Konfiguration und Überprüfung der Layer-2-Sicherheit des Wi-Fi 6E-WLAN

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Layer-2-Sicherheit des Wi-Fi 6E-WLAN konfigurieren und was Sie von verschiedenen Clients erwarten können.

Voraussetzungen

Anforderungen

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

- Cisco Wireless LAN Controller (WLC) 9800
- Cisco Access Points (APs), die Wi-Fi 6E unterstützen.
- IEEE-Standard 802.11ax
- Tools: Wireshark v4.0.6

Verwendete Komponenten

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

- WLC 9800-CL mit IOS® XE 17.9.3
- APs: C9136, CW9162, CW9164 und CW9166.
- Wi-Fi 6E-Clients:
    - Lenovo X1 Carbon Gen11 mit Intel AX211 Wi-Fi 6 und 6E Adapter mit Treiberversion 22.200.2(1).
    - Netgear A8000 Wi-Fi 6 und 6E Adapter mit Treiber v1(0.0.108)
    - Mobiltelefon Pixel 6a mit Android 13;
    - Handy Samsung S23 mit Android 13.

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

Hintergrundinformationen

Das Wichtigste ist, dass Wi-Fi 6E kein völlig neuer Standard ist, sondern eine Erweiterung. Als Basis dient Wi-Fi 6E als Erweiterung des Wireless-Standards Wi-Fi 6 (802.11ax) in das 6-GHz-Frequenzband.

Wi-Fi 6E basiert auf Wi-Fi 6, der neuesten Generation des Wi-Fi-Standards, aber nur Wi-Fi 6E-Geräte und -Anwendungen können im 6-GHz-Band betrieben werden.

Wi-Fi 6E-Sicherheit

Wi-Fi 6E erhöht die Sicherheit mit Wi-Fi Protected Access 3 (WPA3) und Opportunistic Wireless Encryption (OWE), und es gibt keine Abwärtskompatibilität mit Open- und WPA2-Sicherheit.

WPA3 und Enhanced Open Security sind jetzt für die Wi-Fi 6E-Zertifizierung obligatorisch, und für Wi-Fi 6E ist auch Protected Management Frame (PMF) sowohl auf dem Access Point als auch auf den Clients erforderlich.

Bei der Konfiguration einer 6-GHz-SSID müssen bestimmte Sicherheitsanforderungen erfüllt werden:

- WPA3 L2-Sicherheit mit OWE, SAE oder 802.1x-SHA256
- Geschützter Management-Frame aktiviert;

- Andere L2-Sicherheitsmethoden sind nicht zulässig, d. h., es ist kein gemischter Modus möglich.

WPA3

WPA3 wurde entwickelt, um die Wi-Fi-Sicherheit zu verbessern, indem eine bessere Authentifizierung über WPA2 ermöglicht wird, wodurch die kryptografische Stärke erweitert und die Ausfallsicherheit kritischer Netzwerke erhöht wird.

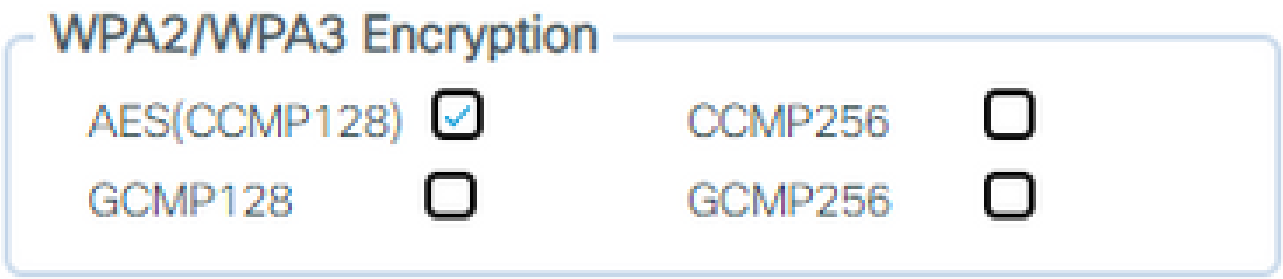
WPA3 zeichnet sich durch folgende Hauptfunktionen aus:

- Protected Management Frame (PMF) schützt Unicast- und Broadcast-Management-Frames und verschlüsselt Unicast-Management-Frames. Wireless Intrusion Detection- und Wireless Intrusion Prevention-Systeme bieten daher weniger Möglichkeiten zur Brute-Force-Durchsetzung von Client-Richtlinien.
- Simultaneous Authentication of Equals (SAE) ermöglicht eine kennwortbasierte Authentifizierung und einen Key Agreement-Mechanismus. Dies schützt vor Brute-Force-Angriffen.
- Der Übergangsmodus ist ein gemischter Modus, der die Verwendung von WPA2 ermöglicht, um Clients zu verbinden, die WPA3 nicht unterstützen.

Bei WPA3 geht es um kontinuierliche Sicherheitsentwicklung, Konformität und Interoperabilität. Es gibt kein Informationselement, das WPA3 (identisch mit WPA2) bezeichnet. WPA3 wird durch AKM/Cipher Suite/PMF-Kombinationen definiert.

Für die WLAN-Konfiguration des 9800 stehen vier verschiedene WPA3-Verschlüsselungsalgorithmen zur Verfügung.

Sie basieren auf Galois/Counter Mode Protocol (GCMP) und Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP): AES (CCMP128), CCMP256, GCMP128 und GCMP256:



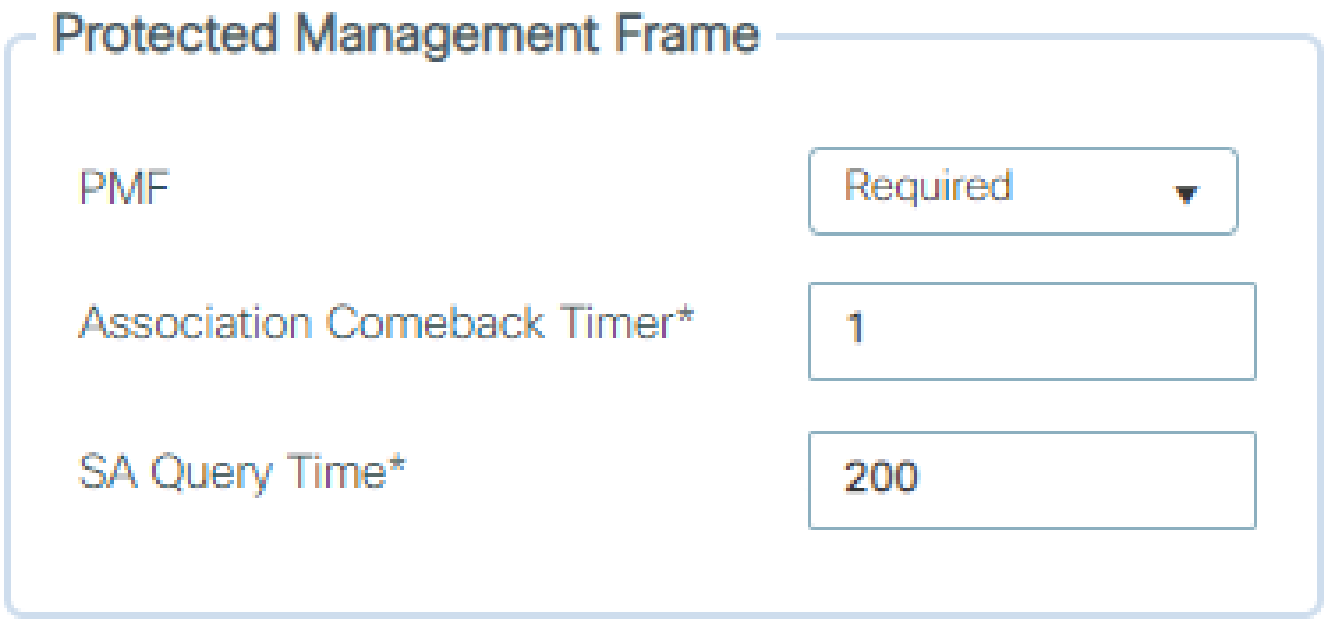
WPA2/3-Verschlüsselungsoptionen

PMF

PMF wird in einem WLAN aktiviert, wenn Sie PMF aktivieren.

Standardmäßig sind 802.11-Management-Frames nicht authentifiziert und daher nicht vor

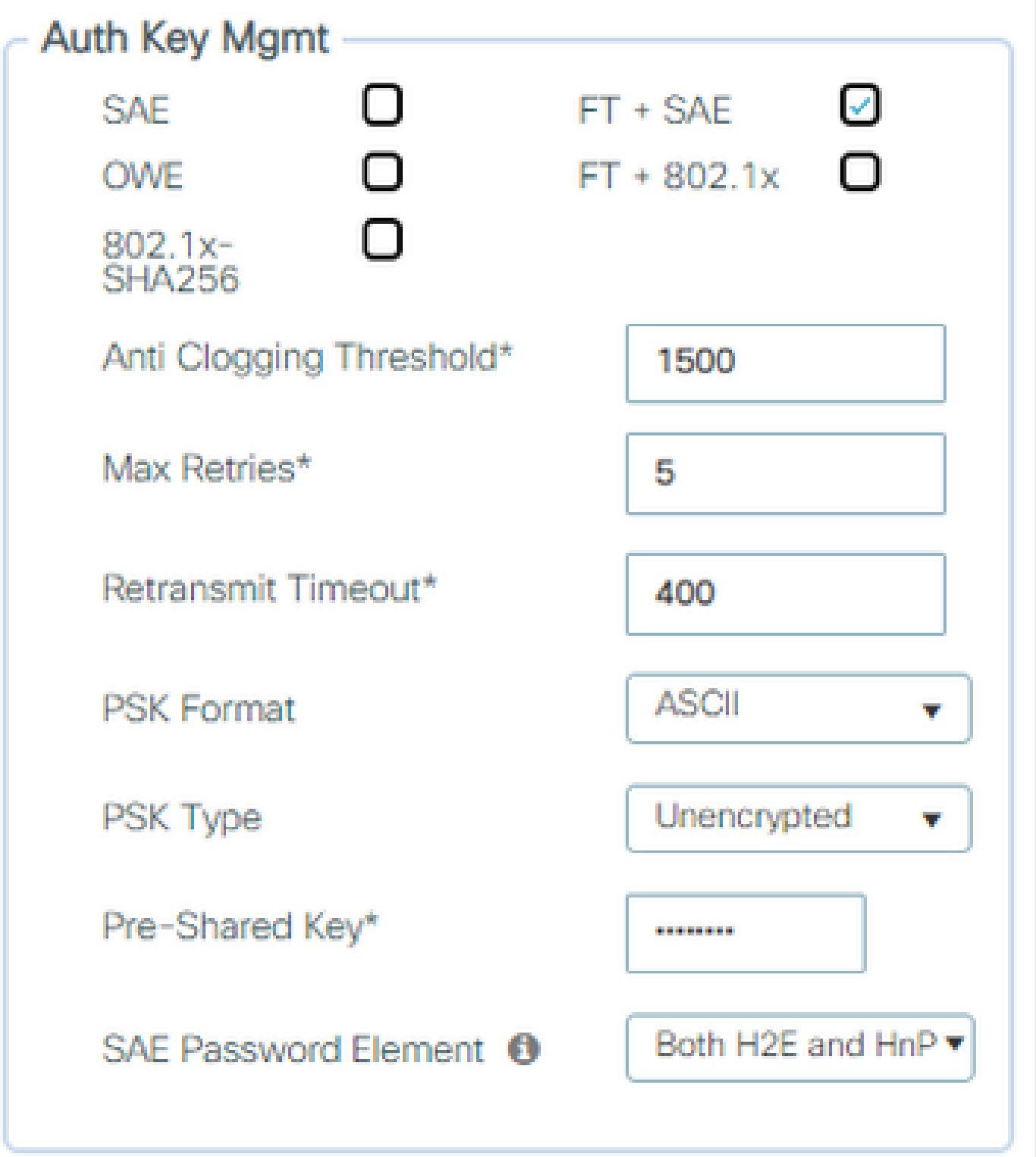
Spoofing geschützt. Infrastructure Management Protection Frame (MFP) und 802.11w Protected Management Frames (PMF) bieten Schutz vor solchen Angriffen.



