Begrijp opportunistische draadloze encryptiestroom

Inhoud

Inleiding

Dit document beschrijft de OWE-overgangsstroom en hoe het werkt op de Catalyst 9800 draadloze LAN-controller (WLC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Hoe de 9800 WLC, het access point (AP) te configureren voor basisbediening
- Hoe WLAN- en beleidsprofielen te configureren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C9800-80, Cisco IOS® XE 17.12.4 en ook getest in Cisco IOS® XE 17.9.6
- AP-model : C9136I, ingeschakeld in zowel de lokale als de flex-verbindingsmodus.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Beschrijving

- OWE (Opportunistic Wireless Encryption) is een uitbreiding van IEEE 802.11 die encryptie voor het draadloze medium verstrekt. Het doel van op OWE gebaseerde verificatie is om open onbeveiligde draadloze connectiviteit tussen de AP's en clients te voorkomen.
- De OWE gebruikt de op Diffie-Hellman algoritmen gebaseerde Cryptografie om de draadloze encryptie in te stellen.
- Met OWE voeren de client en AP tijdens de toegangsprocedure een Diffie-Hellman sleuteluitwisseling uit en gebruiken ze het resulterende paarsgewijze geheim met de 4-voudige handdruk.
- Het gebruik van OWE verbetert de draadloze netwerkbeveiliging voor implementaties waar op Open of gedeelde PSK gebaseerde netwerken worden geïmplementeerd.

Stappen

1. Configureer één OPEN WLAN zonder encryptie/beveiliging en schakel het uitzenden in.
2. Configureer een andere SSID met OWE-beveiligingsinstellingen en wijs het OPEN WLAN-id-nummer toe in de overgangsmodus-WLAN-id. Schakel de optie broadcast-SSID uit in deze OWE-overgangsSSID.
3. Wijs het OWE-overgangsWLAN-id-nummer toe in het veld OPEN WLAN "transition-mode-WLAN-id".

Details van Lab Repro

- Naam SID openen: OPENLIJK

- Naam OWE-transitie SSID: OWE-transitie
- BASIS VAN OPEN OWE: 40:ce:24:dd:2 e:87
- BSSID van OWE-Transition: 40:ce:24:dd:24e:81f

DEBET FLOW

1. De bakens kunnen voor OPEN SSID worden uitgezonden. U kunt het door zijn naam van SSID in AIR PCAP zien.
2. We kunnen ook de verborgen veiligheid toegelaten SSID met de naam "Wildcard" in plaats van zijn eigen SSID naam in AIR PCAP zien.
3. Zodra de cliënten het beacon frame voor OPEN SSID ontvangen, als het OWE heeft of steunt, dan kan het beginnen met het verzenden van sonde verzoek naar OWE transitie SSID (dat is dat veiligheid toegelaten SSID in plaats van OPEN SSID).
4. Door OWE ondersteunde clients kunnen een sonderrespons krijgen van transitie SSID.
5. Verificatie VOOR OPENEN kan plaatsvinden tussen client en AP.
6. De klant kan associatieverzoek verzenden naar de AP met DH-sleuteluitwisselingsdetails en het resulterende paarsgewijze geheim gebruiken voor 4-weg handdruk.
7. AP kan associatiereactie verzenden.
8. Vier-manier handdruk kan gebeuren tussen AP en cliënt apparaat.
9. Na succesvol sleutelbeheer kan L2 PSK succesvol zijn.
10. De client kan IP verkrijgen van DHCP, ARP etc.
11. De client kan naar RUN status gaan.
12. Als client-apparaten die geen OWE ondersteunen, dan kan het sonde-verzoek verzenden naar OPEN SSID zelf en kan het direct IP krijgen dan kan het gaan naar RUN-status.

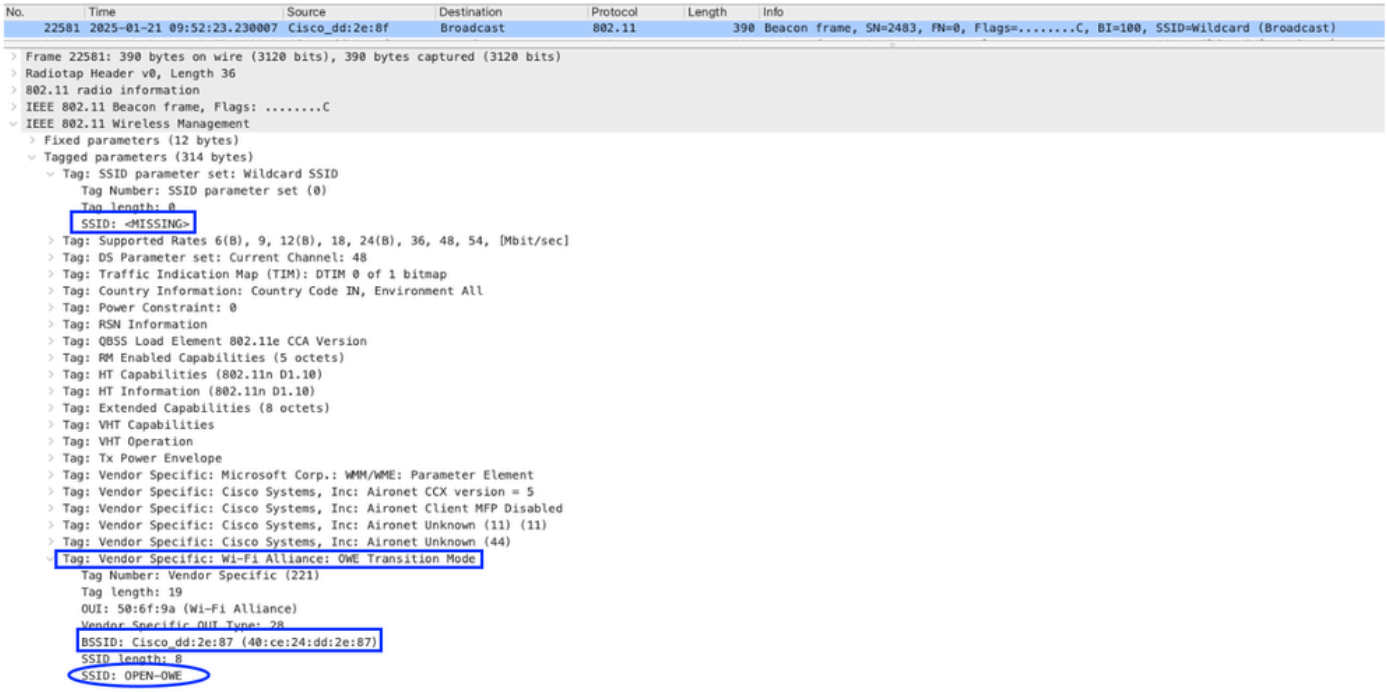
Origineel beacon frame

- Hier laat AIR PCAP dat zien, de SSID "OPEN-OWE"-uitzending (Beacon Frame). Dat bevat transitie-SSID-details en het noemde "OWE-Transition".

