# Wi-Fi 6E WLAN Layer 2-beveiliging configureren en controleren

## Inhoud



## Inleiding

Dit document beschrijft hoe u Wi-Fi 6E WLAN Layer 2-beveiliging kunt configureren en wat u op verschillende clients kunt verwachten.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco draadloze LAN-controllers (WLC) 9800
- Cisco Access points (AP's) die Wi-Fi 6E ondersteunen.
- IEEE-standaard 802.11ax.
- Tools: Wireshark v4.0.6

### Gebruikte componenten

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

- WLC 9800-CL met IOS® XE 17.9.3
- AP9136, CW9162, CW9164 en CW9166.
- Wi-Fi 6E-clients:
  - Lenovo X1 Carbon Gen11 met Intel AX211 Wi-Fi 6 en 6E adapter met driver versie 22.200.2(1).
  - Netgear A8000 Wi-Fi 6- en 6E-adapter met stuurprogramma v1(0.0.108);
  - Mobiele telefoon Pixel 6a met Android 13;
  - Mobiele telefoon Samsung S23 met Android 13.

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.

## Achtergrondinformatie

Het belangrijkste om te weten is dat Wi-Fi 6E geen geheel nieuwe standaard is, maar een uitbreiding. Op de basis is Wi-Fi 6E een uitbreiding van de Wi-Fi 6 (802.11ax) draadloze standaard in de 6-GHz radiofrequentieband.

Wi-Fi 6E bouwt voort op Wi-Fi 6, de nieuwste generatie van de Wi-Fi standaard, maar alleen Wi-Fi 6E apparaten en toepassingen kunnen werken in de 6-GHz band.

### Wi-Fi 6E security

Wi-Fi 6E verhoogt de beveiliging met Wi-Fi Protected Access 3 (WPA3) en Opportunistische Draadloze Encryptie (OWE) en er is geen achterwaartse compatibiliteit met Open en WPA2-beveiliging.

WPA3 en Enhanced Open Security zijn nu verplicht voor Wi-Fi 6E-certificering en Wi-Fi 6E vereist ook Protected Management Frame (PMF) in zowel AP als Clients.

Bij het configureren van een 6GHz SSID zijn er bepaalde beveiligingsvereisten waaraan moet worden voldaan:

- WPA3 L2-beveiliging met WAE, SAE of 802.1x-SHA256
- Beschermd beheerframe ingeschakeld;
- Een andere L2-beveiligingsmethode is niet toegestaan, dat wil zeggen geen gemengde

modus mogelijk.

WPA3

WPA3 is ontworpen om de Wi-Fi-beveiliging te verbeteren door betere verificatie via WPA2 mogelijk te maken, en uitgebreide cryptografische kracht te bieden en de veerkracht van kritieke netwerken te vergroten.

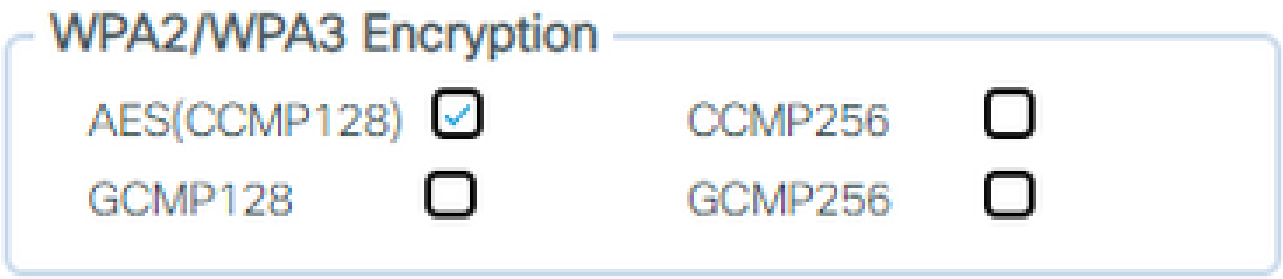
De belangrijkste kenmerken van WPA3 zijn:

- Protected Management Frame (PMF)beschermt unicast- en broadcast-beheerframes en versleutelt unicast-beheerframes. Dit betekent dat draadloze inbraakdetectie en draadloze inbraakpreventiesysteem-sneeuw minder brute-kracht manieren hebben om clientbeleid af te dwingen.
- Gelijktijdige verificatie van equals (SAE) maakt wachtwoordgebaseerde verificatie en een sleutelovereenkomstmechanisme mogelijk. Dit beschermt tegen grof geweld aanvallen.
- Overgangsmodus is een gemengde modus die het gebruik van WPA2 mogelijk maakt om clients te verbinden die geen WPA3 ondersteunen.

WPA3 gaat over continue security ontwikkeling en conformantie en interoperabiliteit.
Er is geen informatie-element dat WPA3 aanwijst (hetzelfde als WPA2). WPA3 is gedefinieerd door AKM/Cypher Suite/PMF combinaties.

Op de 9800 WLAN-configuratie hebt u vier verschillende WPA3-coderingsalgoritmen die u kunt gebruiken.

Ze zijn gebaseerd op het Galois/Counter Mode Protocol (GCMP) en de Counter Mode met Cycle Block Chaining Message Authenticatie Protocol (CCMP): AES (CCMP128), CCMP256, GCMP128 en GCMP256:

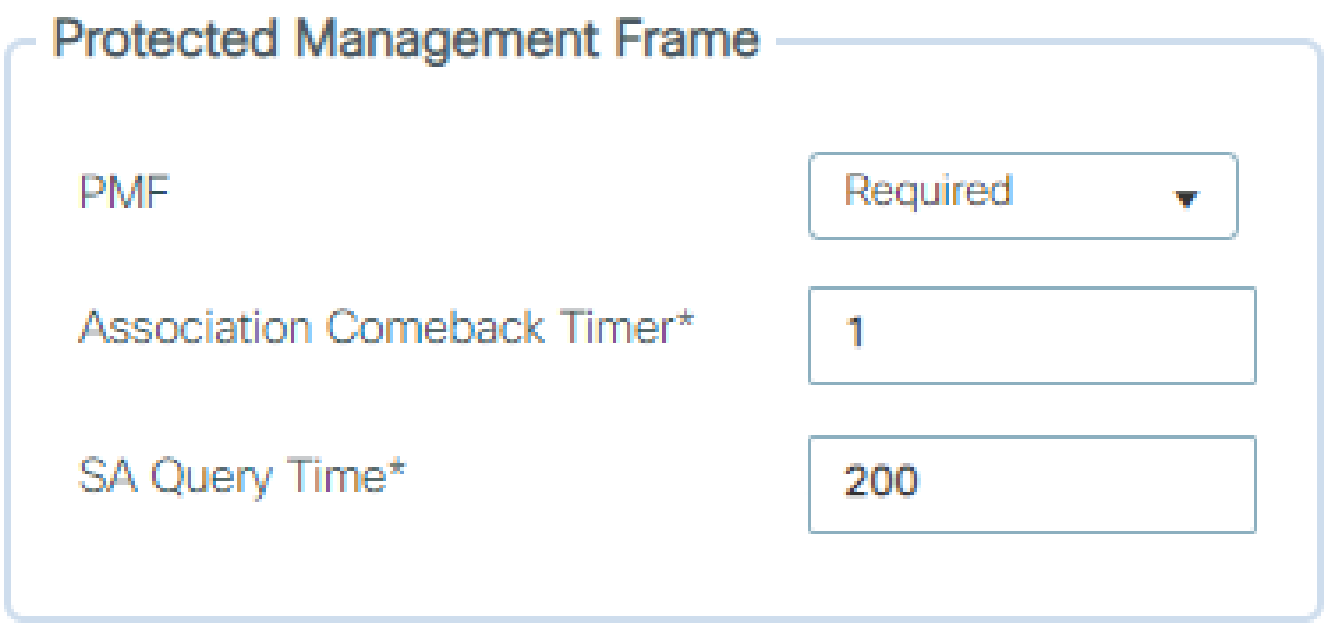



WAP2/3-versleutelingsopties

PMF

PMF wordt geactiveerd op een WLAN wanneer u PMF inschakelt.

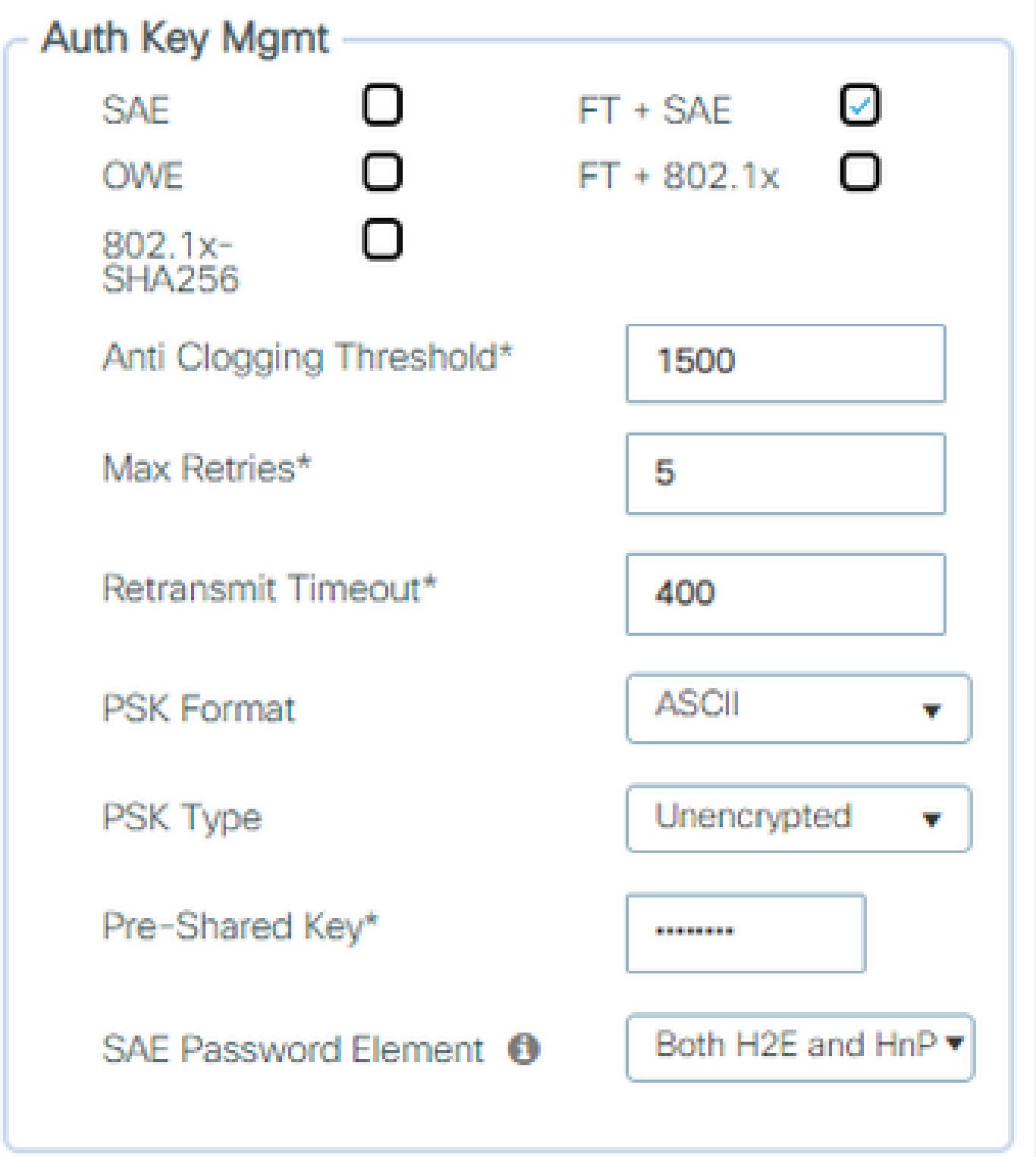
Standaard zijn 802.11-beheerframes niet geverifieerd en dus niet beschermd tegen spoofing. Infrastructure Management Protection Frame (MFP) en 802.11w protected management frames (PMF) bieden bescherming tegen dergelijke aanvallen.




PMF-opties

Beheer van verificatiesleutels

Dit zijn de AKM-opties die beschikbaar zijn in de 17.9.x-versie:

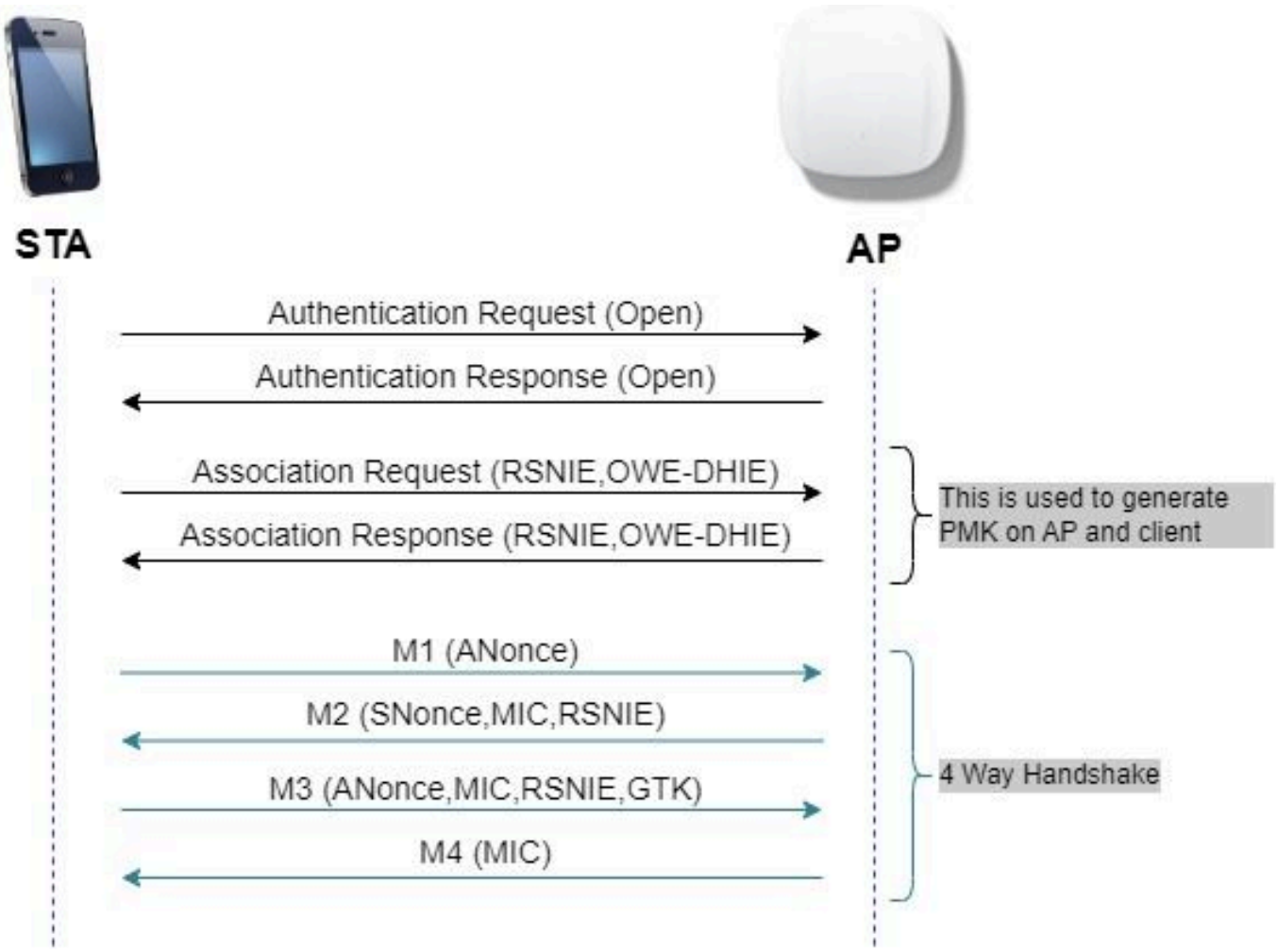



AKM-opties

VERSCHULDIGD

Opportunistische draadloze encryptie (OWE) is een uitbreiding van IEEE 802.11 die codering van het draadloze medium biedt (IETF RFC 8110). Het doel van op OWE gebaseerde verificatie is het vermijden van open onbeveiligde draadloze connectiviteit tussen de AP's en clients. De OWE gebruikt de Diffie-Hellman algoritmen op basis van Cryptografie om de draadloze codering in te stellen. Met OWE voeren de client en AP tijdens de toegangsprocedure een Diffie-Hellman sleuteluitwisseling uit en gebruiken de resulterende paarsgewijze hoofdsleutel (PMK) 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.




OWE frame exchange

SAE

WPA3 maakt gebruik van een nieuw authenticatie- en sleutelbeheermechanisme genaamd Gelijktijdige verificatie van Gelijken. Dit mechanisme wordt verder versterkt door het gebruik van SAE Hash-to-Element (H2E).

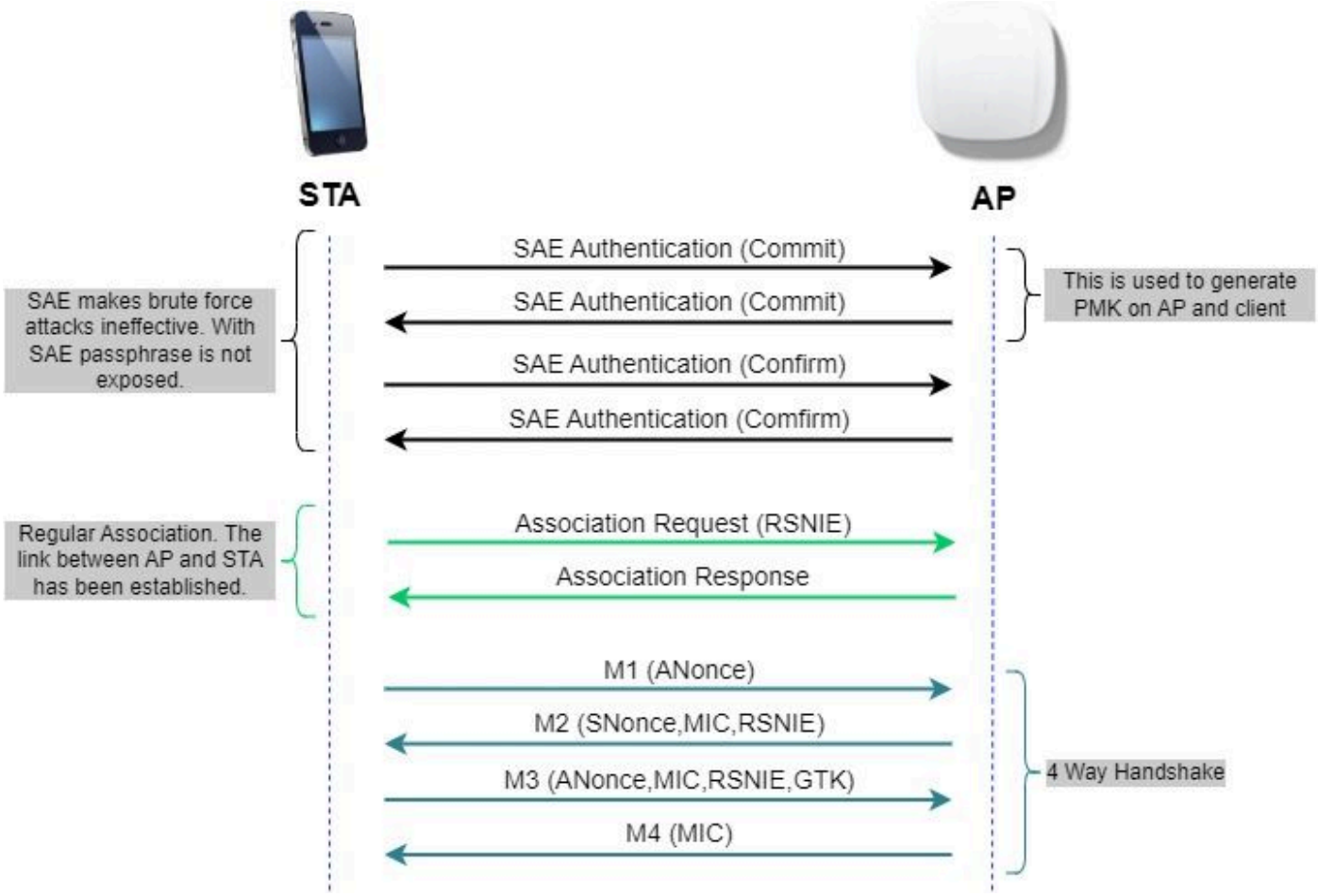
SAE met H2E is verplicht voor WPA3 en Wi-Fi 6E.

SAE maakt gebruik van een discrete logaritme cryptografie om een efficiënte uitwisseling uit te voeren op een manier die wederzijdse authenticatie uitvoert met behulp van een wachtwoord dat waarschijnlijk bestand is tegen een offline woordenboekaanval.

Een offline woordenboekaanval is waarbij een tegenstander probeert een netwerkwachtwoord te bepalen door mogelijke wachtwoorden te proberen zonder verdere netwerkinteractie.

Wanneer de client verbinding maakt met het toegangspunt, wordt een SAE-uitwisseling uitgevoerd. Indien succesvol, maken ze elk een cryptografisch sterke sleutel, waaruit de sessiesleutel is afgeleid. In principe gaat een client en access point naar de fasen van commit en vervolgens bevestig.

Zodra er een toezegging is, kunnen de client en het access point vervolgens naar de bevestigende staten gaan telkens als er een sessiesleutel moet worden gegenereerd. De methode gebruikt voorwaartse geheimhouding, waarbij een indringer één enkele sleutel kon kraken, maar niet alle andere sleutels.




SAE frame exchange

Hash-to-element (H2E)

Hash-to-Element (H2E) is een nieuwe SAE Password Element (PWE) methode. Bij deze methode wordt de geheime PWE die in het SAE-protocol wordt gebruikt, gegenereerd met een wachtwoord.

Wanneer een station (STA) dat H2E ondersteunt een SAE start met een AP, controleert het of AP H2E ondersteunt. Zo ja, gebruikt het toegangspunt de H2E om de PWE af te leiden met behulp van een nieuw gedefinieerde statuscodewaarde in het SAE Commit-bericht.

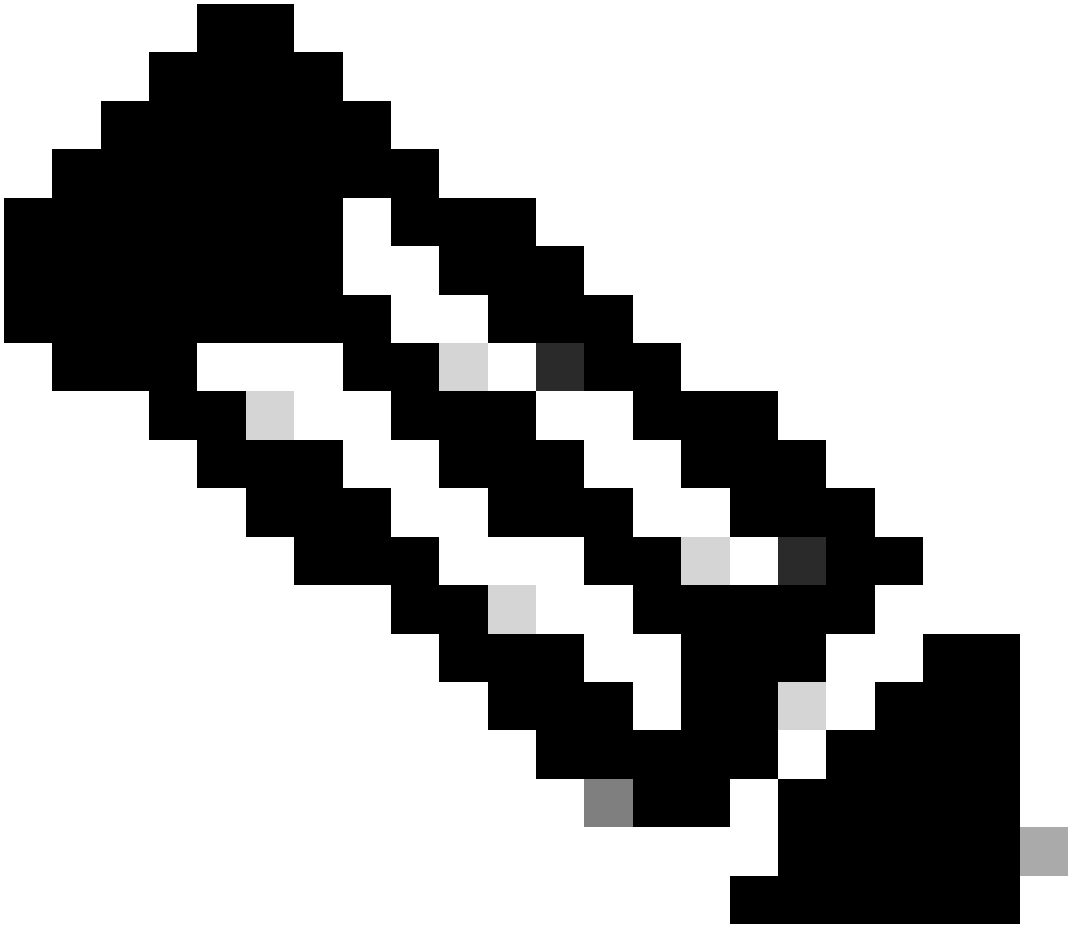
Als STA Hunting-and-Pecking (HnP) gebruikt, blijft de gehele SAE-uitwisseling ongewijzigd.