PMF-Optionen

Verwaltung von Authentifizierungsschlüsseln

Folgende AKM-Optionen sind in der Version 17.9.x verfügbar:

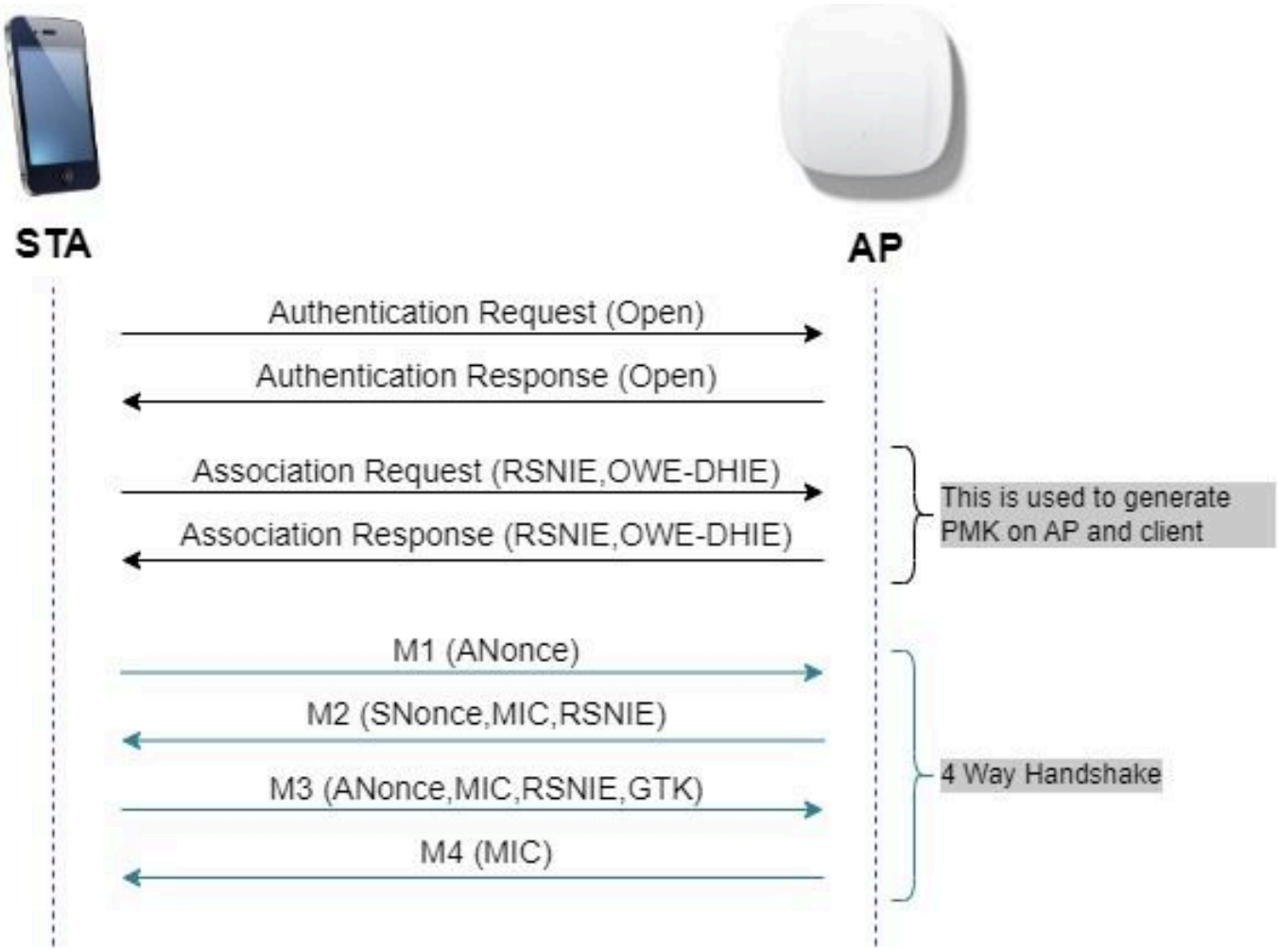


AKM-Optionen

SCHULD

Opportunistic Wireless Encryption (OWE) ist eine Erweiterung von IEEE 802.11 für die Verschlüsselung des Wireless-Mediums (IETF RFC 8110). Der Zweck der OWE-basierten Authentifizierung besteht in der Vermeidung offener, ungesicherter Wireless-Verbindungen zwischen den APs und Clients. Der OWE verwendet die auf dem Diffie-Hellman-Algorithmus basierende Verschlüsselung, um die Wireless-Verschlüsselung einzurichten. Mit OWE führen der Client und AP während des Zugriffsvorgangs einen Diffie-Hellman-Schlüsselaustausch durch und

verwenden den resultierenden paarweisen Master Key (PMK)-Schlüssel mit dem 4-Wege-Handshake. Die Verwendung von OWE erhöht die Sicherheit von Wireless-Netzwerken in Bereitstellungen, in denen offene oder gemeinsam genutzte PSK-basierte Netzwerke bereitgestellt werden.



OWE-Frame-Austausch

SAE

WPA3 verwendet einen neuen Authentifizierungs- und Schlüsselverwaltungsmechanismus, der als Simultane Authentifizierung von Equals bezeichnet wird. Dieser Mechanismus wird durch den Einsatz von SAE Hash-to-Element (H2E) weiter verbessert.

SAE mit H2E ist für WPA3 und Wi-Fi 6E obligatorisch.

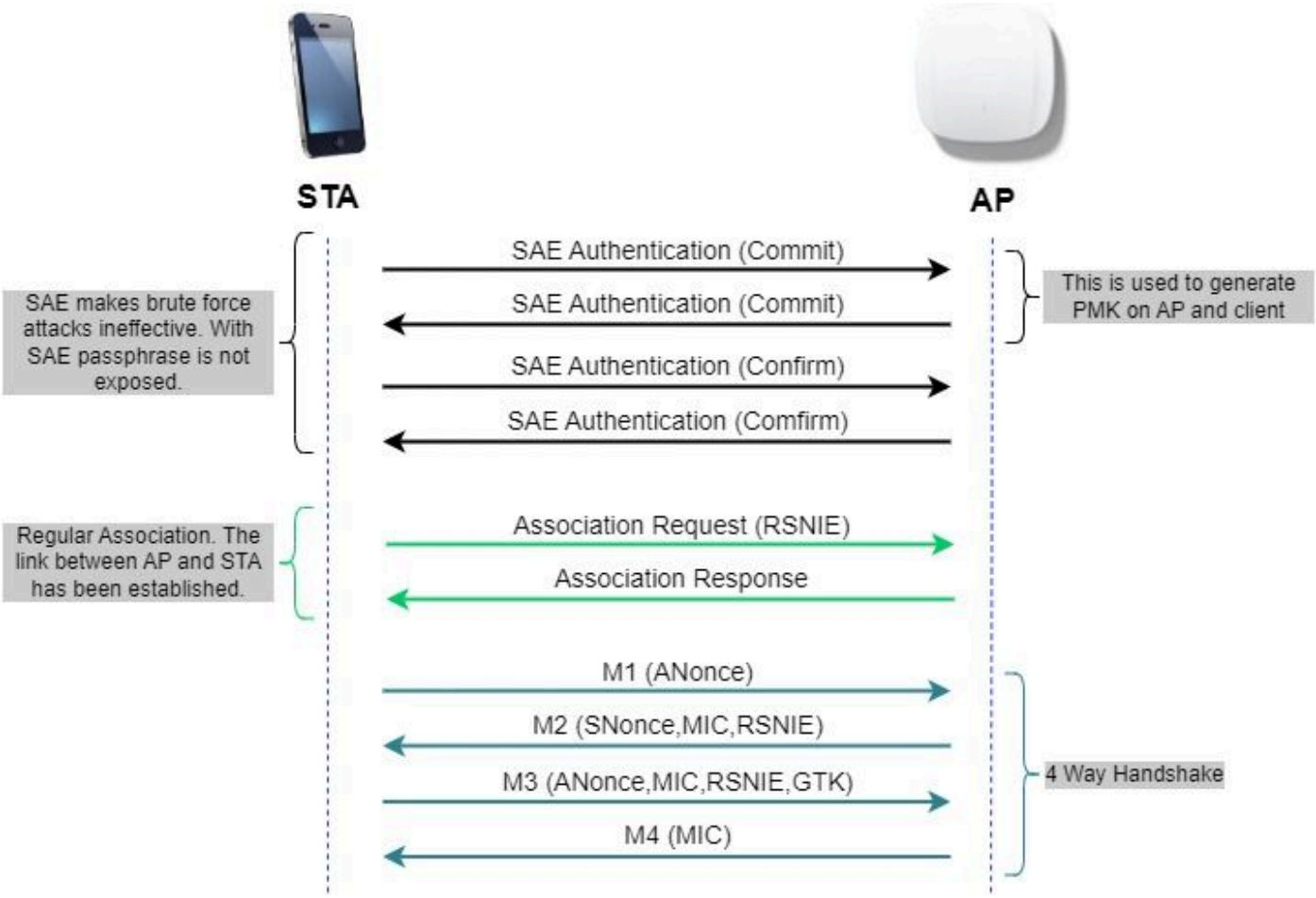
SAE verwendet eine diskrete Logarithmuskryptographie, um einen effizienten Austausch auf eine Weise durchzuführen, die eine gegenseitige Authentifizierung mit einem Passwort ermöglicht, das wahrscheinlich gegen einen Offline-Wörterbuchangriff resistent ist.

Bei einem Angriff auf ein Offline-Wörterbuch versucht ein Angreifer, ein Netzwerkkennwort zu ermitteln, indem er mögliche Kennwörter ohne weitere Netzwerkinteraktion ausprobiert.

Wenn der Client eine Verbindung mit dem Access Point herstellt, führt er einen SAE-Austausch durch. Bei Erfolg erstellen sie jeweils einen kryptographisch starken Schlüssel, von dem der

Sitzungsschlüssel abgeleitet wird. Grundsätzlich geht ein Client und Access Point in Phasen des Commit und dann bestätigen.

Sobald eine Vereinbarung besteht, können der Client und der Access Point bei jeder Generierung eines Sitzungsschlüssels in den Bestätigungsstatus wechseln. Die Methode verwendet die Weiterleitungsgeheimnis, bei der ein Eindringling einen einzelnen Schlüssel knacken könnte, aber nicht alle anderen Schlüssel.



SAE Frame Exchange

Hash-to-Element (H2E)

Hash-to-Element (H2E) ist eine neue PWE-Methode (SAE Password Element). Bei diesem Verfahren wird die im SAE-Protokoll verwendete geheime PWE aus einem Passwort generiert.

Wenn eine Station (STA), die H2E unterstützt, SAE mit einem AP initiiert, prüft sie, ob AP H2E unterstützt. Wenn ja, leitet der AP die PWE über H2E mithilfe eines neu definierten Statuscodewerts in der SAE-Commit-Nachricht ab.

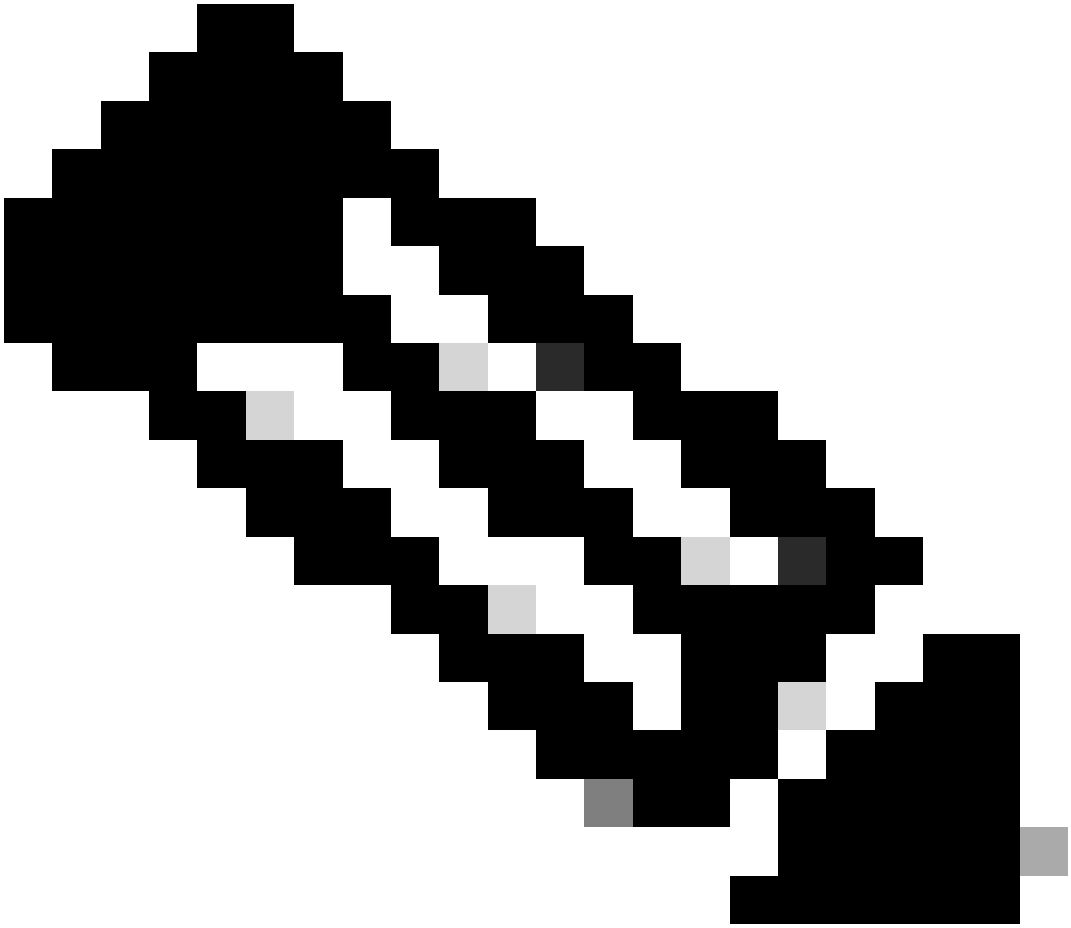
Wenn STA Hunting-and-Pecking (HnP) verwendet, bleibt der gesamte SAE-Austausch unverändert.

