# Comprendre le flux de chiffrement sans fil opportuniste

## Table des matières



## Introduction

Ce document décrit le flux de transition OWE et comment il fonctionne sur le contrôleur LAN sans fil (WLC) Catalyst 9800.

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comment configurer le WLC 9800, le point d'accès (AP) pour le fonctionnement de base
- Comment configurer les profils WLAN et de stratégie.

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- C9800-80, Cisco IOS® XE 17.12.4 et également testé sous Cisco IOS® XE 17.9.6
- Modèle AP : C9136I, coché en mode de connexion locale et en mode de connexion flexible.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

## Description

- OWE (Opportunistic Wireless Encryption) est une extension de la norme IEEE 802.11 qui assure le cryptage du support sans fil. L'objectif de l'authentification basée sur OWE est d'éviter une connectivité sans fil ouverte et non sécurisée entre les points d'accès et les clients.
- L'OWE utilise le cryptage basé sur les algorithmes Diffie-Hellman pour configurer le cryptage sans fil.
- Avec OWE, le client et le point d'accès effectuent un échange de clés Diffie-Hellman pendant la procédure d'accès et utilisent le secret par paire résultant avec la connexion en 4 étapes.
- L'utilisation d'OWE améliore la sécurité du réseau sans fil pour les déploiements où des réseaux basés sur une clé prépartagée ouverte ou partagée sont déployés.

## Étapes

1. Configurez un WLAN OUVERT sans chiffrement/sécurité et activez la diffusion.
2. Configurez un autre SSID avec les paramètres de sécurité OWE et mappez le numéro d'ID WLAN OUVERT dans transition-mode-wlan-id. Désactivez l'option SSID de diffusion dans ce SSID de transition OWE.
3. Mappez le numéro d'ID WLAN de transition OWE dans le champ OPEN WLAN "transition-mode-wlan-id".

## Détails de Lab Repro

- Nom SSID ouvert : DOUÉ DE TOUS

- Nom SSID de transition OWE : Transition OWE
- BSSID d'OPEN-OWE : 40:ce:24:dd:2e:87
- BSSID de OWE-Transition : 40:ce:24:dd:2e:8f

# DÉBIT DE LA DETTE

1. Les balises peuvent être diffusées pour un SSID OUVERT. Vous pouvez le voir par son nom SSID dans AIR PCAP.
2. Nous pouvons également voir le SSID activé de sécurité cachée avec le nom "Wildcard" au lieu de son propre nom SSID dans AIR PCAP.
3. Une fois que les clients reçoivent la trame de balise pour le SSID OUVERT, s'il a ou prend en charge OWE, il peut commencer à envoyer une requête de sonde au SSID de transition OWE (qui est le SSID activé par la sécurité au lieu du SSID OUVERT).
4. Les clients pris en charge par OWE peuvent obtenir une réponse de sonde du SSID de transition.
5. L'authentification OPEN peut se produire entre le client et le point d'accès.
6. Le client peut envoyer une requête d'association au point d'accès avec des détails d'échange de clé DH et utiliser le secret par paire résultant pour la connexion en 4 étapes.
7. AP peut envoyer une réponse d'association.
8. Un échange en quatre étapes peut avoir lieu entre le point d'accès et le périphérique client.
9. Une fois la gestion des clés réussie, L2 PSK peut réussir.
10. Le client peut obtenir l'adresse IP auprès de DHCP, ARP, etc.
11. Le client peut passer à l'état EXÉCUTÉ.
12. Si les périphériques clients ne prennent pas en charge OWE, il peut alors envoyer une requête de sonde au SSID OUVERT lui-même et obtenir directement l'adresse IP avant de passer à l'état RUN.

## trame Beacon d’origine

- Ici, AIR PCAP montre que, la diffusion SSID "OPEN-OWE" (Beacon Frame). Qui contient des détails SSID de transition et il a appelé "OWE-Transition".


Image-1 : Trame de balise du SSID OUVERT

## Balises SSID masquées

- Selon la configuration WLAN, la « diffusion » est désactivée pour ce SSID « OWE-Transition », cependant, vous pouvez voir les balises SSID masquées dans AIR PCAP qui contiennent le nom SSID « Wildcard ». Cependant, si vous vérifiez ce paquet, il contient des détails sur OWE-Transition.
- Obtenez le BSSID du SSID masqué en utilisant ce paquet, comme « 40:ce:24:dd:2e:8f » et recherchez-le dans la capture de paquets.
- Dans ce paquet, il montre que, SSID "Missing" et il contient son SSID de transition comme "OPEN-OWE" et son BSSID "40:ce:24:dd:2e:87".

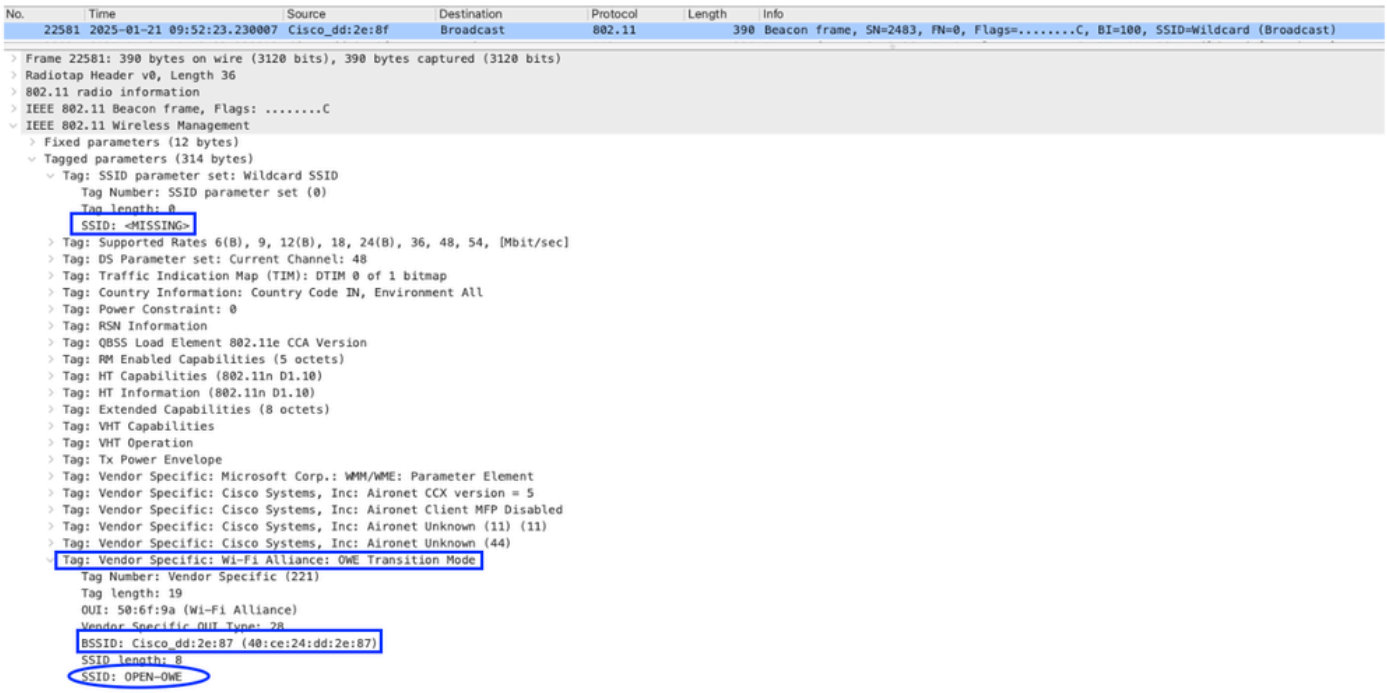

Image-2 : SSID masqué - Transition OWE

## Requête de sondage envoyée du client au SSID de transition OWE

- Sur la base du SSID de la trame de balise « OPEN-OWE », le client apprend à connaître les autres détails du SSID dont il a besoin pour se connecter, dans ce scénario, il s'agit de « OWE-Transition ». Si le client est capable de prendre en charge le cryptage OWE, il peut alors envoyer la demande de sonde au SSID « OWE-Transition » et obtenir une réponse.
- Requête d'analyse envoyée au BSSID OWE-Transition « 40:ce:24:dd:2e:8f » et une réponse a été obtenue. À l'intérieur de ce paquet de réponse de sonde également, vous pouvez voir les détails du SSID OPEN-OWE.