Afbeelding 1: Beacon Frame van OPEN SSID

Verborgen SSID-bakens

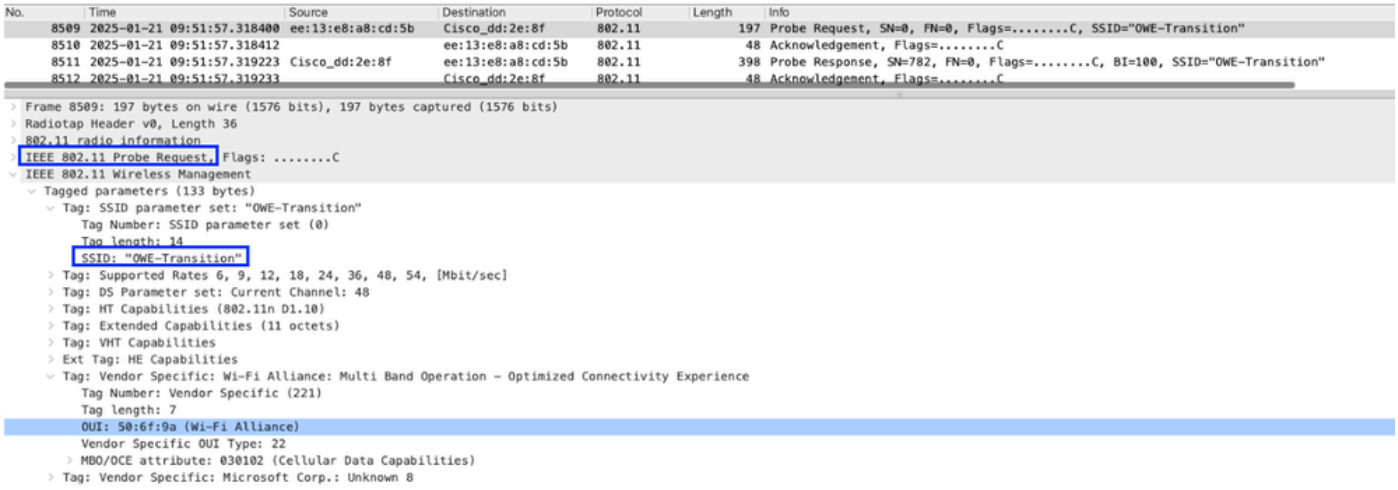
- In de WLAN-configuratie is "broadcast" uitgeschakeld voor deze "OWE-Transition"-SSID, maar u kunt verborgen SID-bakens in AIR PCAP zien die de SSID-naam "Wildcard" bevatten. Als u dat pakket controleert, bevat het echter OWE-Overgangdetails.
- Krijg de BSSID van verborgen SSID door dit pakket, zoals "40:ce:24:dd:2e:8f" te gebruiken en zoek het in pakketopname.
- In dit pakket, toont het dat, SSID "ontbreekt" en het bevat zijn overgang SSID als "OPEN-OWE" en zijn BSSID "40:ce:24:dd:2e:87".



Afbeelding 2 : Verborgen SSID - OWE Transition

Probe-aanvraag verzonden van client naar OWE Transition SSID

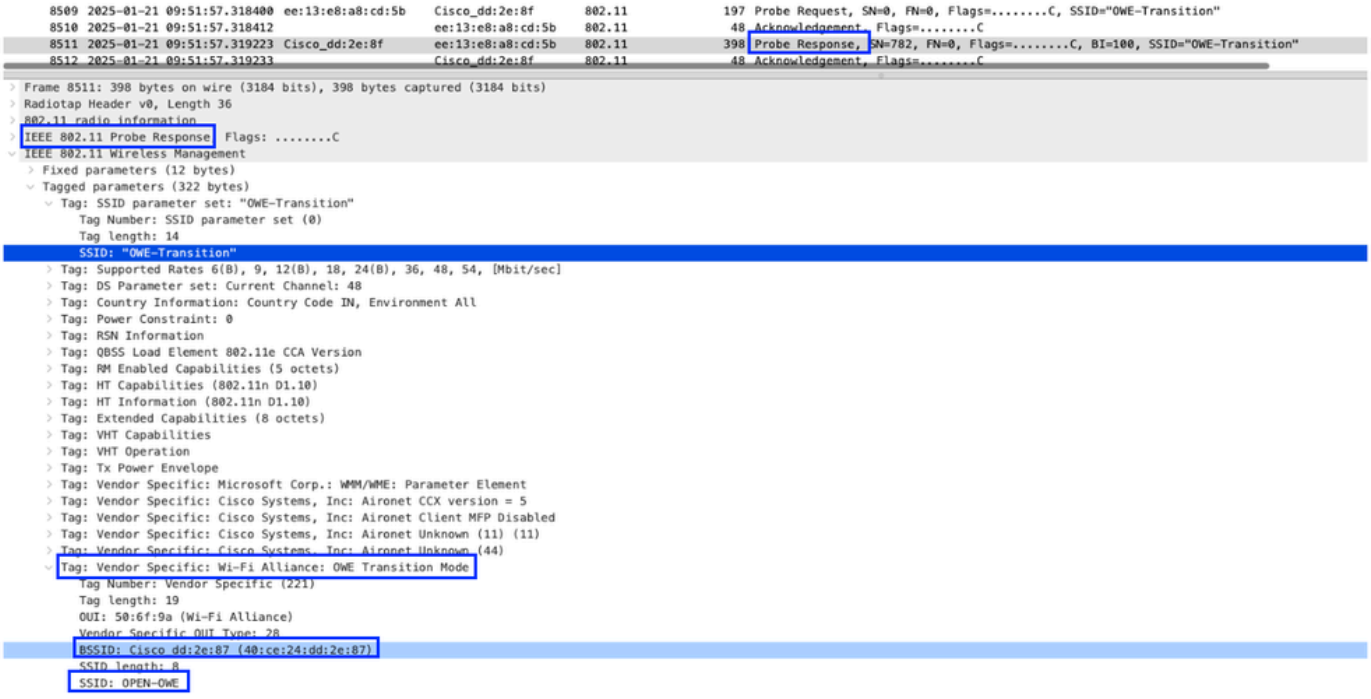
- Gebaseerd op het beacon frame "OPEN-OWE" SSID, komt de client de andere SSID details te kennen die het nodig heeft om te verbinden, in dit scenario, het is "OWE-Transition". Als client OWE-encryptie kan ondersteunen, dan kan het de sonderaanvraag naar "OWE-Transition" SSID sturen en een antwoord krijgen.
- Probe-aanvraag verzonden naar OWE-Transition BSSID "40:ce:24:dd:2e:8f" en kreeg een antwoord. Ook in dit reactiepakket voor sonde kunt u Open-OWE SSID-details zien.



Afbeelding 3: Probe-aanvraag

Probe Response verzonden van AP naar client

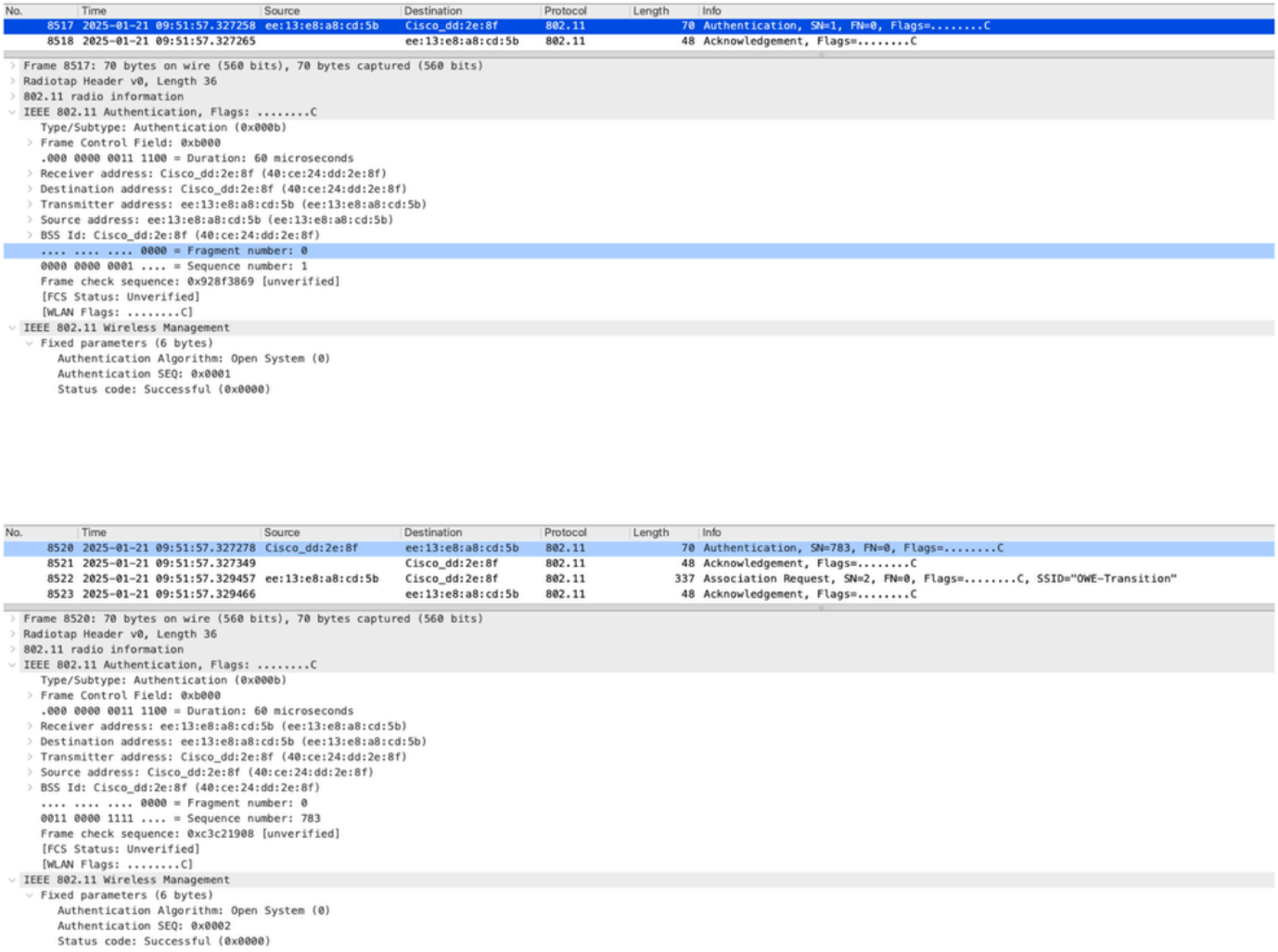
- De client heeft een probe-antwoord ontvangen voor de SSID "OWE-Transition", maar heeft zijn oorspronkelijke SSID-details "OPEN-OWE" in WiFi Alliance.