Bei Verwendung von H2E wird die PWE-Ableitung in folgende Komponenten unterteilt:

- Ableitung eines Secret Intermediary Elements (PT) aus dem Passwort. Dies kann offline

durchgeführt werden, wenn das Kennwort für jede unterstützte Gruppe auf dem Gerät konfiguriert wurde.

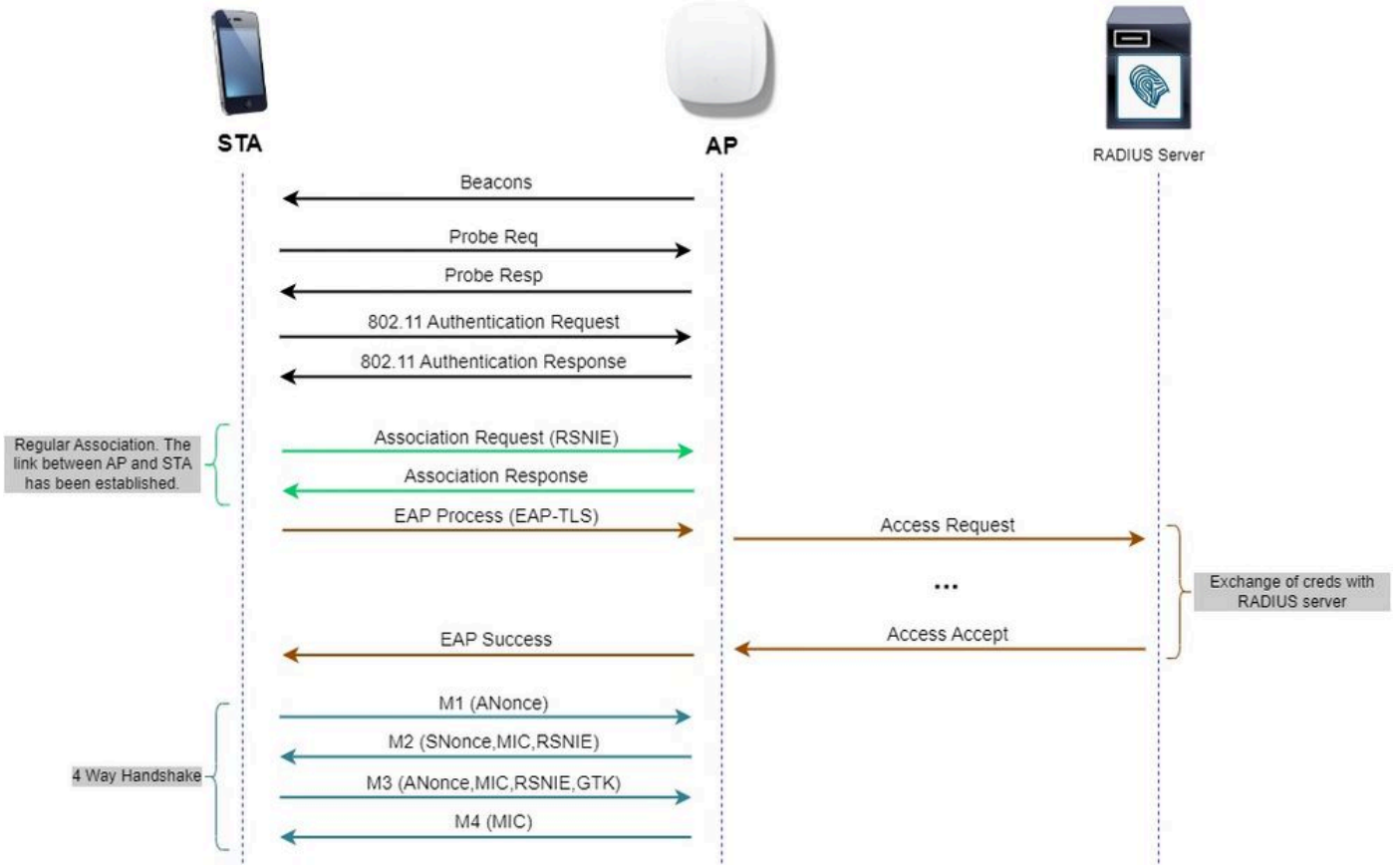
- Ableitung des PWE aus dem gespeicherten PT. Dies hängt von der ausgehandelten Gruppe und den MAC-Adressen der Peers ab. Dies erfolgt in Echtzeit während des SAE-Austauschs.



Hinweis: 6 GHz unterstützt nur die Hash-to-Element SAE PWE-Methode.

WPA-Enterprise (802.1x)

WPA3-Enterprise ist die sicherste Version von WPA3 und verwendet eine Kombination aus Benutzername und Kennwort mit 802.1X für die Benutzerauthentifizierung mit einem RADIUS-Server. Standardmäßig verwendet WPA3 eine 128-Bit-Verschlüsselung, führt jedoch auch eine optional konfigurierbare Verschlüsselungsstärke-Verschlüsselung mit 192 Bit ein, die ein Netzwerk, das sensible Daten überträgt, zusätzlich schützt.



WPA3-Enterprise-Diagramm

Stufensatz: WPA3-Modi

- WPA3-Personal
  - Nur WPA3-Personal-Modus
    - PMF erforderlich
  - WPA3-Personal-Übergangsmodus
    - Konfigurationsregeln: Wenn WPA2-Personal auf einem WAP aktiviert ist, muss standardmäßig auch der WPA3-Personal-Übergangsmodus aktiviert sein, es sei denn, der Administrator hat dies explizit überschrieben, um nur im WPA2-Personal-Modus zu arbeiten.

- WPA3-Enterprise
  - WPA3 - Nur Enterprise-Modus
    - Die PMF wird für alle WPA3-Verbindungen ausgehandelt.
  - WPA3-Enterprise-Übergangsmodus
    - Die PMF wird für eine WPA3-Verbindung ausgehandelt.
    - PMF optional für eine WPA2-Verbindung
  - WPA3-Enterprise Suite-B "192-Bit"-Modus abgestimmt auf Commercial National Security Algorithm (CNSA)
    - Mehr als nur für die Bundesregierung
    - Konsistente Verschlüsselung zur Vermeidung von Fehlkonfigurationen
    - Ergänzung von GCMP und ECCP für Crypto- und bessere Hash-Funktionen

(SHA384)
- PMF erforderlich

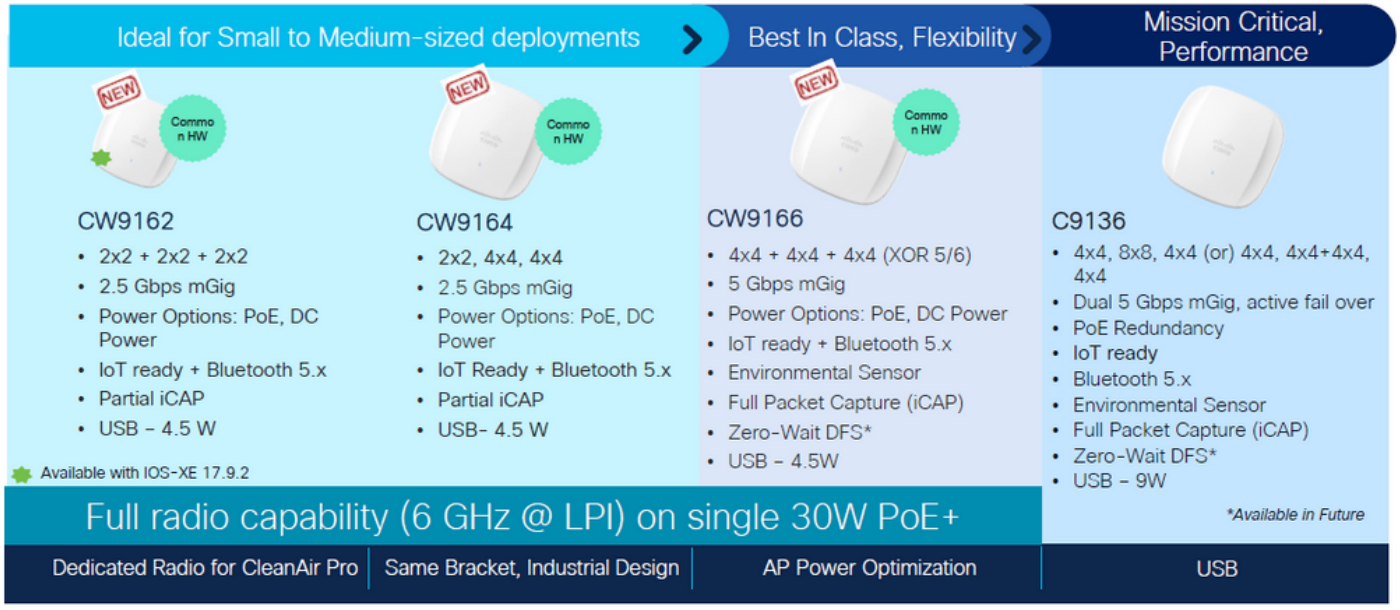
- Die WPA3-192-Bit-Sicherheit gilt ausschließlich für EAP-TLS, für das Zertifikate sowohl auf dem Supplicant als auch auf dem RADIUS-Server erforderlich sind.

- Um WPA3 192-Bit Enterprise verwenden zu können, müssen die RADIUS-Server eine der zulässigen EAP-Verschlüsselungen verwenden:

  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Weitere Informationen zur WPA3-Implementierung in Cisco WLANs, einschließlich der Kompatibilitätsmatrix für die Client-Sicherheit, finden Sie im WPA3-Bereitstellungsleitfaden.

Cisco Catalyst Wi-Fi 6E APs



Wi-Fi 6E Access Points

Von Clients unterstützte Sicherheitseinstellungen

Welche Produkte WPA3-Enterprise unterstützen, erfahren Sie auf der WiFi Alliance Produktsuche.

Auf Windows-Geräten können Sie mithilfe des Befehls "netsh wlan show drivers" überprüfen, welche Sicherheitseinstellungen vom Adapter unterstützt werden.

Hier sehen Sie die Ausgabe der 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-Ausgabe von _netsh wlan show driver_ für Client AX211