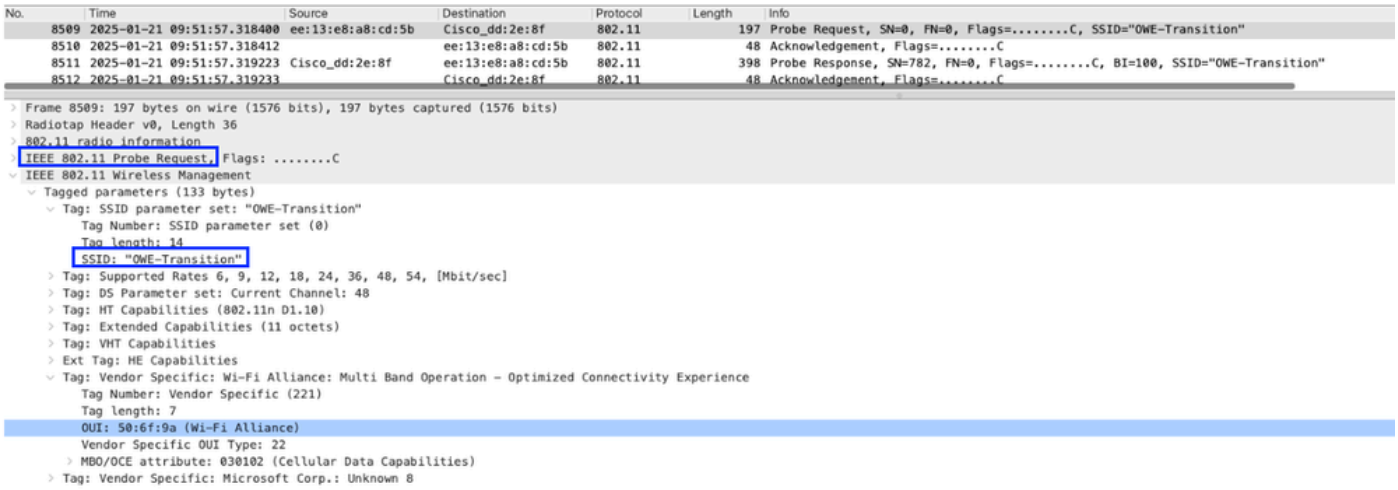


Image-3 : Requête de sonde

## Réponse d'enquête envoyée du point d'accès au client

- Le client a reçu une réponse de sonde pour le SSID « OWE-Transition », mais il a ses détails SSID d'origine « OPEN-OWE » dans WiFi Alliance.

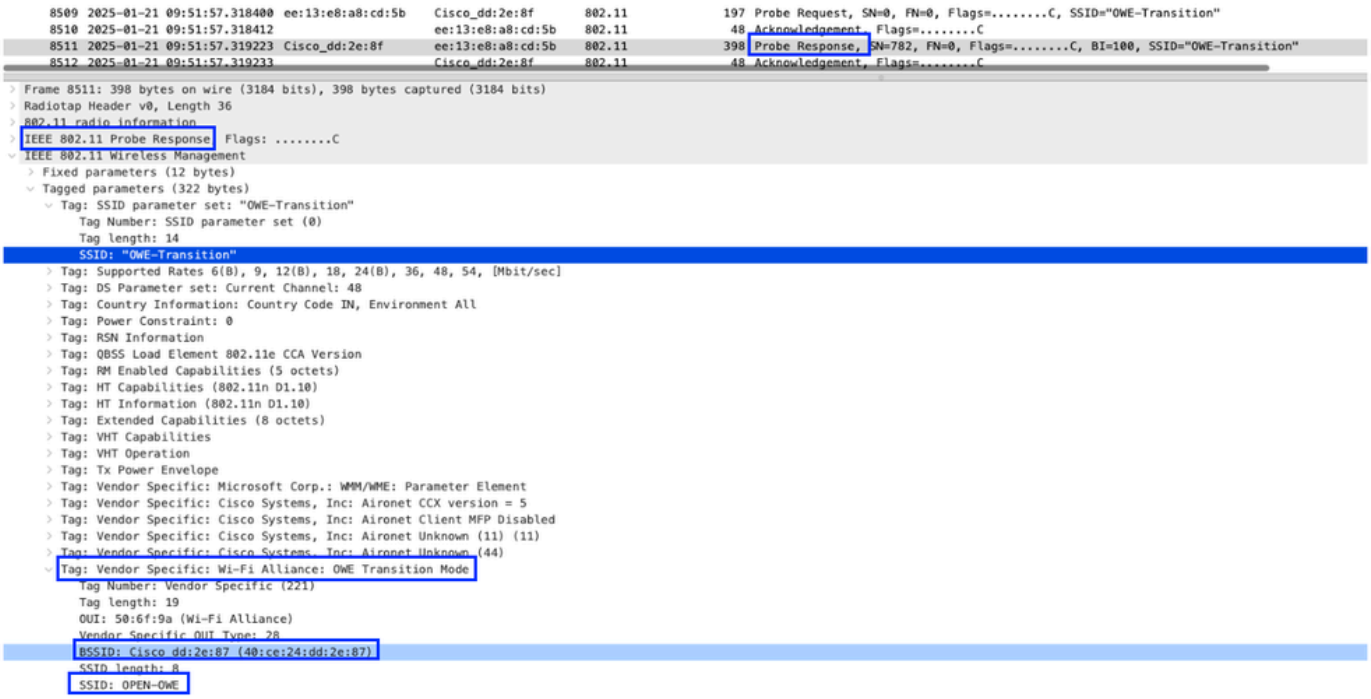


Image-4 : Réponse De Sonde

## Authentification ouverte

- Après avoir obtenu la réponse de sonde, l'authentification OPEN peut se produire entre le client et le point d'accès pour vérifier les détails/capacités du wifi du client, avant l'association.