Afbeelding 4 : Probe Response

VERIFICATIE OPENEN

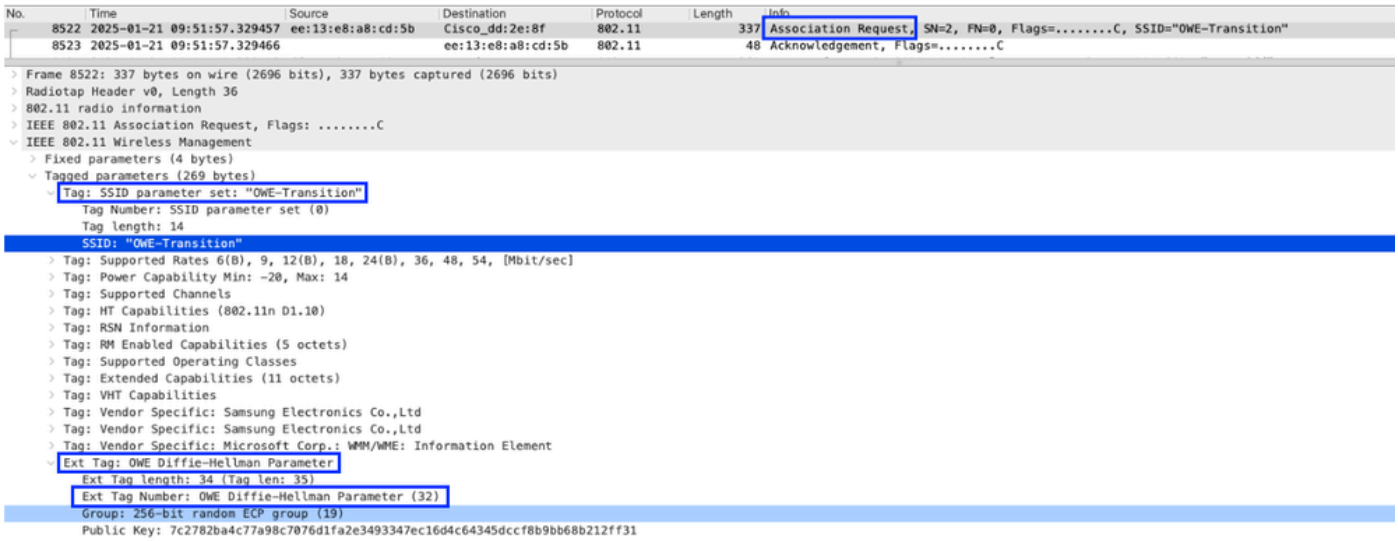
- Na het verkrijgen van de sonde reactie, kan de Open authentificatie tussen Cliënt en AP gebeuren om de de details/mogelijkheden van de cliënten wifi, vóór vereniging te controleren.



Afbeelding 5: OPEN verificatie na succesvolle test

Associatieaanvraag van client naar AP

- Merk op dat in dit pakket de client een Diffie-Hellman parameterwaarde voor codering kan toevoegen.

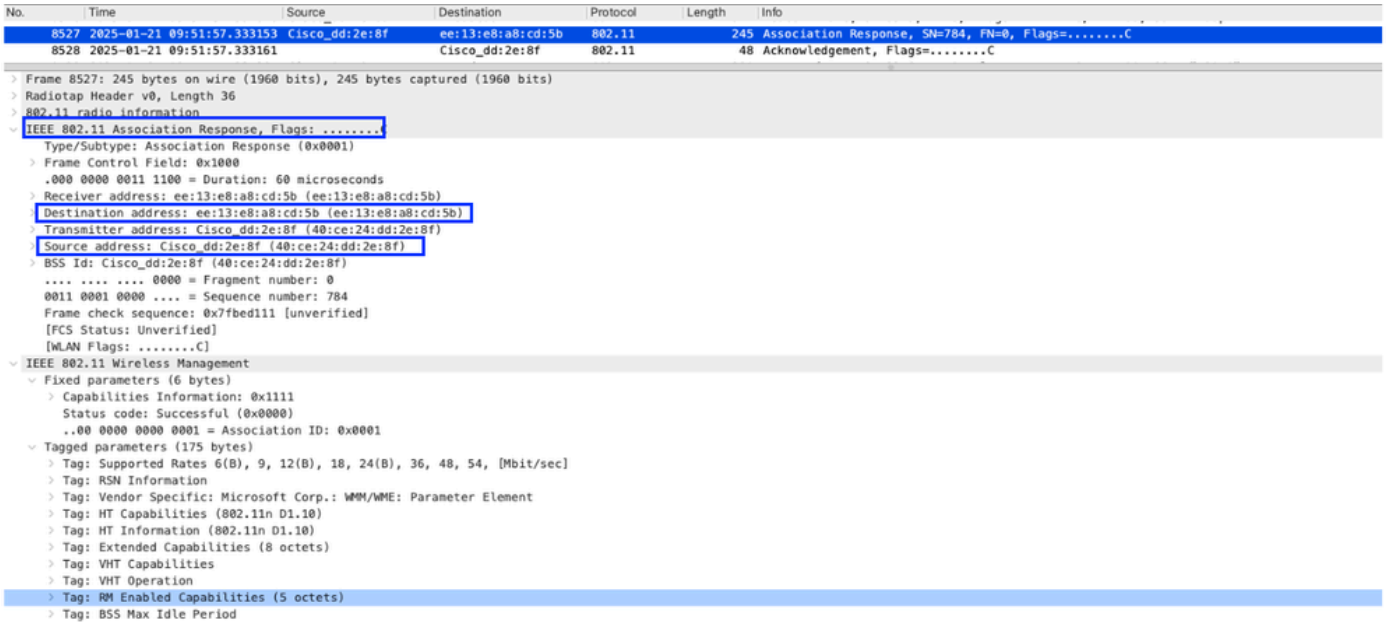


Afbeelding 6 : Associatieaanvraag

- In RA spoor, kunt u beginnen de cliëntlogboeken van de fase van de Vereniging te zien,

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

Reactie van associatie verzonden van AP naar client



Afbeelding 7: Reactie op associatie

```
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
```