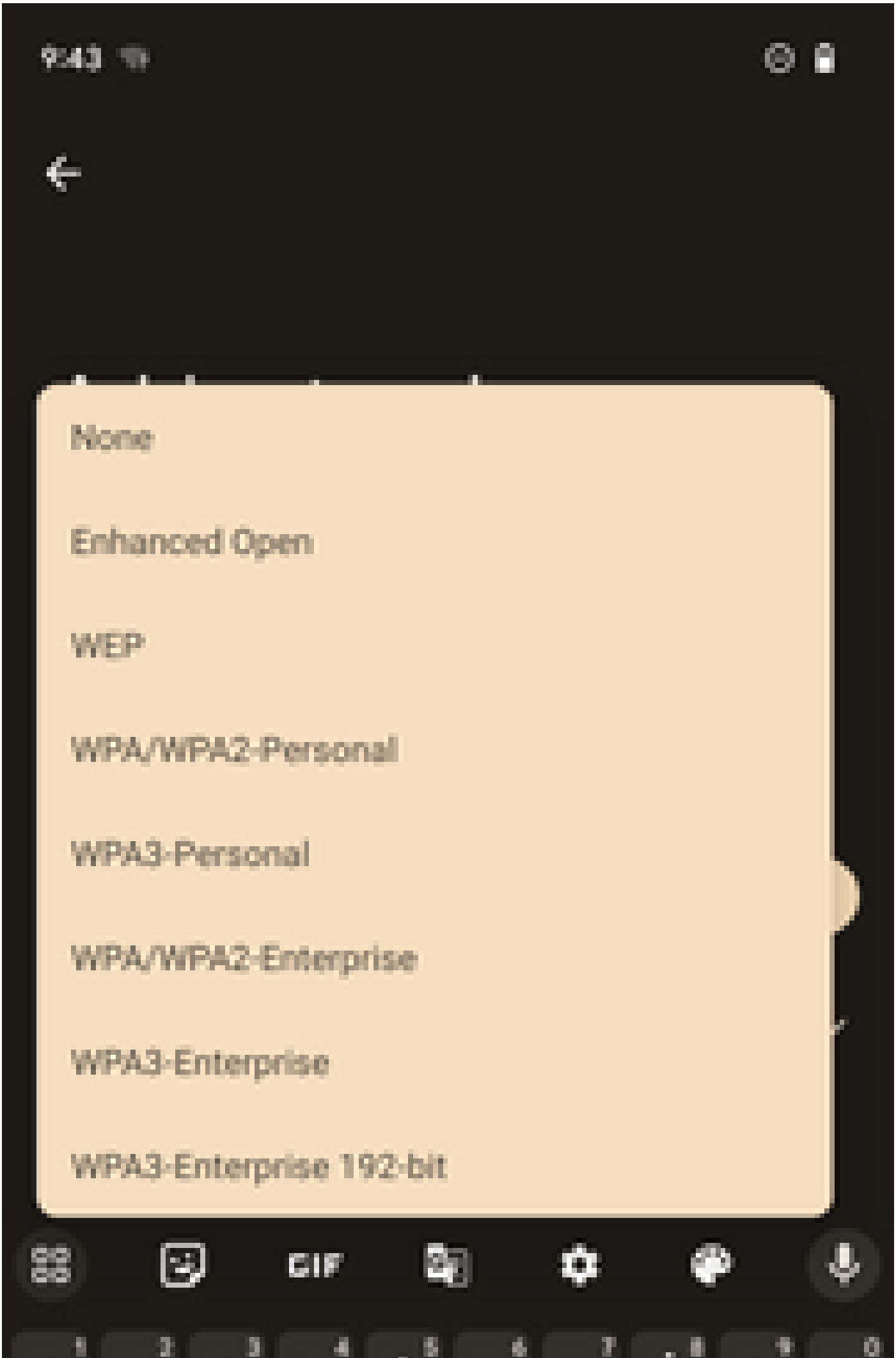
Netgear A8000:

```
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-Ausgabe von _netsh wlan show driver_ für Client Netgear A8000s

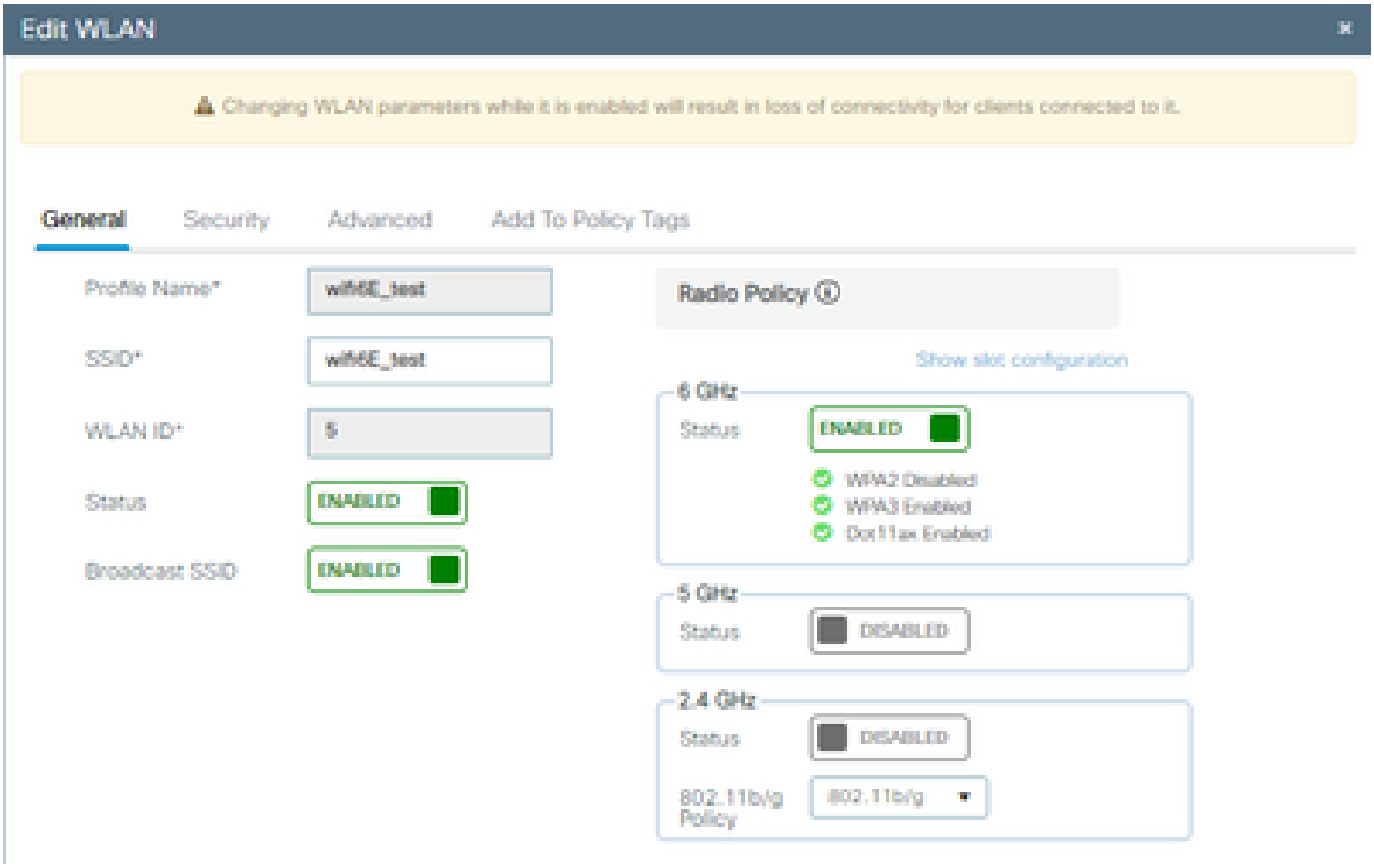
Android-Pixel 6a:


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

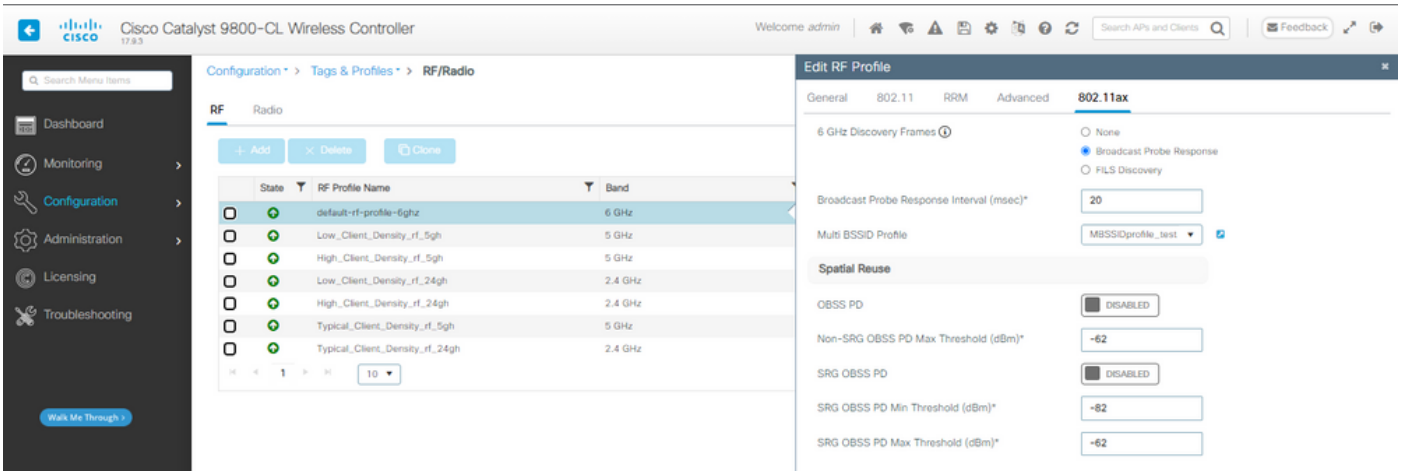
- WPA3- + AES-Verschlüsselung + 802.1x-SHA256 (FT) AKM
- WPA3 + AES-Verschlüsselung + OWE AKM
- WPA3 + AES-Verschlüsselung + SAE (FT) AKM
- WPA3 + CCMP256-Chiffre + SUITEB192-1X AKM
- WPA3 + GCMP128-Chiffre + SUITEB-1X AKM
- WPA3 + GCMP256-Chiffre + SUITEB192-1X AKM

Basiskonfiguration

Das WLAN wurde mit der Ermittlungsmethode "Nur Funkrichtlinie 6 GHz" und "UPR (Broadcast Probe Response)" konfiguriert:



WLAN-Basiskonfiguration



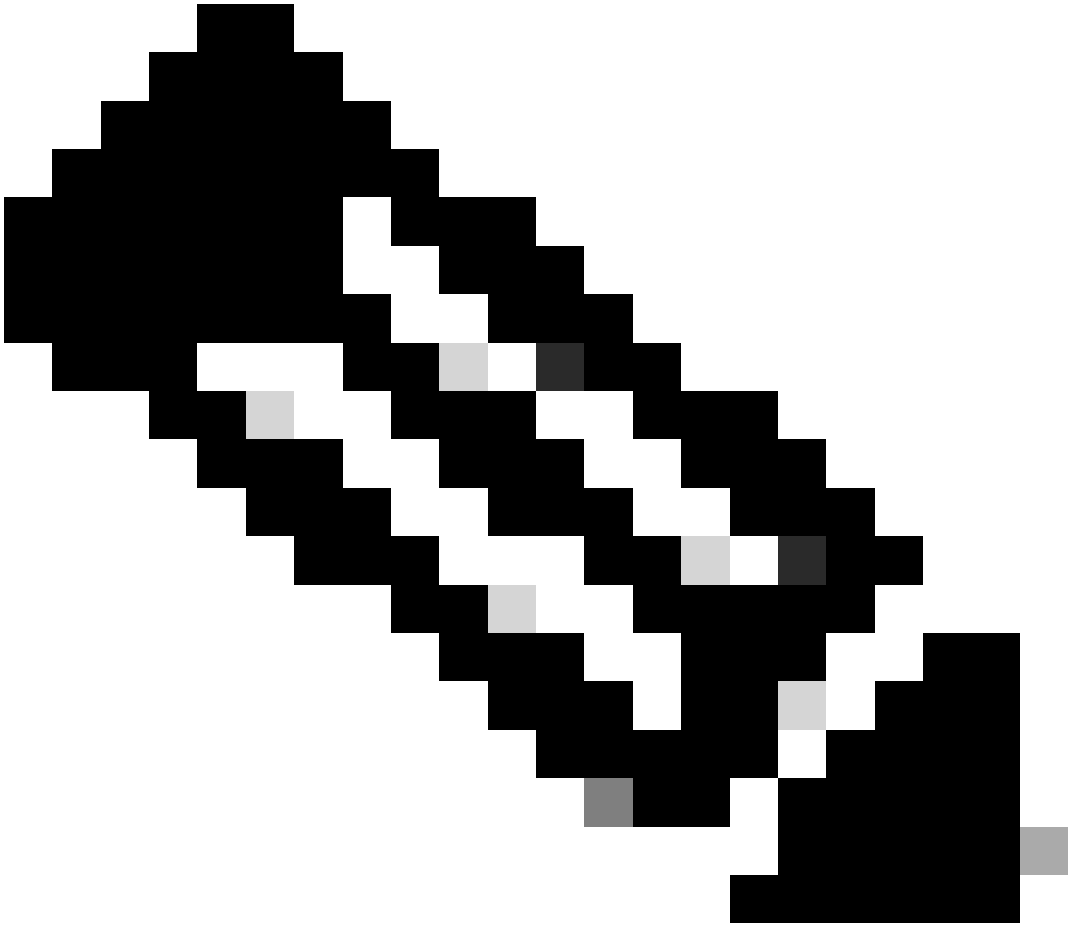
Konfiguration des 6-GHz-RF-Profils

Überprüfung

Sicherheitsüberprüfung

In diesem Abschnitt wird die Phase der Sicherheitskonfiguration und der Client-Zuordnung mithilfe der folgenden WPA3-Protokollkombinationen erläutert:

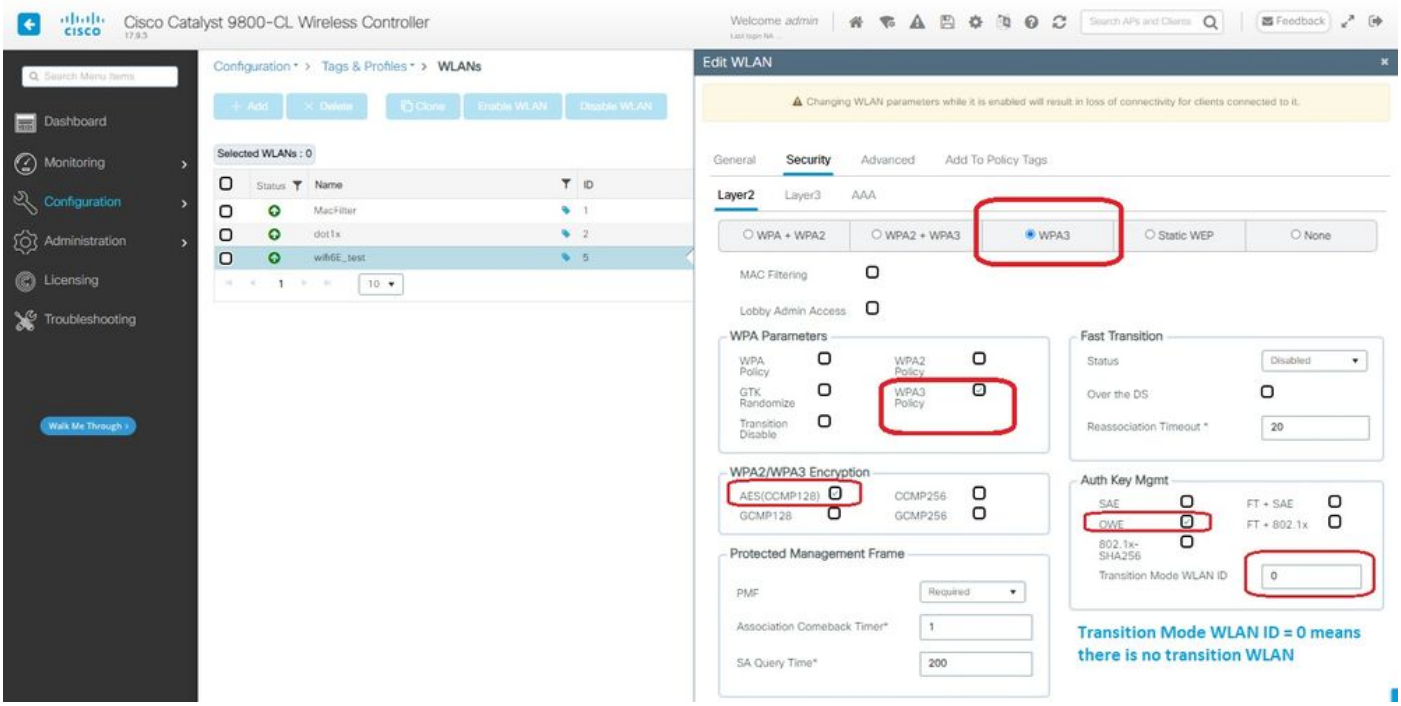
- WPA3- AES(CCMP128) + SCHULDENSTÜCK
  - OWE-Übergangsmodus
- WPA3-Personal
  - AES (CCMP128) + SAE
- WPA3-Enterprise
  - AES (CCMP128) + 802.1x-SHA256
  - AES (CCMP128) + 802.1x-SHA256 + FT
  - GCMP128-Chiffre + SUITEB-1X
  - GCMP256-Chiffre + SUITEB192-1X



Hinweis: Obwohl es keine Clients gibt, die GCMP128 cipher + SUITEB-1X unterstützen, als sie dieses Dokument geschrieben haben, wurde es getestet, um zu beobachten, dass es gesendet wird, und die RSN-Informationen in den Beacons zu überprüfen.

WPA3 - AES (CCPM128) + SCHULDENSTÜCK

Dies ist die WLAN-Sicherheitskonfiguration:



OWE-Sicherheitseinstellungen

Auf der WLC-GUI der WLAN-Sicherheitseinstellungen anzeigen:

WLAN-Sicherheitseinstellungen auf der WLC-GUI

Hier können wir den Verbindungsvorgang der Wi-Fi 6E Clients beobachten:

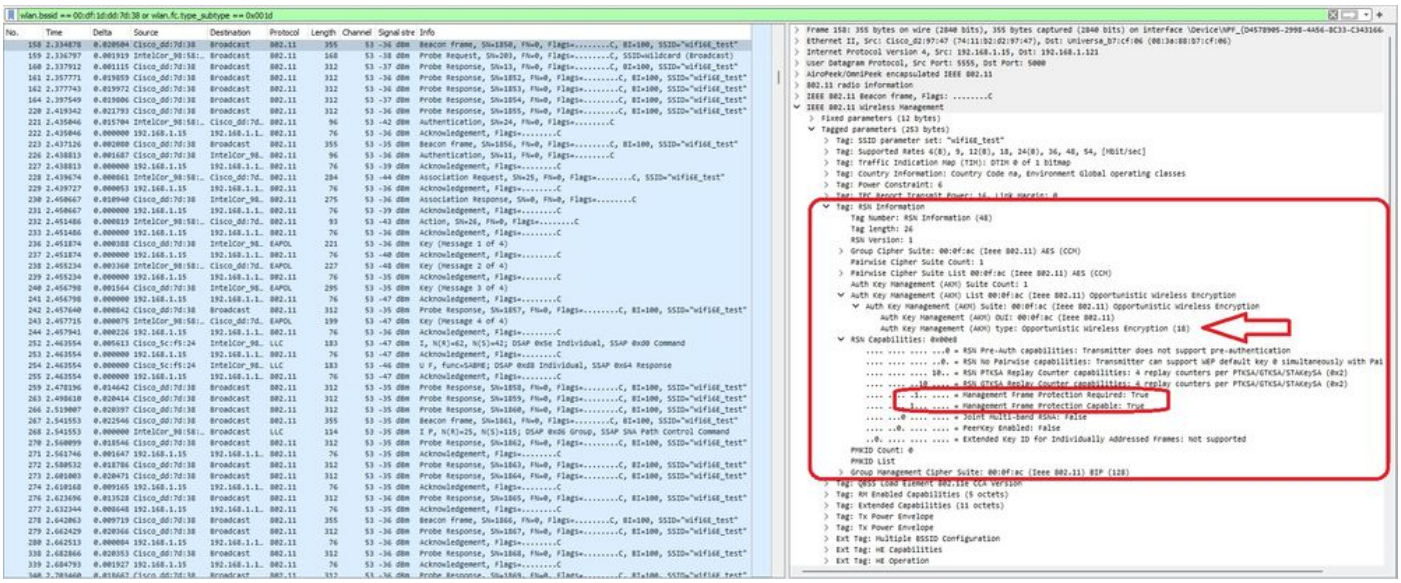
Intel AX211

Hier zeigen wir den vollständigen Verbindungsvorgang des Intel AX211-Client.