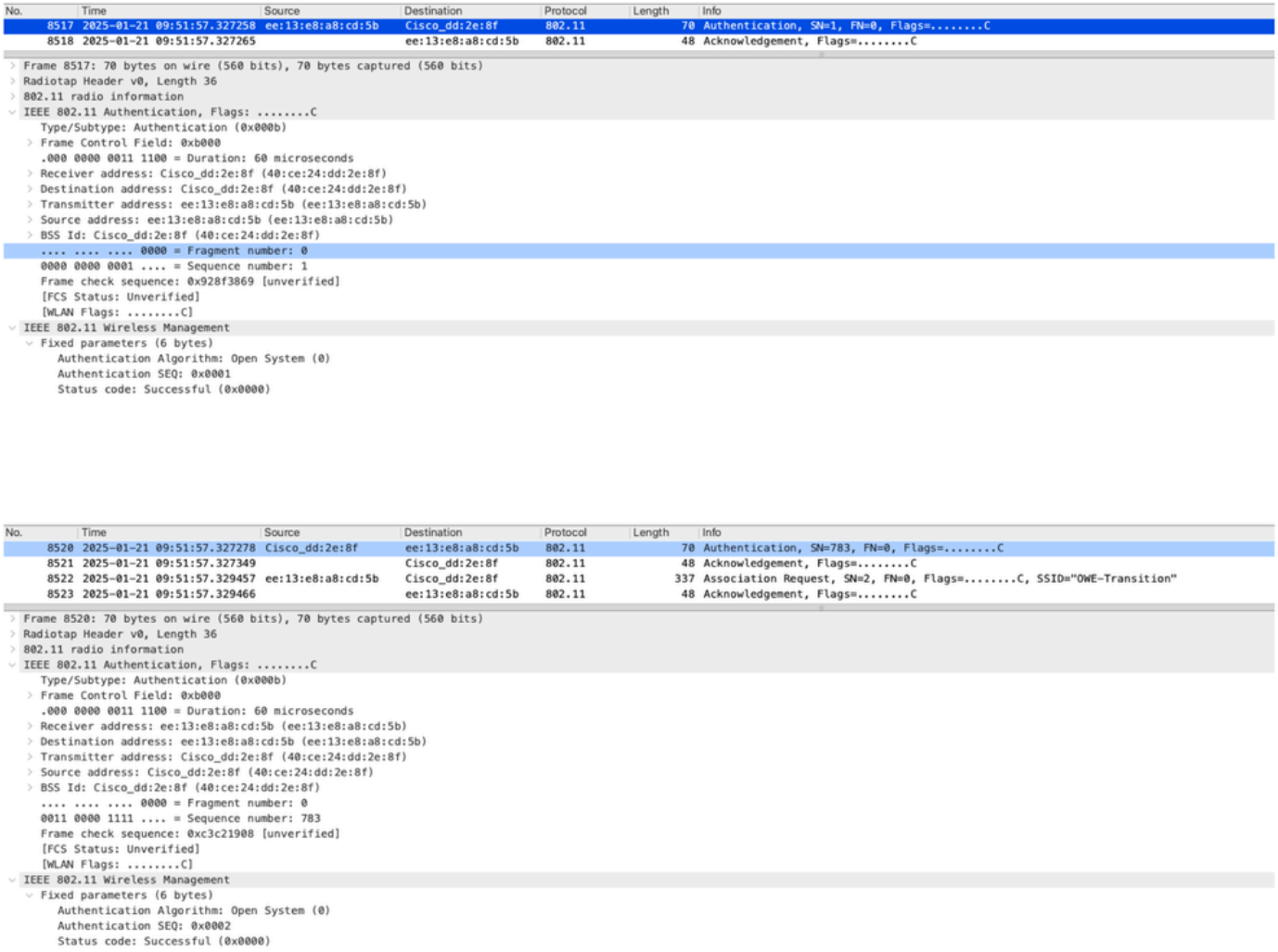


Image-5 : Authentification OPEN après une analyse réussie

## Demande d'association du client au point d'accès

- Dans ce paquet, notez que le client peut joindre une valeur de paramètre Diffie-Hellman pour le chiffrement.

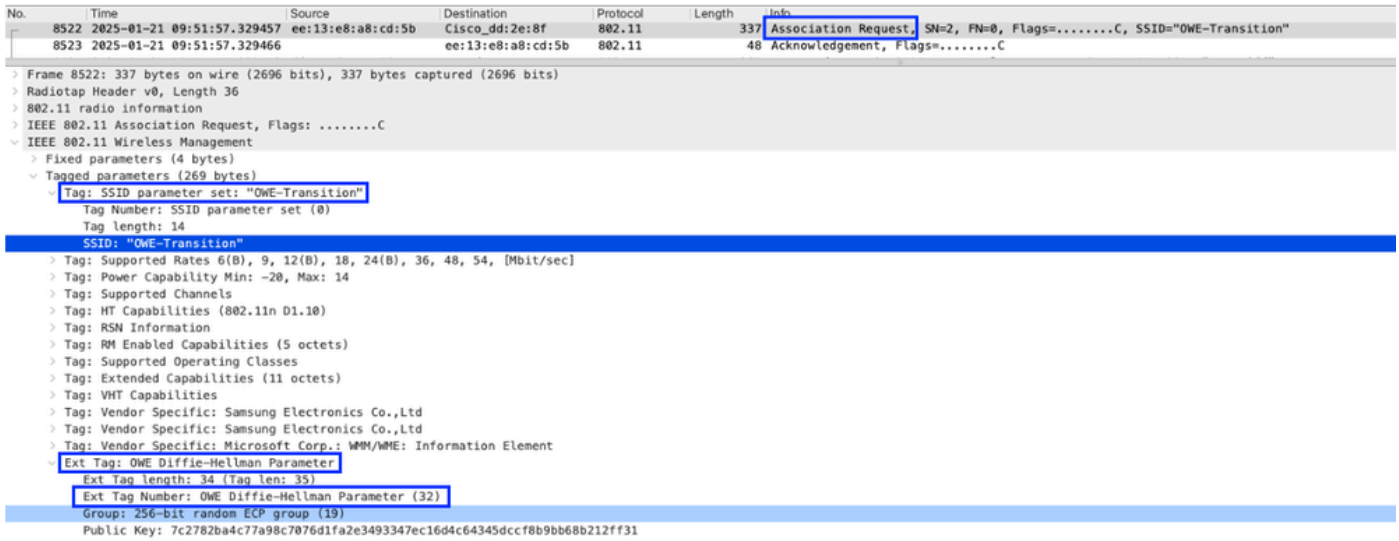


Image-6 : Demande D'Association

- Dans RA trace, vous pouvez commencer à voir les journaux du client depuis la phase d'association,

```
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
```

## Réponse d'association envoyée du point d'accès au client

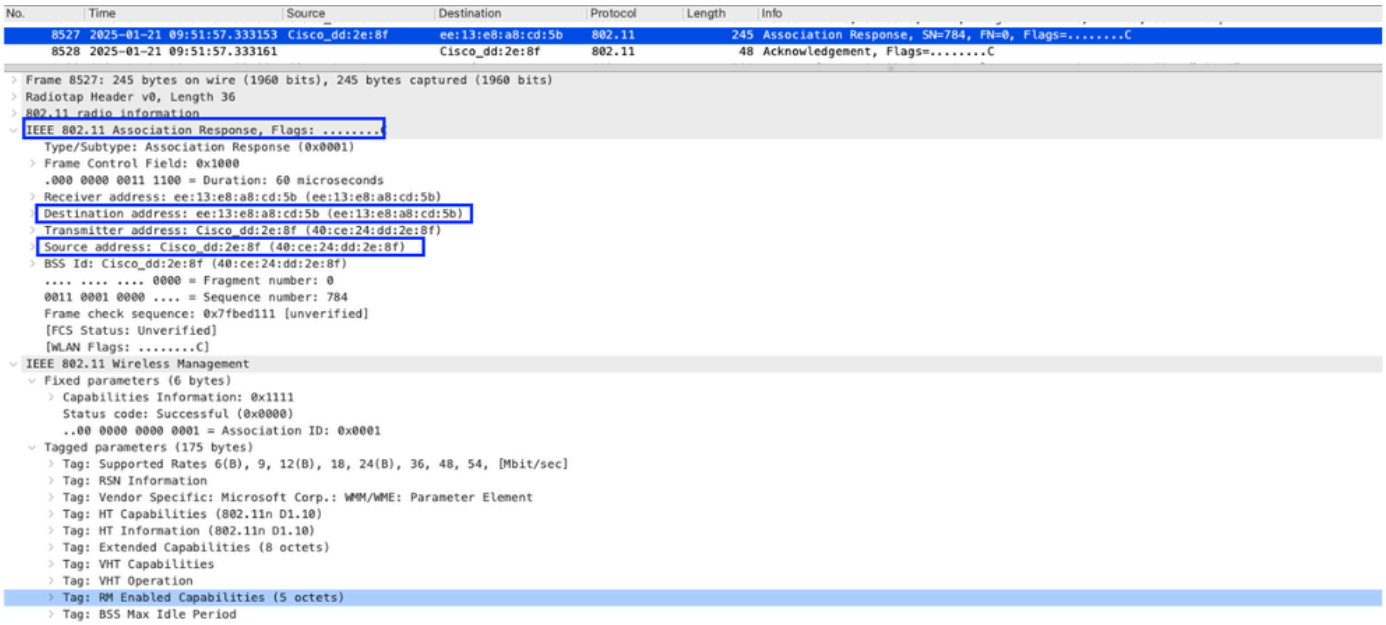


Image-7 : Réponse d'association

```
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
```

## Échange De Clés

Un échange en quatre étapes peut avoir lieu entre le point d'accès et le périphérique client.