Key exchange

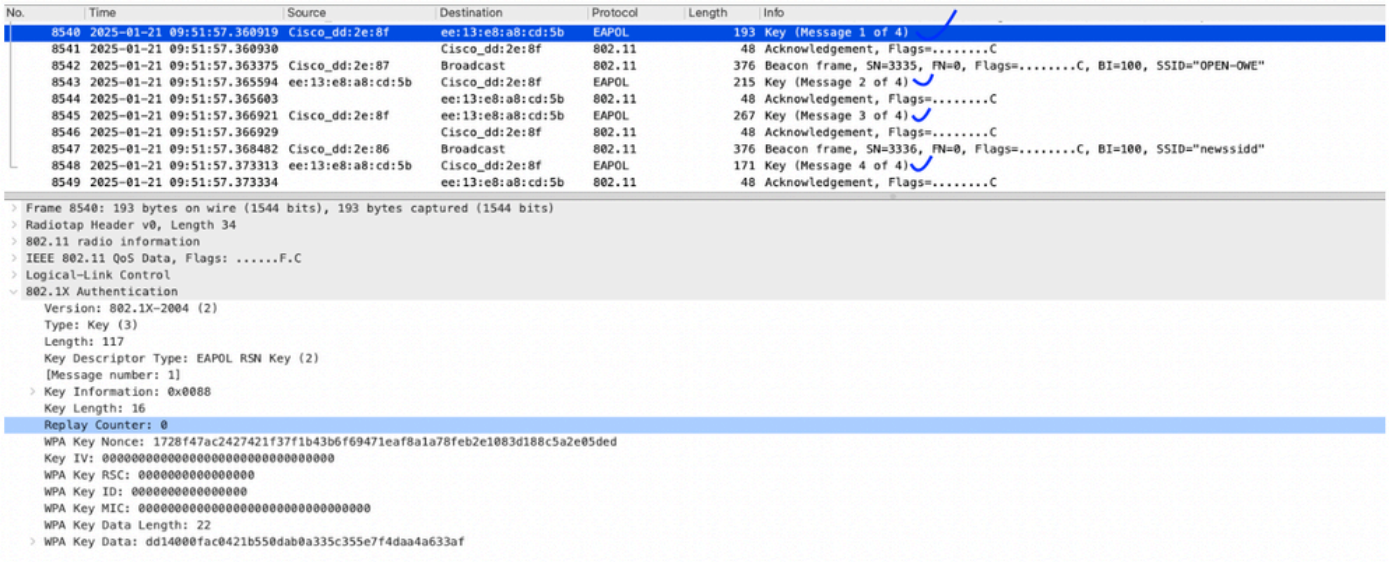
Er kan een 4-voudige handdruk optreden tussen het toegangspunt en het clientapparaat.

Sleutel-1 verzenden via AP

Key-2 verzenden per client

Key-3 verzenden via AP

Key-4 verzenden per client



Afbeelding 8: 4-voudige handdruk

```
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-verificatie geslaagd

```
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-leerstatus

```
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
```

Cliënt in LOOPPAS staat

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

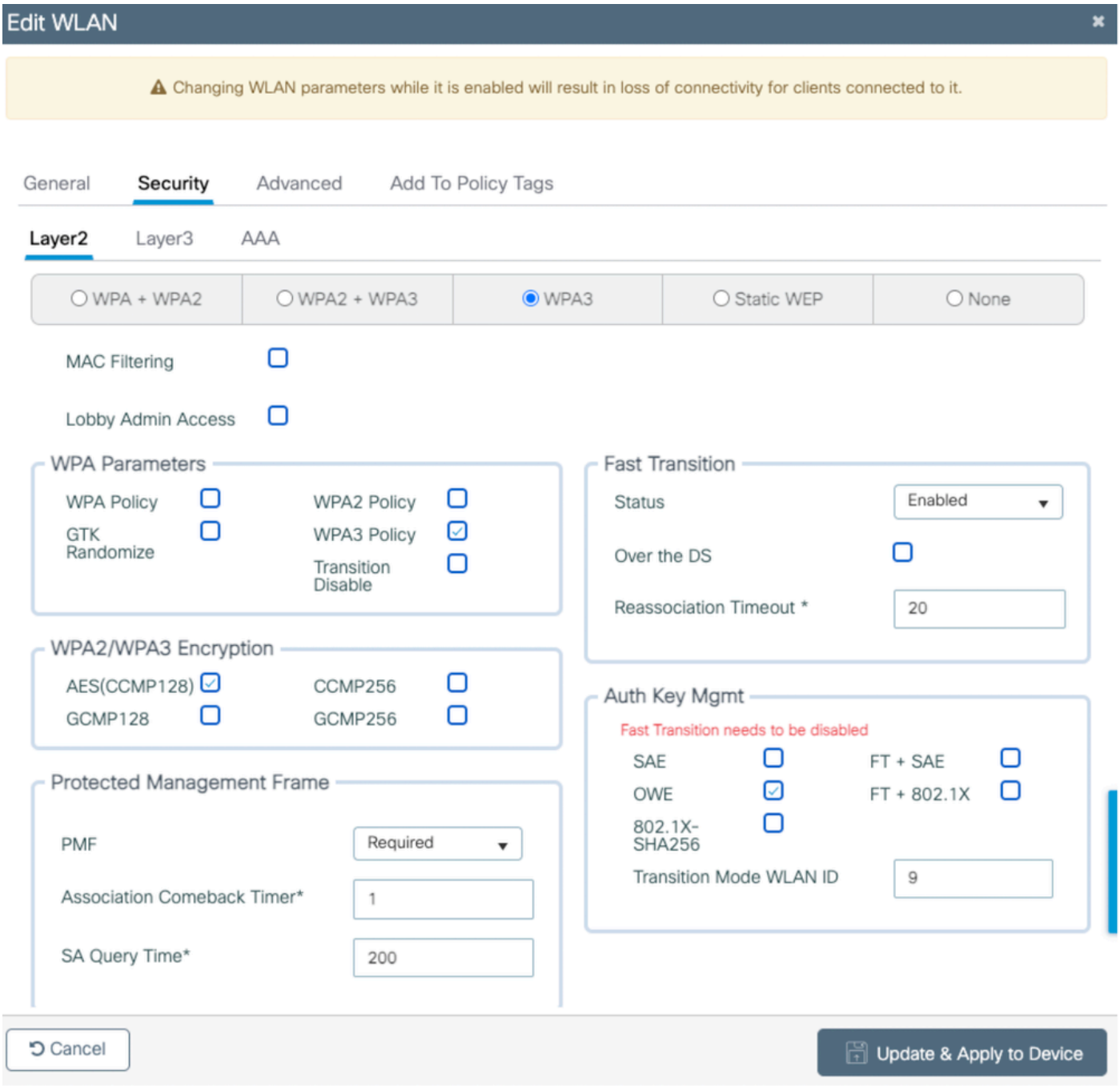
Clients die niet worden ondersteund voor OWE-codering

- Door een beacon frame zelf te bekijken, komen de clients te weten of ze deze encryptie methode kunnen ondersteunen of niet. Als het niet wordt ondersteund, dan kan het gewoon een sonde aanvraag sturen om SSID "OPEN-OWE" te openen en kan een normale open verificatie doen, IP-adres krijgen, dan kan het gaan de RUN staat.

```
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
```

Informatie over snelle overgang

- We zijn in staat om OWE alleen in OPEN authenticatie of in Webauth (CWA/LWA/EWA) te configureren.
- FT wordt niet ondersteund bij de OWE-overgang.
- Als je FT inschakelt, krijg je deze foutmelding:



Afbeelding 9 : Foutmelding wanneer we FT in OWE Transition SSID inschakelen

De OWE wordt niet ondersteund door PSK/dot1x

We zijn niet in staat om OWE in deze combinaties toe te laten,

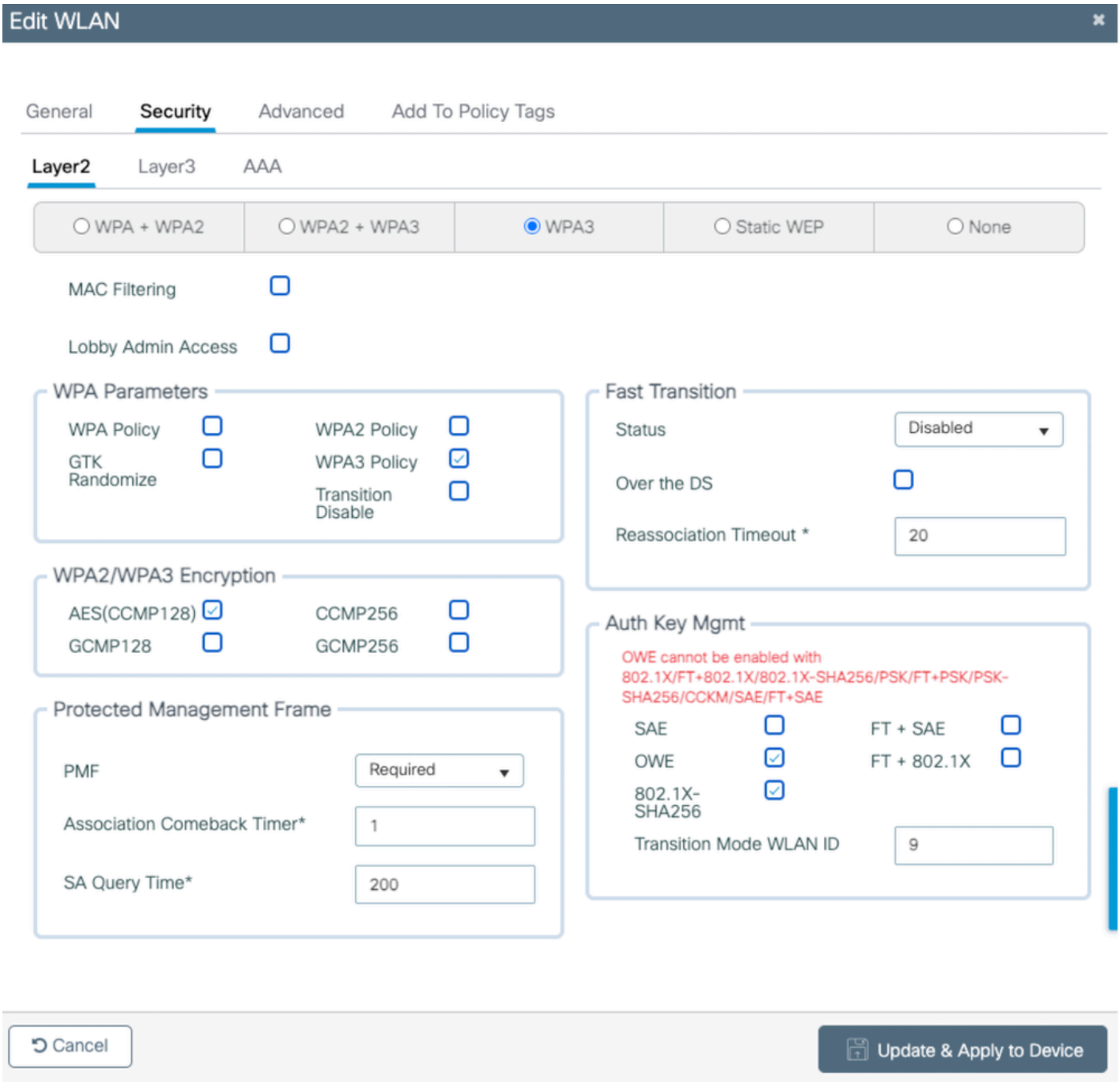
1. 802.1x of FT+802.1x

2. PSK of FT+PSK of PSK-SHA256

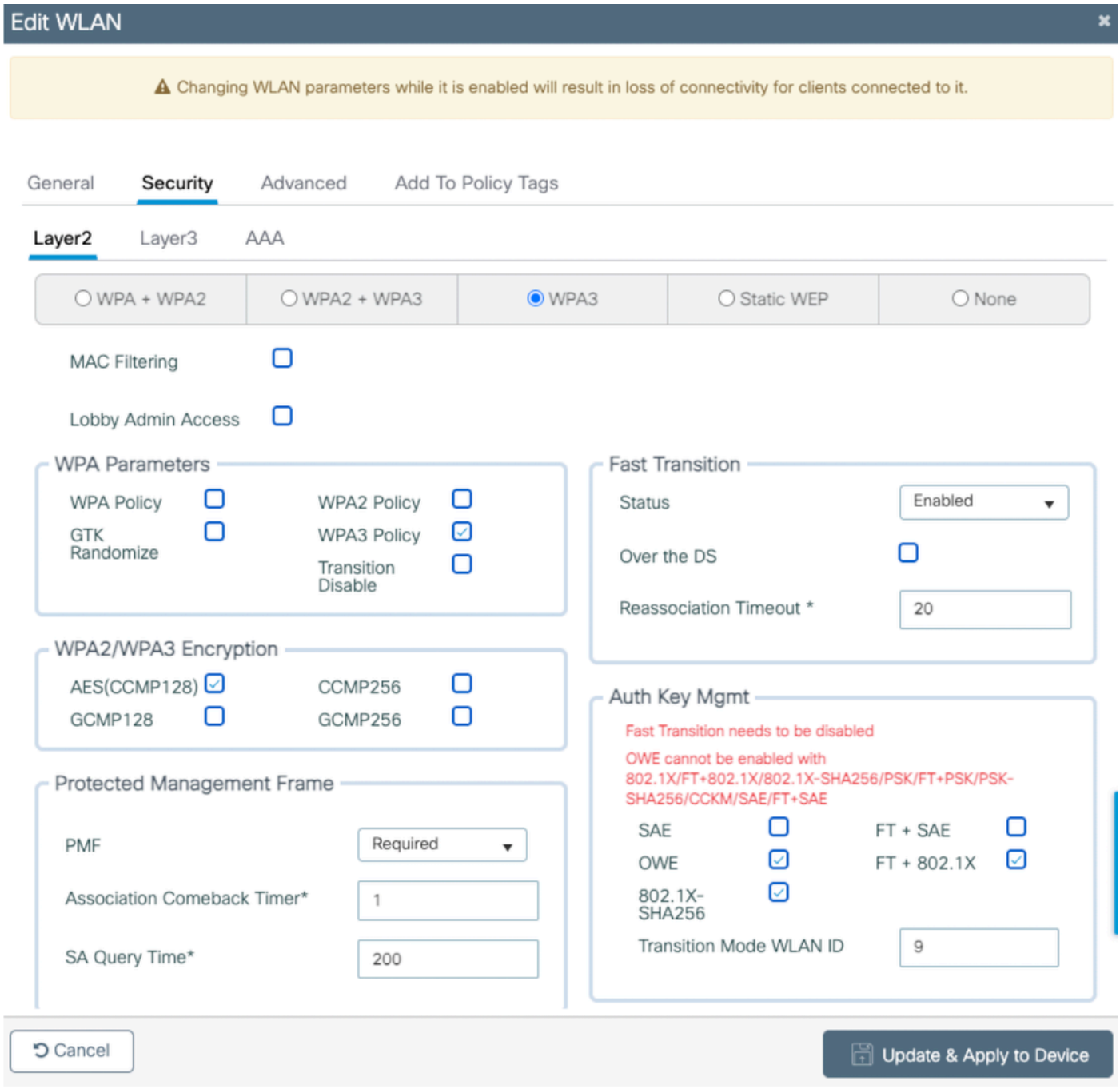
3. SAE of FT+SAE

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

Als u een van deze methoden probeert in te schakelen, krijgt u de foutmelding:

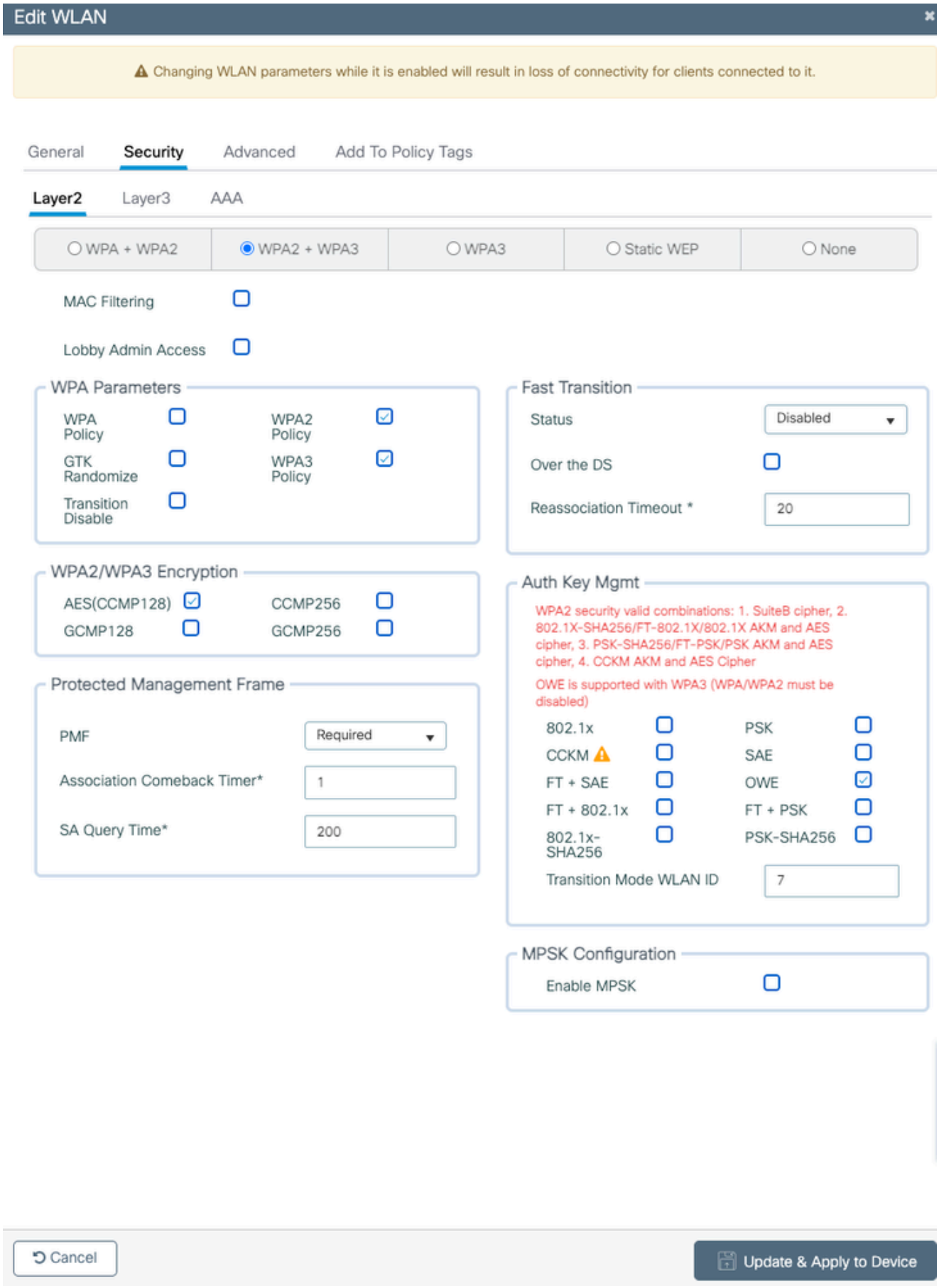


Afbeelding 10: Foutmelding ontvangen terwijl andere verificatiemethoden in OWE SSID zijn ingeschakeld



Afbeelding 11: Foutmelding bij het inschakelen van AKM

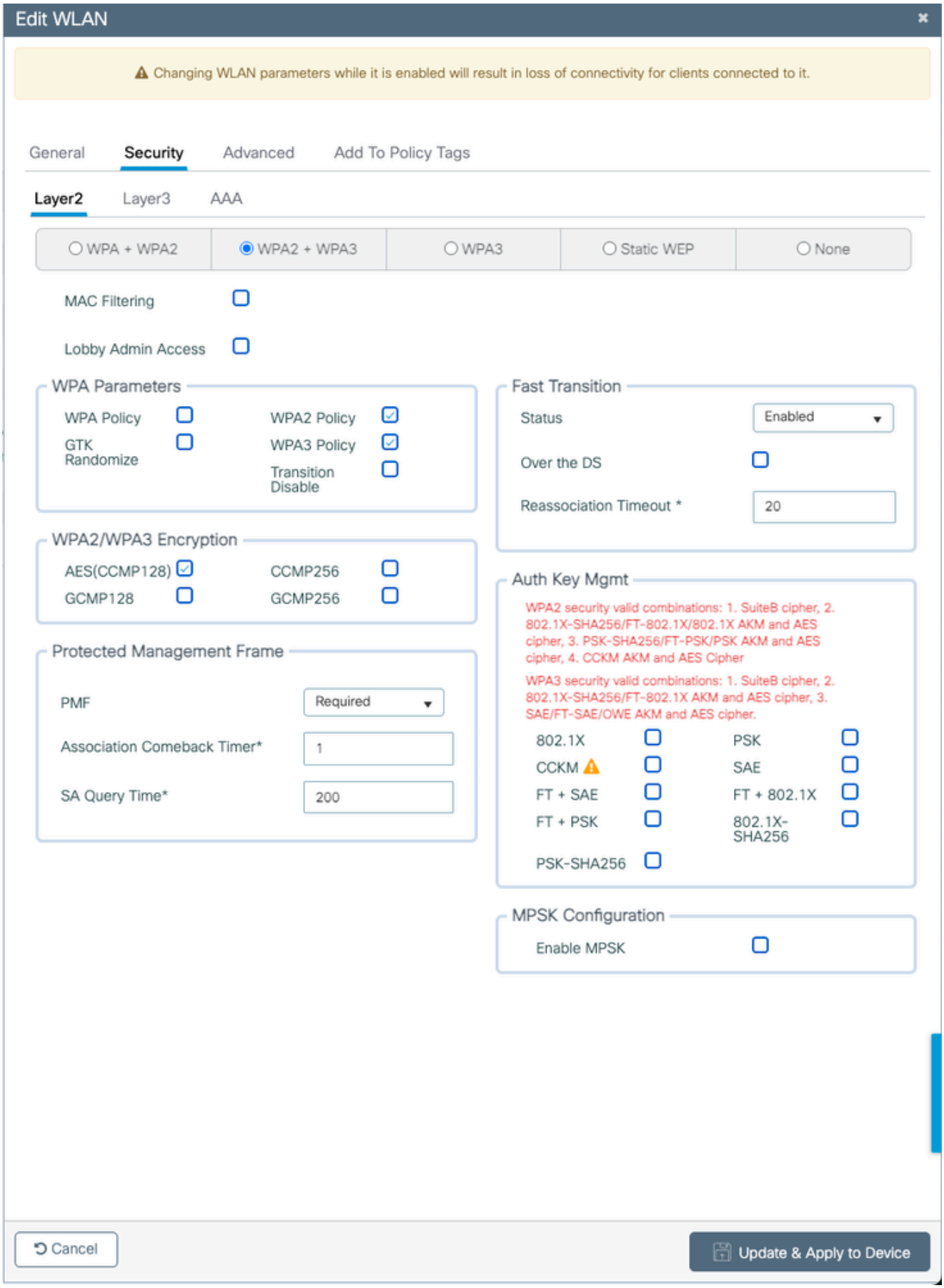
- In Cisco IOS® XE 17.9.6 IOS-versie kunt u de optie "OWE" onder AKM zien wanneer u "WPA2+WPA3" selecteert, maar u kunt de foutmelding krijgen; u kunt OWE met deze combinatie niet gebruiken.



Afbeelding 12: Foutmelding bij kiezen voor WPA2+WPA3

- In Cisco IOS® XE 17.12.4 versie kunt u, wanneer u "WPA2+WPA3" kiest, de optie "OWE"

niet in de AKM ophalen,



Afbeelding 13: Foutmelding - geen OWE-optie in AKM

Probleemoplossing

1. Controleer de configuraties in zowel de WLAN's, in OPEN SSID als in OWE-overgang SSID moet een WLAN-id van de overgang in kaart zijn gebracht.
2. De omroepoptie moet in OWE transitie SSID worden onbruikbaar gemaakt, moet het slechts in OPEN SSID worden toegelaten.
3. Controleer de ondersteunde verificatie-/encryptie-/FT-methoden die in dit artikel worden beschreven.
4. Als de configuraties van WLC eind fijn zijn, dan verzamel gelieve de vereiste logboeken en de output om de kwestie te versmallen,

RA Trace en EPC (Embedded PAcket Capture)

Aanmelden bij WLC GUI -> Problemen oplossen -> Radioactive Trace -> Add client wifi MAC-adres -> Klik op dat client checkbox -> Start

Aanmelden bij WLC GUI -> Problemen oplossen -> Packet Capture -> Nieuwe bestandsnaam toevoegen -> De uplink-interface en WMI VLAN/interface kiezen -> Start.