Bij gebruik van H2E wordt de PWE-afleiding onderverdeeld in de volgende componenten:

- Afleiding van een geheim tussenliggend element (PT) uit het wachtwoord. Dit kan offline worden uitgevoerd wanneer het wachtwoord in eerste instantie op het apparaat voor elke ondersteunde groep is ingesteld.
- Afleiding van de PWE uit de opgeslagen PT. Dit is afhankelijk van de onderhandelde groep

en MAC-adressen van peers. Dit wordt in real-time uitgevoerd tijdens de SAE-uitwisseling.

---

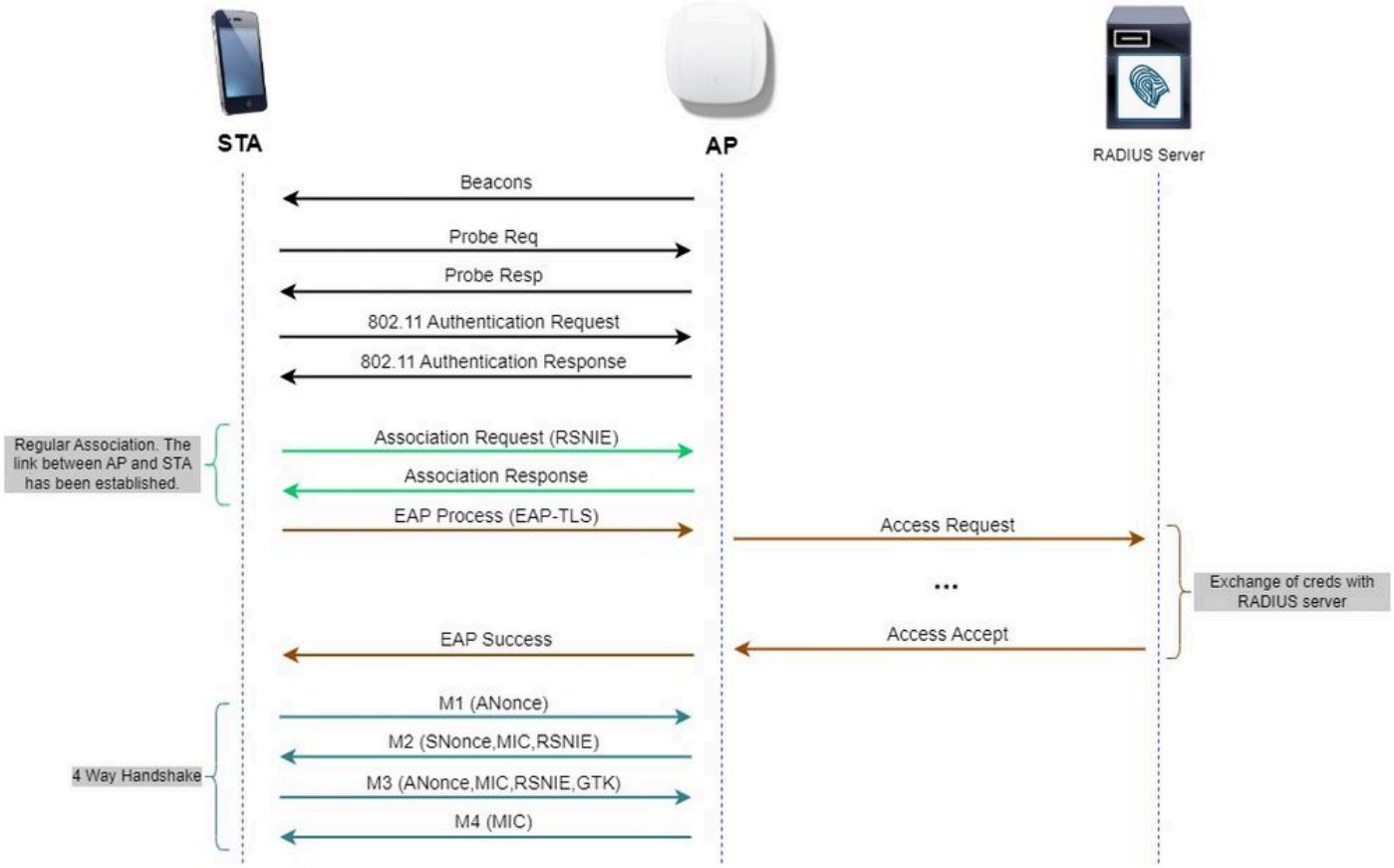


Opmerking: 6 GHz ondersteunt alleen Hash-to-Element SAE PWE-methode.

---

WPA-Enterprise ook bekend als 802.1x

WPA3-Enterprise is de veiligste versie van WPA3 en gebruikt een gebruikersnaam plus wachtwoordcombinatie met 802.1X voor gebruikersverificatie met een RADIUS-server. Standaard maakt WPA3 gebruik van 128-bits codering, maar wordt ook een optioneel configureerbare 192-bits codering van cryptografische sterkte geïntroduceerd, die extra bescherming biedt aan elk netwerk dat gevoelige gegevens doorgeeft.




Stroom WPA3-ondernemingsdiagram

Niveau ingesteld: WPA3-modi

- WPA3-Personal
  - alleen WPA3-Personal-modus
    - PMF vereist
  - WPA3-Personal-overgangsmodus
    - Configuratieregels: op een AP, wanneer WPA2-Personal is ingeschakeld, moet de WPA3-Personal Transition-modus ook standaard worden ingeschakeld, tenzij deze expliciet door de beheerder wordt overschreven om alleen in de WPA2-Personal-modus te werken

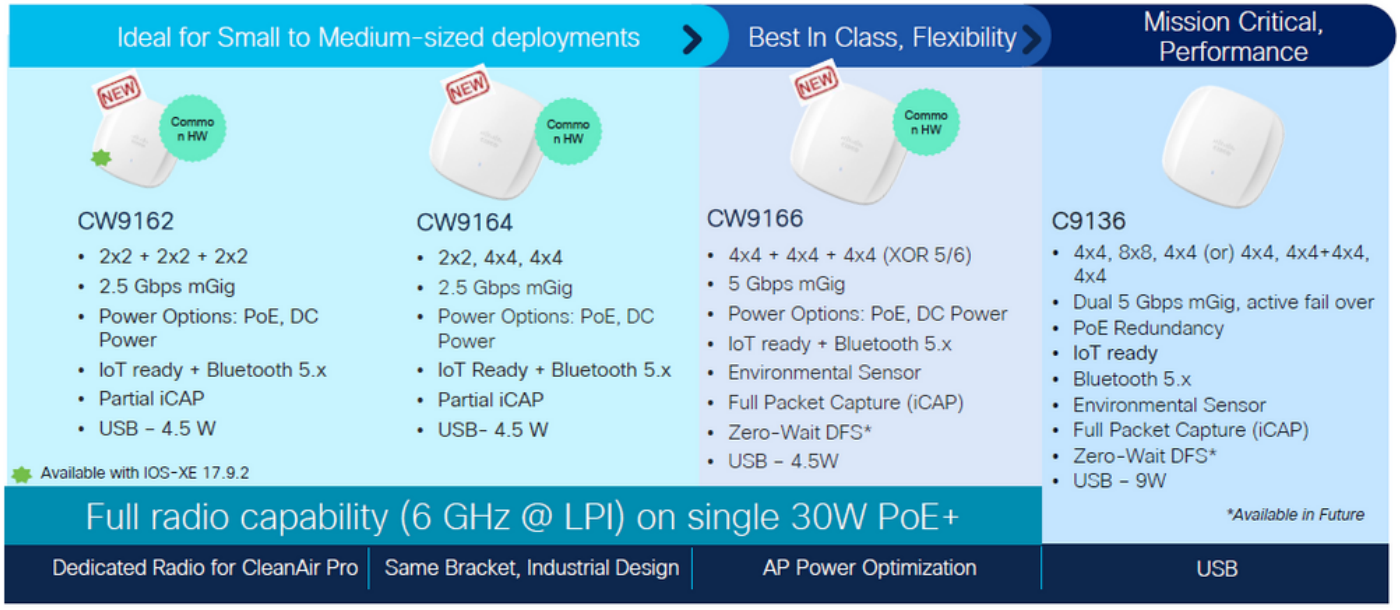
- WPA3-Enterprise
  - WPA3-Enterprise alleen-modus
    - PMF wordt voor alle WPA3-verbindingen onderhandeld
  - WPA3-Enterprise Transition Mode
    - PMF wordt overeengekomen voor een WPA3-verbinding
    - PMF optioneel voor een WPA2-verbinding
  - WAP3-Enterprise suite-B "192-bits" modus afgestemd op commercial-algoritme voor nationale beveiliging (CNSA)
    - Meer dan alleen voor de federale overheid
    - Consistente cryptografische algoritme suites om misconfiguratie te voorkomen
    - Toevoeging van GCMP & ECCP voor crypto en betere hashfuncties (SHA384)

- PMF vereist
- De WPA3 192-bit beveiliging is exclusief voor EAP-TLS, waarvoor certificaten op zowel de aanvrager als de RADIUS-server vereist zijn.
- Om WPA3 192-bit enterprise te gebruiken, moeten de RADIUS-servers een van de toegestane EAP-algoritmen gebruiken:

  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Als u meer wilt weten over gedetailleerde informatie over de implementatie van WPA3 in Cisco WLAN's, inclusief de compatibiliteitsmatrix voor clientbeveiliging, kunt u de implementatiegids voor WPA3 raadplegen.

Cisco Catalyst Wi-Fi 6E access points




Wi-Fi 6E access points

Door clients ondersteunde beveiligingsinstellingen

U kunt vinden welk product WPA3-Enterprise ondersteunen met behulp van WiFi Alliance webpagina productzoeker.

Op Windows-apparaten kunt u controleren wat de beveiligingsinstellingen zijn die door de adapter worden ondersteund met de opdracht "netsh WLAN show drivers".

Hier ziet u de uitvoer van de Intel AX211:

```
C:\Users\tantunes>netsh wlan show drivers

Interface name: Wi-Fi

    Driver                  : Intel(R) Wi-Fi 6E AX211 160MHz
    Vendor                  : Intel Corporation
    Provider                : Intel
    Date                    : 3/9/2023
    Version                 : 22.200.2.1
    INF file                : oem151.inf
    Type                    : Native Wi-Fi Driver
    Radio types supported   : 802.11b 802.11g 802.11n 802.11a 802.11ac 802.11ax
    FIPS 140-2 mode supported : Yes
    802.11w Management Frame Protection supported : Yes
    Hosted network supported  : No
    Authentication and cipher supported in infrastructure mode:
                            Open            None
                            Open            WEP-40bit
                            Open            WEP-104bit
                            Open            WEP
                            WPA-Enterprise  TKIP
                            WPA-Enterprise  CCMP
                            WPA-Personal    TKIP
                            WPA-Personal    CCMP
                            WPA2-Enterprise TKIP
                            WPA2-Enterprise CCMP
                            WPA2-Personal   TKIP
                            WPA2-Personal   CCMP
                            Open            Vendor defined
                            WPA3-Personal   CCMP
                            Vendor defined  Vendor defined
                            WPA3-Enterprise 192 Bits GCMP-256
                            OWE             CCMP
                            WPA3-Enterprise CCMP
                            WPA3-Enterprise TKIP
    Number of supported bands : 3
                            2.4 GHz [ 0 MHz - 0 MHz]
                            5 GHz   [ 0 MHz - 0 MHz]
                            6 GHz   [ 0 MHz - 0 MHz]
    IHV service present     : Yes
    IHV adapter OUI         : [00 00 00], type: [00]
    IHV extensibility DLL path: C:\WINDOWS\System32\DriverStore\FileRepository\netwtw6e.inf_amd64_eda979fbdedea064\IntelIHVRouter12.dll
```

Windows-uitvoer van _netsh WLAN show driver_ voor client AX211

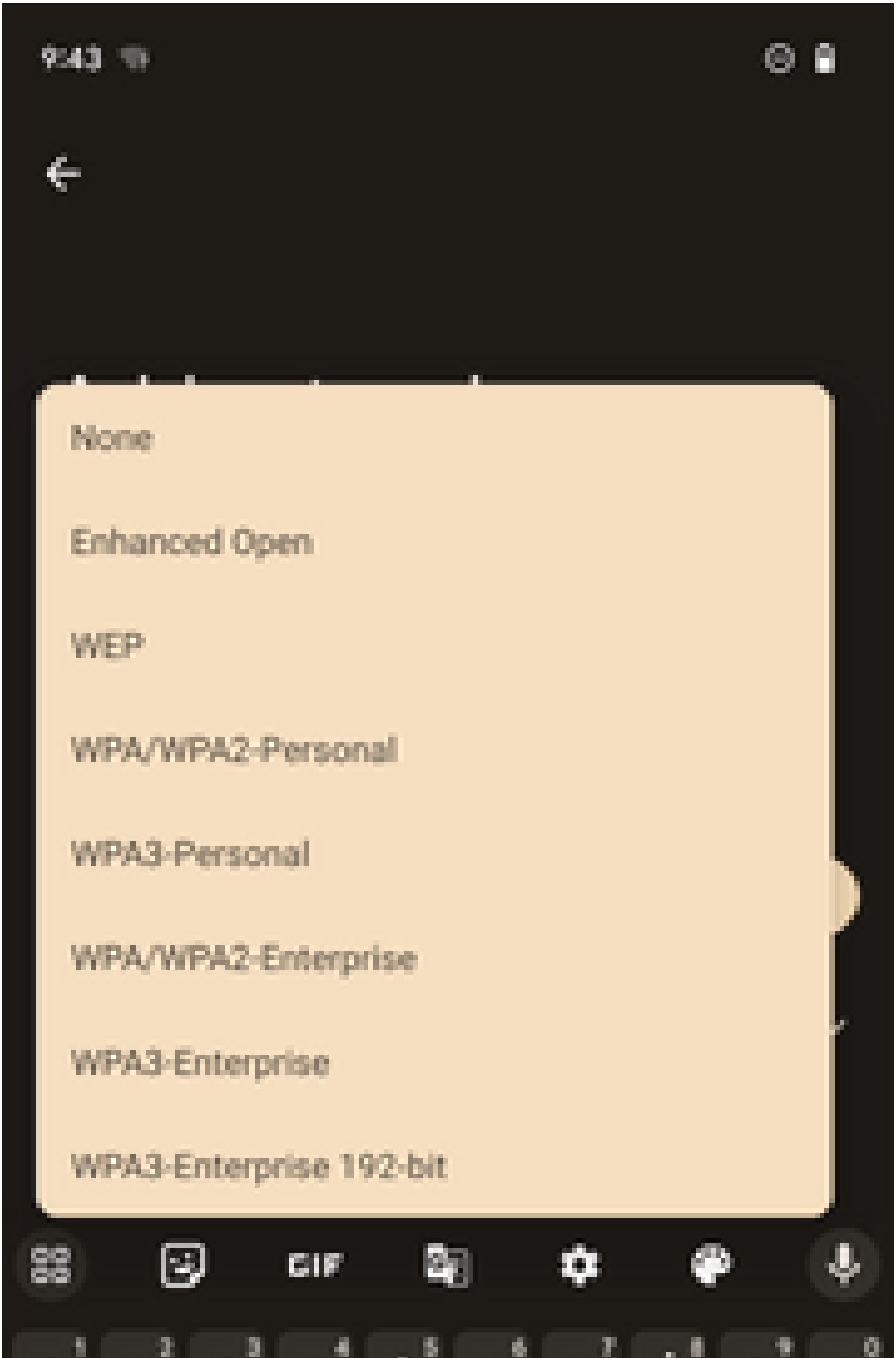
## Netgear A8000:

```
Interface name: A8000_NETGEAR

    Driver                     : NETGEAR A8000 WiFi 6 & 6E Adapter
    Vendor                     : NETGEAR Inc.
    Provider                   : MediaTek, Inc.
    Date                       : 11/25/2022
    Version                    : 1.0.0.108
    INF file                   : oem9.inf
    Type                       : Native Wi-Fi Driver
    Radio types supported      : 802.11b 802.11a 802.11g 802.11n 802.11ac 802.11ax
    FIPS 140-2 mode supported : Yes
    802.11w Management Frame Protection supported : Yes
    Hosted network supported  : No
    Authentication and cipher supported in infrastructure mode:
                                Open             None
                                Open             WEP-40bit
                                Open             WEP-104bit
                                Open             WEP
                                WPA-Enterprise   TKIP
                                WPA-Enterprise   CCMP
                                WPA3-Personal    CCMP
                                OWE              CCMP
                                WPA-Personal     TKIP
                                WPA-Personal     CCMP
                                WPA2-Enterprise  TKIP
                                WPA2-Enterprise  CCMP
                                WPA2-Personal    TKIP
                                WPA2-Personal    CCMP
    Number of supported bands : 3
                                2.4 GHz [ 0 MHz - 0 MHz]
                                5 GHz   [ 0 MHz - 0 MHz]
                                6 GHz   [ 0 MHz - 0 MHz]
    IHV service present        : Yes
    IHV adapter OUI            : [00 00 00], type: [00]
    IHV extensibility DLL path: C:\WINDOWS\system32\mtkihvux.dll
    IHV UI extensibility ClSID: {00000000-0000-0000-0000-000000000000}
    IHV diagnostics CLSID      : {00000000-0000-0000-0000-000000000000}
    Wireless Display Supported: Yes (Graphics Driver: Yes, Wi-Fi Driver: Yes)
```

Windows-uitvoer van _netsh wlan show driver_ voor client Netgear A8000s

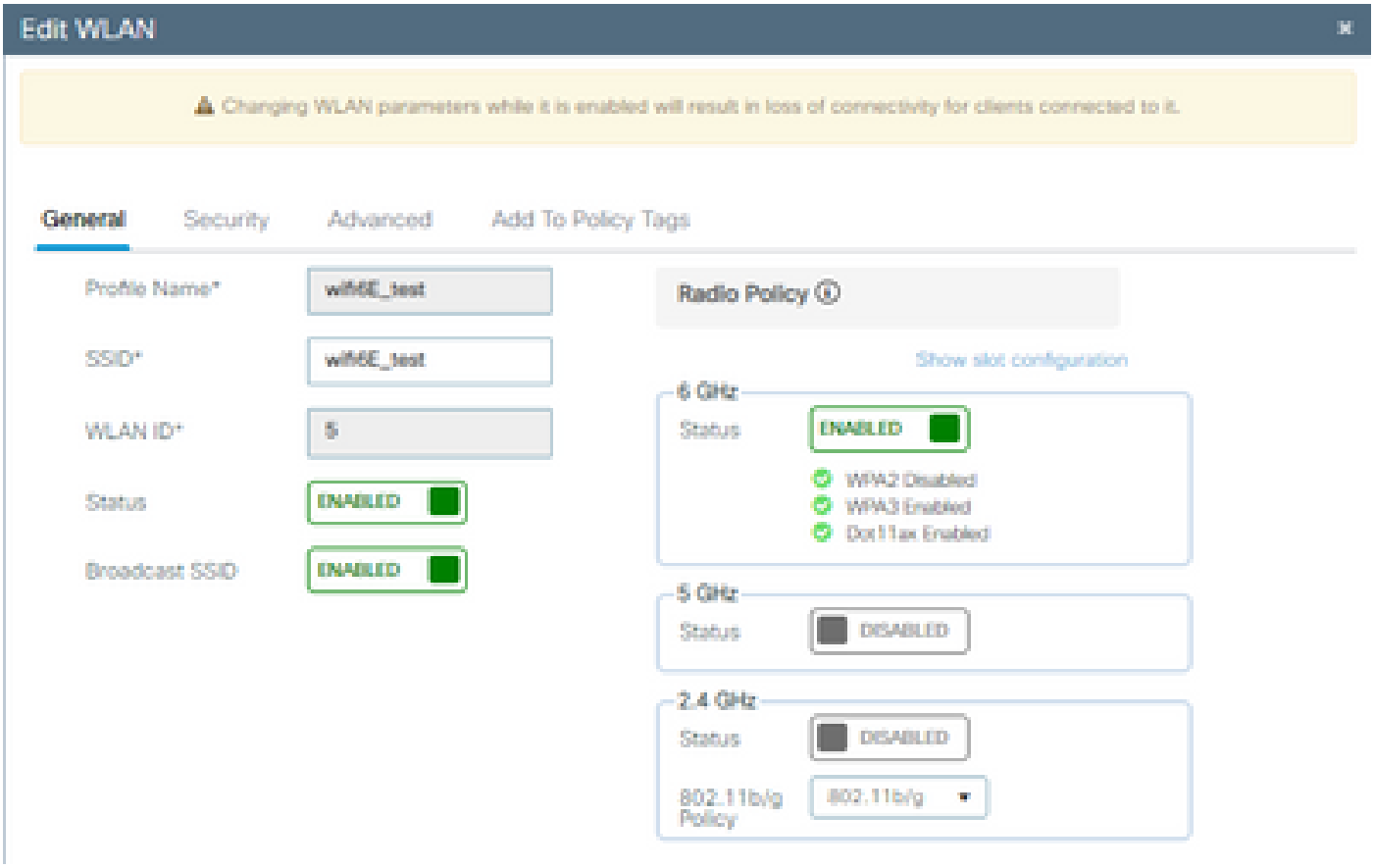
Android Pixel 6a:


9:43
None
Enhanced Open
WEP
WPA/WPA2-Personal
WPA3-Personal
WPA/WPA2-Enterprise
WPA3-Enterprise
WPA3-Enterprise 192-bit
GIF

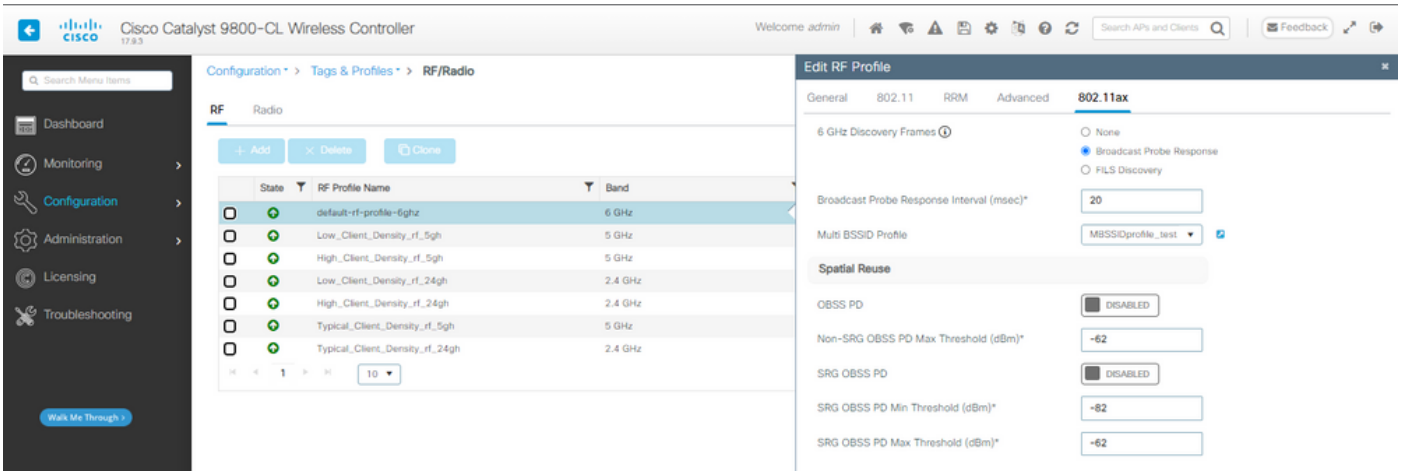
- WPA3 + AES-algoritme + 802.1x-SHA256 (FT) AKM
- WPA3 + AES-algoritme + OWE AKM
- WPA3 + AES-algoritme + SAE (FT) AKM
- WPA3 + CCMP256-algoritme + SUITEB192-1X AKM
- WPA3 + GCMP128-algoritme + SUITEB-1X AKM
- WPA3 + GCMP256-algoritme + SUITEB192-1X AKM

Basisconfiguratie

WLAN is geconfigureerd met 6GHz alleen radio beleid en UPR (Broadcast Probe Response) detectiemethode:




WLAN-basisconfiguratie



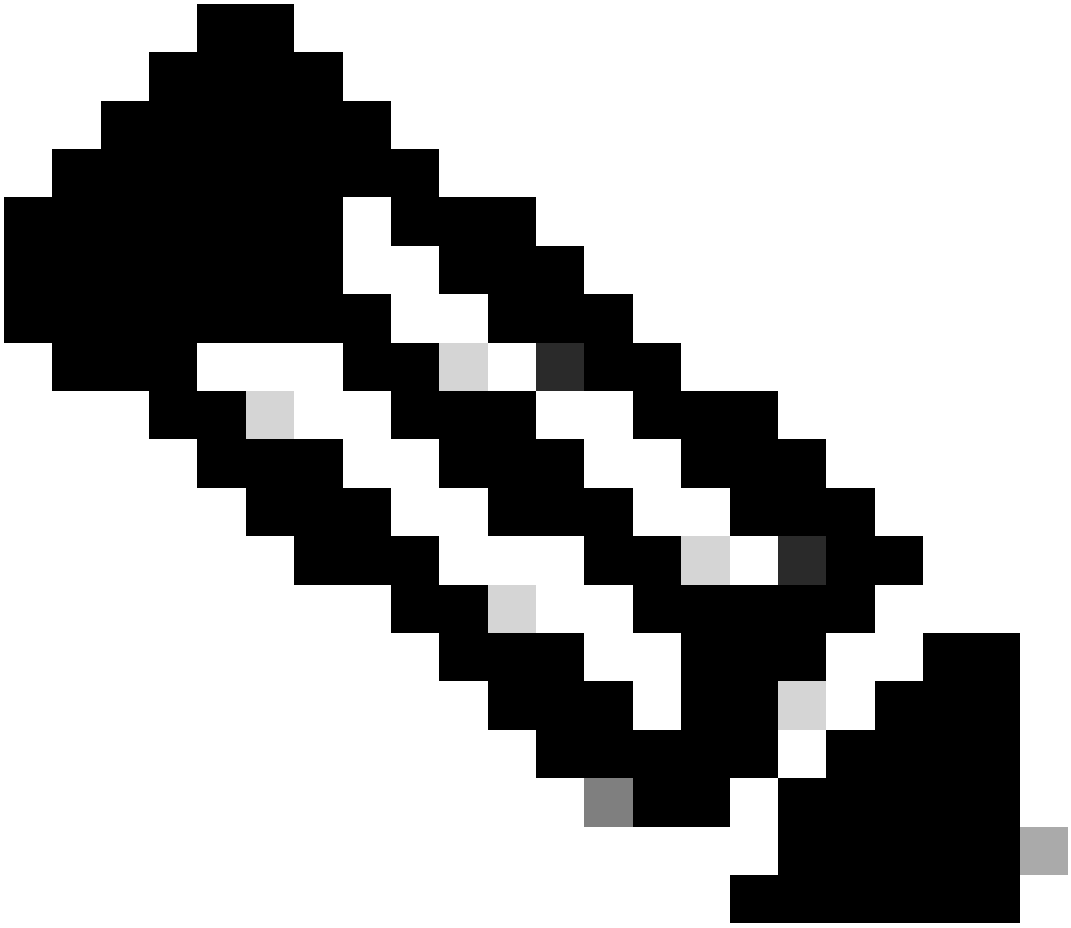
6 GHz RF-profielconfiguratie

# Verifiëren

## Beveiligingsverificatie

In deze sectie wordt het gepresenteerd de configuratie van de beveiliging en de associatiefase van de client met behulp van deze WPA3-protocolcombinaties:

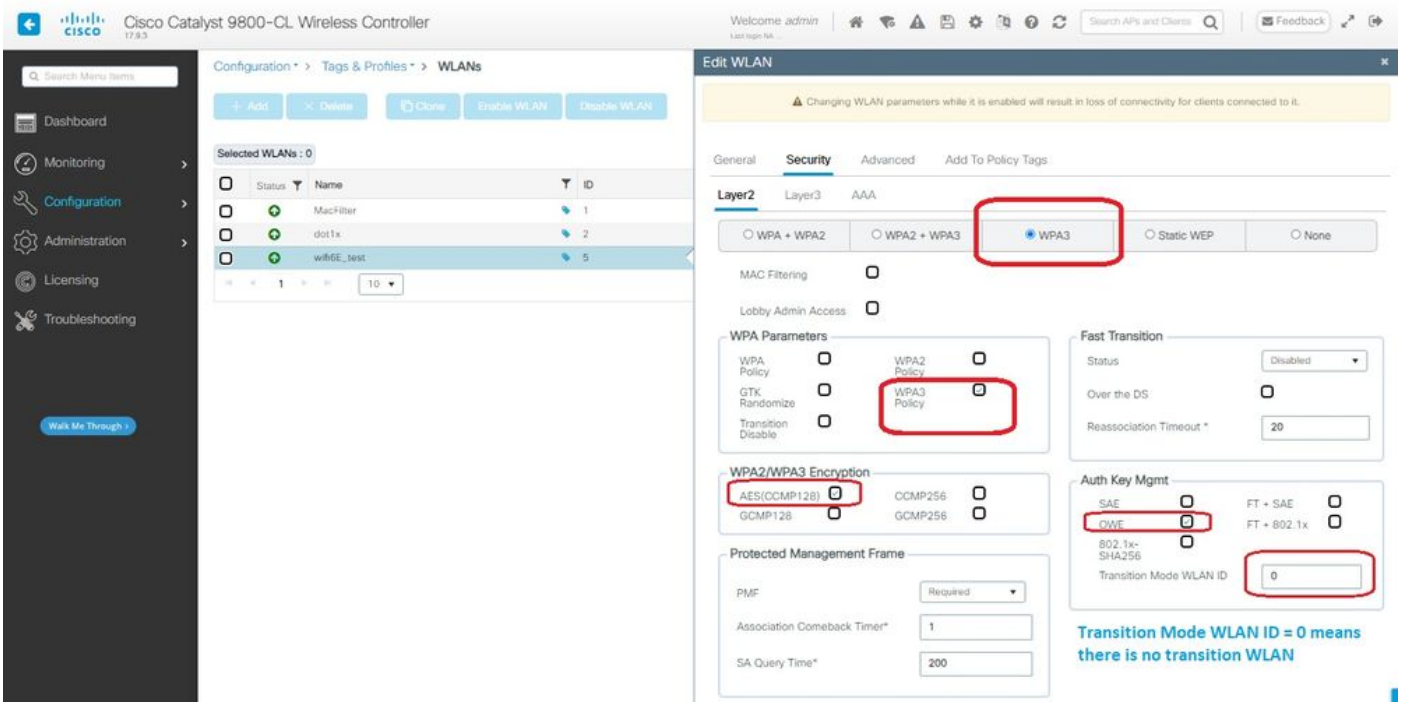
- WPA3- AES(CCMP128) + OWE
  - OWE-overgangsmodus
- WPA3-Personal
  - AES(CCMP128) + SAE
- WPA3-Enterprise
  - AES(CCMP128) + 802.1x-SHA256
  - AES(CCMP128) + 802.1x-SHA256 + FT
  - GCMP128-algoritme + SITEB-1X
  - GCMP256-algoritme + SITEB192-1X



Opmerking: Hoewel er vanaf het schrijven van dit document geen clients zijn die het GCMP128-algoritme + SUITEB-1X ondersteunen, is getest om te zien dat het wordt uitgezonden en de RSN-informatie in de bakens te controleren.

WPA3 - AES(CCPM128) + OWE

Dit is de WLAN-beveiligingsconfiguratie:




Beveiligingsinstellingen van het type OWE

Bekijk op WLC GUI van de WLAN security instellingen:




WLAN-beveiligingsinstellingen op WLC GUI

Hier kunnen we het Wi-Fi 6E-clientverbindingsproces waarnemen:

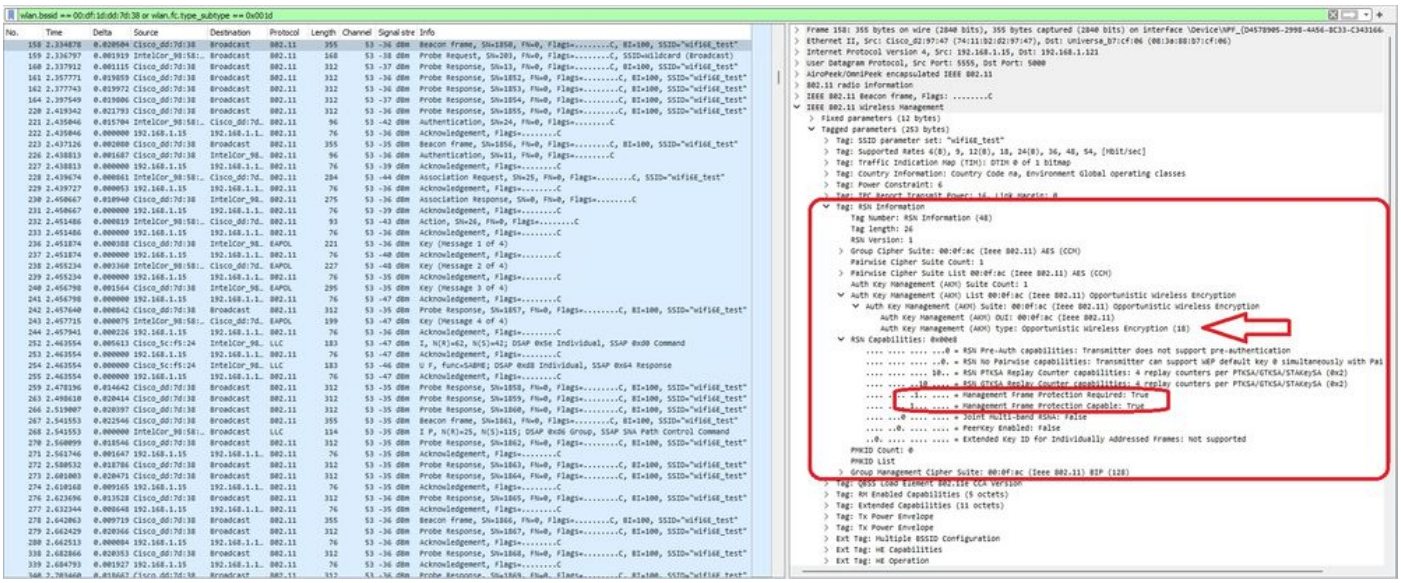
Intel AX211 switch

Hier tonen we het volledige verbindingsproces van de client Intel AX211.

OWE-detectie

Hier zie je de bakens OTA. De AP adverteert ondersteuning voor OWE met behulp van AKM suite selector voor OWE onder RSN informatie element.

Je ziet AKM suite type value 18 (00-0F-AC:18) dat aangeeft OWE ondersteuning.



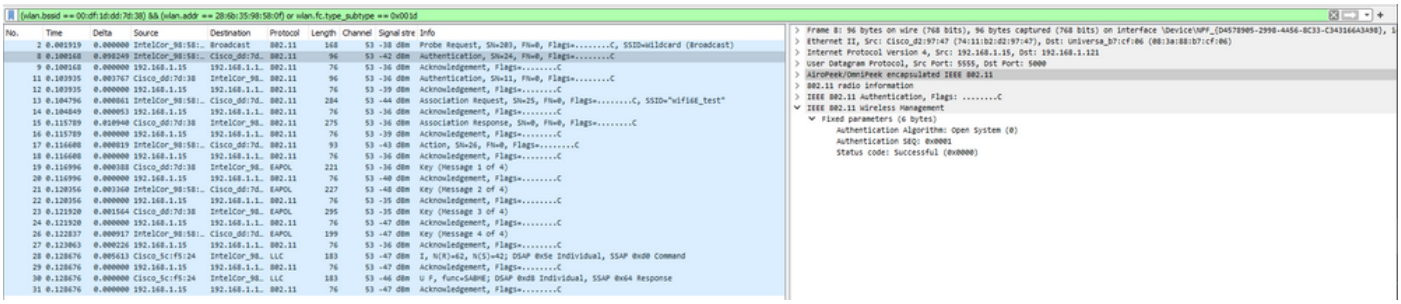
OWE beacon frame

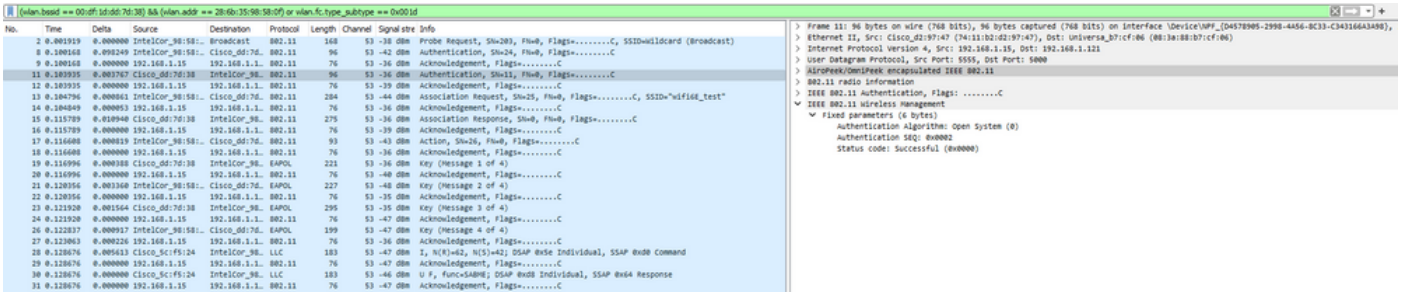
Als u kijkt naar het veld RSN-functies, ziet u dat AP adverteert met zowel MFP-functies (Management Frame Protection) als MFP Required bit set to 1.

OWE-associatie

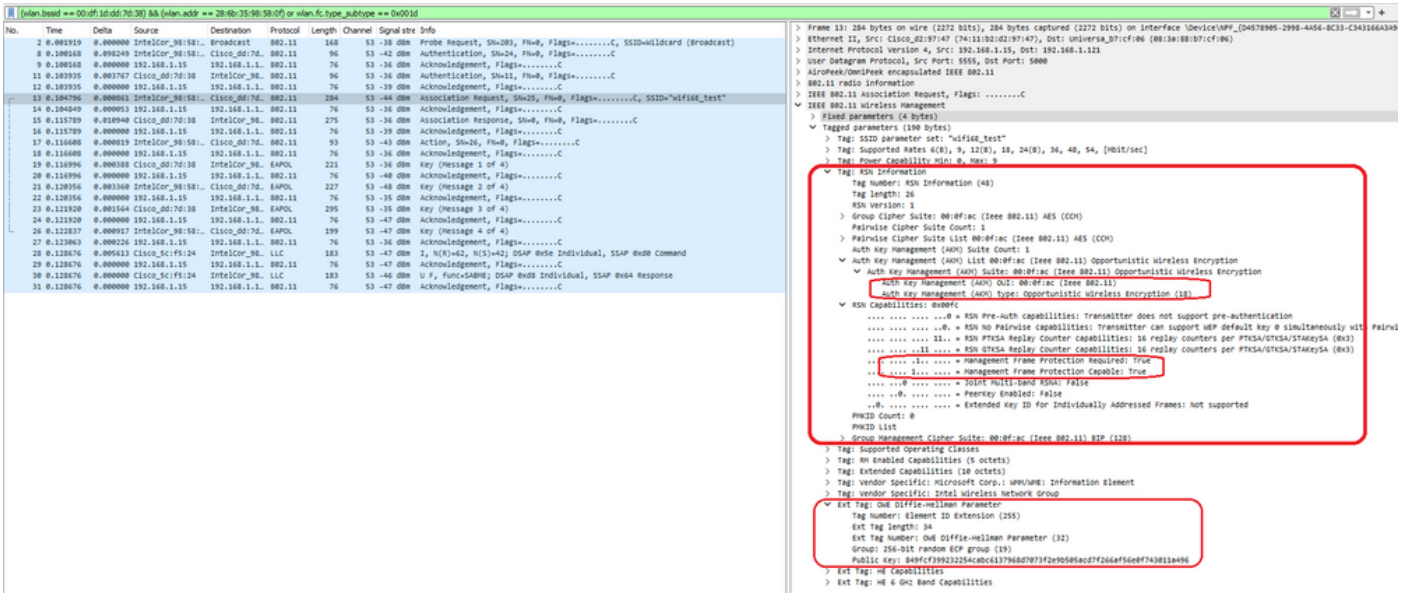
U kunt de UPR zien die in de uitzendmodus wordt verstuurd en vervolgens de associatie zelf.

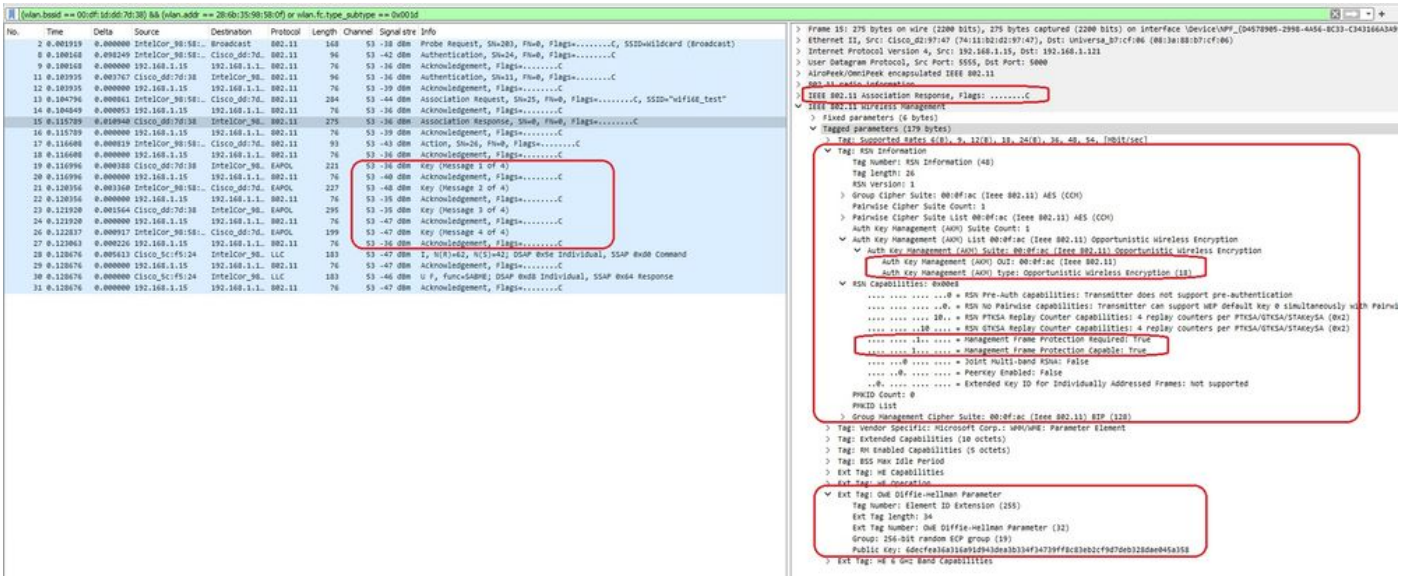
De OWE begint met het Open authenticatieverzoek en antwoord:





Vervolgens moet een client die OWE wil doen OWE AKM aangeven in het RSN IE of Association request frame en Diffie Helman (DH) parameter element opnemen:

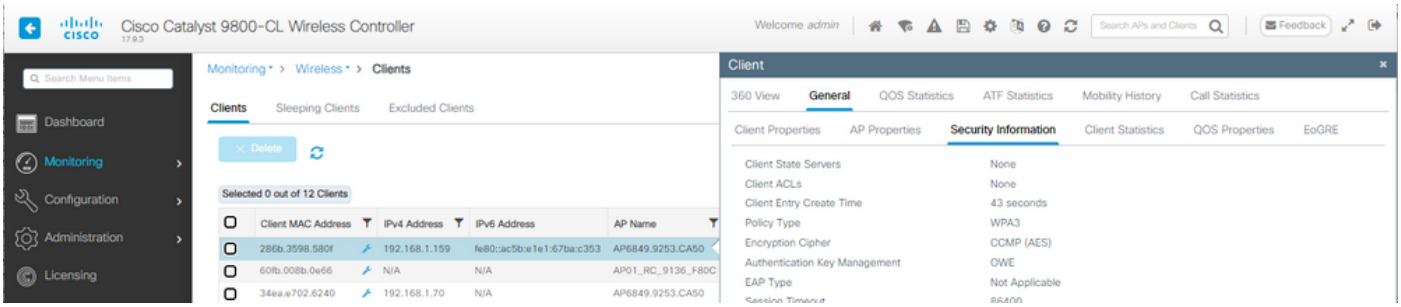




Antwoord van OWE Association

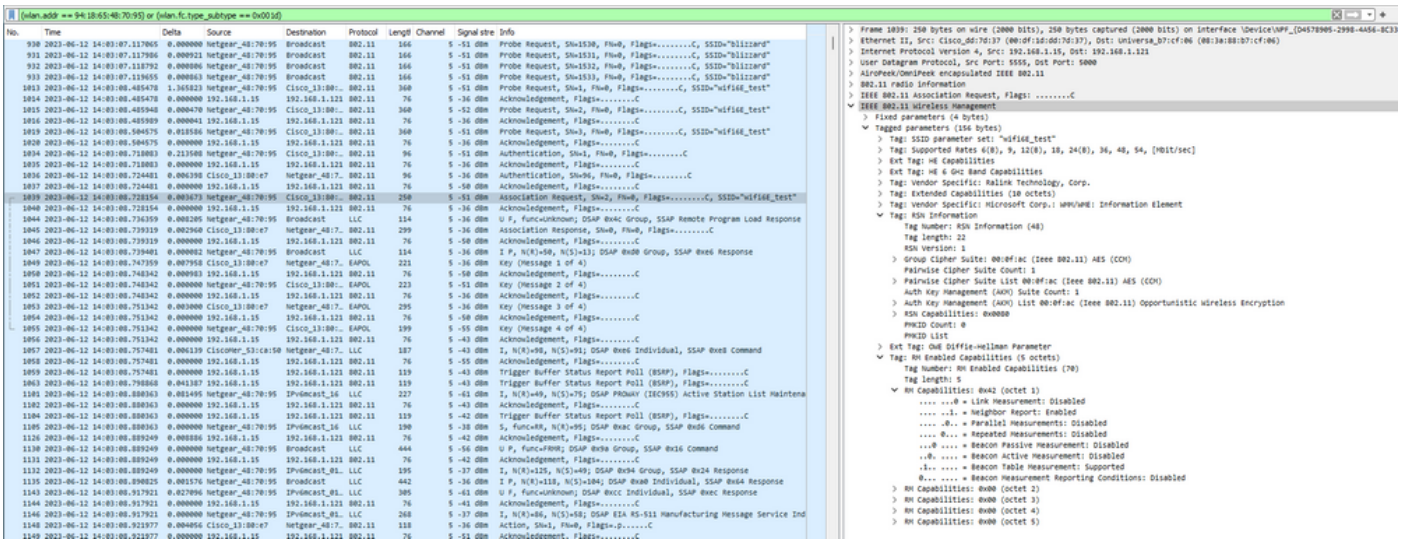
Na de associatiereactie kunnen we de 4-voudige handdruk en client-bewegingen naar verbonden staat zien.