Key-1 envoyé par AP

Clé 2 envoyée par le client

Key-3 envoyé par AP

Envoi de la clé 4 par le client

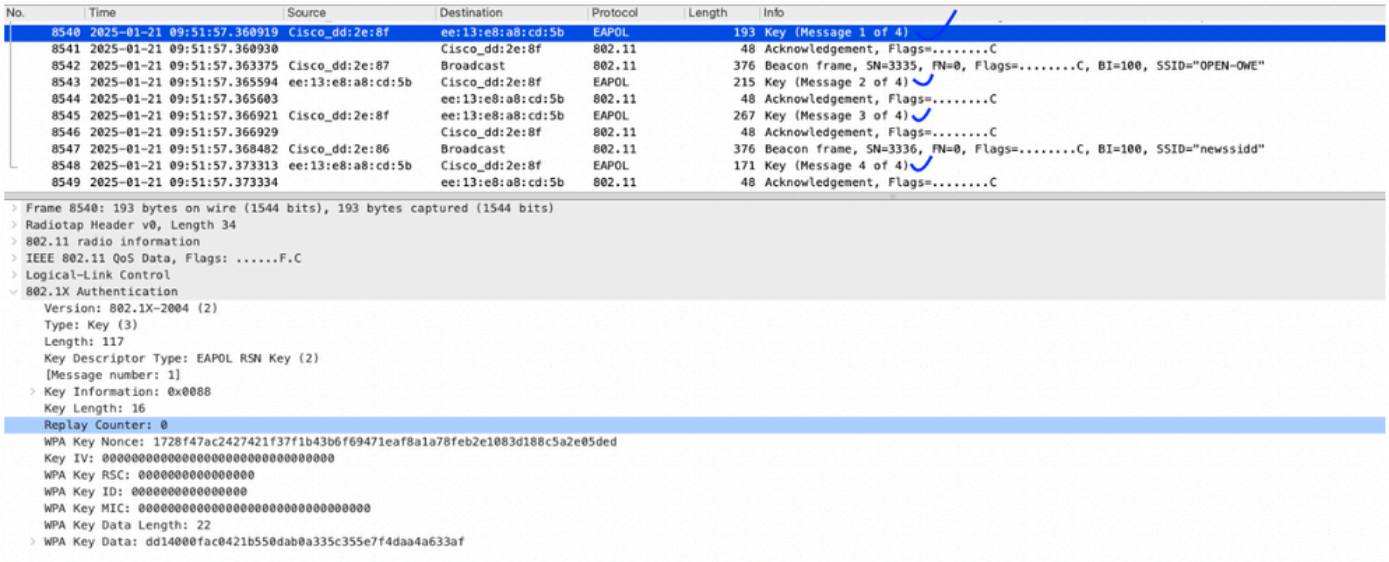


Image-8 : Connexion en quatre étapes

```
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
```

## Authentification L2 réussie

```
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
```

## État d’apprentissage IP

```
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 en état d'exécution

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

### Clients non pris en charge pour le cryptage OWE

- En examinant une trame de balise elle-même, les clients savent s’ils sont en mesure de prendre en charge cette méthode de chiffrement ou non. S'il n'est pas pris en charge, alors il peut simplement envoyer une demande d'enquête pour ouvrir le SSID « OPEN-OWE » et peut faire une authentification ouverte normale, obtenir une adresse IP, puis il peut passer à l'état RUN.