OWE-Analyse

Hier sehen Sie die Beacons OTA. Der Access Point kündigt mithilfe des Selektors der AKM-Suite für OWE unter dem RSN-Informationselement die Unterstützung für OWE an.

Sie können den Wert 18 (00-0F-AC:18) für den Typ der AKM-Suite sehen, der auf die OWE-Unterstützung hinweist.



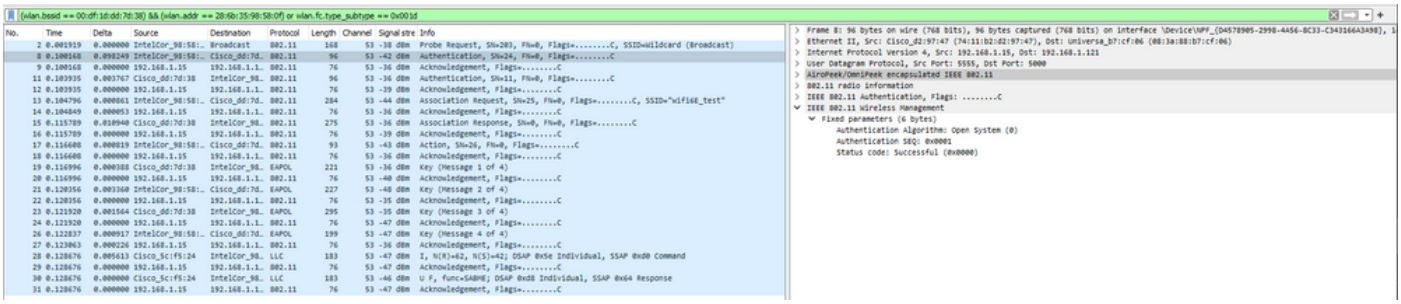
OWE-Bakenrahmen

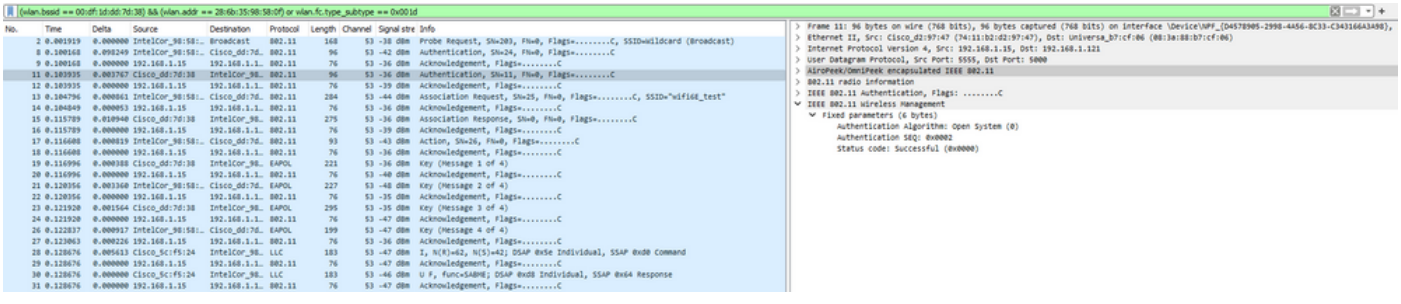
Wenn Sie sich das Feld "RSN-Funktionen" ansehen, sehen Sie, dass der Access Point sowohl MFP-Funktionen (Management Frame Protection) als auch das erforderliche MFP-Bit (1) ankündigt.

OWE-Verband

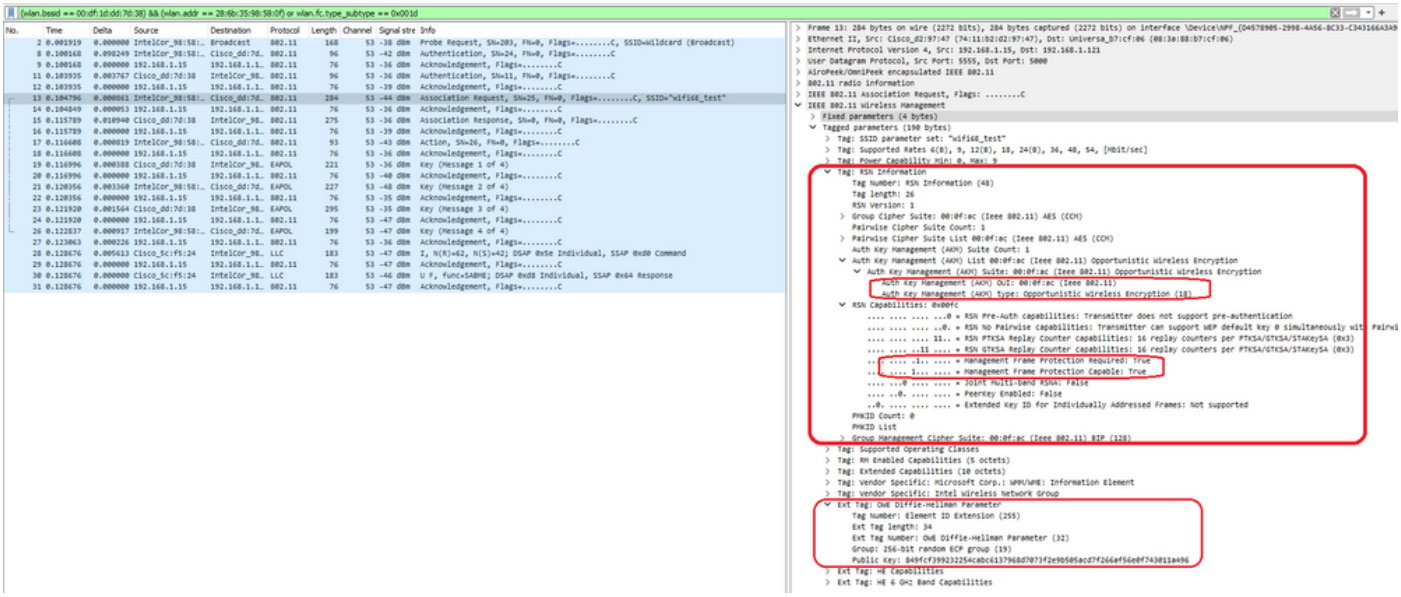
Sie können den UPR im Broadcast-Modus und dann die Zuordnung selbst sehen.

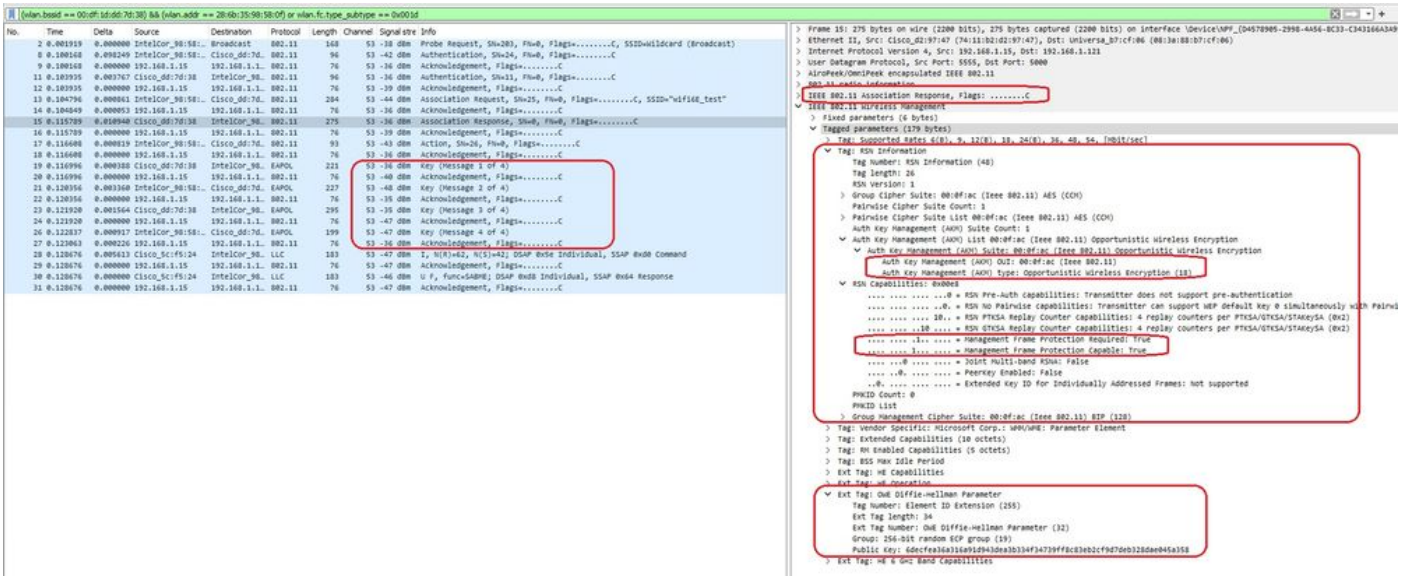
Das OWE beginnt mit der OPEN-Authentifizierungsanfrage und -antwort:





Anschließend muss ein Client, der OWE durchführen möchte, OWE AKM im RSN IE des Association Request-Frames angeben und das Diffie Helman (DH)-Parameterelement einschließen:

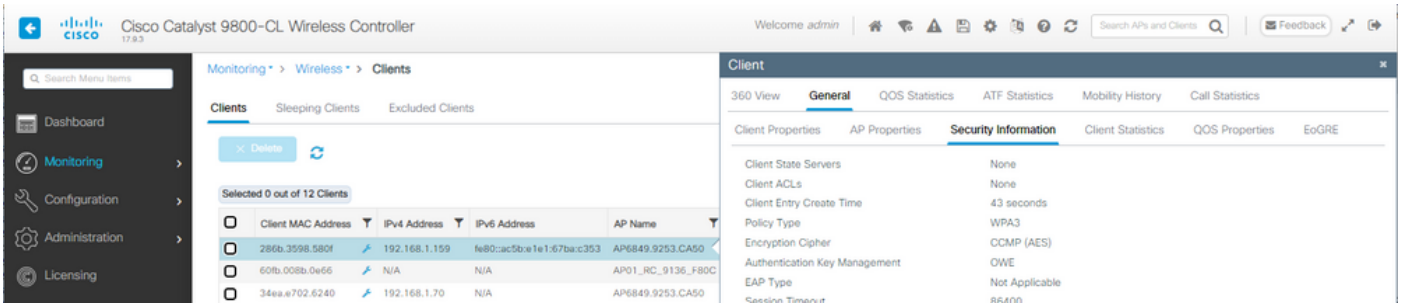




Antwort der OWE-Vereinigung

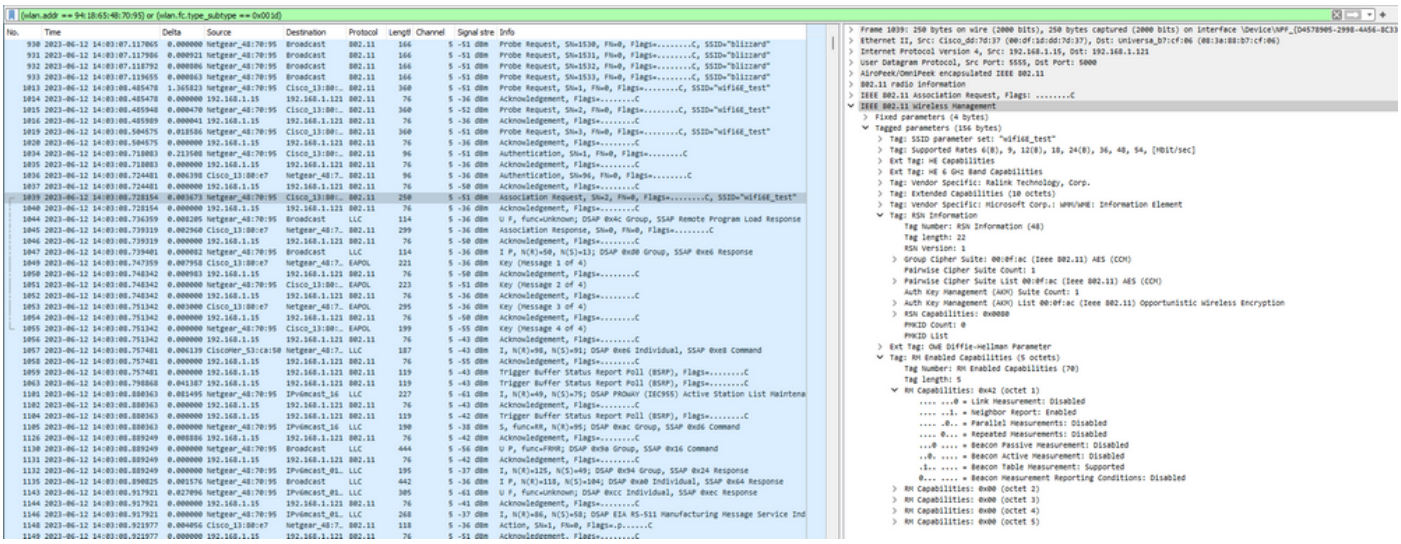
Nach der Zuordnungsantwort wird der 4-Wege-Handshake angezeigt, und der Client wechselt in den verbundenen Zustand.

Hier sehen Sie die Client-Details auf der WLC-GUI:

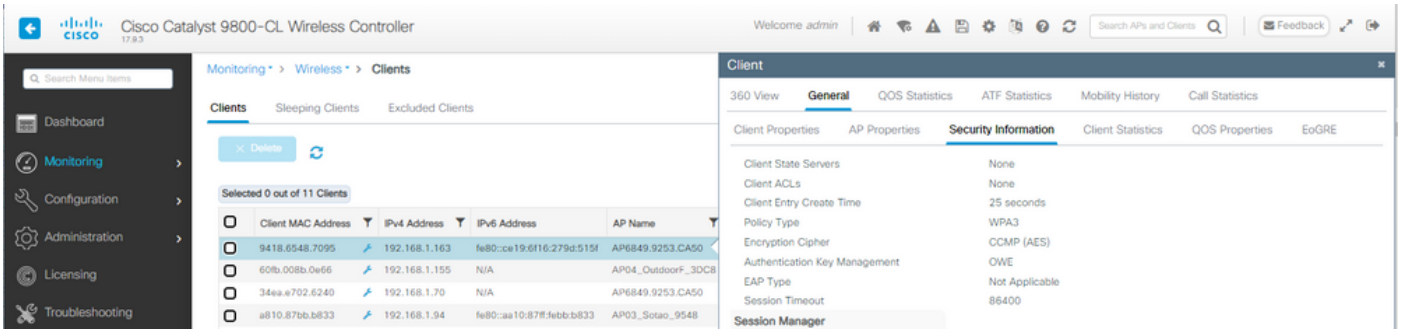


NetGear A8000

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

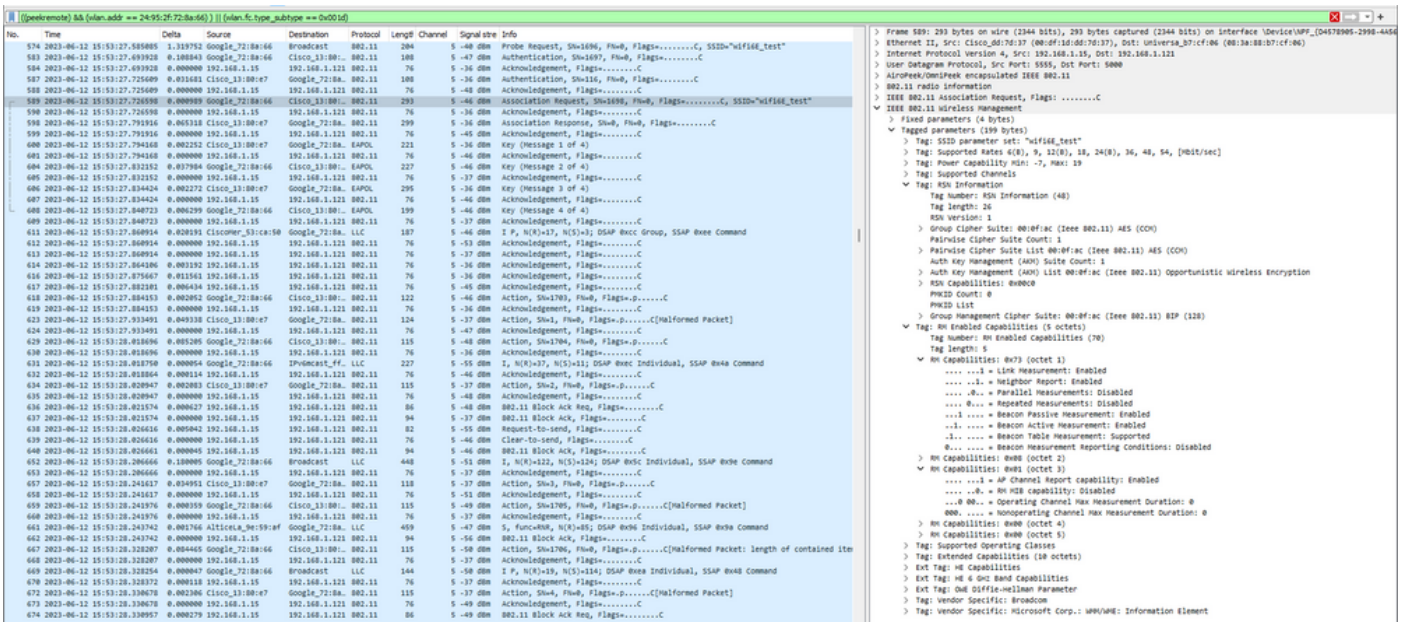


Client-Details in WLC:

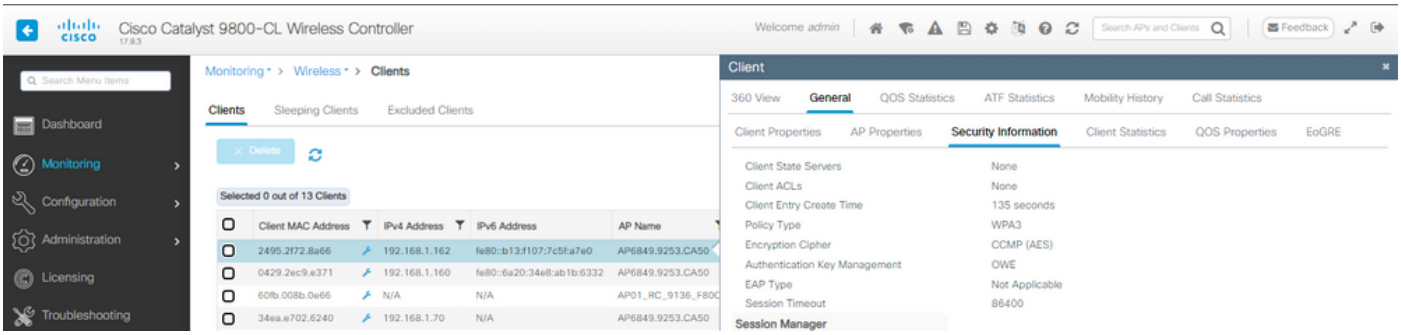


Pixel 6a

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

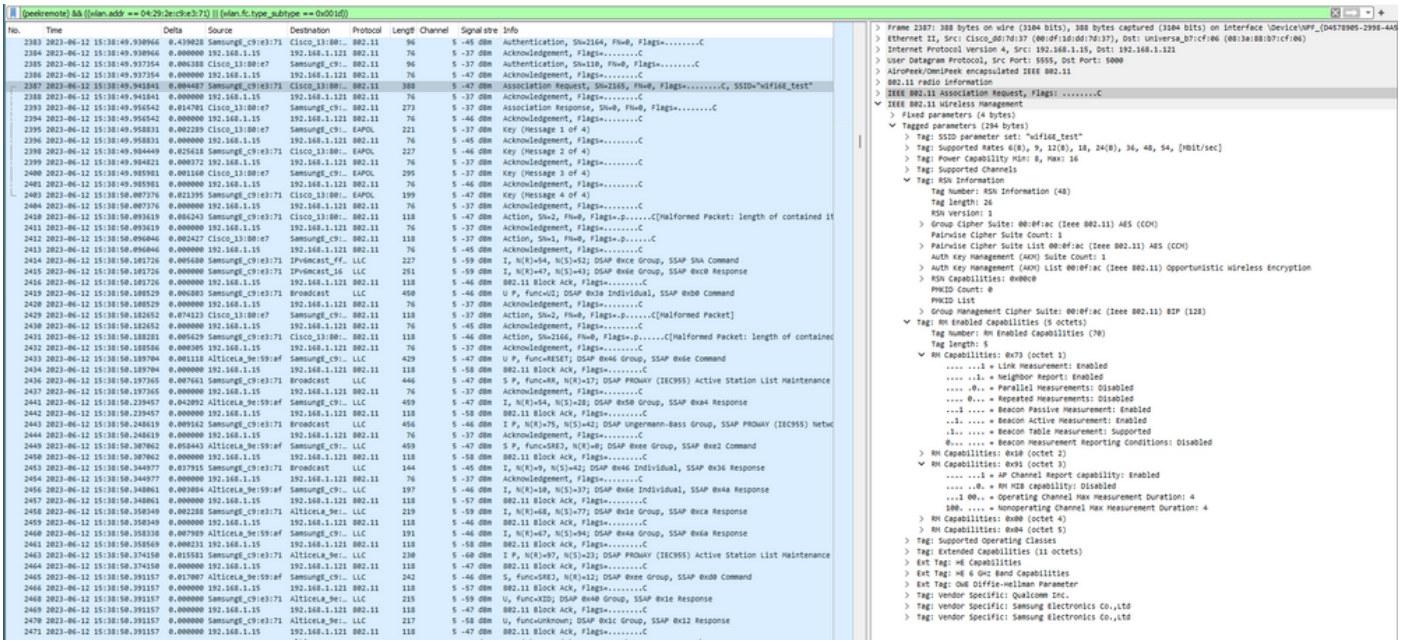


Client-Details in WLC:

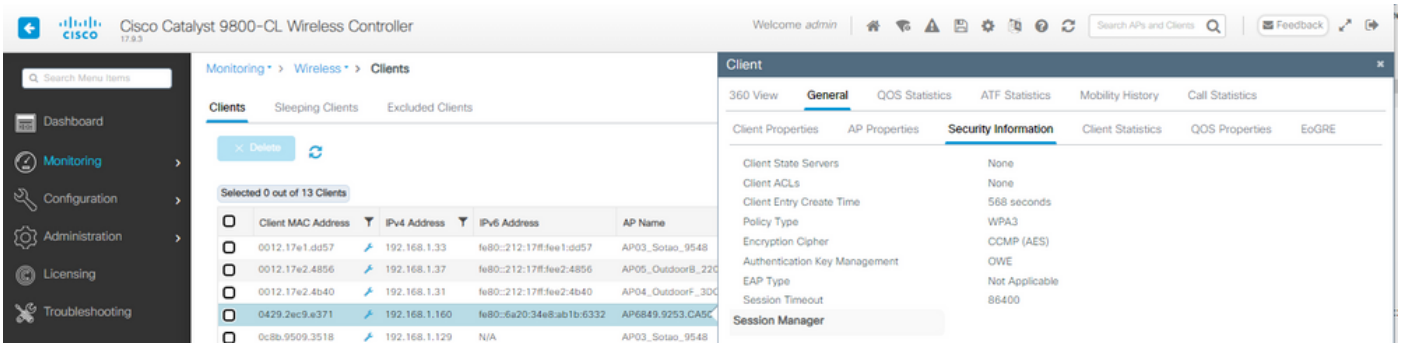


Samsung S23

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:



Client-Details in WLC:

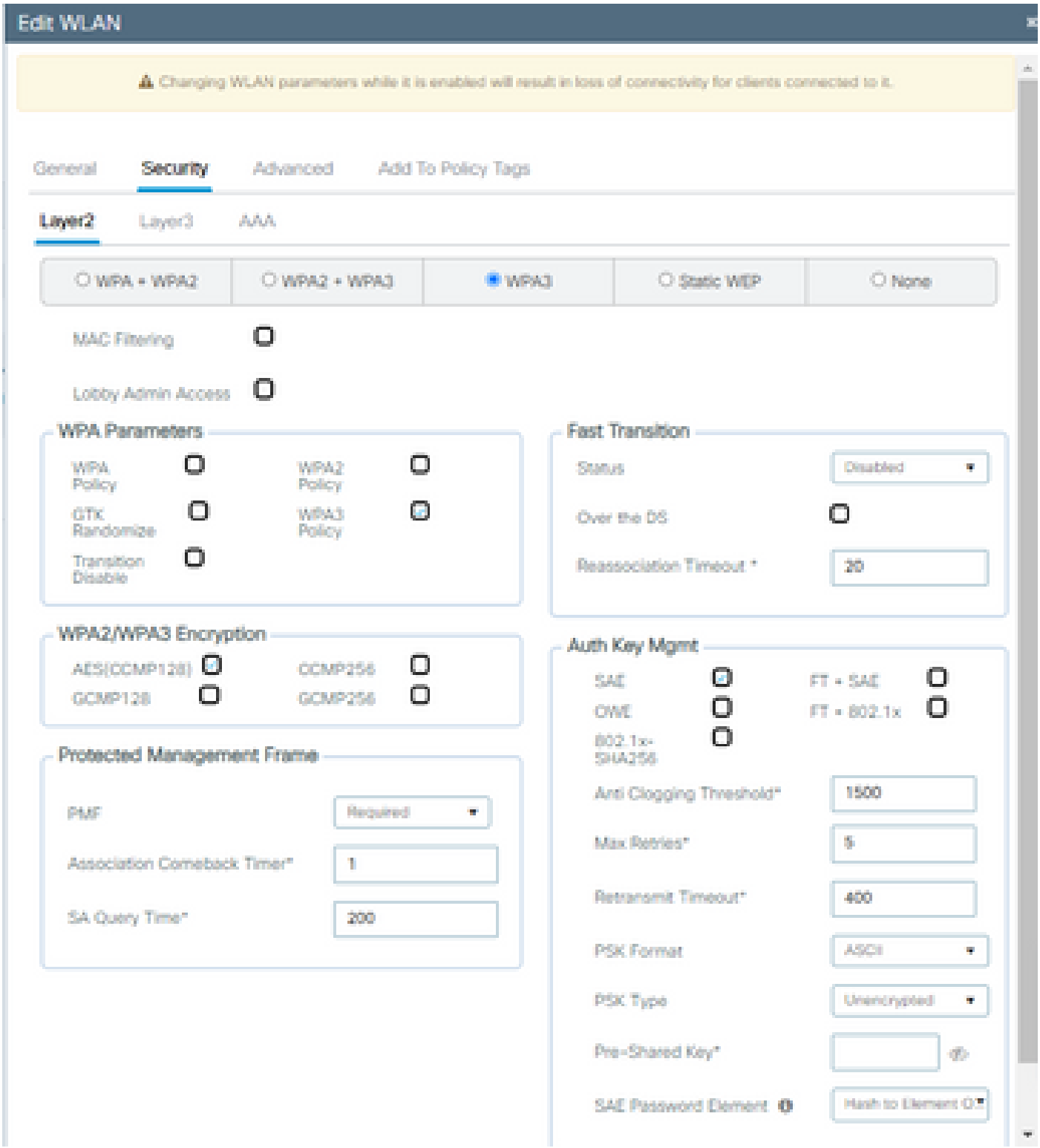


WPA3 - AES(CCPM128) + OWE mit Übergangsmodus

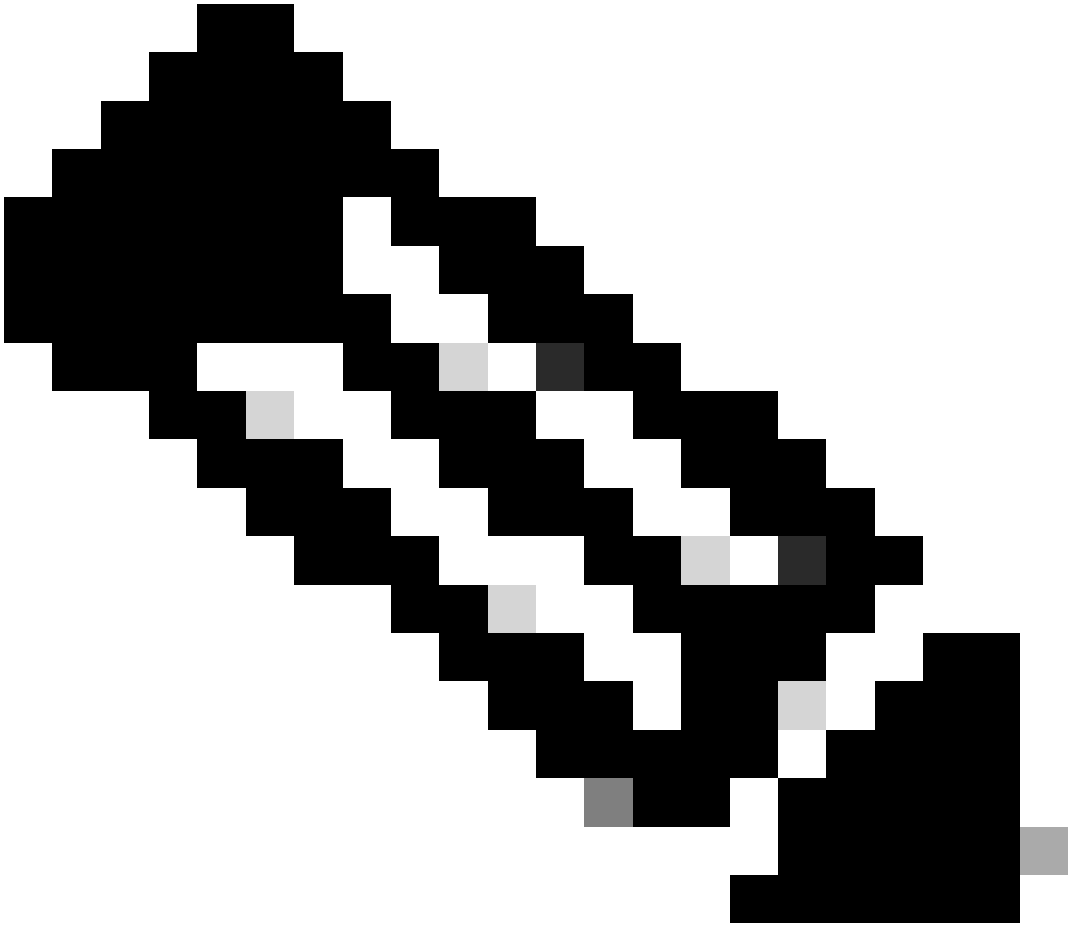