Hier kunt u de klantgegevens zien op de WLC GUI:

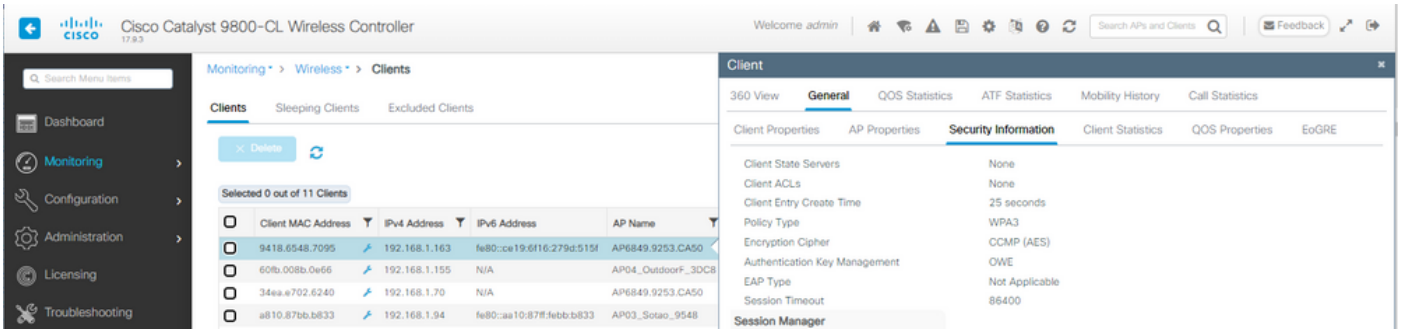



NetGear A800

OTA-verbinding met focus op RSN-informatie van client:

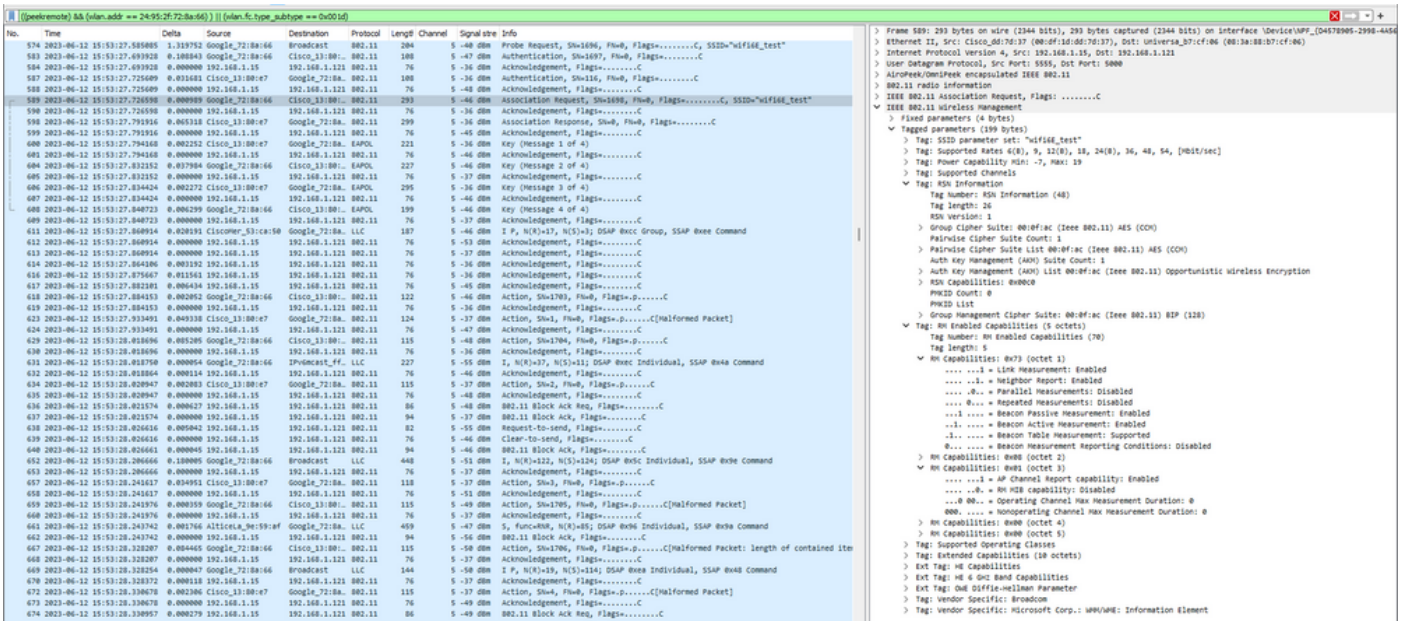


Klantgegevens in WLC:

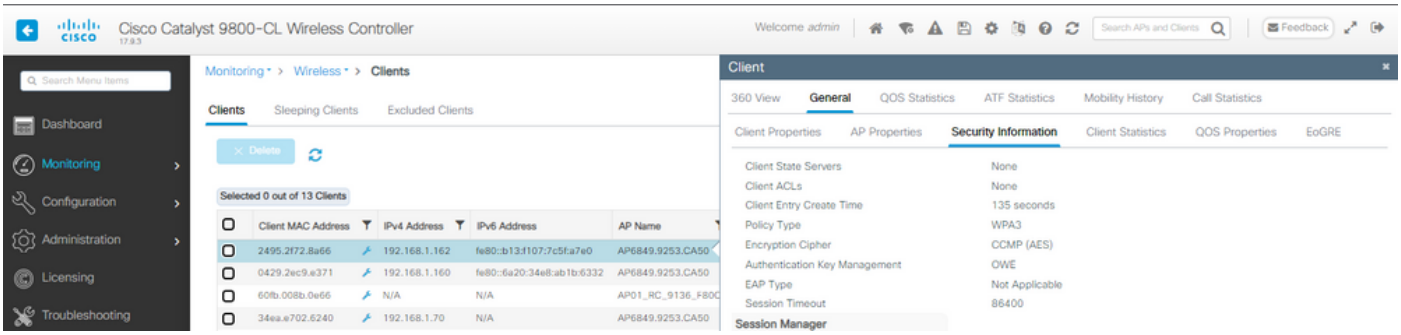



Pixel 6a

OTA-verbinding met focus op RSN-informatie van client:

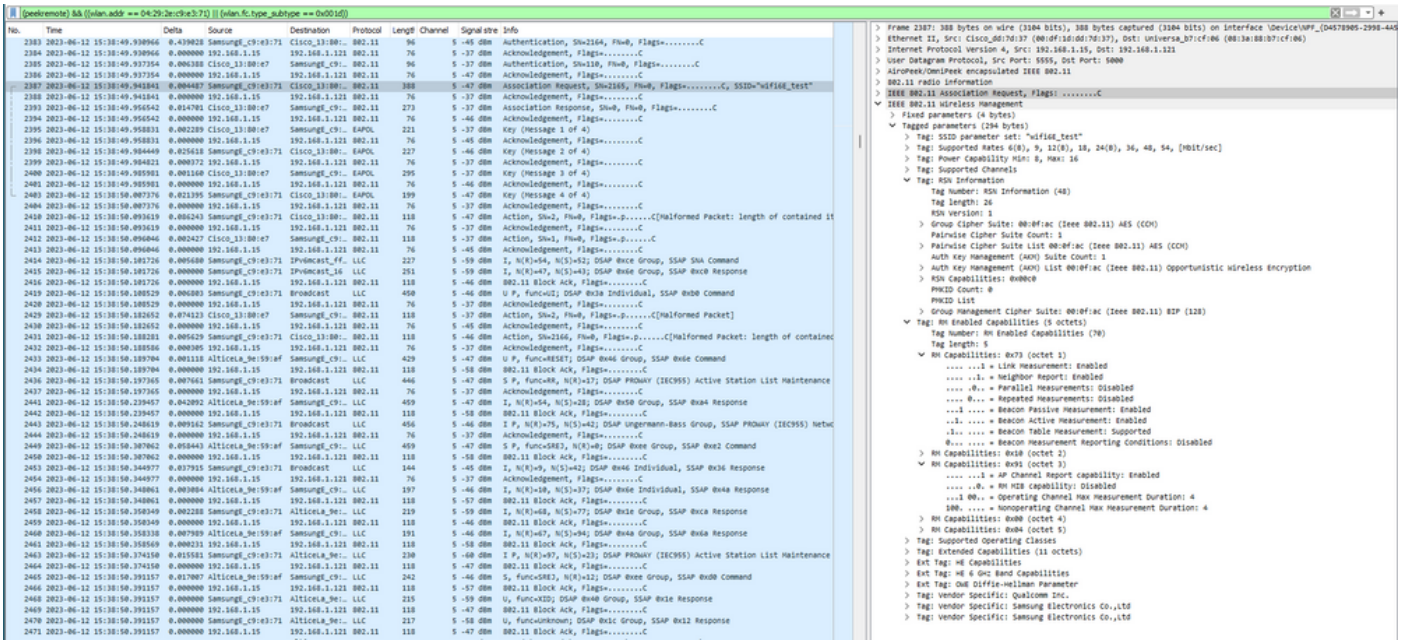


Klantgegevens in WLC:

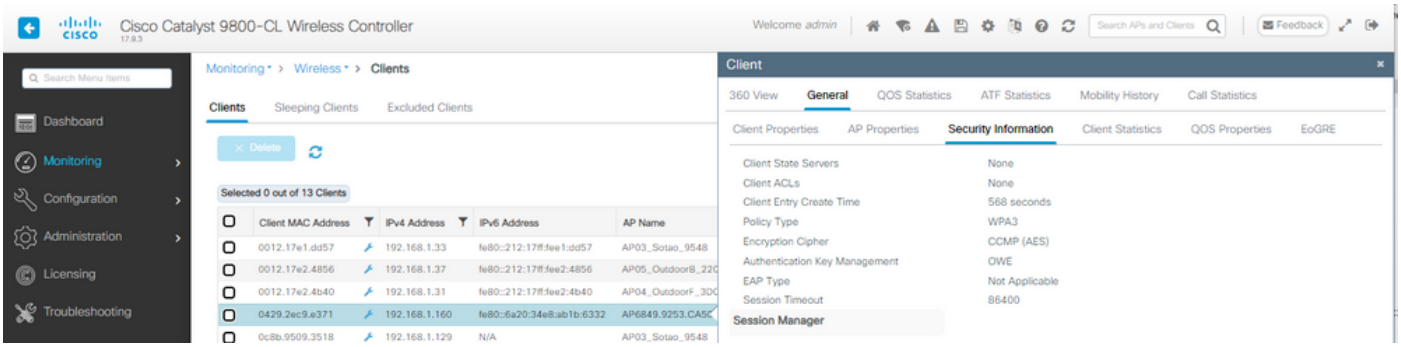



Samsung S23

OTA-verbinding met focus op RSN-informatie van client:



Klantgegevens in WLC:

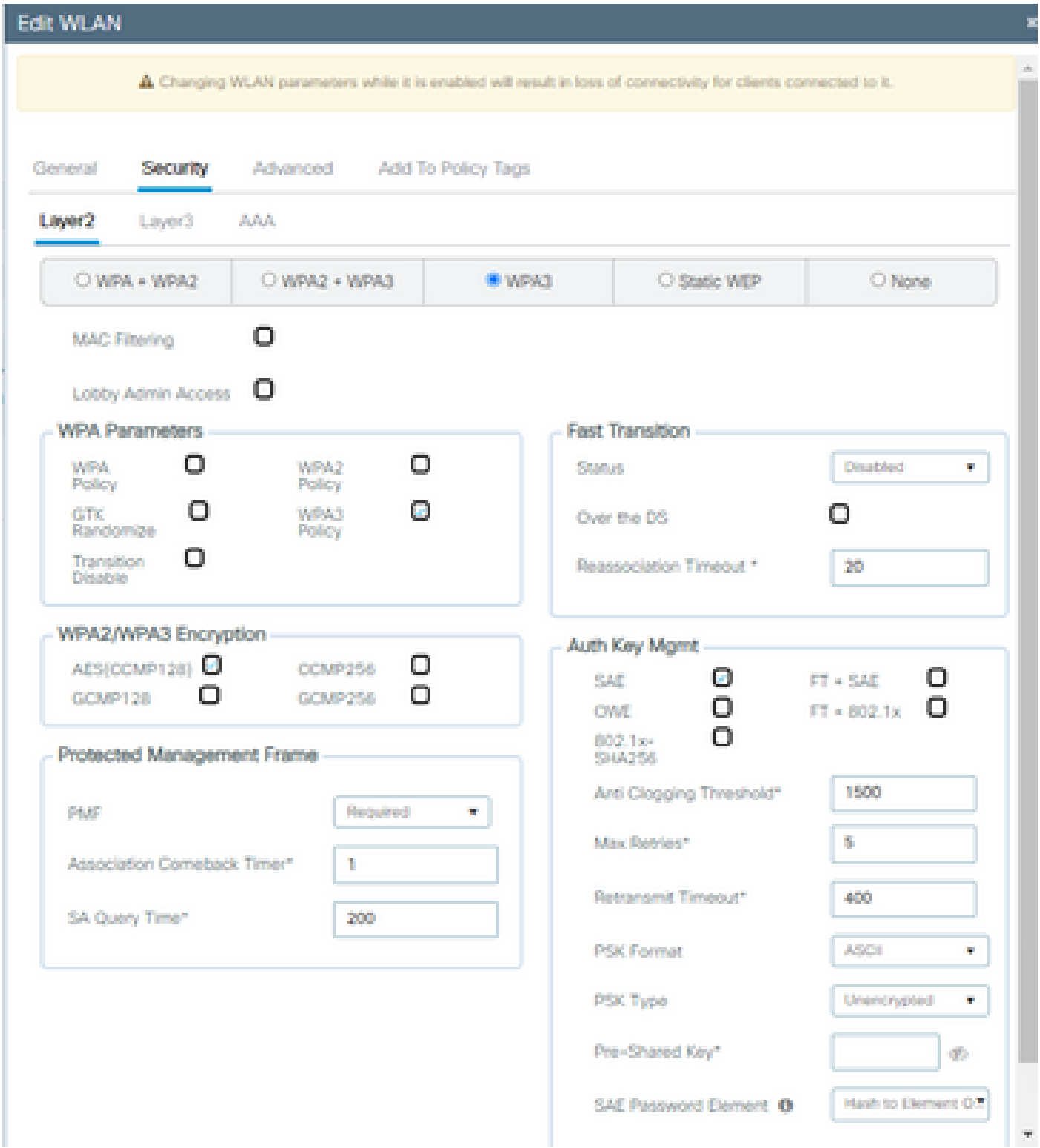



WPA3 - AES(CCPM128) + OWE met overgangsmodus

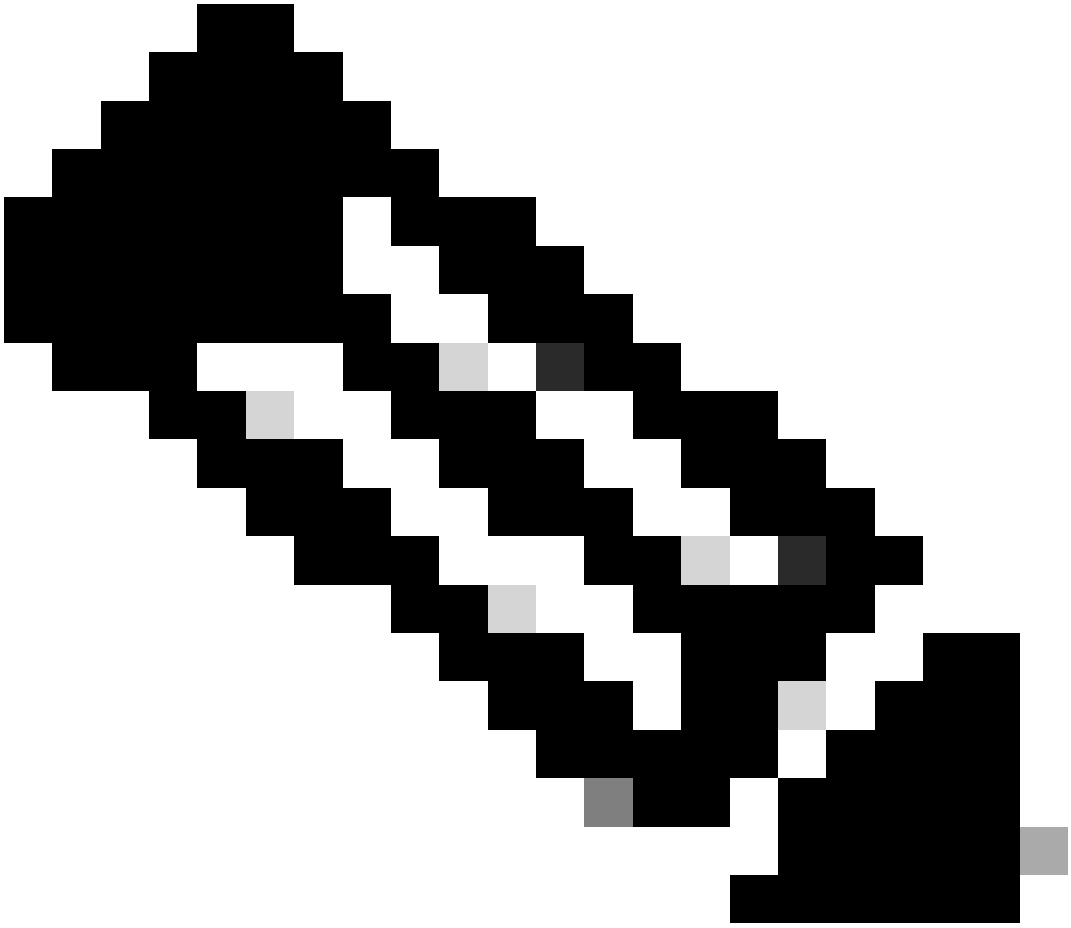
Gedetailleerde configuratie en probleemoplossing van de OWE Transition Mode beschikbaar in dit document: [Configure Enhanced Open SSID with Transition Mode - OWE].

WPA3-Personal - AES(CCMP128) + SAE

WLAN-beveiligingsconfiguratie:



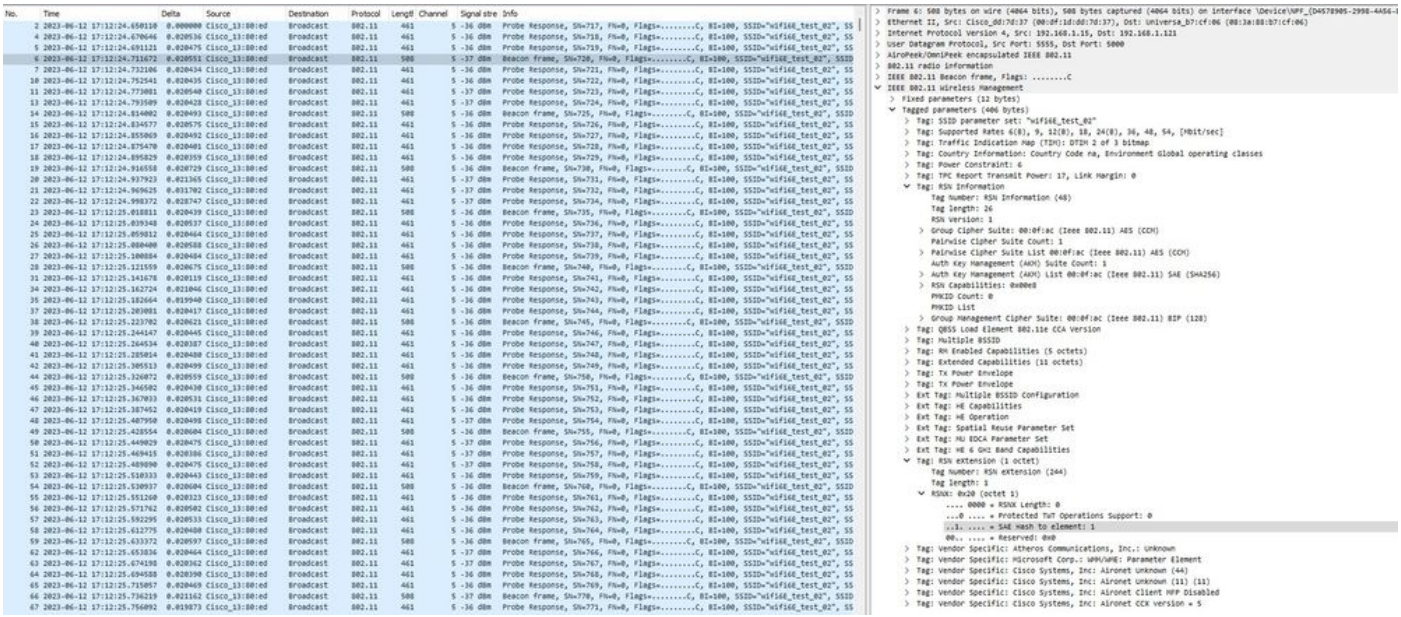

Configuratie WPA3 SAE



Opmerking: Houd er rekening mee dat jagen en pecken niet is toegestaan met 6 GHz radiobeleid. Wanneer u een 6GHz alleen WLAN configureert, moet u H2E SAE-wachtwoordelement selecteren.

Bekijk op WLC GUI van de WLAN security instellingen:


Verificatie van de OTA van bakens:

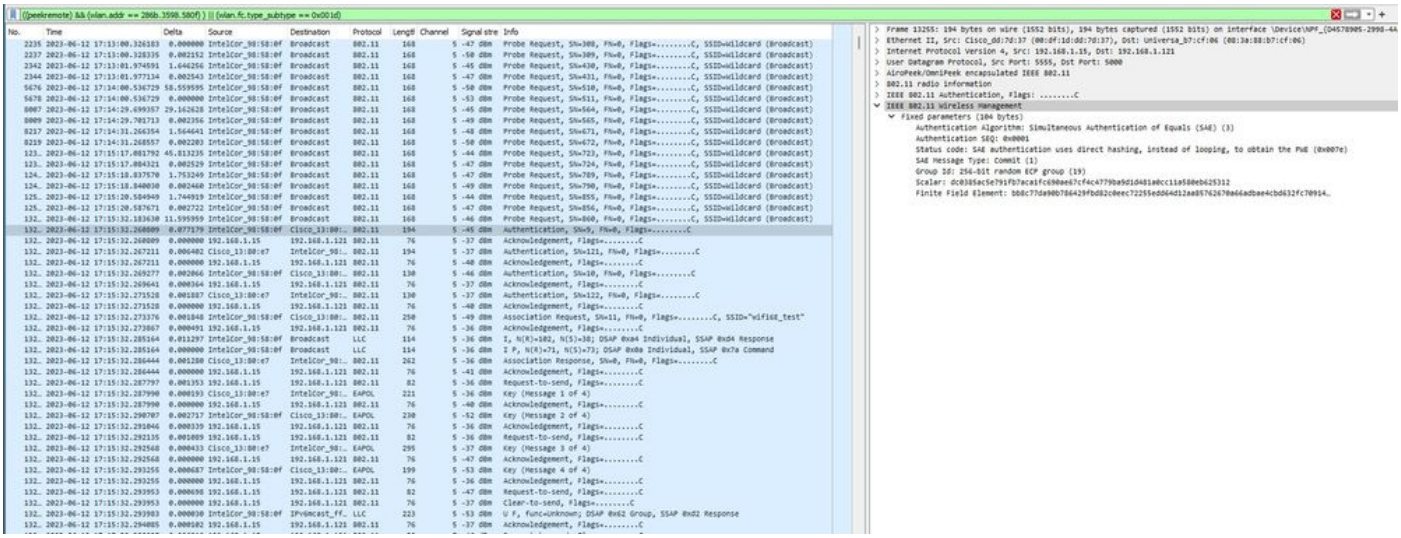


WPA3 SAE-bakens

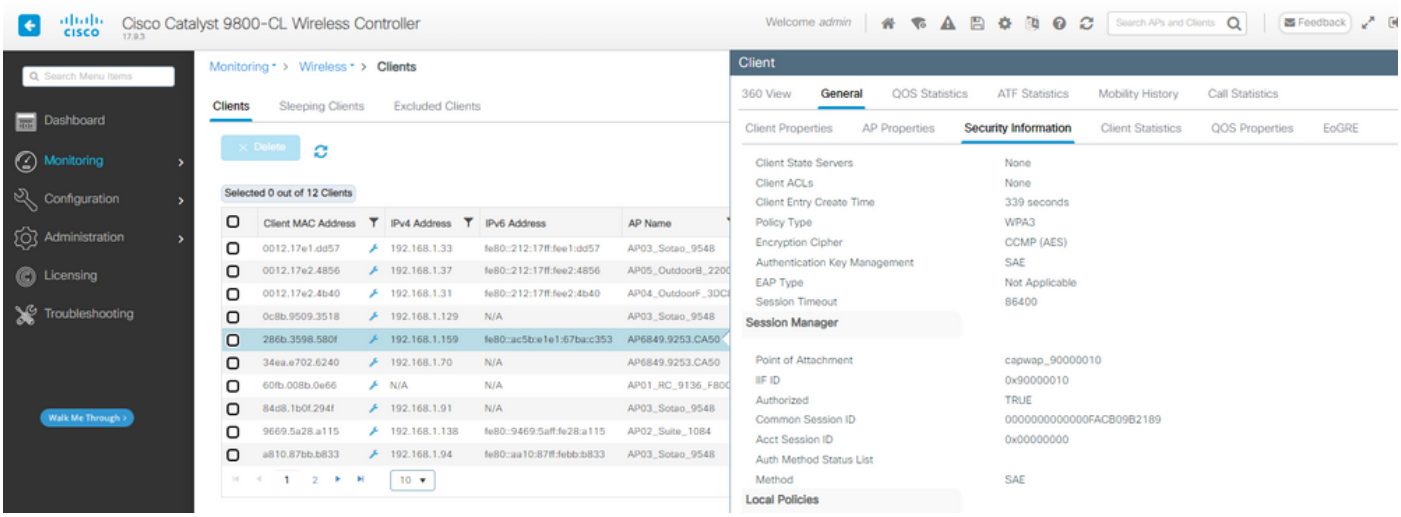
Hier kunnen we Wi-Fi 6E-clients waarnemen die associëren:

Intel AX211 switch

OTA-verbinding met focus op RSN-informatie van client:

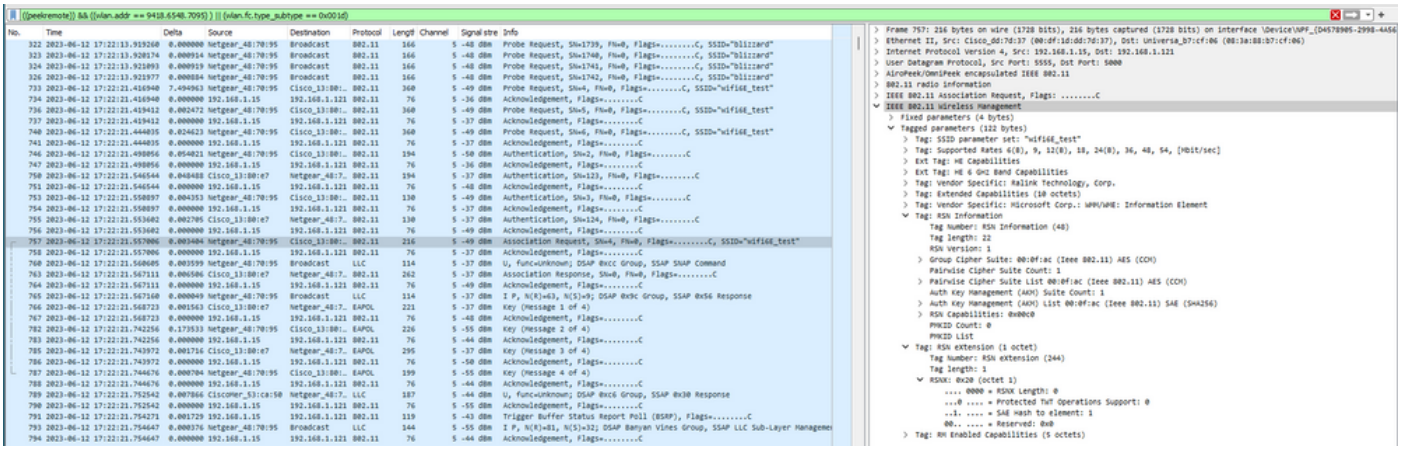


Klantgegevens in WLC:

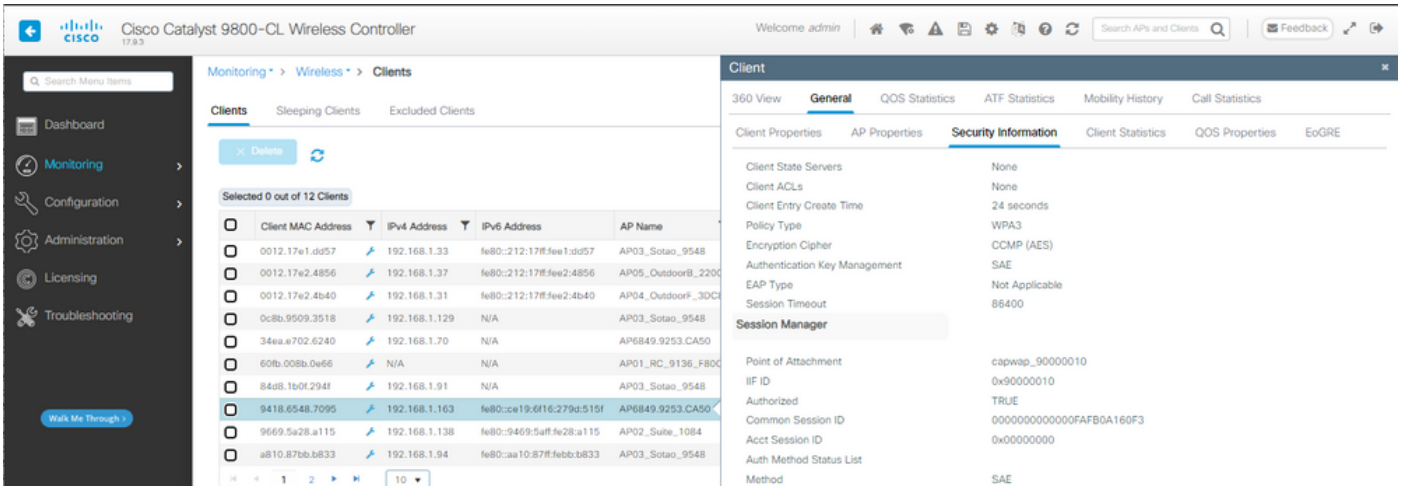



NetGear A800

OTA-verbinding met focus op RSN-informatie van client:

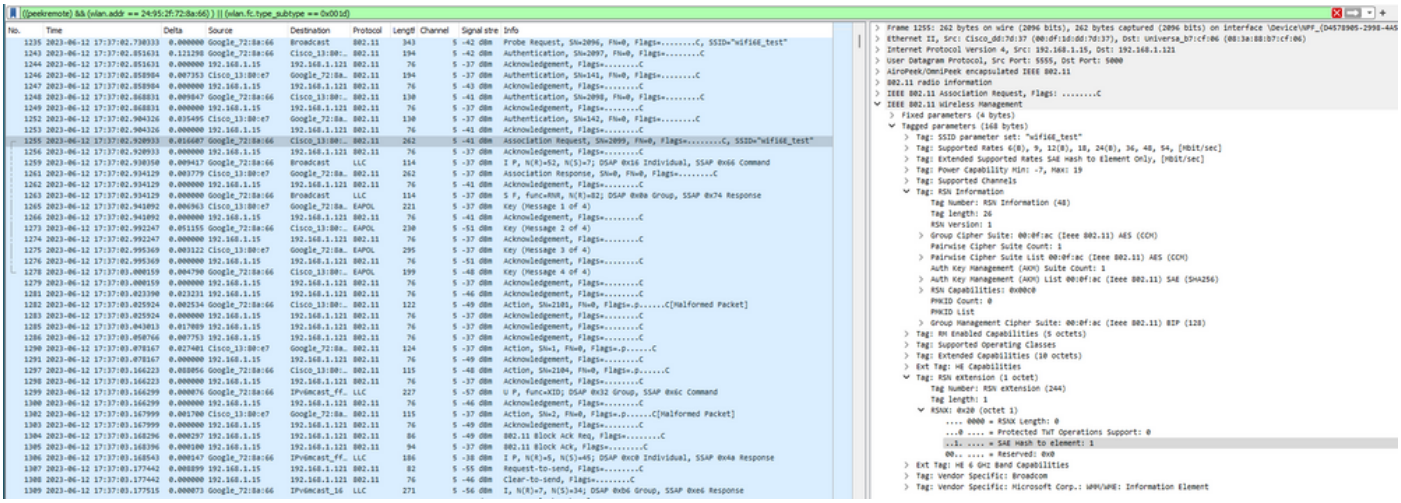


Klantgegevens in WLC:

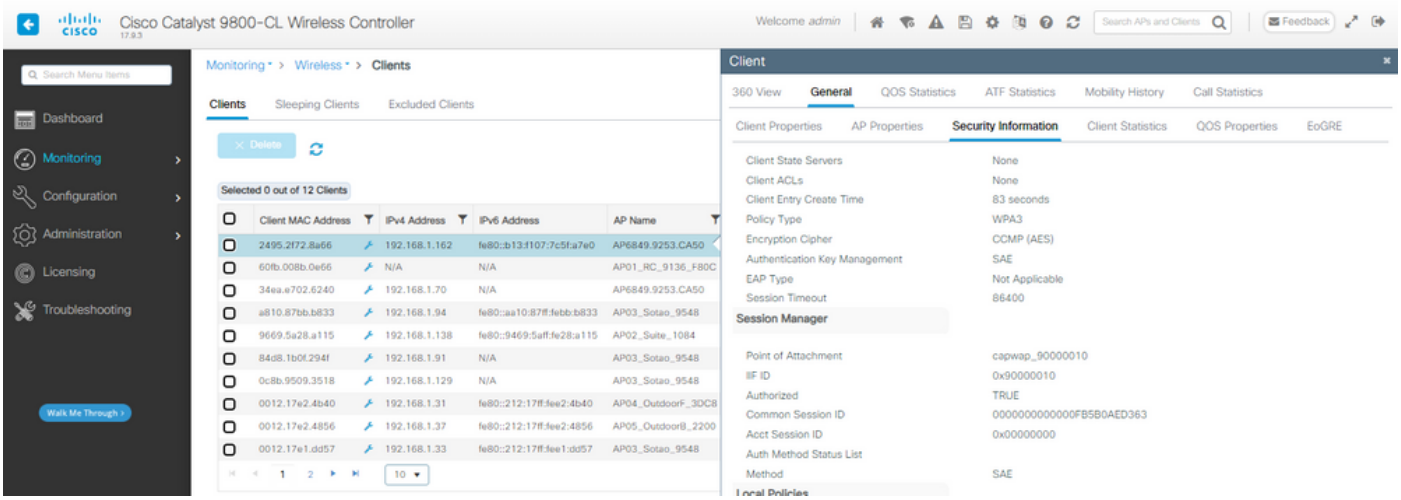



Pixel 6a

OTA-verbinding met focus op RSN-informatie van client:

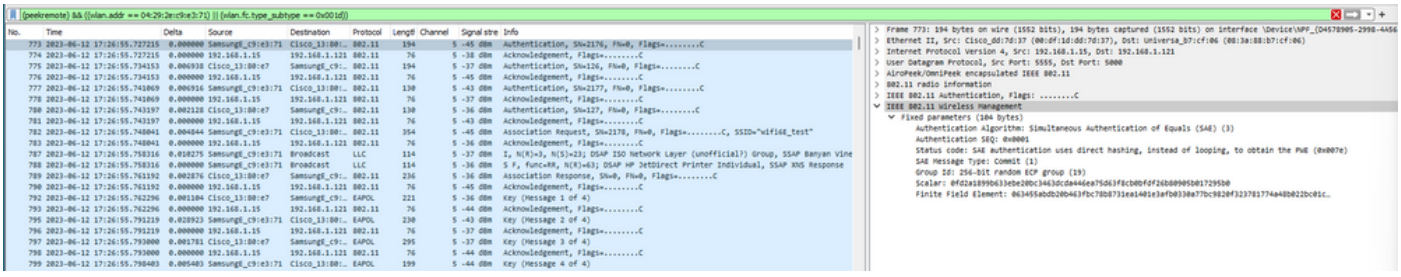


Klantgegevens in WLC:

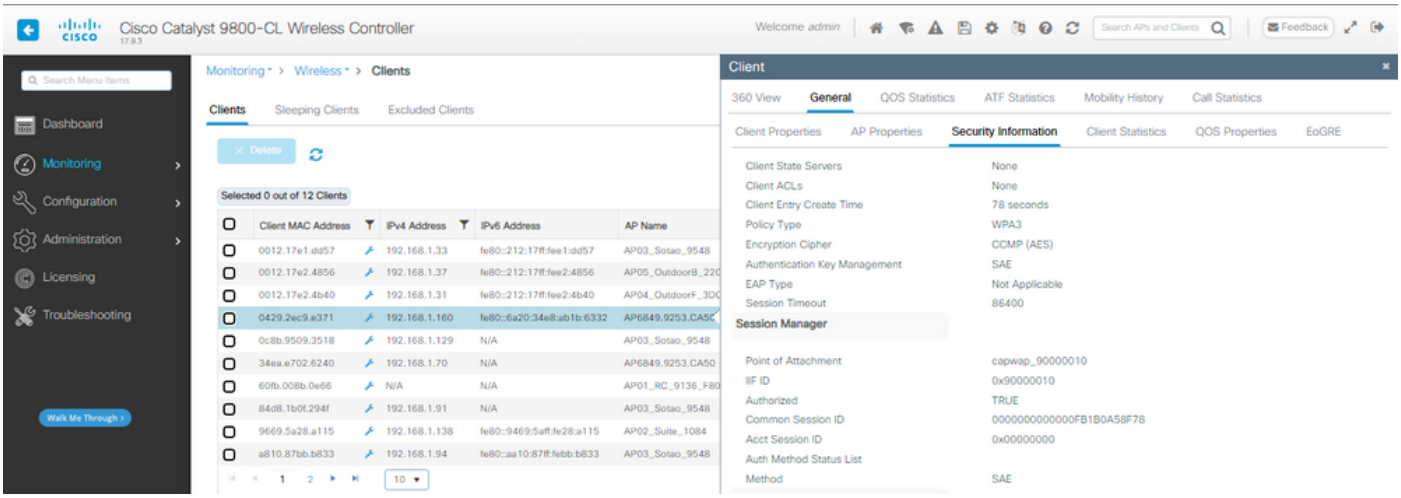



Samsung S23

OTA-verbinding met focus op RSN-informatie van client:

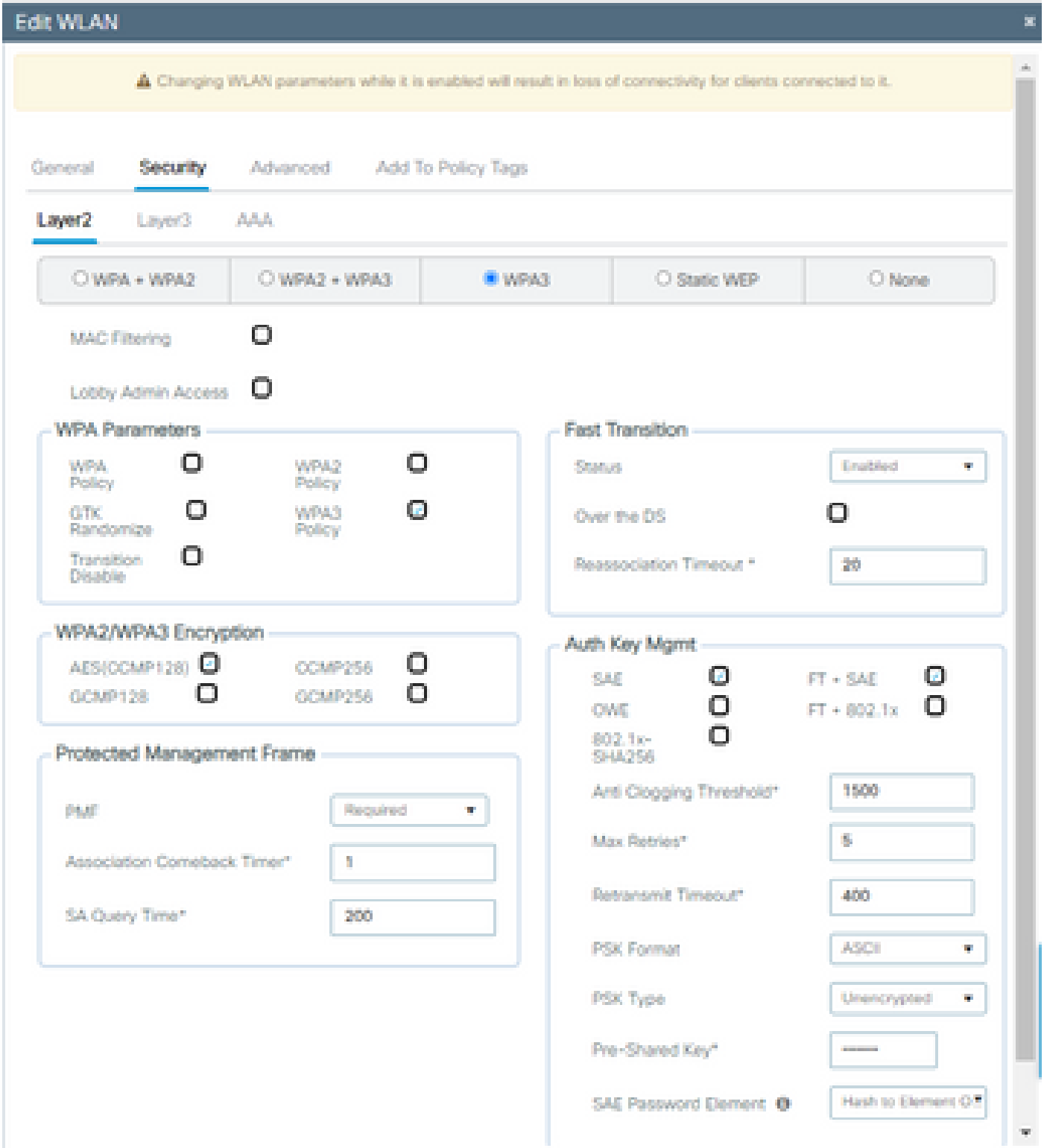


Klantgegevens in WLC:




WPA3-Personal - AES(CCMP128) + SAE + FT

WLAN-beveiligingsconfiguratie:


Edit WLAN
Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.
General
Security
Advanced
Add To Policy Tags
Layer2
Layer3
AAA
WPA + WPA2
WPA2 + WPA3
WPA3
Static WEP
None
MAC Filtering
Lobby Admin Access
WPA Parameters
WPA Policy
WPA2 Policy
GTK Randomize
WPA3 Policy
Transition Disable
WPA2/WPA3 Encryption
AES(CCMP128)
CCMP256
GCMP128
GCMP256
Protected Management Frame
PMF
Required
Association Comeback Timer*
1
SA Query Time*
200
Fast Transition
Status
Enabled
Over the DS
Reassociation Timeout *
20
Auth Key Mgmt
SAE
FT + SAE
OWE
FT + 802.1x
802.1x-SHA256
Anti Clogging Threshold*
1500
Max Retries*
5
Retransmit Timeout*
400
PSK Format
ASCII
PSK Type
Unencrypted
Pre-Shared Key*
SAE Password Element
Hash to Element (H

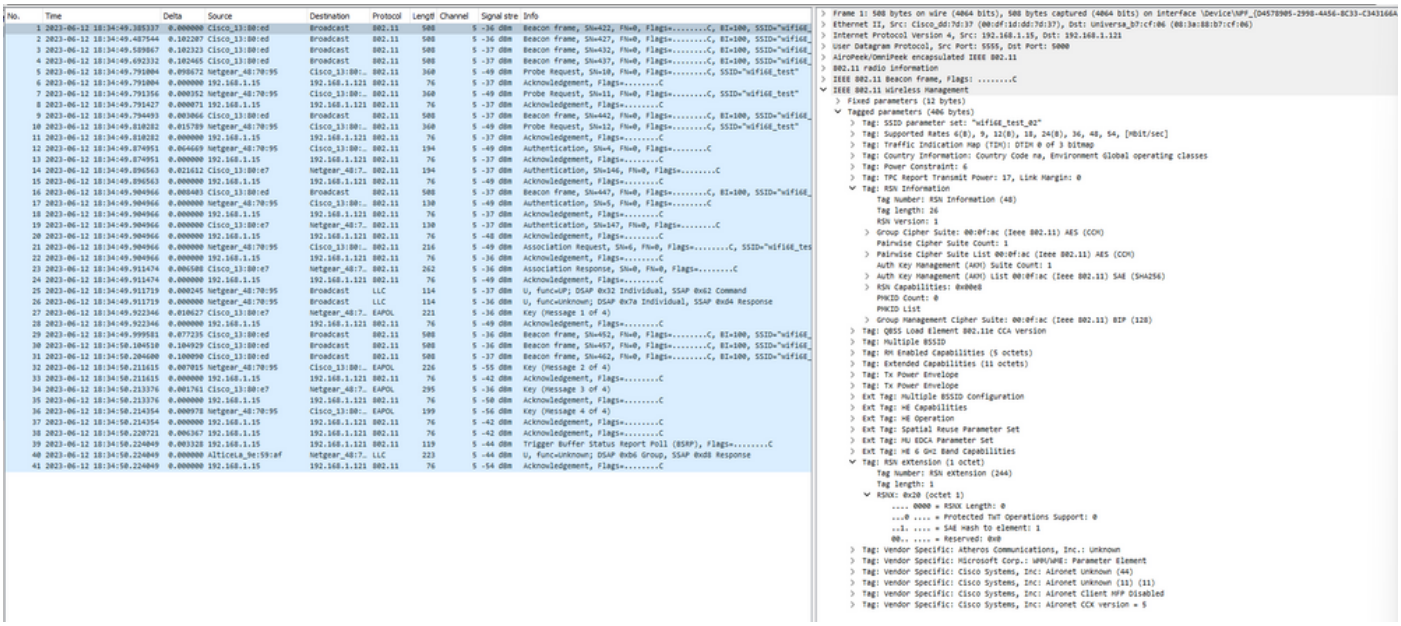
Waarschuwing: in het beheer van de verificatiesleutel staat de WLC toe om FT+SAE te selecteren zonder dat SAE is ingeschakeld, maar er werd geconstateerd dat de clients geen verbinding konden maken. Schakel altijd beide selectievakjes SAE en FT+SAE in als u SAE met Fast Transition wilt gebruiken.

---

Bekijk op WLC GUI van de WLAN security instellingen:




Verificatie van de OTA van bakens:

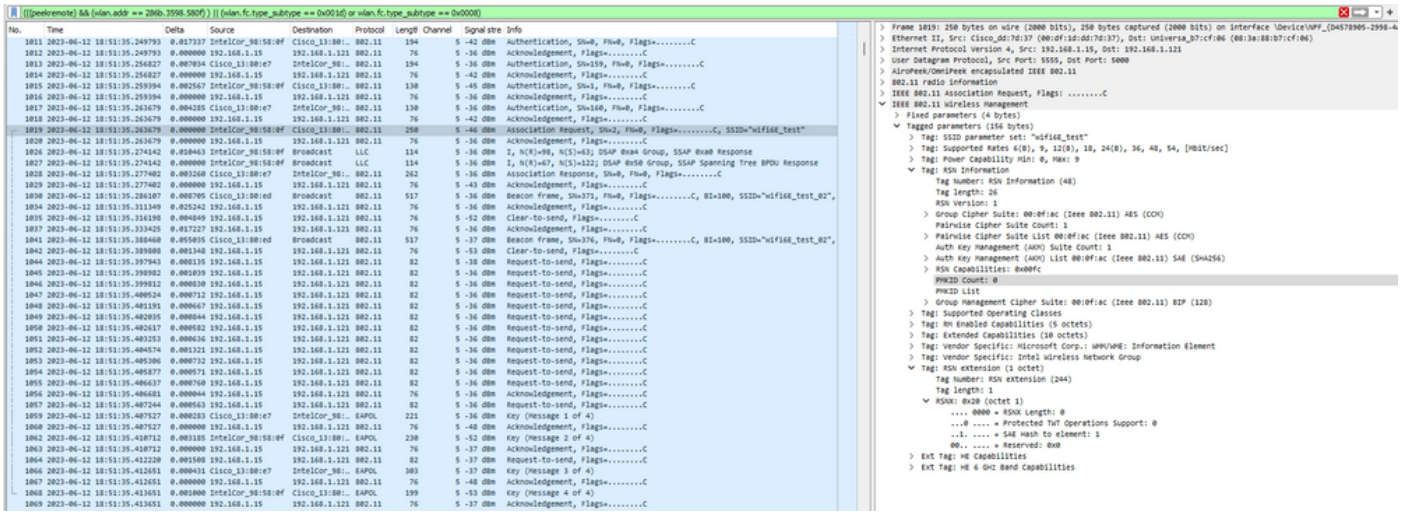


WPA3 SAE + FT-bakens

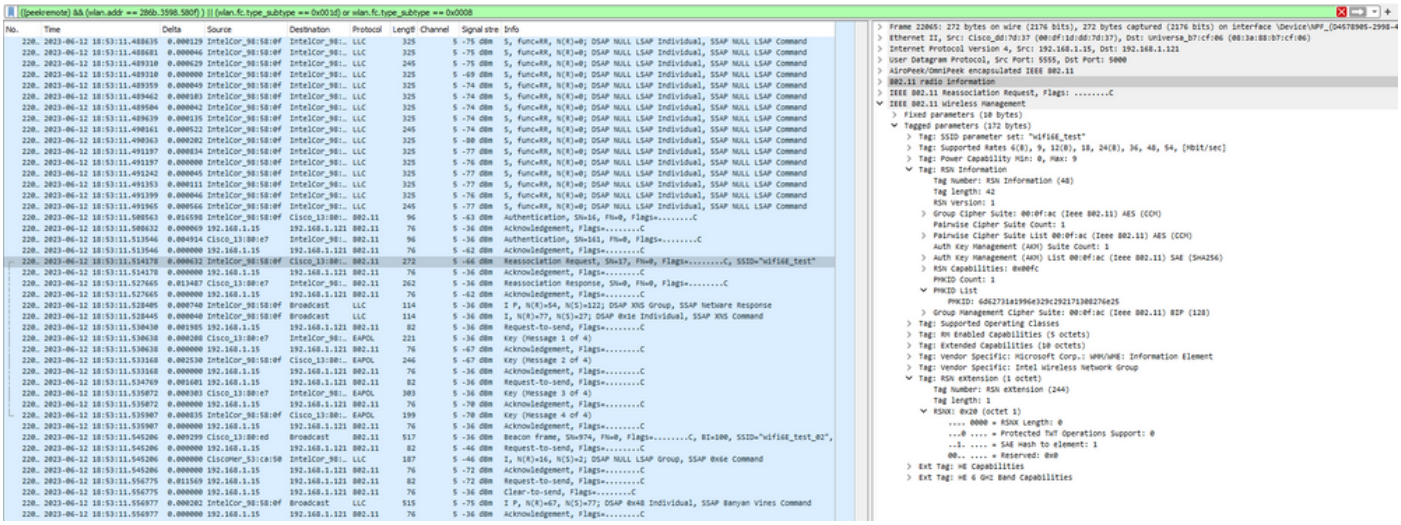
Hier kunnen we Wi-Fi 6E-clients waarnemen die associëren:

Intel AX211 switch

OTA-verbinding met focus op RSN-informatie van client:

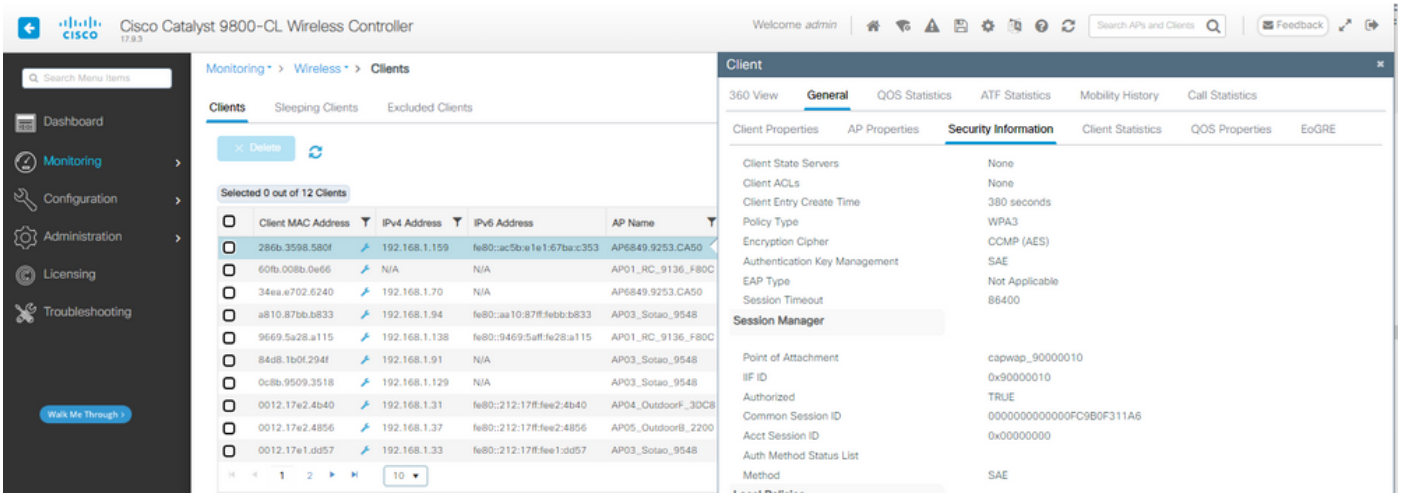


Zwervend evenement waar u de PMKID kunt zien:



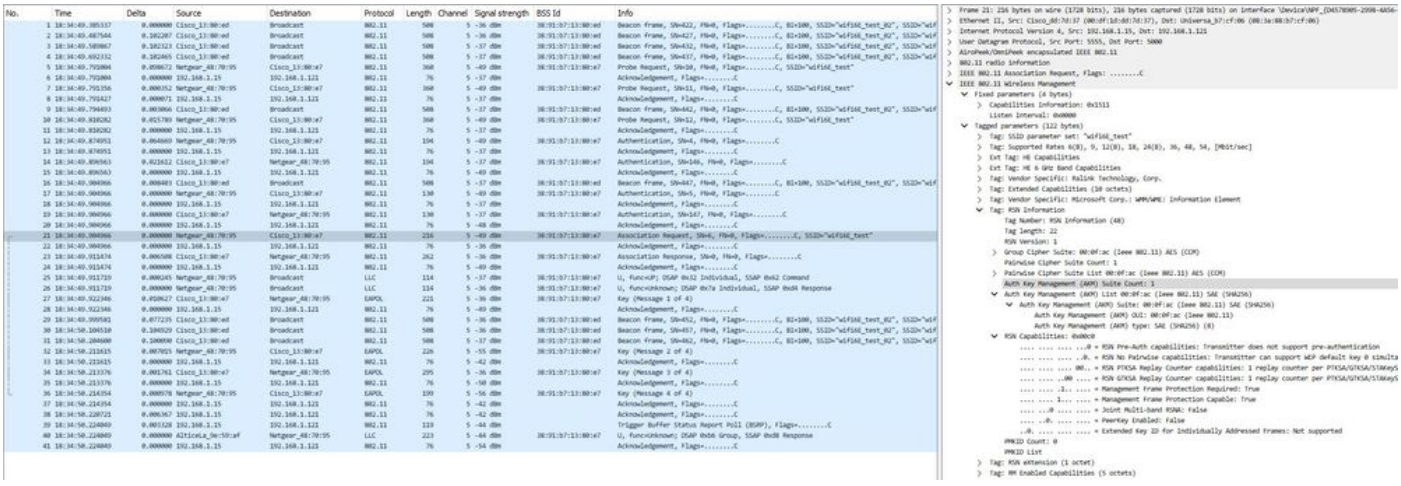
WPA3 SAE + FT-reassociatieaanvraag

## Klantgegevens in WLC:



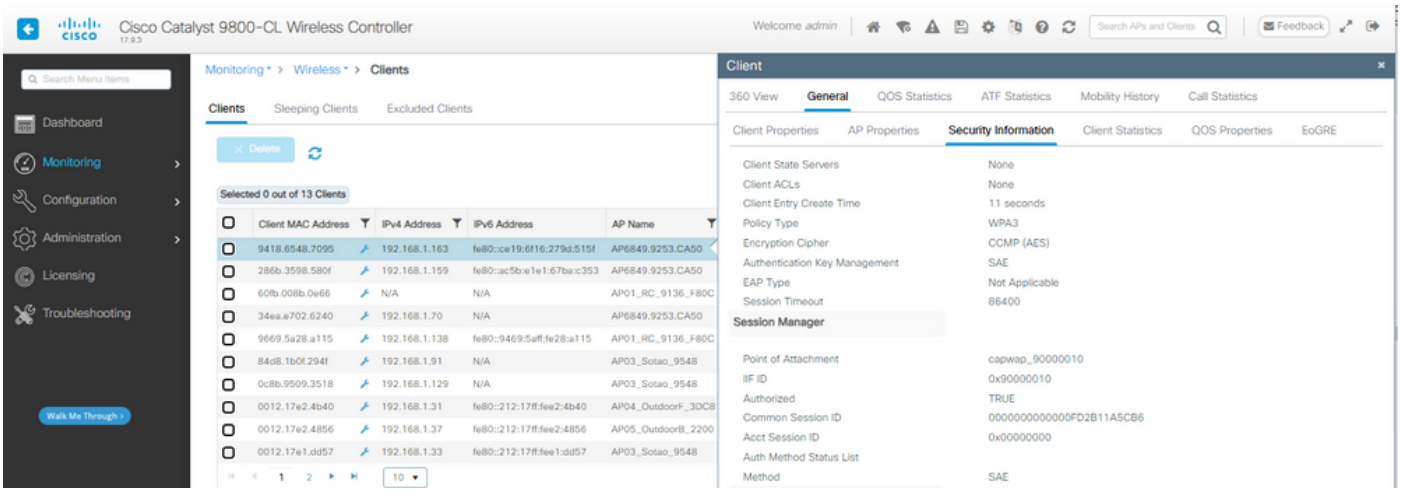

## NetGear A800

## OTA-verbinding met focus op de RSN-informatie van de client. Eerste aansluiting:



ssss

Klantgegevens in WLC:




Pixel 6a

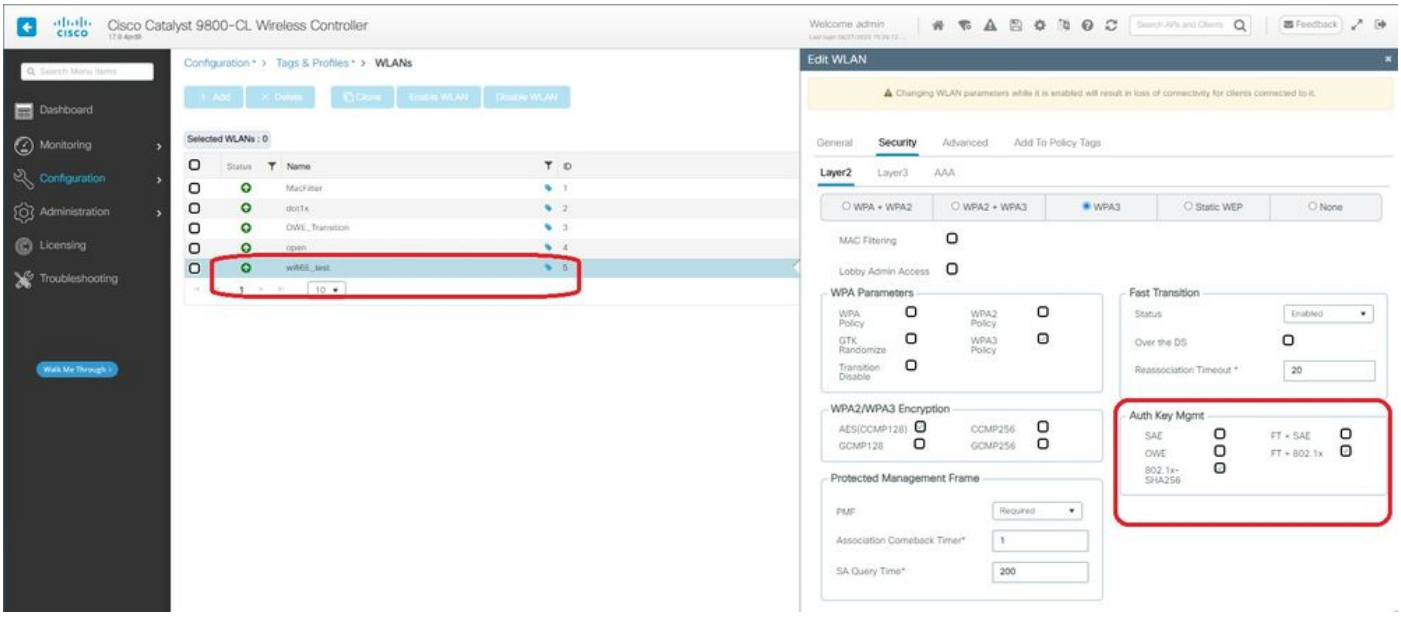
Het apparaat kon niet zwerven wanneer FT is ingeschakeld.

Samsung S23

Het apparaat kon niet zwerven wanneer FT is ingeschakeld.

WPA3-Enterprise + AES(CCMP128) + 802.1x-SHA256 + FT

WLAN-beveiligingsconfiguratie:




WPA3 Enterprise 802.1x-SHA256 + FTWLAN-beveiligingsconfiguratie

Bekijk op WLC GUI van de WLAN security instellingen:



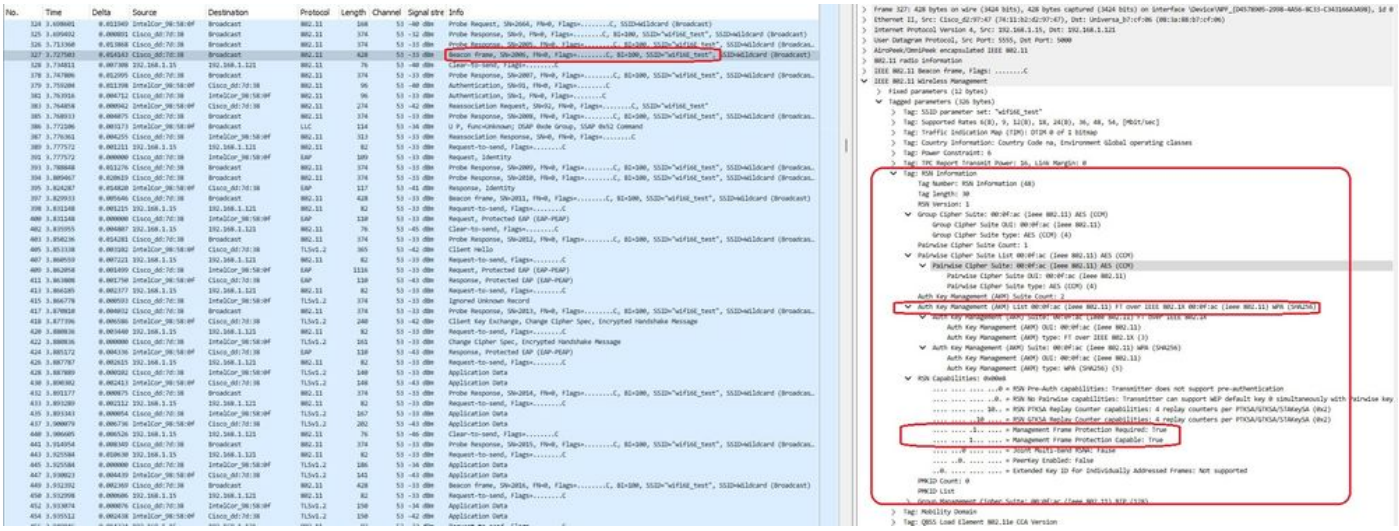
Hier kunnen we de Live-logboeken van ISE zien met de authenticaties die van elk apparaat

komen:

| | Time | Status | Details | Repeat ... | Identity | Endpoint ID | Endpoint Profile | Authenticat... | Authorizati... | Authorizati... | IP Address | Network Device |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| × | | | | | Identity | Endpoint ID | Endpoint Profile | Authentication | Authorization | Authorization | IP Address | Network Device |
| | Jun 27, 2023 01:52:38.130 PM | | | 0 | tantunes | 04:29:2E:C9:E3:71 | | WirelessDot... | WirelessDot... | PermitAccess | | |
| | Jun 27, 2023 01:52:38.130 PM | | | | tantunes | 04:29:2E:C9:E3:71 | | WirelessDot... | WirelessDot... | PermitAccess | | eWLC-9800-01 |
| | Jun 27, 2023 01:51:53.850 PM | | | 0 | tantunes | 24:95:2F:72:8A:66 | Unknown | WirelessDot... | WirelessDot... | PermitAccess | | |
| | Jun 27, 2023 01:51:53.850 PM | | | | tantunes | 24:95:2F:72:8A:66 | Unknown | WirelessDot... | WirelessDot... | PermitAccess | | eWLC-9800-01 |
| | Jun 27, 2023 01:50:58.679 PM | | | 0 | tantunes | 94:18:65:48:70:95 | Netgear-Device | WirelessDot... | WirelessDot... | PermitAccess | | |
| | Jun 27, 2023 01:50:58.679 PM | | | | tantunes | 94:18:65:48:70:95 | Netgear-Device | WirelessDot... | WirelessDot... | PermitAccess | | eWLC-9800-01 |
| | Jun 27, 2023 01:50:43.883 PM | | | | tantunes | 94:18:65:48:70:95 | Netgear-Device | WirelessDot... | WirelessDot... | PermitAccess | | eWLC-9800-01 |
| | Jun 27, 2023 01:50:42.877 PM | | | 0 | tantunes | 28:6B:35:98:58:0F | Intel-Device | WirelessDot... | WirelessDot... | PermitAccess | | |
| | Jun 27, 2023 01:50:42.877 PM | | | | tantunes | 28:6B:35:98:58:0F | Intel-Device | WirelessDot... | WirelessDot... | PermitAccess | | eWLC-9800-01 |

ISE-livelogs

Beacons OTA ziet er zo uit:

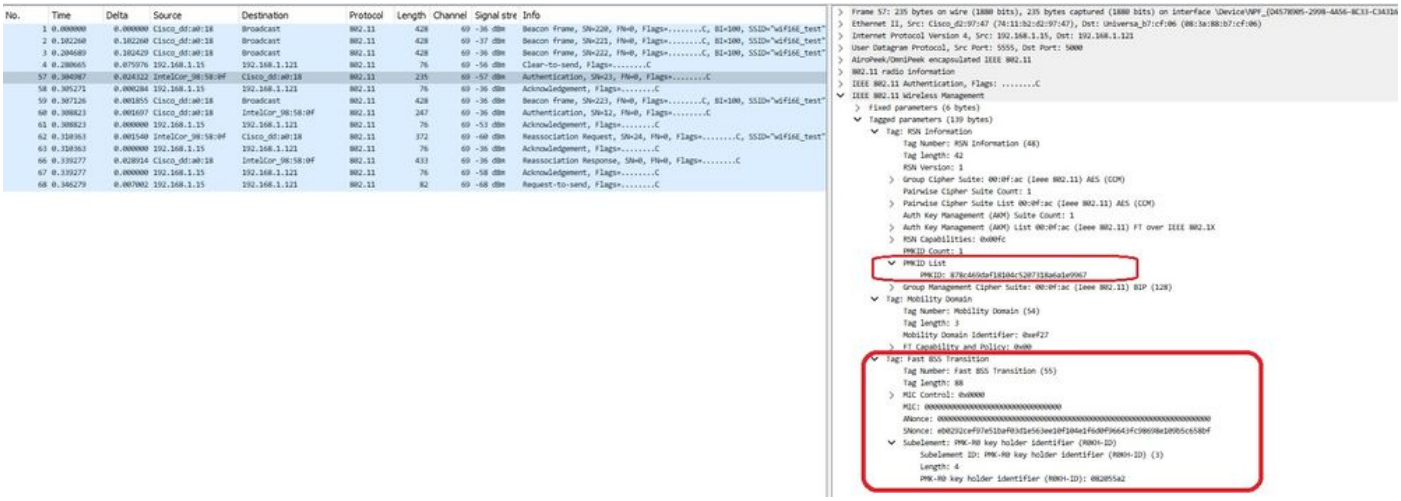


WPA3 Enterprise 802.1x +FT-beacon

Hier kunnen we Wi-Fi 6E-clients waarnemen die associëren:

Intel AX211 switch

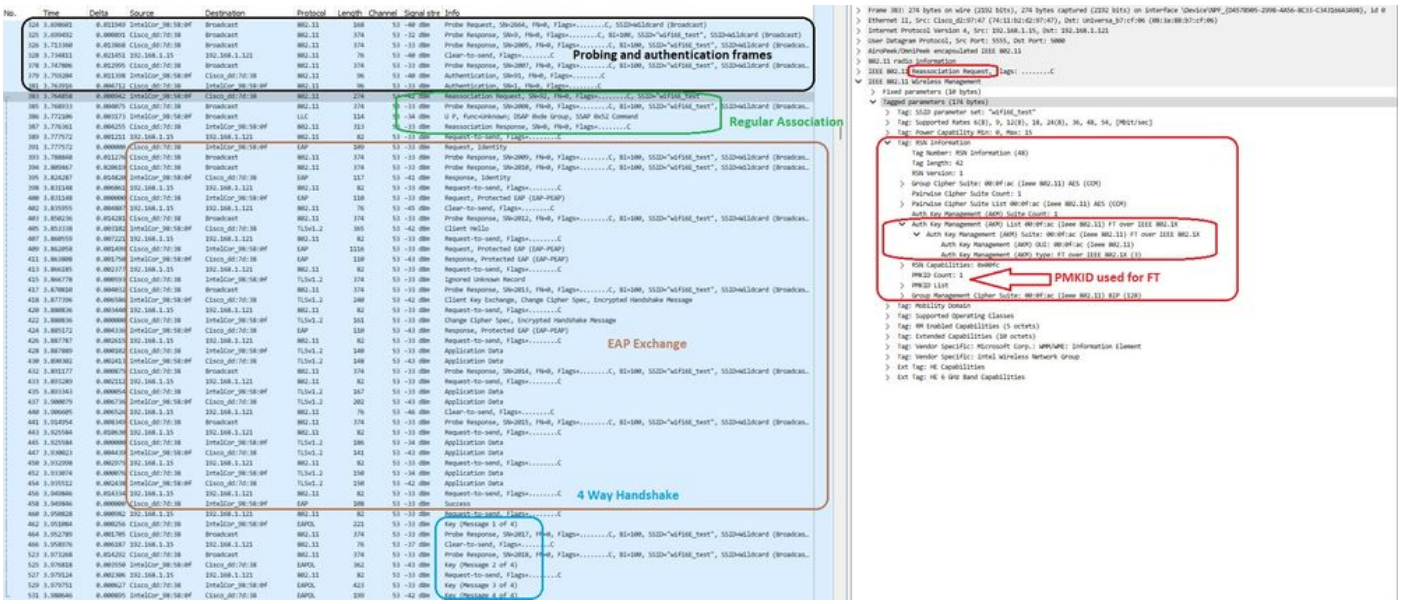
OTA-verbinding met focus op RSN-informatie van client op een roamingevenement:



WPA3 Enterprise 802.1x + FT-roaminggebeurtenis

Een interessant gedrag gebeurt als u de client handmatig uit het WLAN verwijdert (bijvoorbeeld vanuit WLC GUI). De client ontvangt een disassociatiekader maar probeert opnieuw verbinding te maken met dezelfde AP en gebruikt een reassociatiekader gevolgd door een volledige EAP-uitwisseling omdat de clientgegevens werden verwijderd van de AP/WLC.

Dit is in principe dezelfde frameuitwisseling als in een nieuw associatieproces. Hier kunt u de frameversie zien:




WPA3 Enterprise 802.1x + FT AX211-verbindingsstroom

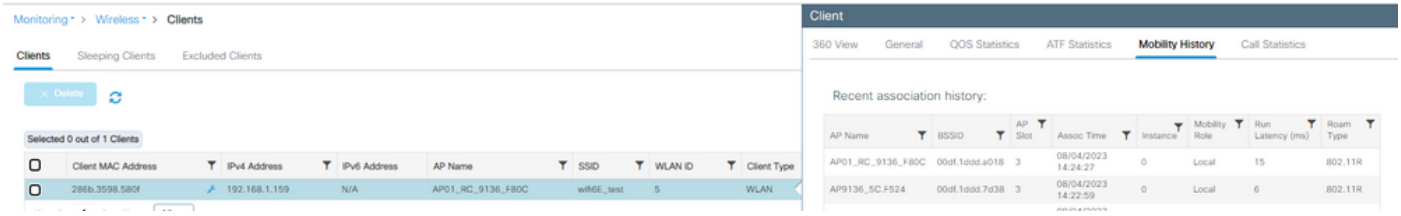
Klantgegevens in WLC:


WPA3 Enterprise 802.1x + FT-clientgegevens

Deze client werd ook getest met behulp van FT over de DS en kon zwerven met 802.11r:

AX211 roaming met FT over DS

We kunnen ook de FT roaming-evenementen zien:



WPA3 Enterprise met FT

En client ra spoor van wlc:

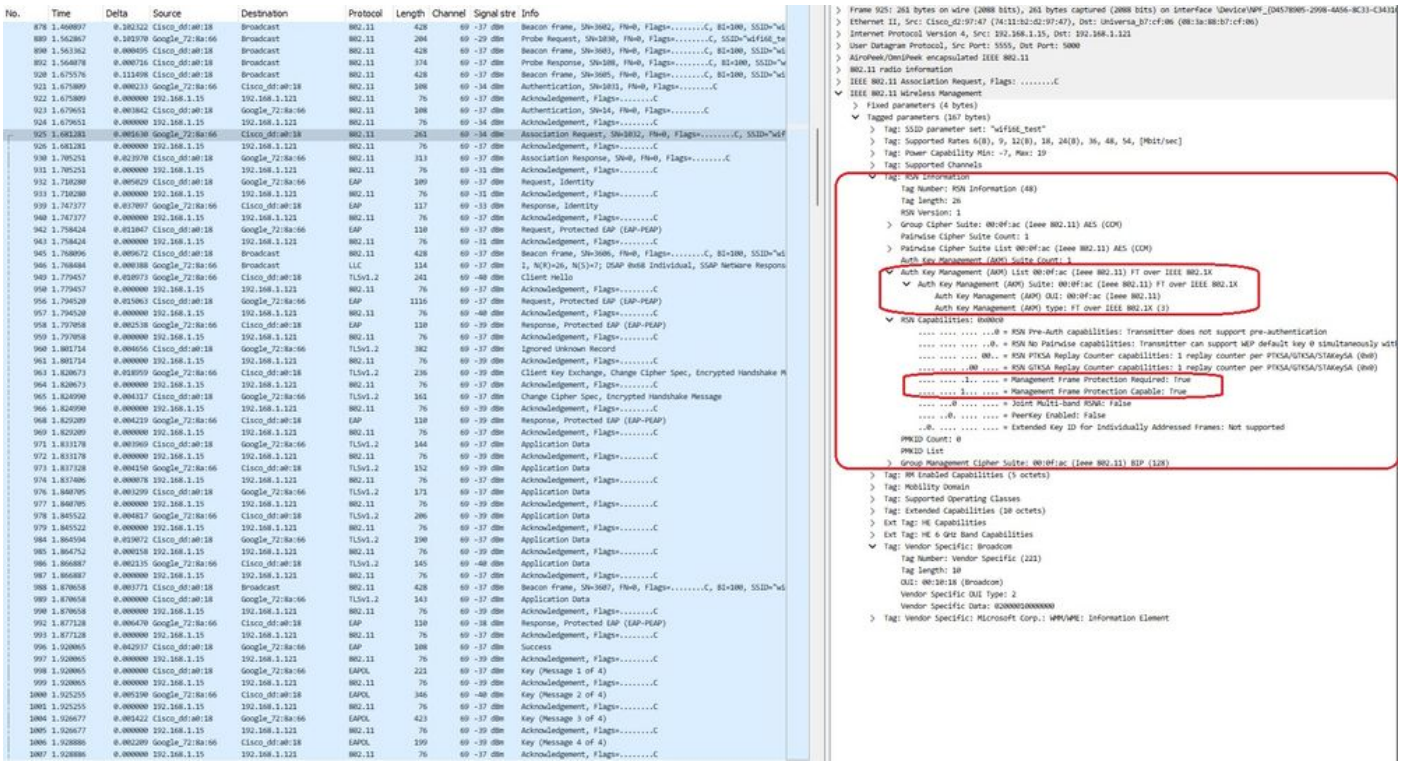
```
Logging display requested on 2023/08/04 14:27:55 (GMT) for Hostname: [eWLC-9800-01], Model: [C9800-CL-K9], Version: [17.09.03], SN: [9RY35HS10G9], MD_SN: [9RY35HS10G9]
2023/08/04 14:22:59.315300237 {wncd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 204b.3590.580f Re-Association received. BSSID 00df.1ddd.7d30, WLAN wifi6E_test, Slot 3 AP 00df.1ddd.7d30, AP9136_5C.F524, old BSSID 00df.1ddd.a010
2023/08/04 14:22:59.315844120 {wncd_x_R0-0}{1}: [dot11] [15210]: (note): MAC: 204b.3590.580f Association success. AID 33, Roaming = True, WGB = False, 11r = True, 11w = True Fast roam = True
2023/08/04 14:22:59.316408412 {wncd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 204b.3590.580f Delete mobile payload sent for BSSID: 00df.1ddd.a010 WTP mac: 00df.1ddd.a010 slot id: 3
2023/08/04 14:22:59.316652383 {wncd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 204b.3590.580f Client state transition: S_CO_RUN -> S_CO_L2_AUTH_IN_PROGRESS
2023/08/04 14:22:59.317328574 {wncd_x_R0-0}{1}: [client-auth] [15210]: (note): MAC: 204b.3590.580f ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00df.1ddd.7d30 capwap IFID: 0x9000000d, Add mobiles sent: 1
2023/08/04 14:22:59.321041947 {wncd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 204b.3590.580f Mobility discovery triggered. Client mode: Local
2023/08/04 14:22:59.321044391 {wncd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 204b.3590.580f Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
2023/08/04 14:22:59.321064980 {wncd_x_R0-0}{1}: [mm-client] [15210]: (note): MAC: 204b.3590.580f Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_INTRA_INSTANCE, Previous BSSID MAC: 00df.1ddd.a010  Client IFID: 0xa0000003, Client Role:
Local PoA: 0x9000000d PoP: 0x0
2023/08/04 14:22:59.321213902 {wncd_x_R0-0}{1}: [client-auth] [15210]: (note): MAC: 204b.3590.580f ADD MOBILE sent. Client state flags: 0x76 BSSID: MAC: 00df.1ddd.7d38 capwap IFID: 0x9000000d, Add mobiles sent: 1
2023/08/04 14:22:59.321264062 {wncd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 204b.3590.580f Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS
2023/08/04 14:22:59.321463455 {wncd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 204b.3590.580f Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
2023/08/04 14:22:59.321666600 {wncd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 204b.3590.580f Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN
2023/08/04 14:24:27.918055521 {wncd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 204b.3590.580f Re-Association received. BSSID 00df.1ddd.a010, WLAN wifi6E_test, Slot 3 AP 00df.1ddd.a010, AP01_RC_9136_F80C, old BSSID 00df.1ddd.7d38
2023/08/04 14:24:27.919097444 {wncd_x_R0-0}{1}: [dot11] [15210]: (note): MAC: 204b.3590.580f Association success. AID 33, Roaming = True, WGB = False, 11r = True, 11w = True Fast roam = True
2023/08/04 14:24:27.921992623 {wncd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 204b.3590.580f Delete mobile payload sent for BSSID: 00df.1ddd.7d38 WTP mac: 00df.1ddd.7d30 slot id: 3
2023/08/04 14:24:27.922776547 {wncd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 204b.3590.580f Client state transition: S_CO_RUN -> S_CO_L2_AUTH_IN_PROGRESS
2023/08/04 14:24:27.925409164 {wncd_x_R0-0}{1}: [client-auth] [15210]: (note): MAC: 204b.3590.580f ADD MOBILE sent. Client state flags: 0x71 BSSID: MAC: 00df.1ddd.a010 capwap IFID: 0x9000000e, Add mobiles sent: 1
2023/08/04 14:24:27.931650871 {wncd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 204b.3590.580f Mobility discovery triggered. Client mode: Local
2023/08/04 14:24:27.931611962 {wncd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 204b.3590.580f Client state transition: S_CO_L2_AUTH_IN_PROGRESS -> S_CO_MOBILITY_DISCOVERY_IN_PROGRESS
2023/08/04 14:24:27.931569962 {wncd_x_R0-0}{1}: [mm-client] [15210]: (note): MAC: 204b.3590.580f Mobility Successful. Roam Type None, Sub Roam Type MM_SUB_ROAM_TYPE_INTRA_INSTANCE, Previous BSSID MAC: 00df.1ddd.7d38  Client IFID: 0xa0000003, Client Role:
Local PoA: 0x9000000e PoP: 0x0
2023/08/04 14:24:27.931861935 {wncd_x_R0-0}{1}: [client-auth] [15210]: (note): MAC: 204b.3590.580f ADD MOBILE sent. Client state flags: 0x76 BSSID: MAC: 00df.1ddd.a010 capwap IFID: 0x9000000e, Add mobiles sent: 1
2023/08/04 14:24:27.931913122 {wncd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 204b.3590.580f Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS
2023/08/04 14:24:27.933100101 {wncd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 204b.3590.580f Client state transition: S_CO_DPATH_PLUMB_IN_PROGRESS -> S_CO_IP_LEARN_IN_PROGRESS
2023/08/04 14:24:27.933501101 {wncd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 204b.3590.580f Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN
```

NetGear A800

WPA3-Enterprise wordt niet ondersteund op deze client.

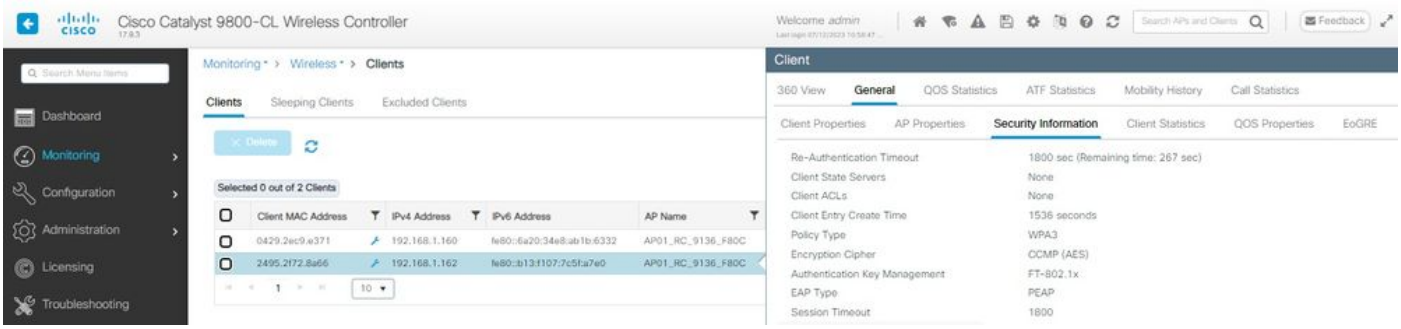
Pixel 6a

OTA-verbinding met focus op RSN-informatie van client:



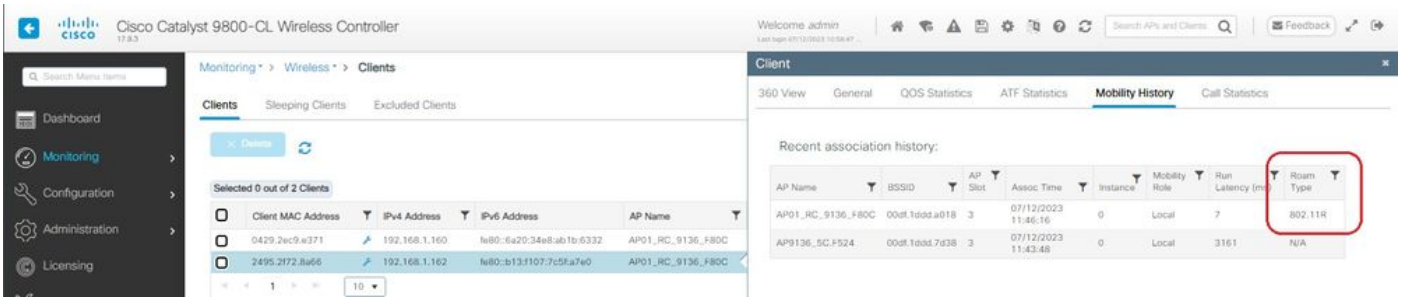
WPA3 Enterprise 802.1x + FT Pixel6a Association

Klantgegevens in WLC:



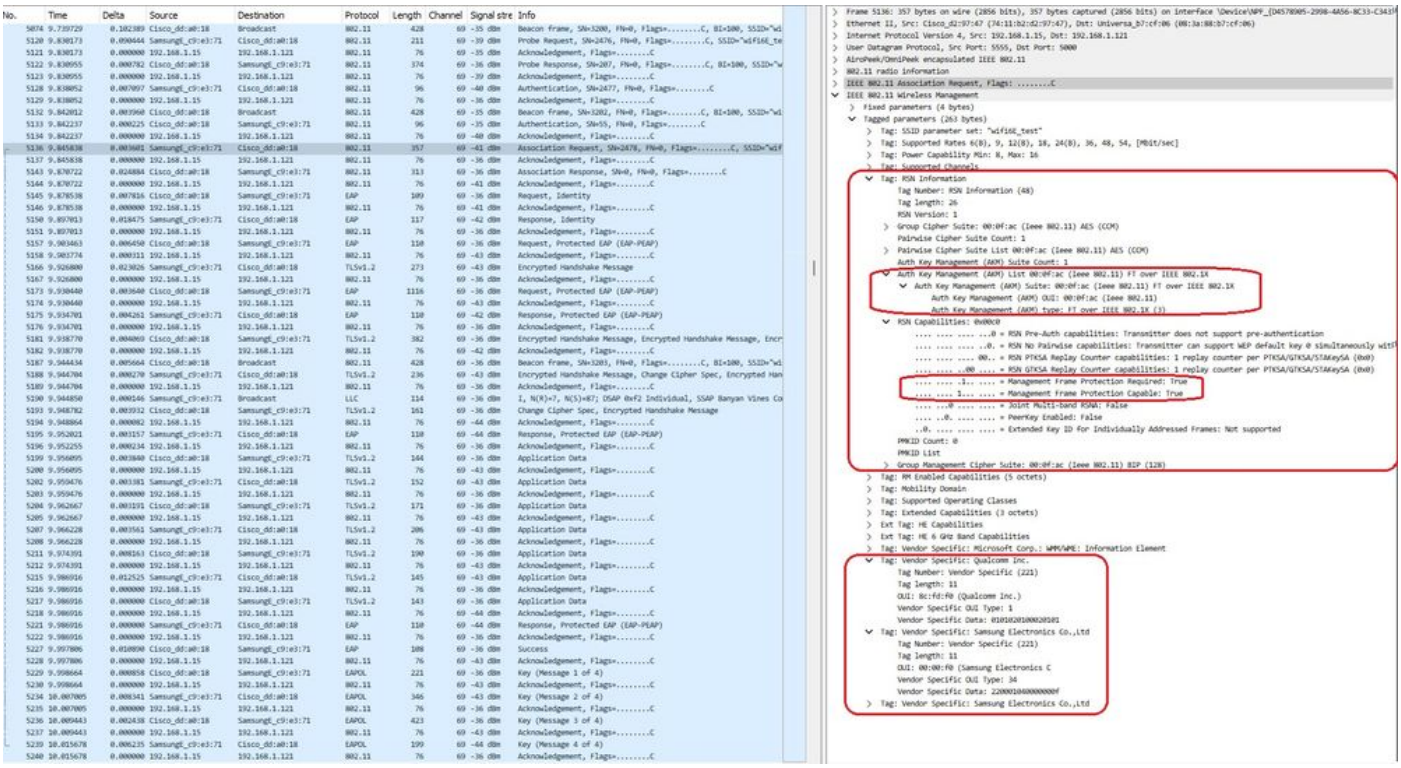

WPA3 Enterprise 802.1x + FT Pixel6a Clientgegevens

Stel scherp op het roamtype Over the Air waar we het roamtype 802.11R kunnen zien:



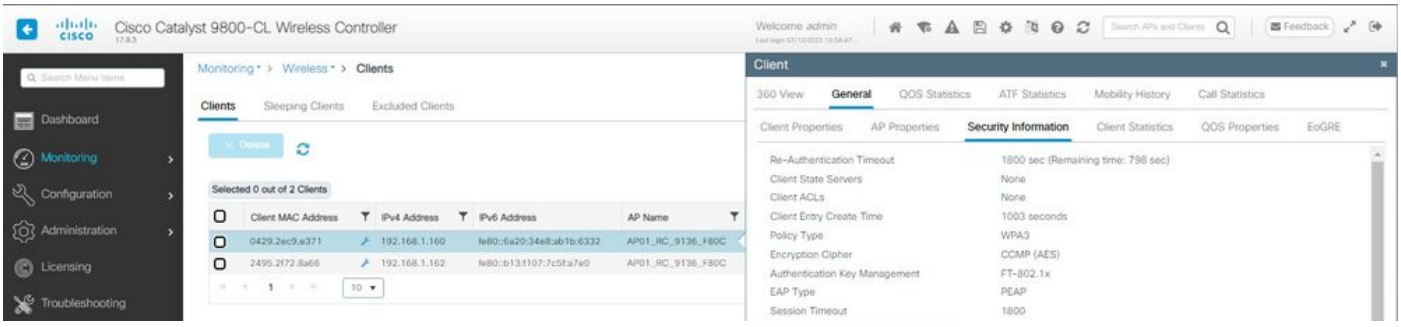

Samsung S23

OTA-verbinding met focus op RSN-informatie van client:



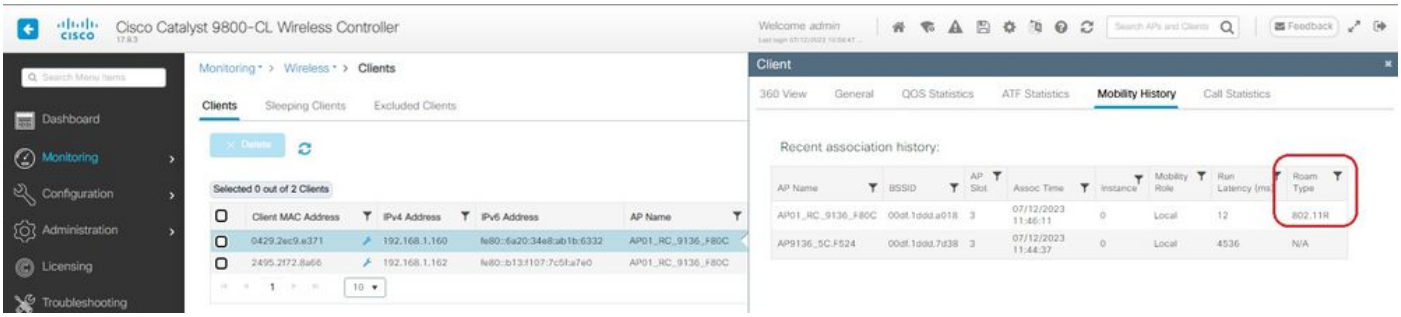
S23 FToTA roamingevenement

## Klantgegevens in WLC:



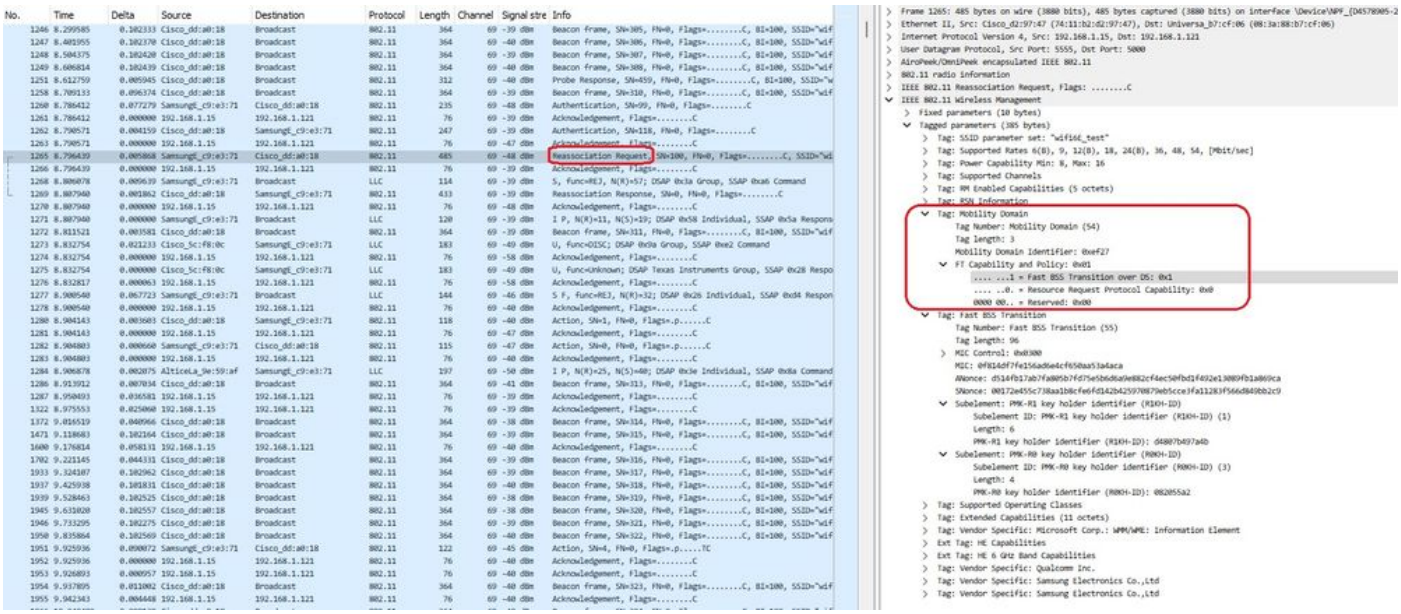

S23 clienteigenschappen

## Stel scherp op het roamtype Over the Air waar we het roamtype 802.11R kunnen zien:




S23 roamingtype 802.11R

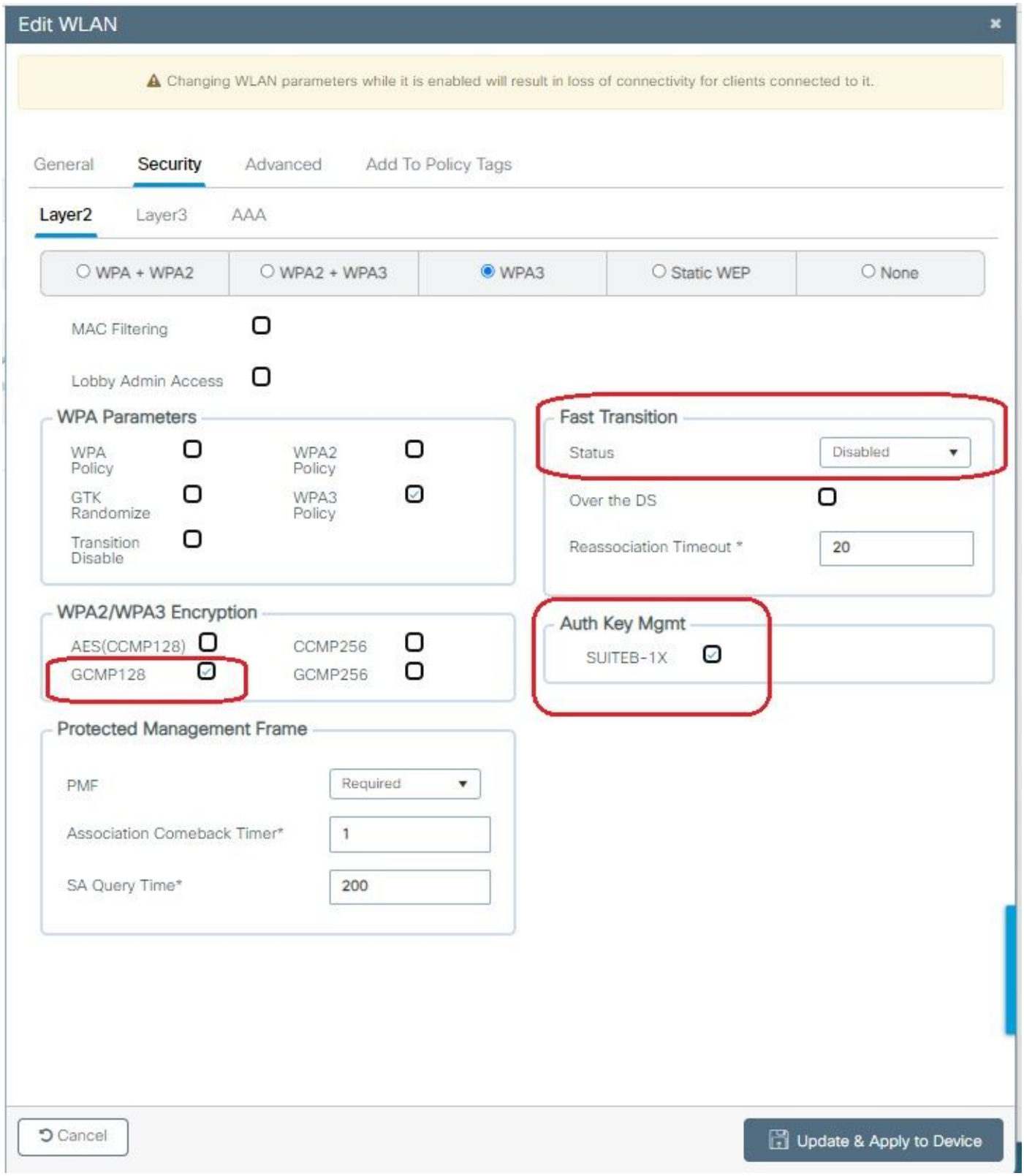
## Deze client werd ook getest met behulp van FT over de DS en kon zwerven met 802.11r:



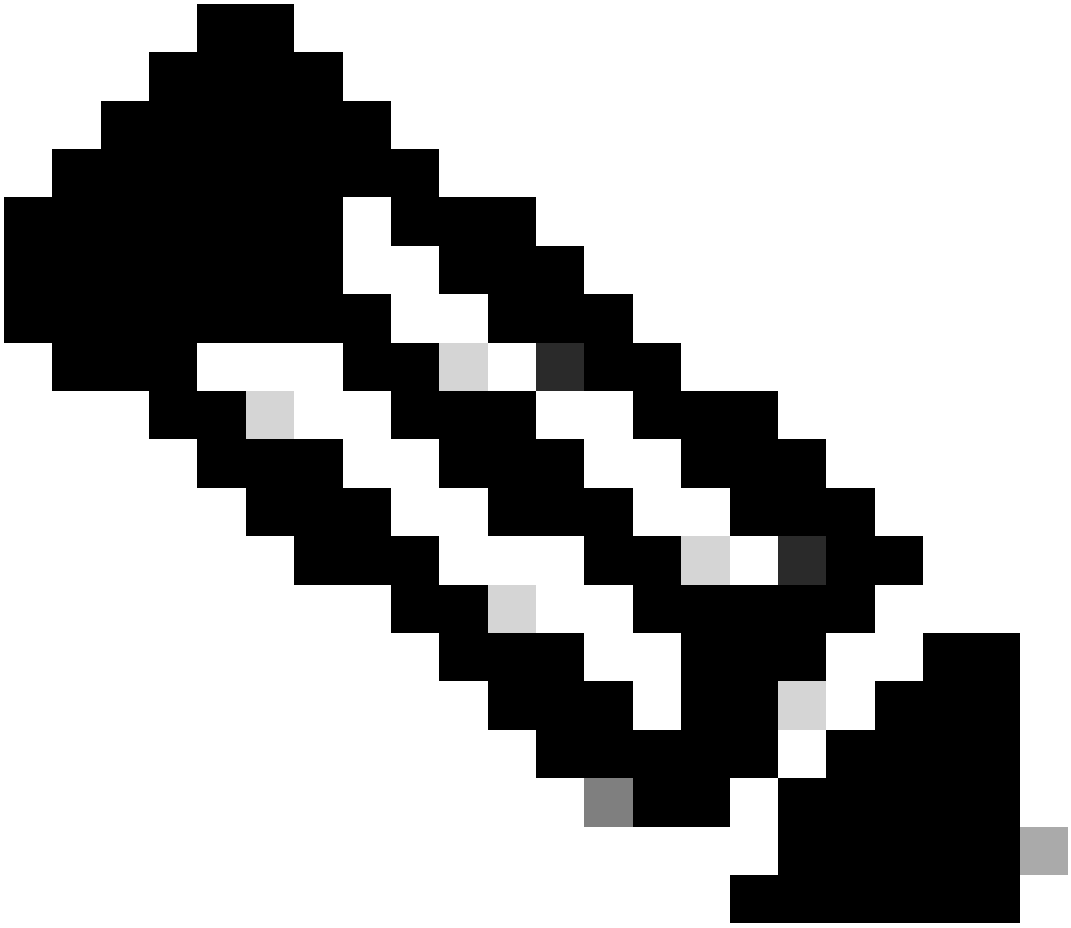
S23 FToDS-pakketten voor roaming

WPA3-Enterprise + GCMP128-algoritme + SUBITB-1X

WLAN-beveiligingsconfiguratie:




Configuratie van WPA3 Enterprise Suite B-1X-beveiliging

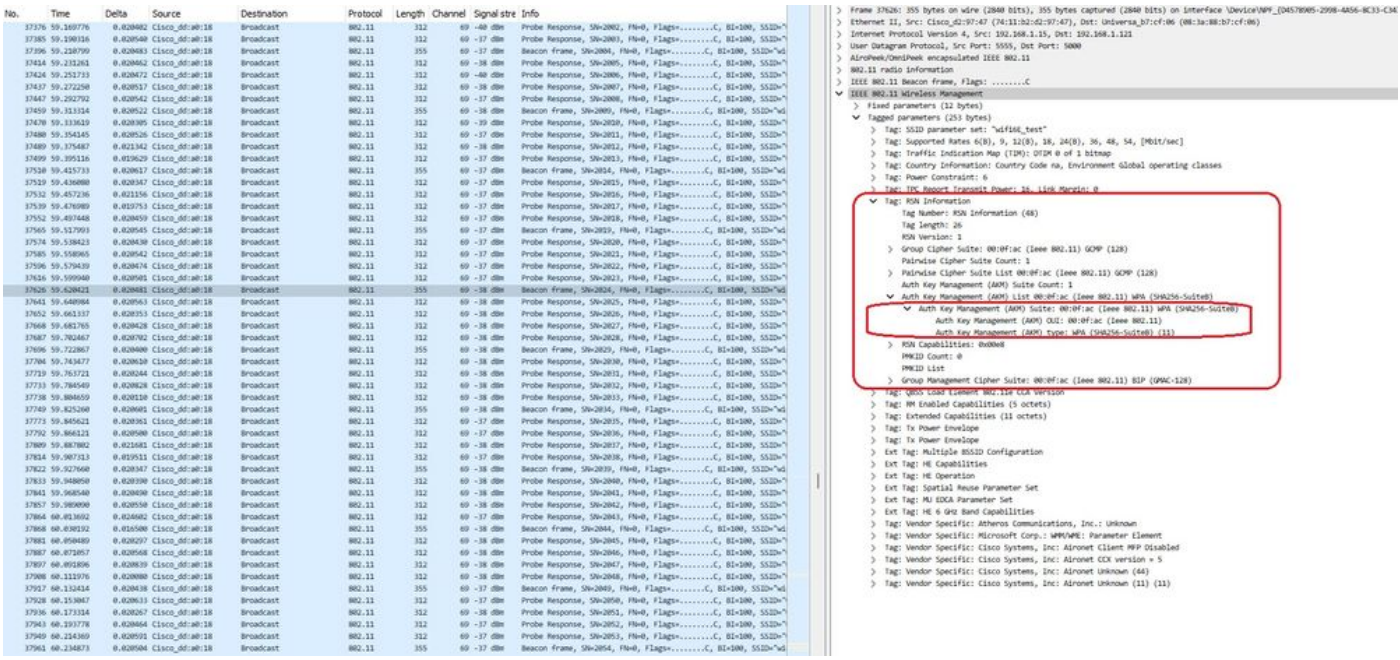


Opmerking: FT wordt niet ondersteund in SUITEB-1X

---

Bekijk op WLC GUI van de WLAN security instellingen:


Verificatie van de OTA van bakens:

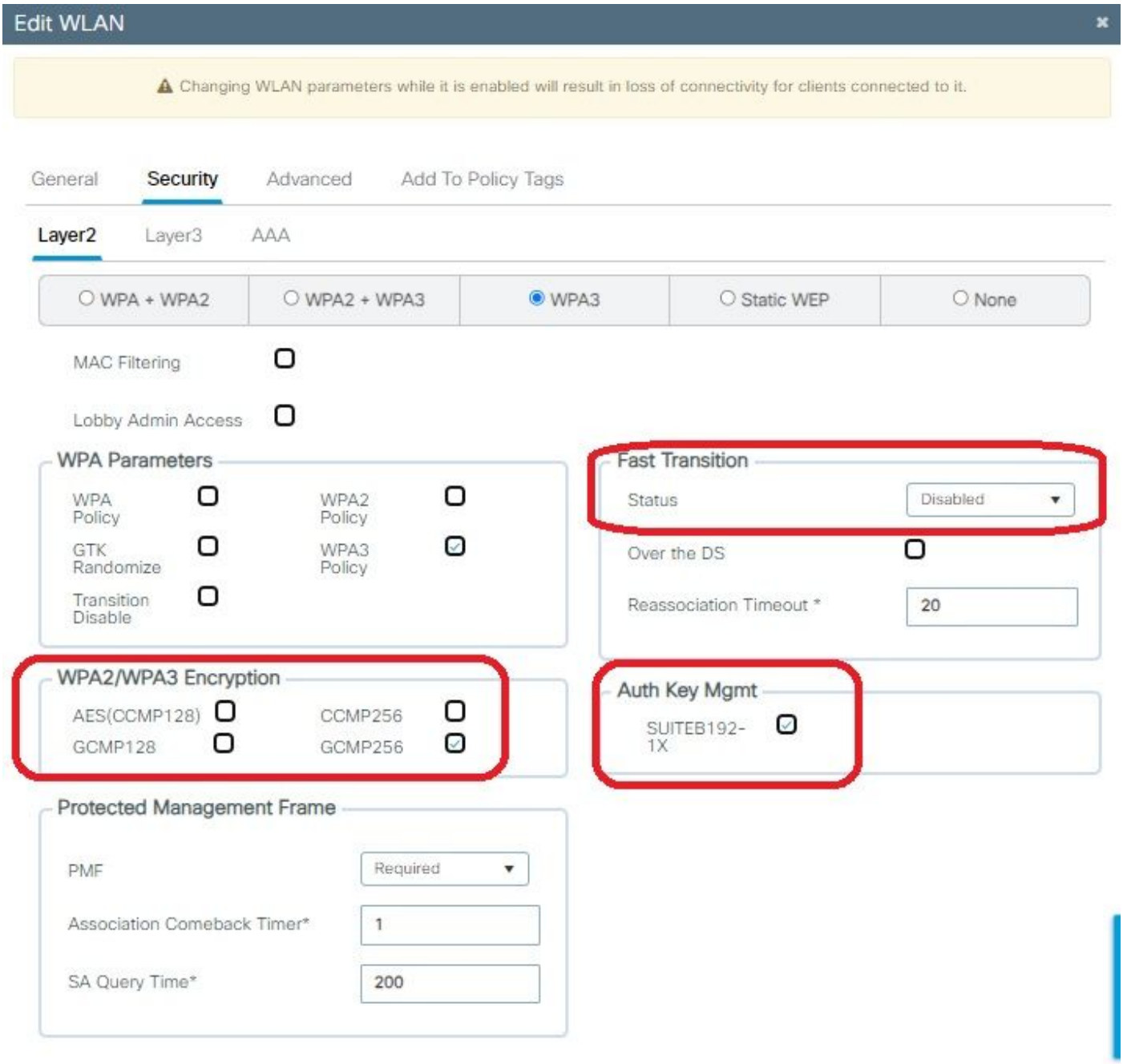


WPA3 Enterprise Suite B-1X-beacon

Geen van de geteste clients kon verbinding maken met het WLAN met behulp van SuiteB-1X, waarbij werd bevestigd dat geen van de clients deze beveiligingsmethode ondersteunt.

WPA3-Enterprise + GCMP256-algoritme + SITEB192-1X

WLAN-beveiligingsconfiguratie:



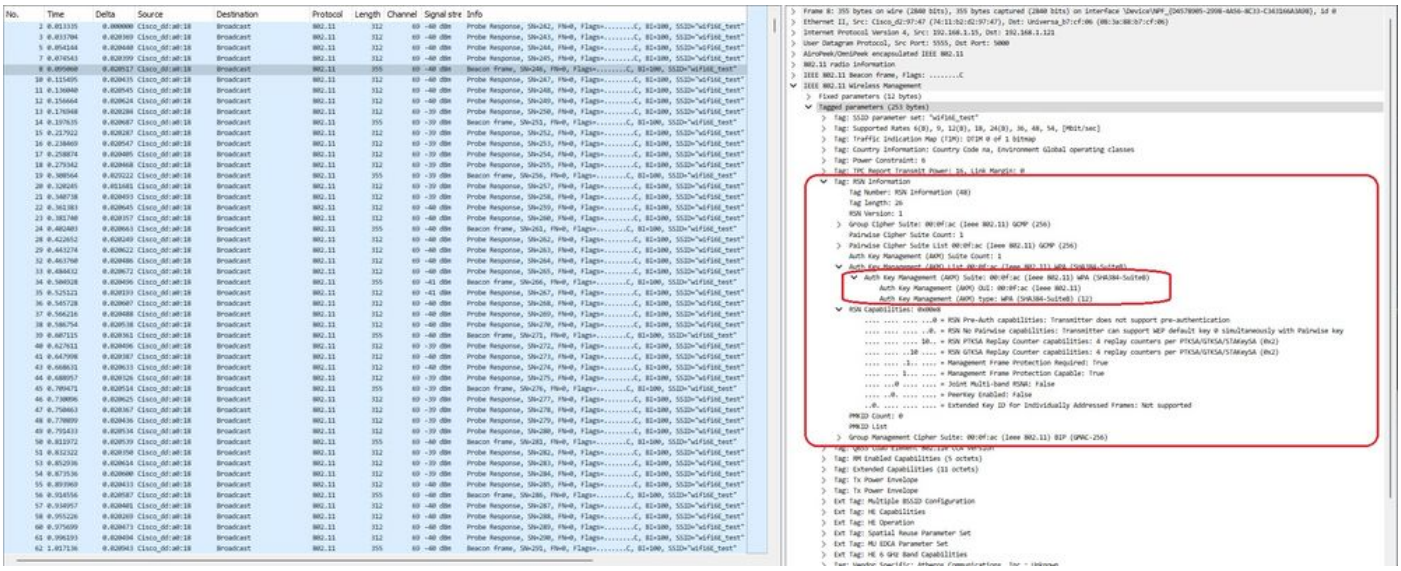

WPA3 Enterprise SUITEB192-1x-beveiligingsinstellingen

Opmerking: FT wordt niet ondersteund door GCMP256+SUITEB192-1X.

WLAN's op WLC GUI WLAN-lijst:


WLAN gebruikt voor tests

Verificatie van de OTA van bakens:

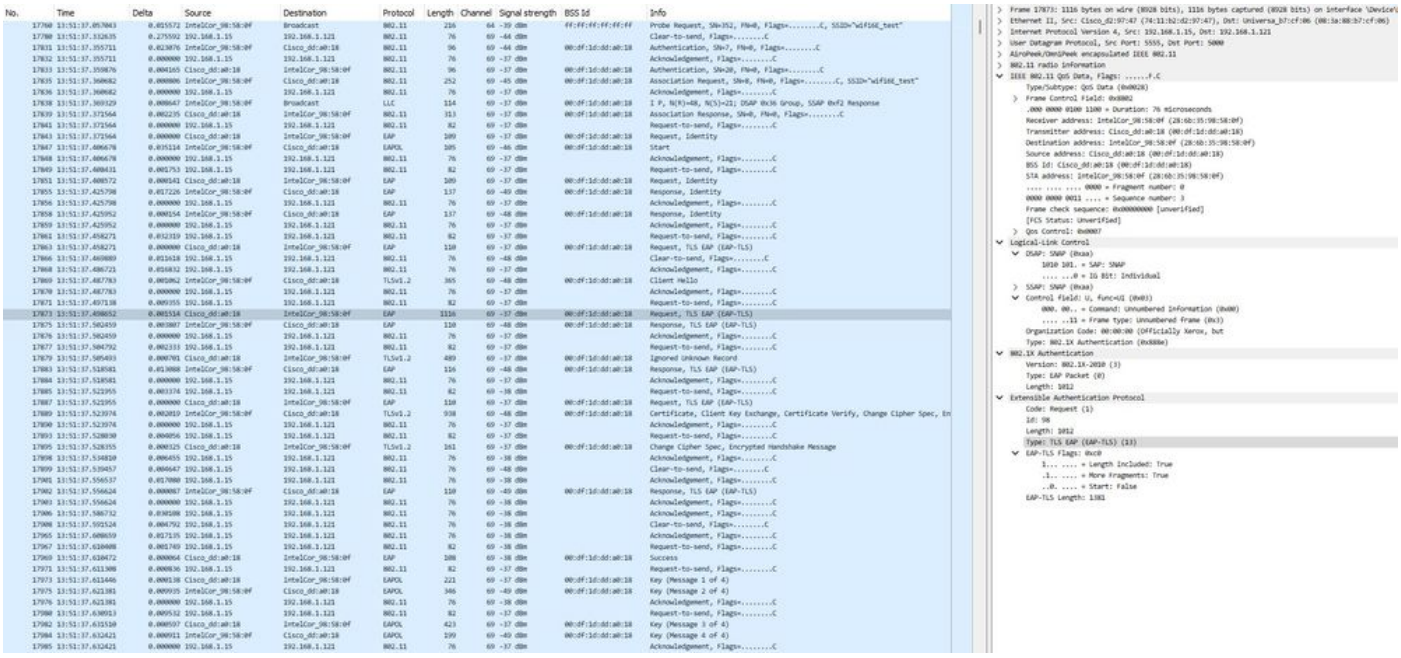


WPA3 Enterprise SUITEB192-1x-bakens

Hier kunnen we Wi-Fi 6E-clients waarnemen die associëren:

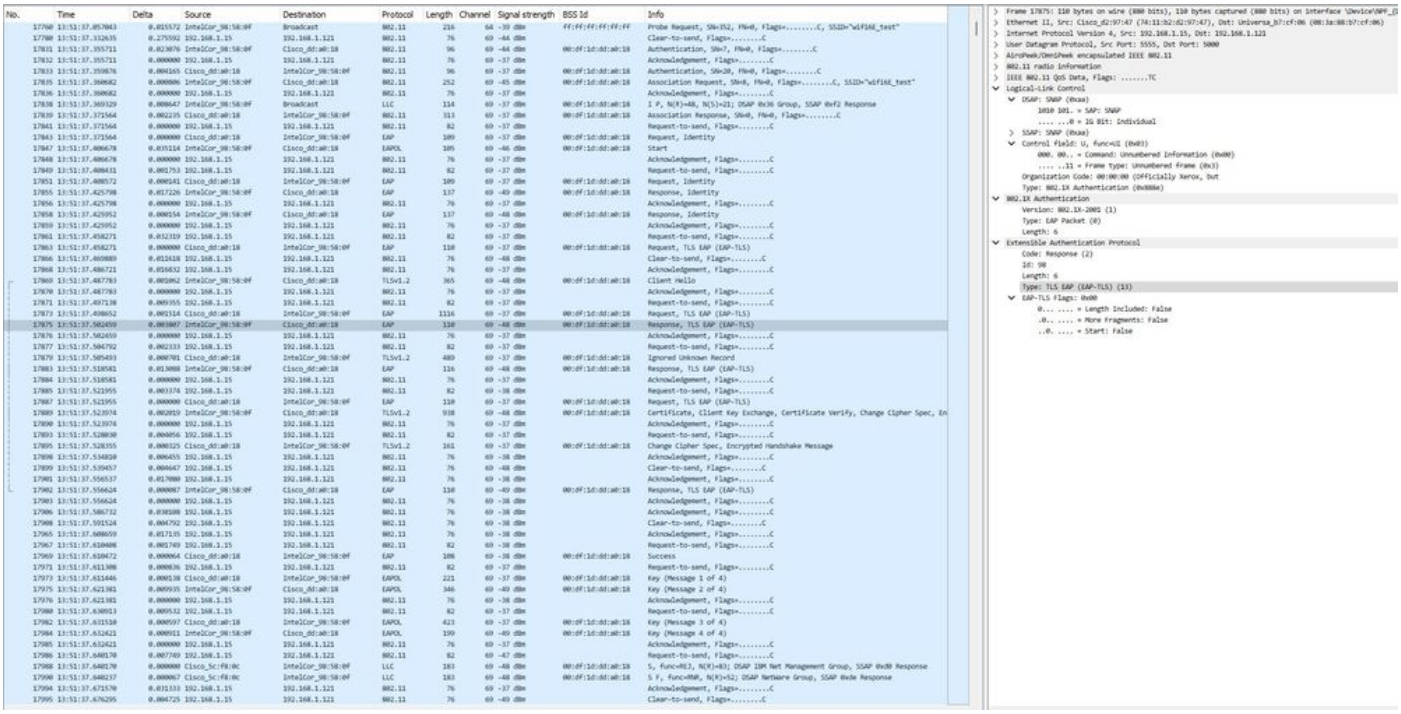
Intel AX211 switch

OTA-verbinding met focus op RSN-informatie van client:



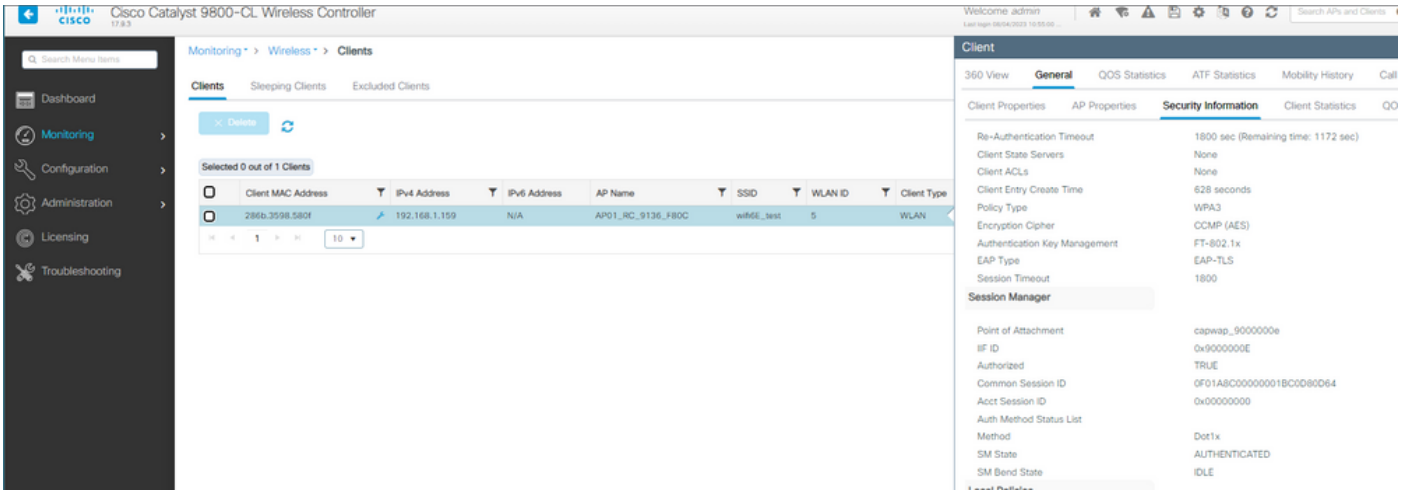
WPA3 Enterprise met EAP-TLS Association met Intel AX211-client en RSN-informatie

En de EAP-TLS-uitwisseling:



WPA3 Enterprise met EAP-TLS Association met Intel AX211-client en EAP-TLS Focus

Klantgegevens in WLC:




WPA3 Enterprise met EAP-TLS-clientgegevens

NetGear A800

WPA3-Enterprise wordt niet ondersteund op deze client.

Pixel 6a

Op de datum waarop dit document is geschreven, kon deze client geen verbinding maken met WPA3 Enterprise met behulp van EAP-TLS.

Dit was een kwestie aan de zijde van de cliënt waaraan wordt gewerkt en zodra het is opgelost, wordt dit document bijgewerkt.

Samsung S23

Op de datum waarop dit document is geschreven, kon deze client geen verbinding maken met WPA3 Enterprise met behulp van EAP-TLS.

Dit was een kwestie aan de zijde van de cliënt waaraan wordt gewerkt en zodra het is opgelost, wordt dit document bijgewerkt.

conclusies inzake beveiliging

Na alle voorgaande tests zijn de volgende conclusies getrokken:

| Protocol | Versleuteling | AKM | AKM Cipher | EAP-methode | FT-OverTA | FT-overDS |
|---|---|---|---|---|---|---|
| VERSCHULDIGD | AES-CCMP128 router | VERSCHULDIGD | NVT. | NVT. | NA | NA |
| SAE | AES-CCMP128 router | SAE (alleen H2E) | SHA256-software | NVT. | Ondersteunde producten | Ondersteund producten |
| Ondernemingen | AES-CCMP128 router | 802.1x-SHA256-router | SHA256-software | PEAP/FAST/TLS | Ondersteunde producten | Ondersteund producten |
| Ondernemingen | GCMP128 router | Suite B-1x | SHA256-Suite B | PEAP/FAST/TLS | Niet ondersteund | Niet ondersteund |
| Ondernemingen | GCMP256 applicatie | Suite B-192 | SHA384-Suite B | TLS | Niet ondersteund | Niet ondersteund |

# Problemen oplossen

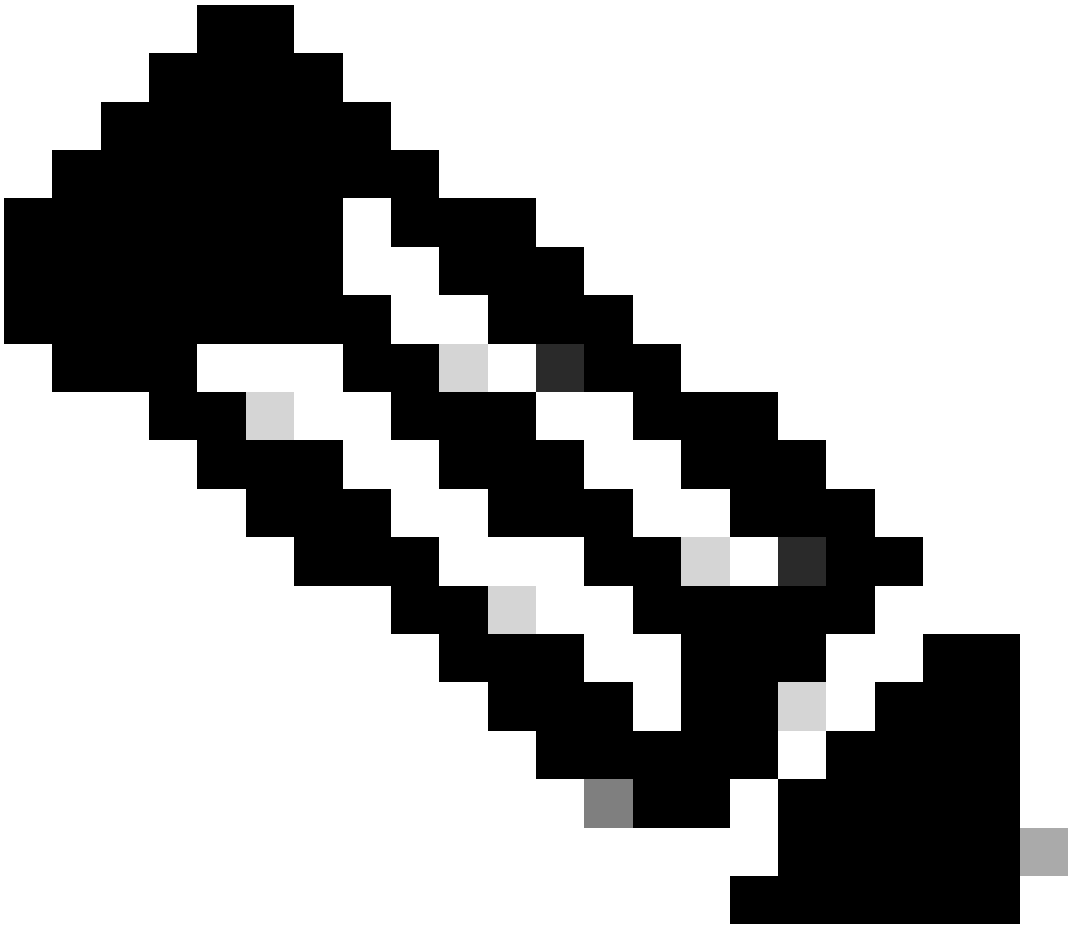
De in dit document gebruikte probleemoplossing is gebaseerd op het online document:

Probleemoplossing voor COS-toegangspunten

De algemene richtlijn voor het oplossen van problemen is om RA-spoor in debug-modus te verzamelen van de WLC met behulp van het client mac-adres, ervoor te zorgen dat de client verbinding maakt met behulp van de apparaat mac en niet een gerandomiseerd mac-adres.

Voor de probleemoplossing via de lucht wordt aanbevolen om AP in de snuffelmodus te gebruiken om het verkeer op te nemen op het kanaal van de client die AP bedient.

---



Opmerking: Raadpleeg Belangrijke informatie over debug commando's voordat u debug commando's gebruikt.

---

## Gerelateerde informatie

Wat is Wi-Fi 6E?

Wat is Wi-Fi 6 versus Wi-Fi 6E?

Wi-Fi 6E At-a-Glance

Wi-Fi 6E: Het volgende grote hoofdstuk in Wi-Fi White Paper

Cisco Live - Architect voor draadloze netwerken van de volgende generatie met Catalyst Wi-Fi 6E access points

Software voor Cisco Catalyst 9800 Series draadloze controller, configuratiehandleiding 17.9.x

Implementatiegids voor WPA3

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.