```
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
```

## information sur la transition rapide

- Nous sommes en mesure de configurer OWE uniquement dans l'authentification OPEN ou dans Webauth (CWA/LWA/EWA).
- FT n'est pas pris en charge dans la transition OWE.
- Si vous activez FT, vous obtenez ce message d'erreur,

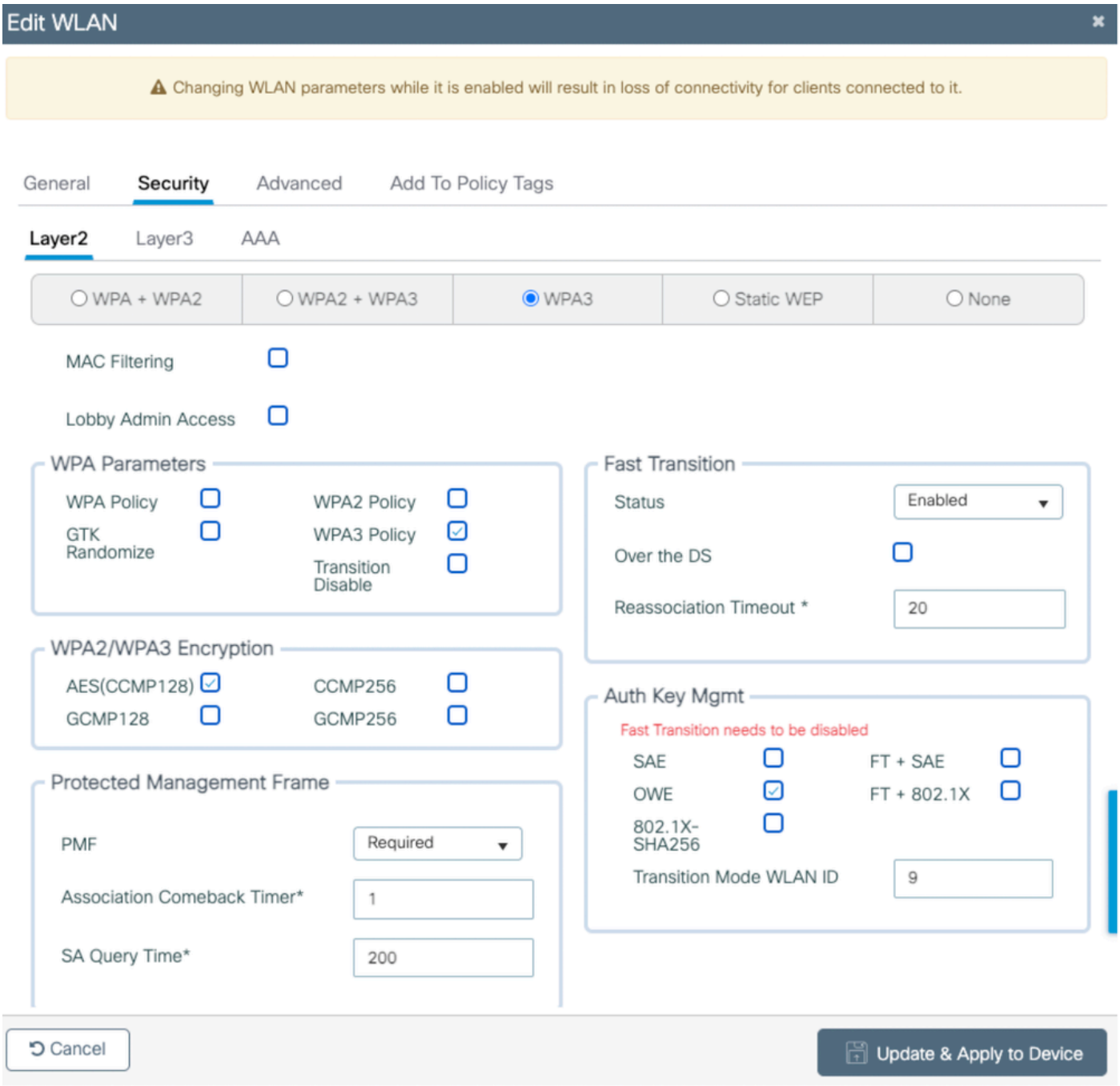


Image-9 : Message d'erreur lorsque nous activons FT dans OWE Transition SSID

# OWE n'est pas pris en charge avec PSK/dot1x

Nous ne sommes pas en mesure d'activer OWE dans ces combinaisons,

1. 802.1x ou FT+802.1x

2. PSK ou FT+PSK ou PSK-SHA256

3. SAE ou FT+SAE

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

Si vous essayez d'activer l'une de ces méthodes, vous pouvez obtenir le message d'erreur,

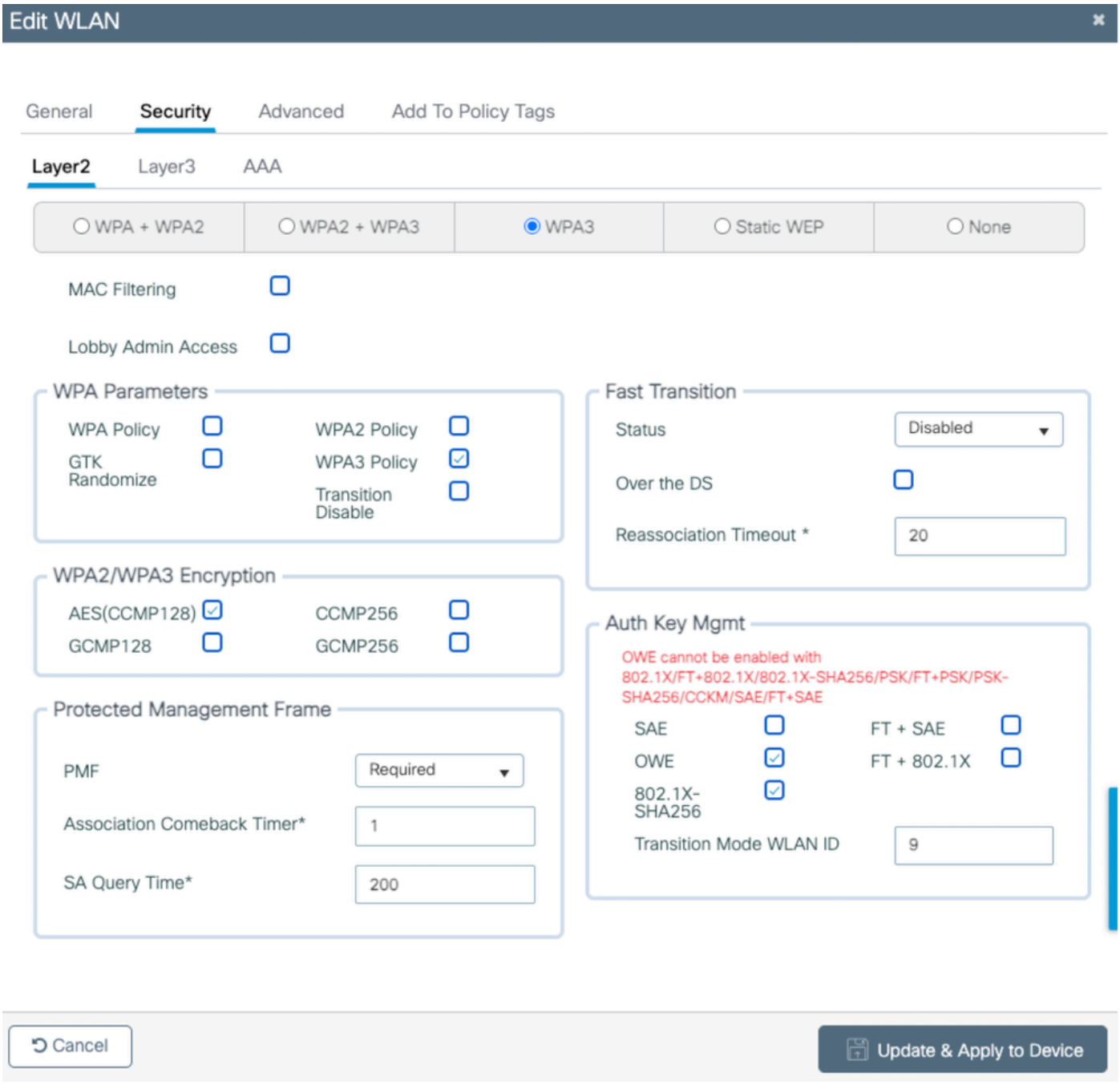


Image-10 : Message d'erreur obtenu lors de l'activation d'autres méthodes d'authentification dans OWE SSID

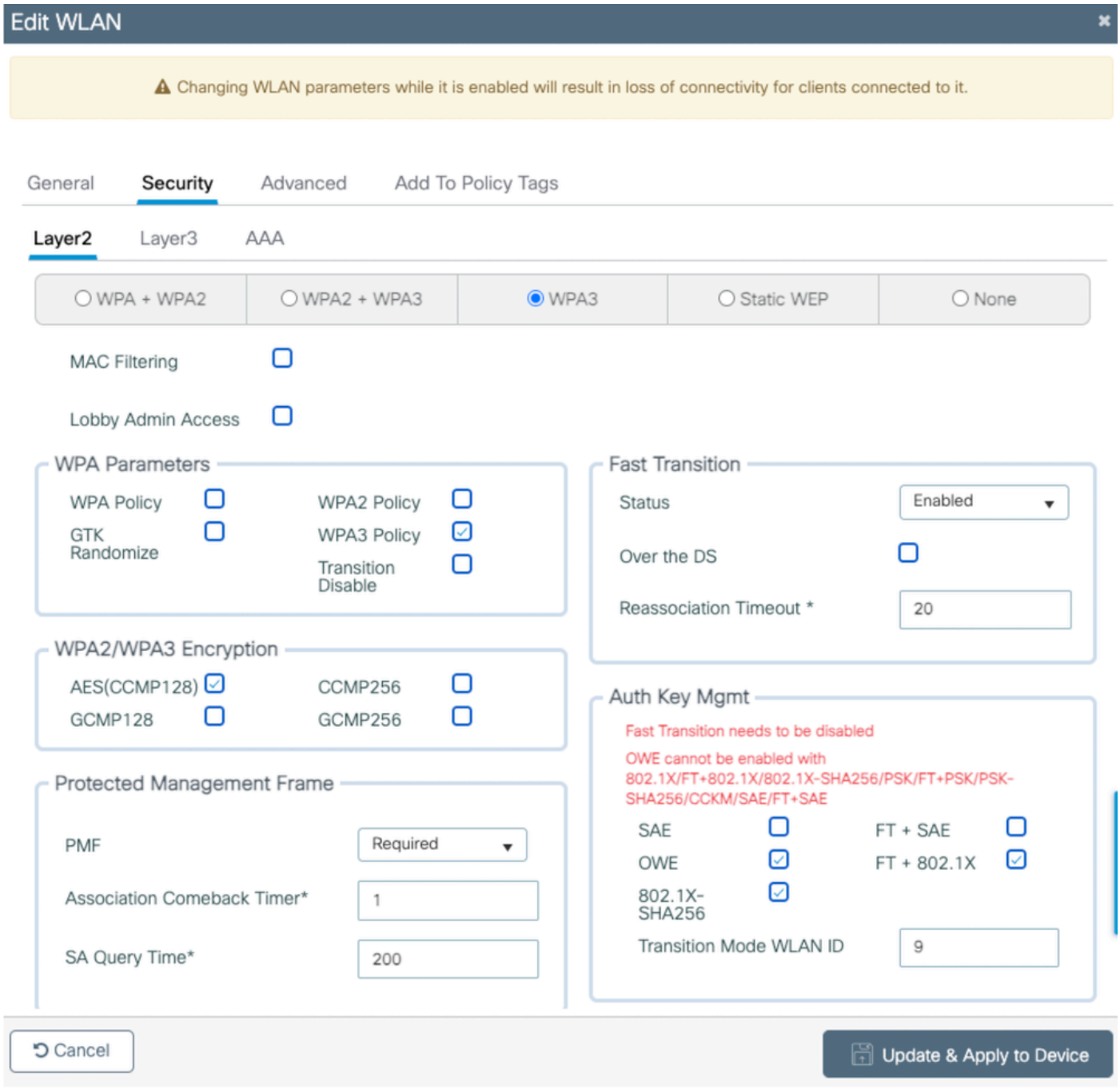


Image-11 : Message d'erreur lors de l'activation AKM

- Dans la version IOS de Cisco IOS® XE 17.9.6, vous pouvez voir l'option "OWE" sous AKM quand vous sélectionnez "WPA2+WPA3" cependant vous pouvez obtenir le message d'erreur, vous ne pouvez pas utiliser OWE avec cette combinaison.

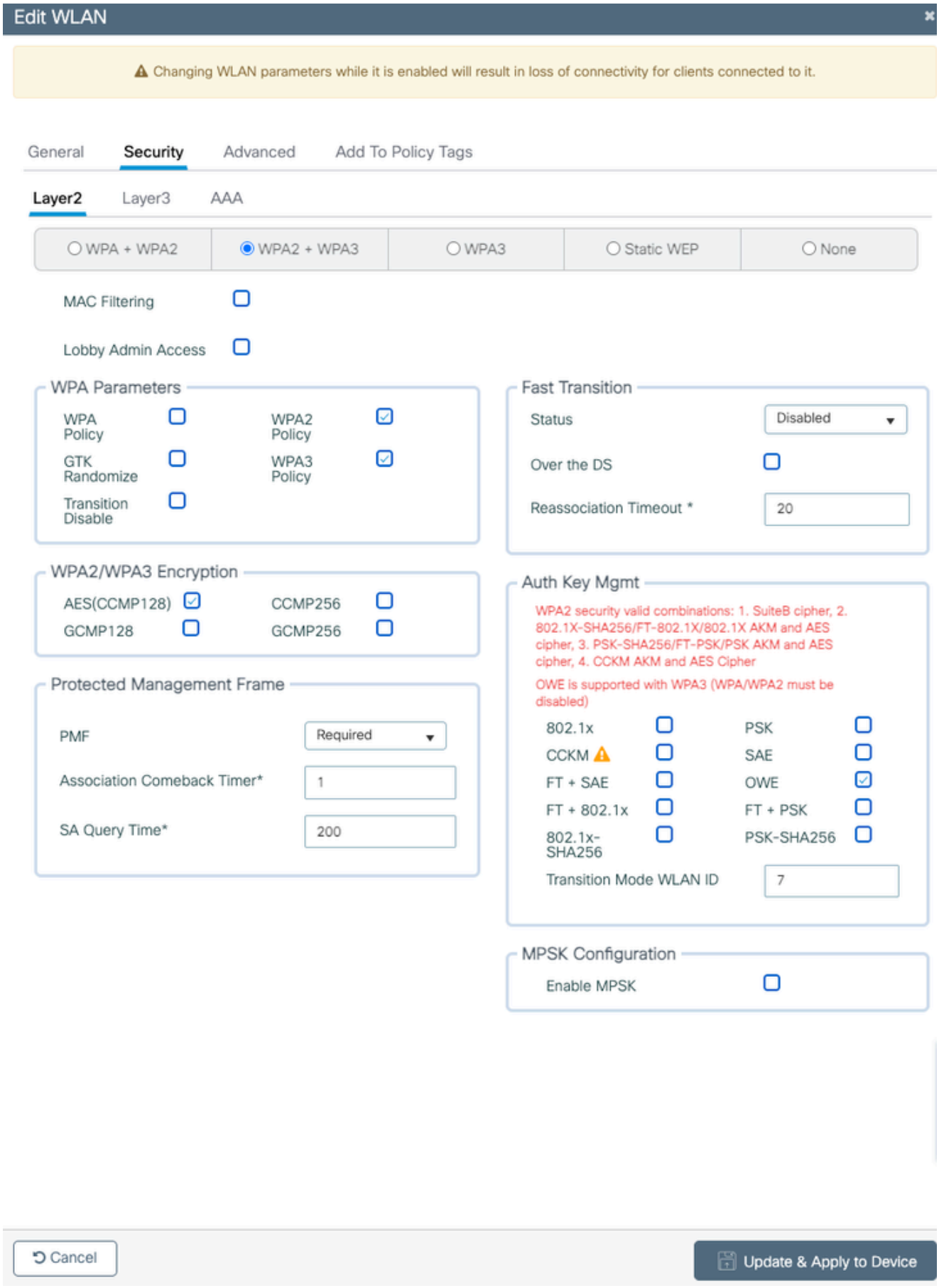


Image-12 : Message d'erreur lorsque nous choisissons WPA2+WPA3

- Dans la version 17.12.4 de Cisco IOS® XE, lorsque vous choisissez "WPA2+WPA3", vous

ne pouvez pas obtenir l'option "OWE" dans AKM,

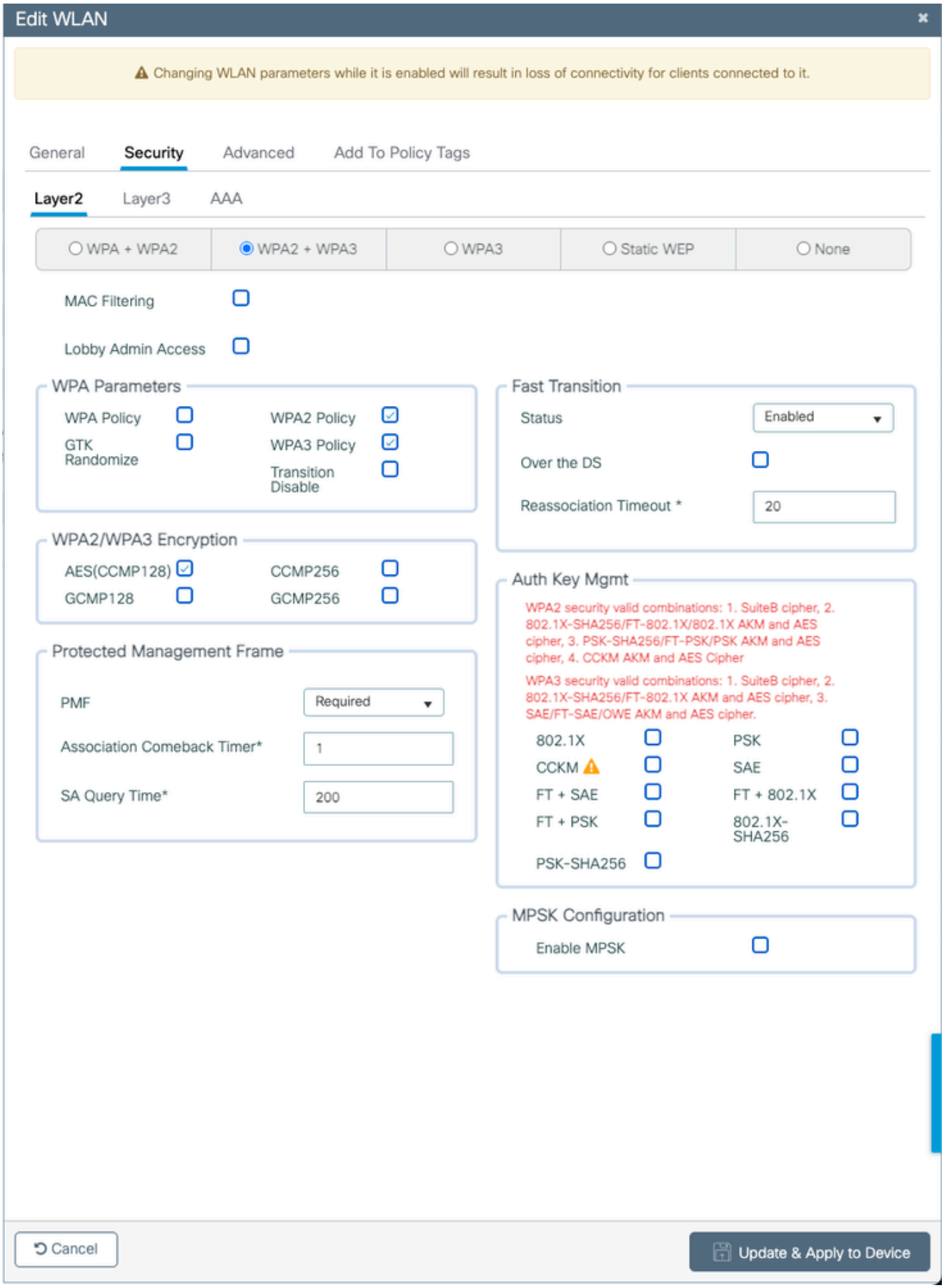


Image-13 : Message d'erreur - Option OWE non obtenue dans AKM

