gelöscht wurde, überprüfen Sie die Meldungen "M1 und M2".

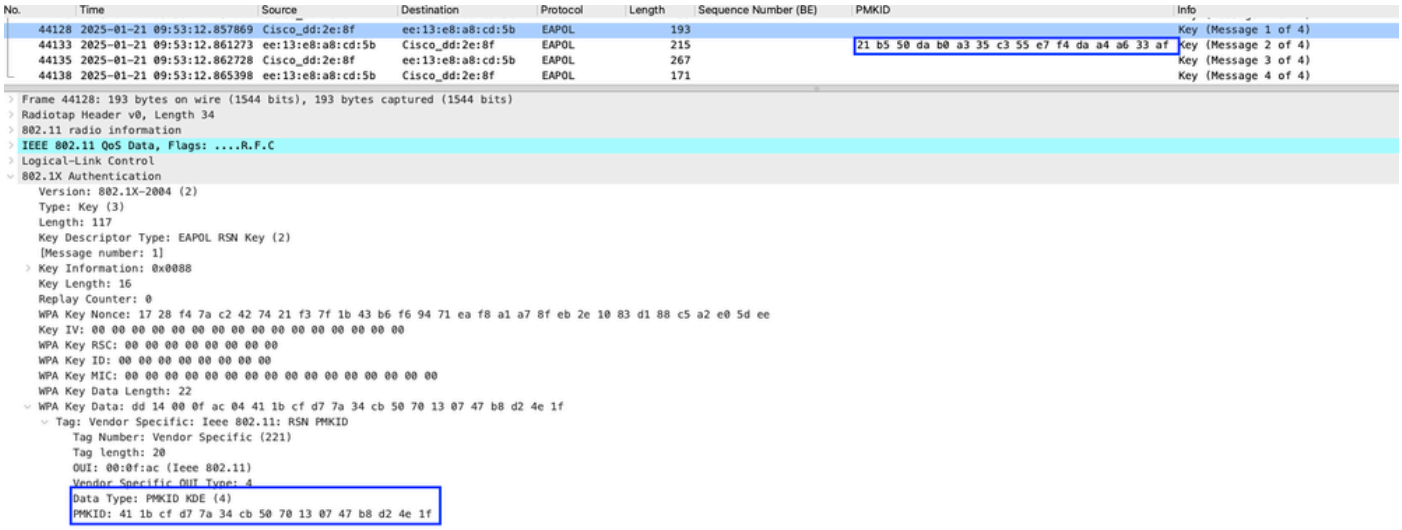

Bild-19: AP und Client mit unterschiedlicher PMKID

Aus interner RA-Verfolgung:

In diesem Beispiel: Der Client sendete DH-Parameter in der Zuordnungsanforderung, und der Access Point wurde verarbeitet als auf dem PMK generiert.

```
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
```

Anschließend hat derselbe Client, der sich mit demselben Access Point verbindet, zu diesem Zeitpunkt keine neue PMKID generiert.

```
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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.