Vanaf clientmachine: Indien mogelijk kunt u een wireshark-toepassing installeren en de pakketopname verzamelen door de WiFi-interface te kiezen.

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

LUCHTDEKSEL

U kunt het verzamelen door MAC laptop of het configureren van een van de AP in om te snuffelen modus, verwijzen naar deze links,

Van MAC-laptop:

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

Van 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

Verbind één laptop (wireshark server) met de switch poort en het moet hebben wireshark applicatie geïnstalleerd in het, deze wireshark server moet bereikbaarheid hebben om WLC WMI interface. Moet toestaan het protocol "5555 of 5000 of 5556" in firewall als het aanwezig is tussen uw WLC en wireshark server.

Controleer of er een "gscaler" geïnstalleerd is in die PC waar wireshark geïnstalleerd is, als het is dan alstublieft "uitzetten" en probeer, als het een firewall zoals windows verdediger of iets

aanwezig in het is, schakel die uit en probeer PCAP te verzamelen.

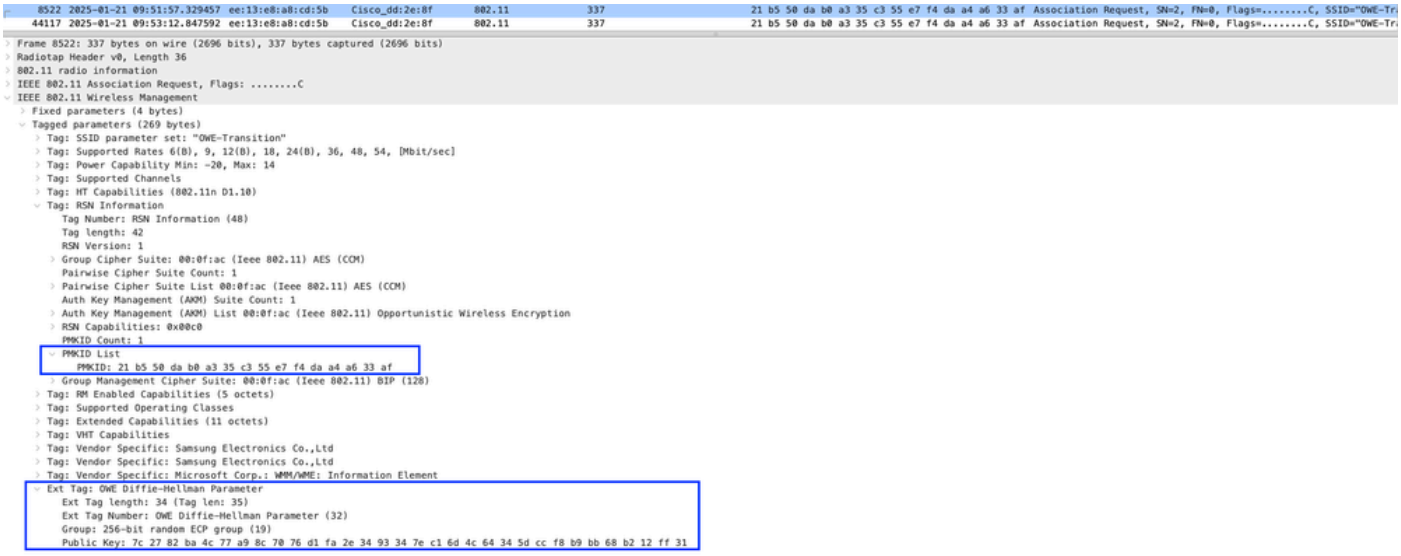
roaming

Wanneer de client van het ene toegangspunt naar het andere zwerft, moet deze stap worden uitgevoerd.

- Noodzaak om re-associatie/associatie te versturen - hangt af van het verzoek van de klant.
- Noodzaak om DH (Diffie-Helman) details te sturen in associatieaanvraag.
- De client kan DH-gegevens verkrijgen in associatiereactie van AP, op basis van deze PMK wordt gegenereerd in zowel client als AP.
- 4-way handshake kan gebeuren tussen AP en client.
- In OWE kunt u FT niet inschakelen, zodat 802.11r niet mogelijk is.
- Elke keer, wanneer de client zwerft, moet het 4-way handshake doen na DH-uitwisseling in associatie.
- Client en AP gebruiken hun eigen PMKID, het is uniek voor elke AP en clients.
- Als client verbinding maakt met dezelfde AP, dan kan dezelfde PMKID gebruikt worden. In sommige scenario, als de client verwijderd dan AP kan een nieuwe PMKID genereren, maar de client gebruikt dezelfde PMKID voor 4-way handshake.

Voorbeeld:

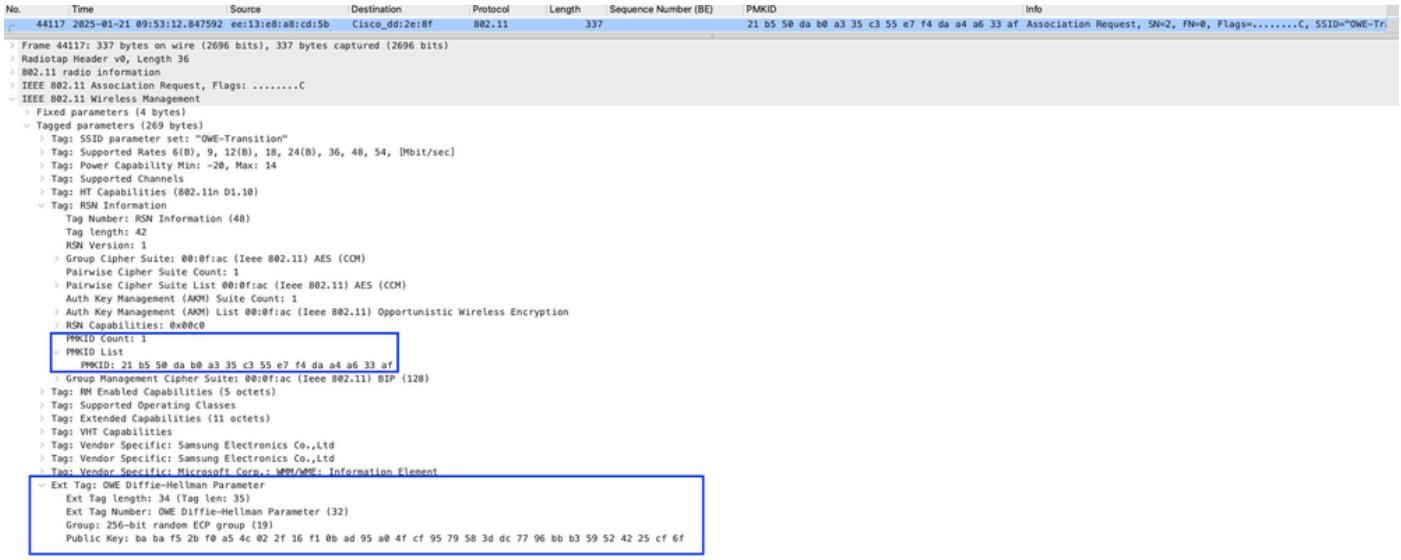
Als client verbinding maakt met dezelfde AP, dan kunt u dezelfde PMKID zien in zowel Association-request als Association-Response. In reactie van de Vereniging, kunt u geen DH details zien als het dezelfde PMKID gebruikt.