# Dépannage

1. Vérifiez les configurations dans les deux WLAN, dans OPEN SSID et dans OWE transition SSID doivent avoir transition WLAN ID mappé.
2. L'option de diffusion doit être désactivée dans le SSID de transition OWE, elle doit être activée uniquement dans le SSID OUVERT.
3. Vérifiez les méthodes d'authentification/cryptage/FT prises en charge décrites dans cet article.
4. Si les configurations sont correctes de l'extrémité WLC, que s'il vous plaît recueillir les journaux et les sorties nécessaires pour réduire le problème,

## RA Trace et EPC (capture PAcket intégrée)

Connexion à l'interface utilisateur graphique WLC -> Dépannage -> Suivi radioactif -> Ajouter l'adresse MAC wifi du client -> Cochez cette case pour les clients -> Démarrer

Connectez-vous à l'interface graphique WLC -> Dépannage -> Capture de paquets -> Ajouter un nouveau nom de fichier -> Choisissez l'interface de liaison ascendante et WMI VLAN/Interface -> Démarrer.

À partir de la machine client : Si possible, vous pouvez installer l'application Wireshark et collecter la capture de paquets en choisissant l'interface WiFi.

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

## BOUCHON PNEUMATIQUE

Vous pouvez le collecter en utilisant un ordinateur portable MAC ou en configurant l'un des points d'accès en mode renifleur, veuillez consulter ces liens,

Depuis un ordinateur portable MAC :

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

À partir de 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

Connectez un ordinateur portable (serveur Wireshark) au port du commutateur et il doit avoir l'application Wireshark installée dedans, ce serveur Wireshark doit avoir l'accessibilité à l'interface WMI WLC. Nécessité d'autoriser le protocole « 5555 ou 5000 ou 5556 » dans le pare-feu s'il se présente entre votre WLC et le serveur Wireshark.

Vérifiez s'il y a un « gscaler » installé dans ce PC où wireshark installé, si c'est que s'il est s'il vous

plaît "éteignez" et essayez, si c'est un pare-feu comme Windows Defender ou tout ce qui y est présent, s'il vous plaît désactiver ceux-ci et essayer de recueillir PCAP.

# Itinérance

Lorsque le client se déplace d'un point d'accès à un autre, il doit effectuer ces étapes,

- Nécessité d'envoyer une nouvelle association/association : dépend de la demande du client.
- Besoin d'envoyer les détails DH (Diffie-Helman) dans la demande d'association.
- Le client peut obtenir des détails DH dans la réponse d'association du point d'accès, en fonction de ce PMK est généré à la fois dans le client et le point d'accès.
- Un échange en quatre étapes peut avoir lieu entre le point d'accès et le client.
- Dans OWE, vous ne pouvez pas activer la fonction FT, donc la norme 802.11r n'est pas possible.
- À chaque fois, lorsque le client se déplace, il doit établir une connexion en quatre étapes après un échange DH en association.
- Client et point d'accès utilisant leur propre PMKID, il est unique pour chaque point d'accès et client.
- Si le client se connecte au même AP, il peut utiliser le même PMKID. Dans certains scénarios, si le client a été supprimé, AP peut générer un nouveau PMKID, mais le client utilise le même PMKID pour la connexion en 4 étapes.

Exemple :