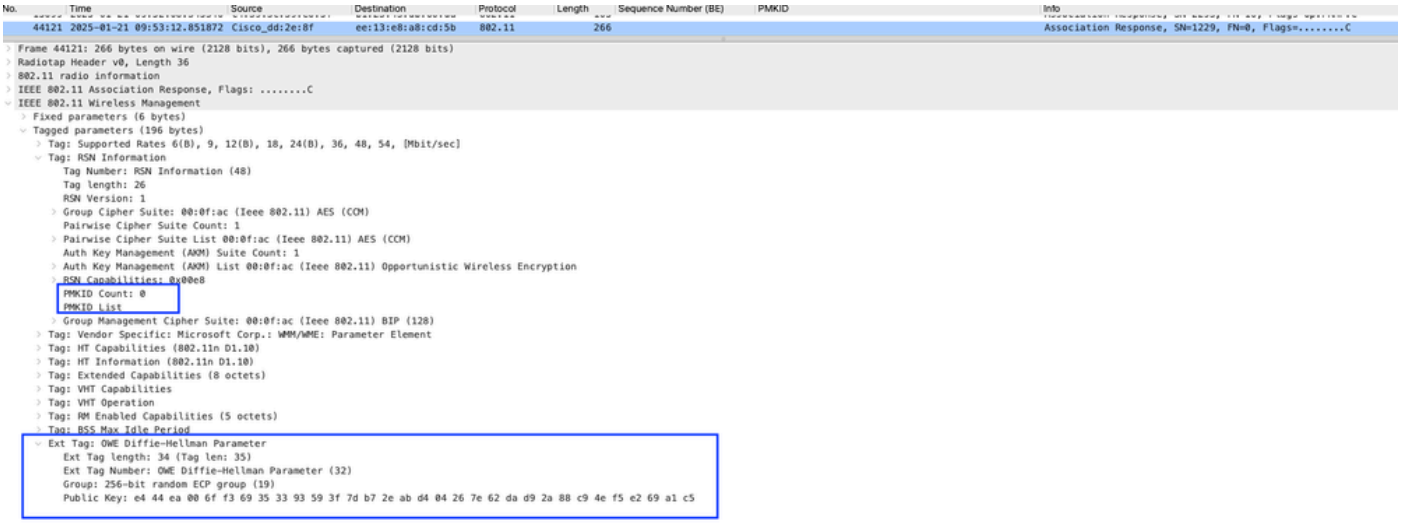
Afbeelding 14: Dezelfde PMKID gebruiken

Afbeelding 15: Associatie-respons met dezelfde PMKID

Voor het testen, verwijderde deze client handmatig uit WLC en het werd opnieuw gekoppeld aan dezelfde AP, op dit moment, de client stuurt een dezelfde PMKID maar AP stuurt DH details in associatiereactie.

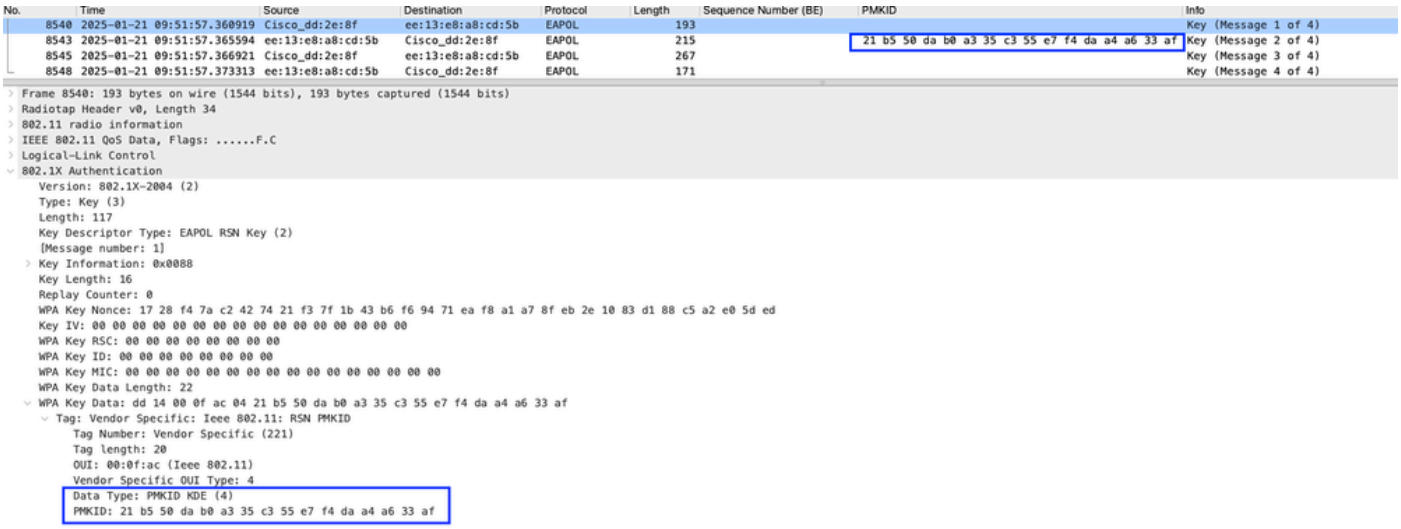


Afbeelding 16: Na het verwijderen, client verzonden dezelfde PMKID met DH details



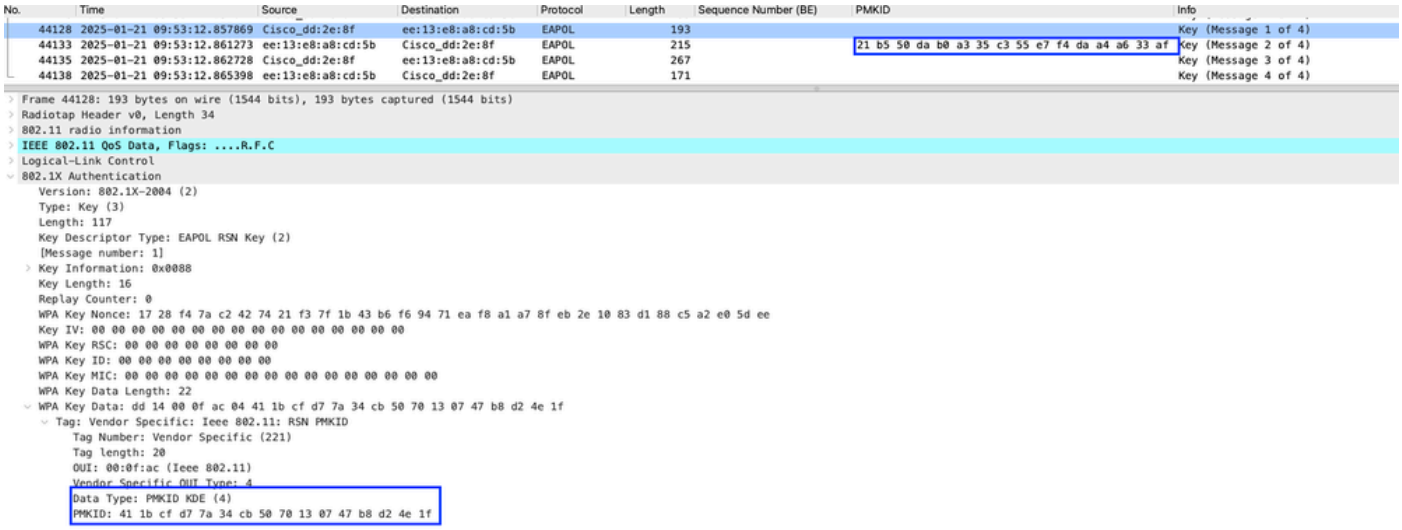
Afbeelding 17: AP gebruikt DH-waarden om zijn nieuwe PMKID te genereren

In dit voorbeeld: Zowel AP als client gebruikt dezelfde PMKID tijdens het 4-way handshake, controleer "M1 en in M2" berichten.



Afbeelding 18: AP en client met dezelfde PMKID

In dit voorbeeld: Cliënt die de zelfde PMKID maar AP gebruiken die verschillende PMKID gebruiken die het produceerde nadat de cliënt werd geschrapt, controleer "M1 en M2"berichten.



Afbeelding 19: AP en client met verschillende PMKID

Interne RA-sporen:

In dit voorbeeld: De client zond DH-parameters in associatieverzoek en AP verwerkt dan de PMK gegenereerd.

```
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
```

Hierna heeft dezelfde client die verbinding maakt met dezelfde AP, op dit moment, AP geen nieuwe PMKID gegenereerd,

```
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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.