Si le client se connecte au même AP, alors vous pouvez voir le même PMKID dans Association-Request et Association-Response. Dans la réponse Association, vous ne pouvez pas voir les détails DH s'il utilise le même PMKID.

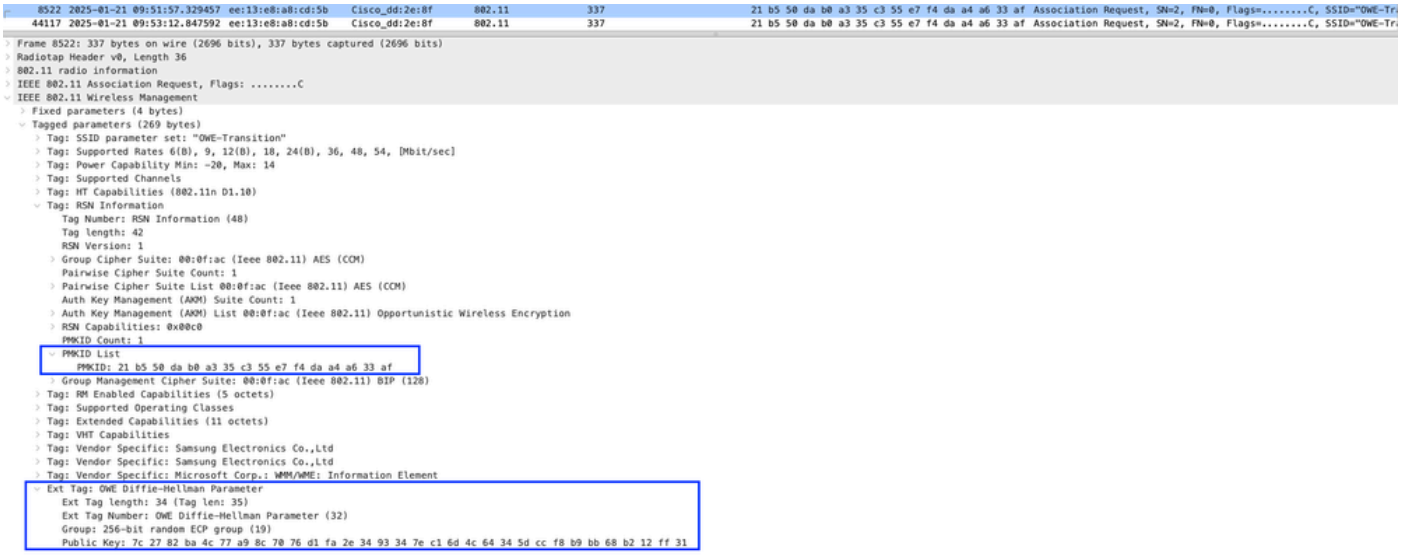


Image-14 : Utilisation du même PMKID


Image-15 : Réponse d'association avec le même PMKID

Pour le test, a supprimé ce client manuellement du WLC et il a été associé à nouveau au même AP, à ce moment, le client envoie un même PMKID mais AP envoie des détails DH dans la réponse d'association.

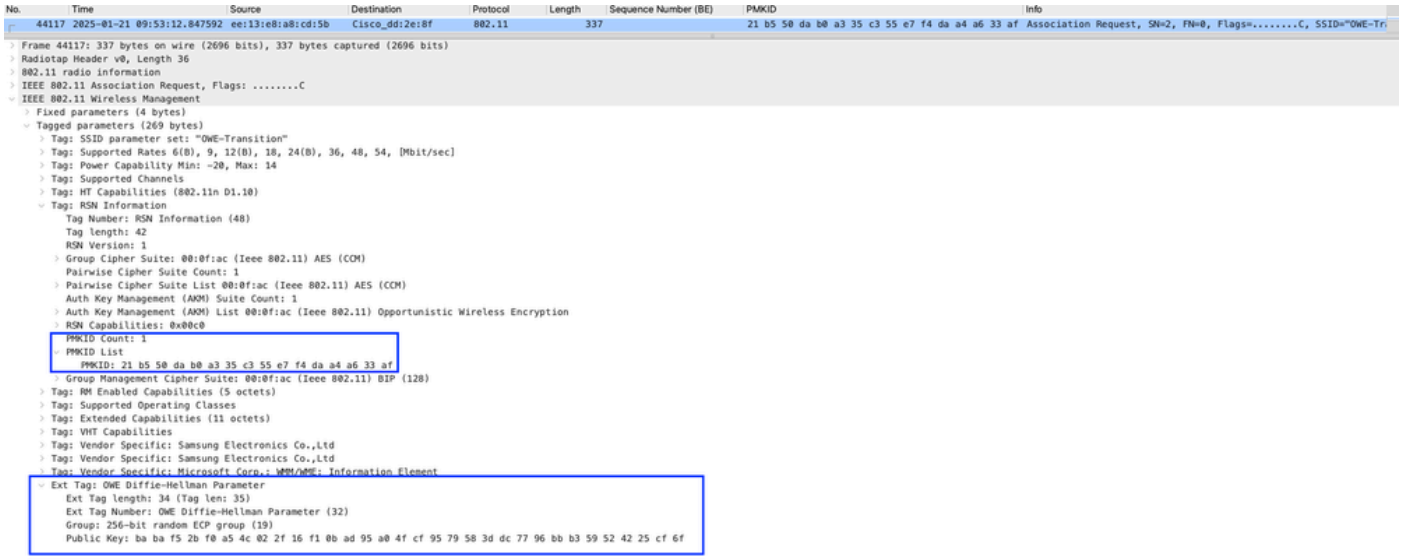


Image-16 : Après la suppression, le client a envoyé le même PMKID avec les détails DH

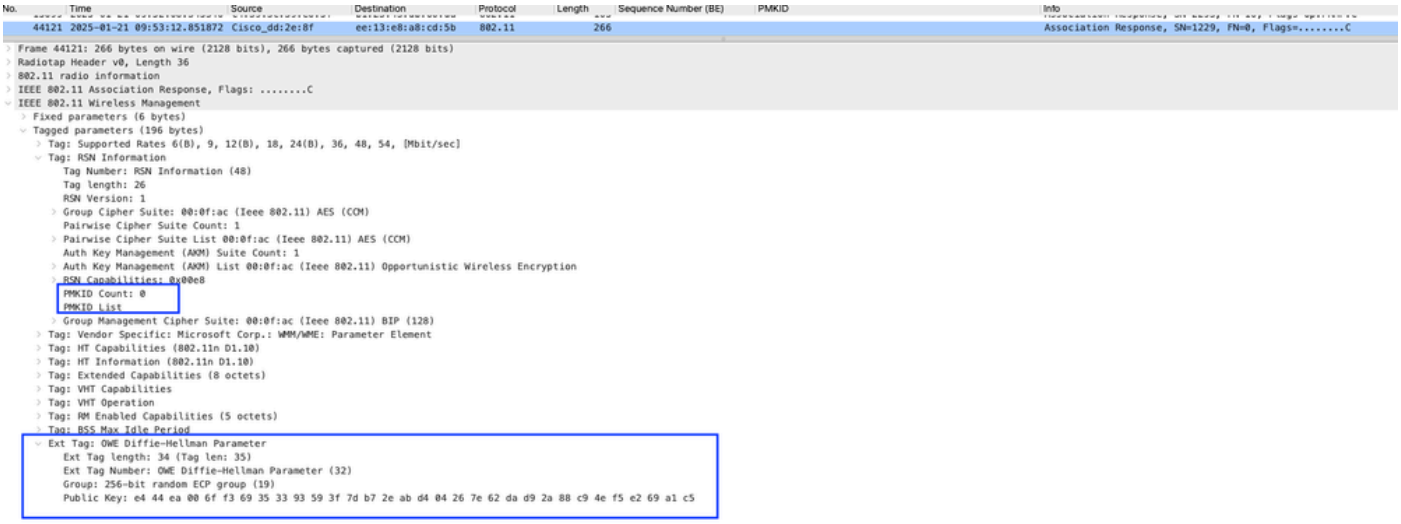


Image-17 : Le point d'accès utilise des valeurs DH pour générer son nouveau PMKID

Dans cet exemple : Le point d'accès et le client utilisent le même PMKID lors de la connexion en 4 étapes. Consultez les messages « M1 et M2 ».

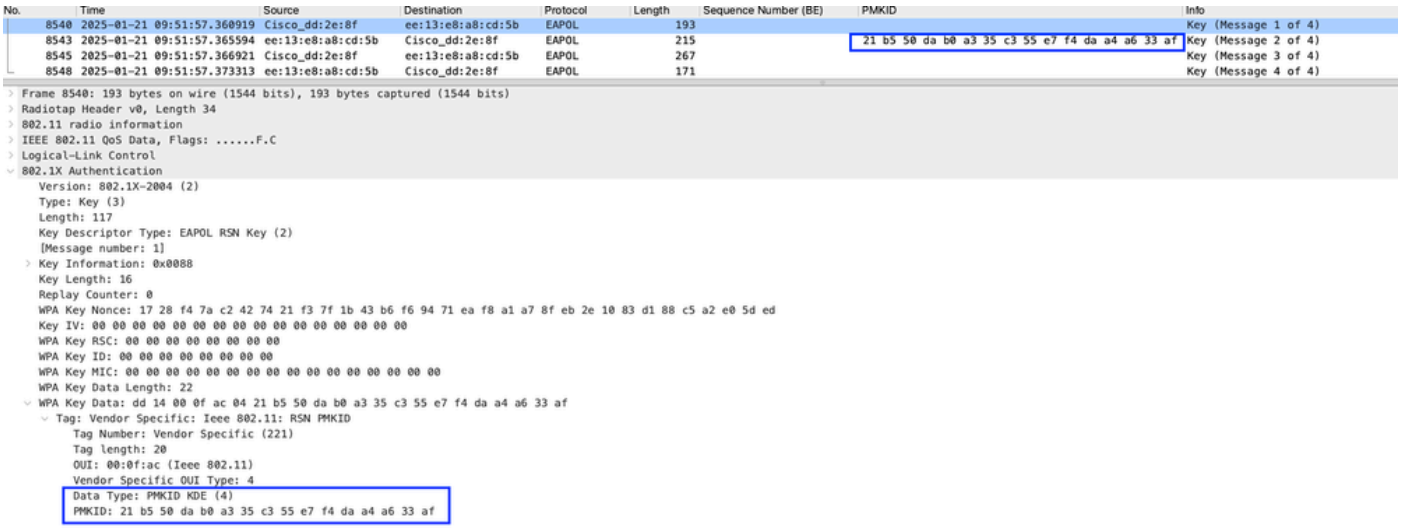


Image- 18 : AP et client utilisant le même PMKID

Dans cet exemple : Le client utilisant le même PMKID mais AP utilisant un PMKID différent qu'il a généré après la suppression du client, cochez les messages "M1 et M2".

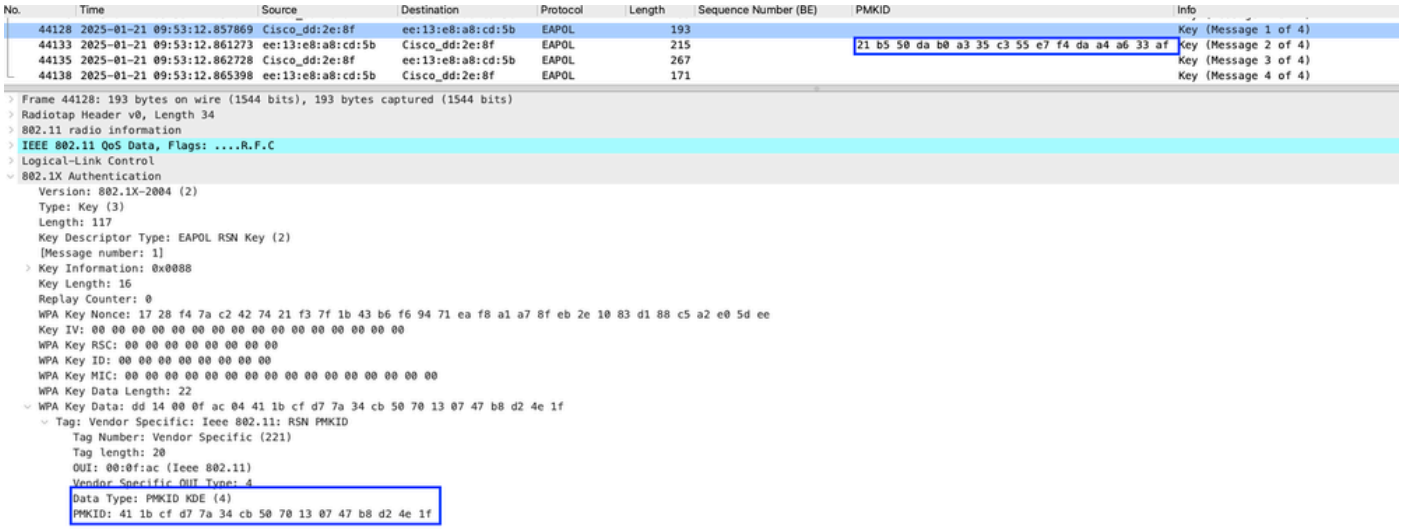


Image-19 : AP et client utilisant un PMKID différent

À partir de la trace RA interne :

Dans cet exemple : Le client a envoyé des paramètres DH dans la demande d'association et le point d'accès a traité la PMK.

```
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
```

Après cela, le même client se connectant au même AP, à ce moment-là, AP n'a pas généré de nouveau PMKID,

```
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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.