Ausführliche Informationen zur Konfiguration und Fehlerbehebung des OWE-Übergangsmodus finden Sie in diesem Dokument: Konfigurieren der erweiterten offenen SSID mit dem Übergangsmodus - OWE.

WPA3-Personal - AES(CCMP128) + SAE

WLAN-Sicherheitskonfiguration:



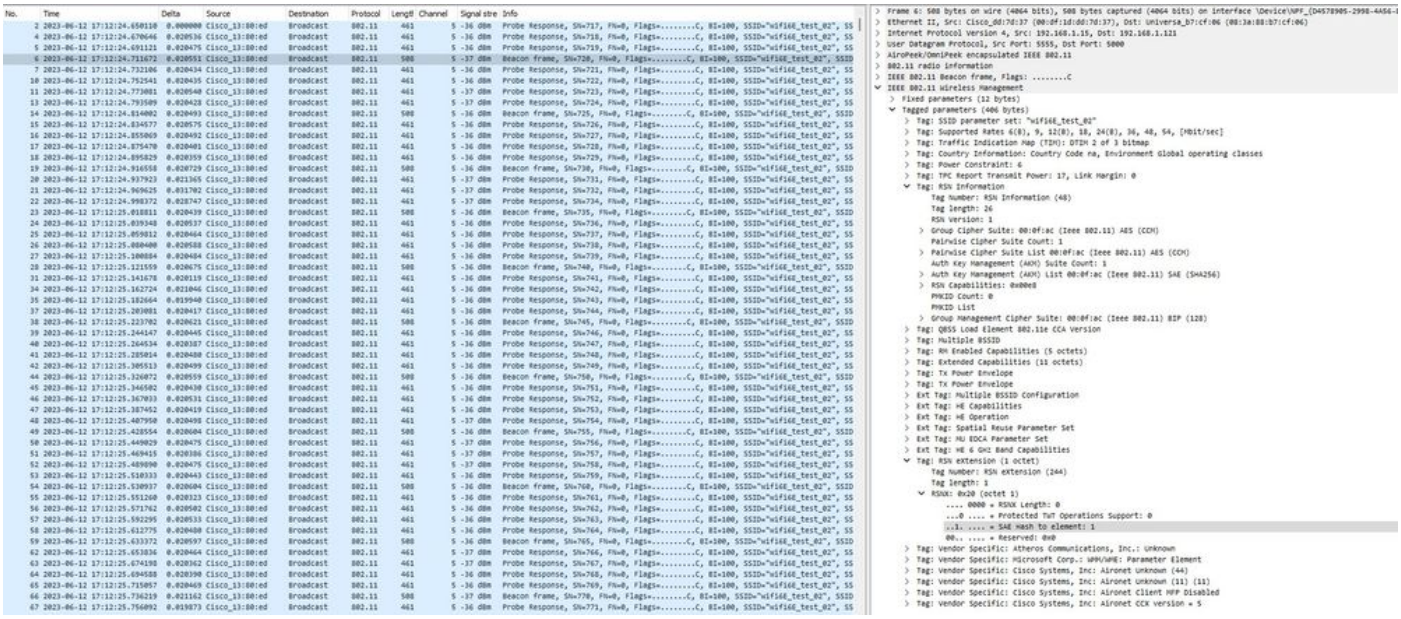
WPA3 SAE-Konfiguration



Hinweis: Beachten Sie, dass Hunting und Pecking gemäß der 6-GHz-Funkrichtlinie nicht zulässig sind. Wenn Sie ein reines 6-GHz-WLAN konfigurieren, müssen Sie H2E SAE Password Element auswählen.

Auf der WLC-GUI der WLAN-Sicherheitseinstellungen anzeigen:

Verifizierung von Beacons OTA:

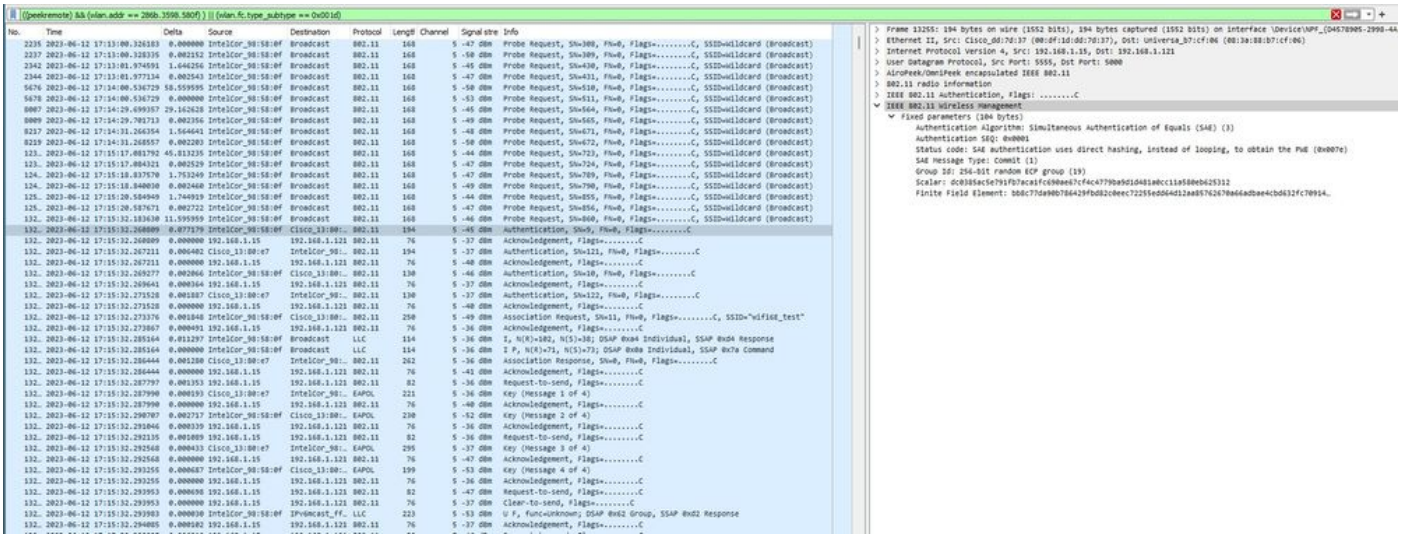


WPA3 SAE-Beacons

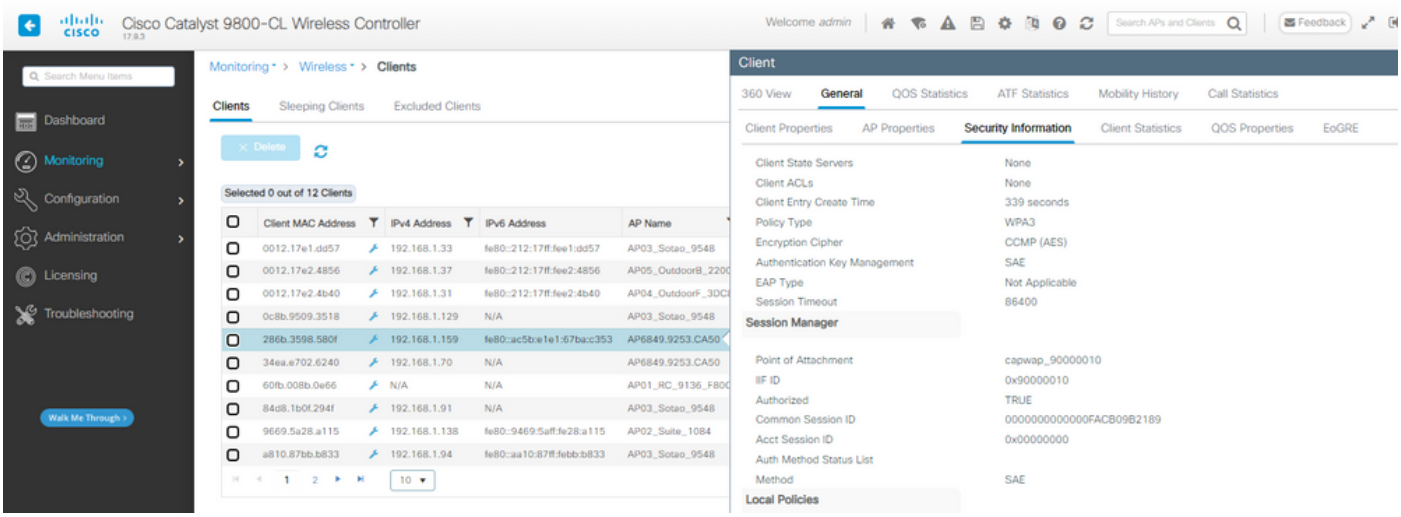
Hier können wir beobachten, wie Wi-Fi 6E-Clients sich verbinden:

Intel AX211

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

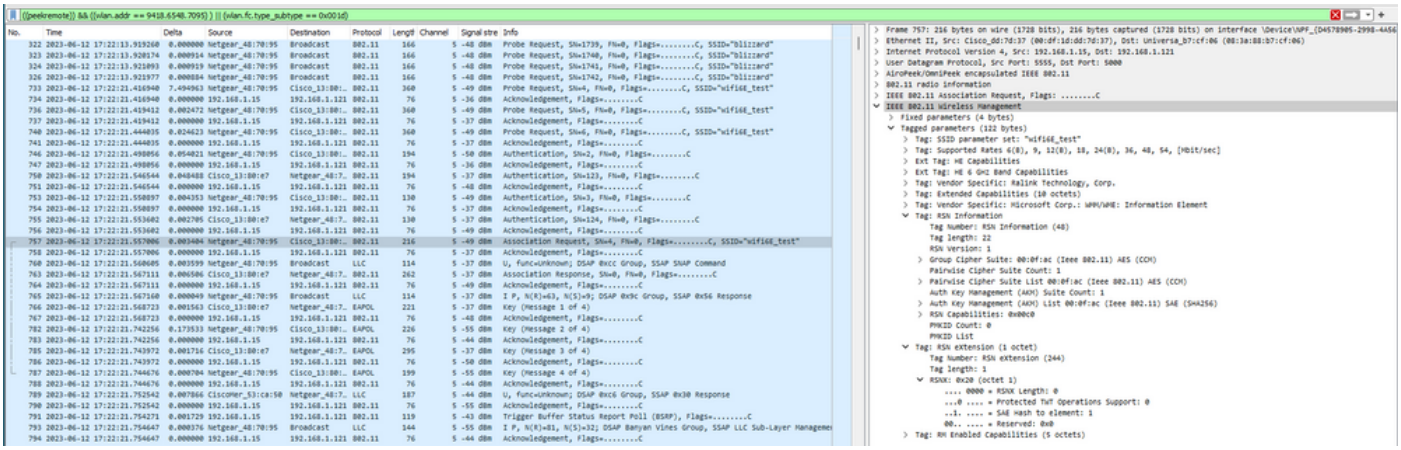


Client-Details in WLC:

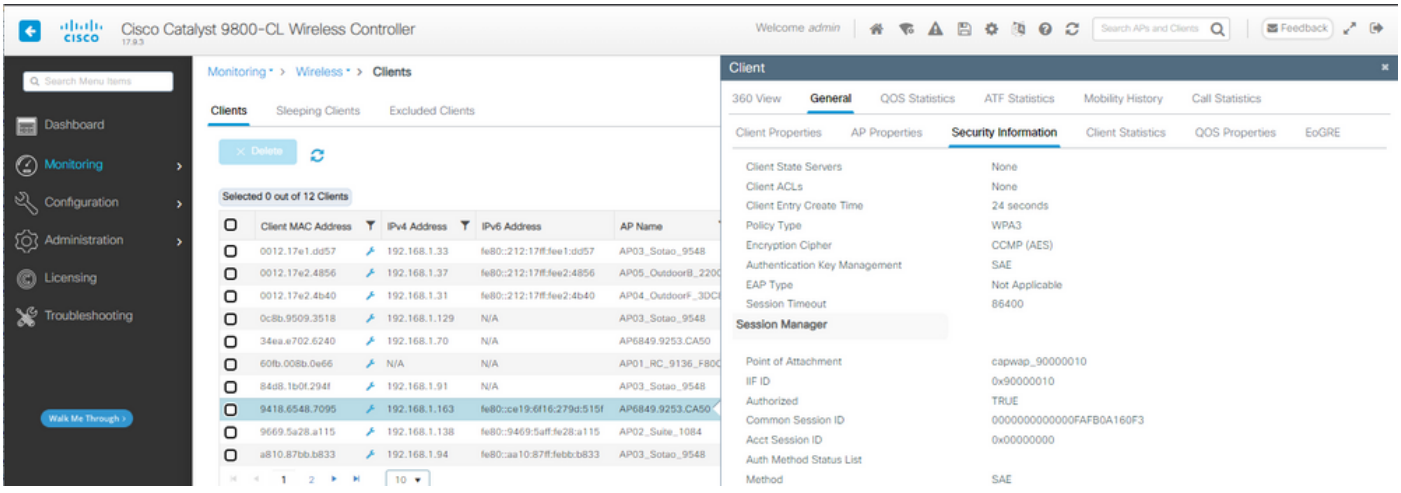


NetGear A8000

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

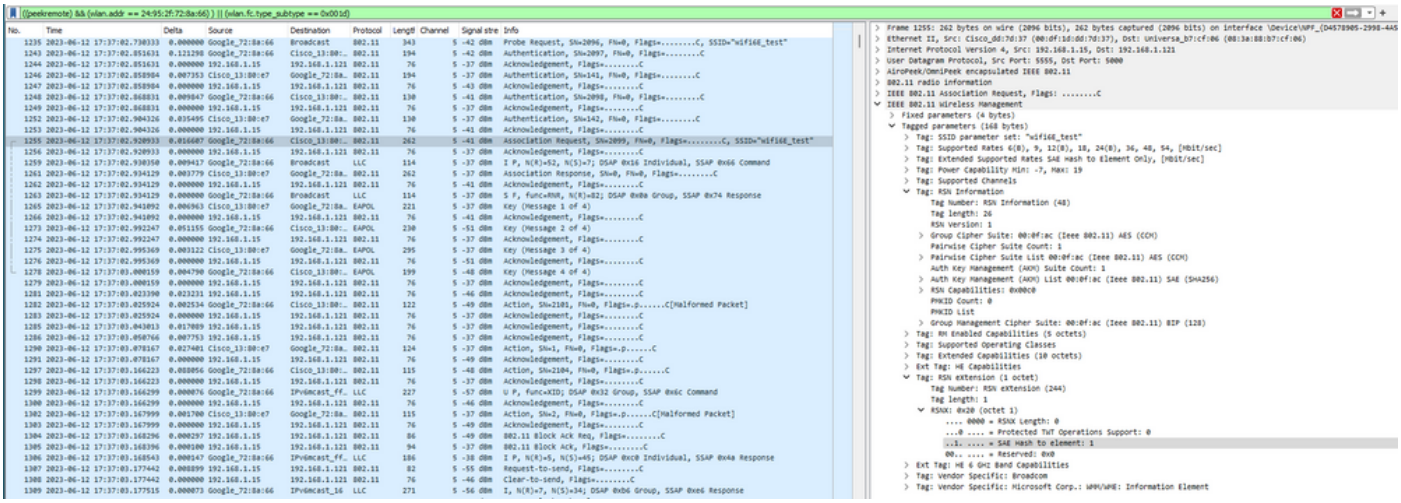


Client-Details in WLC:

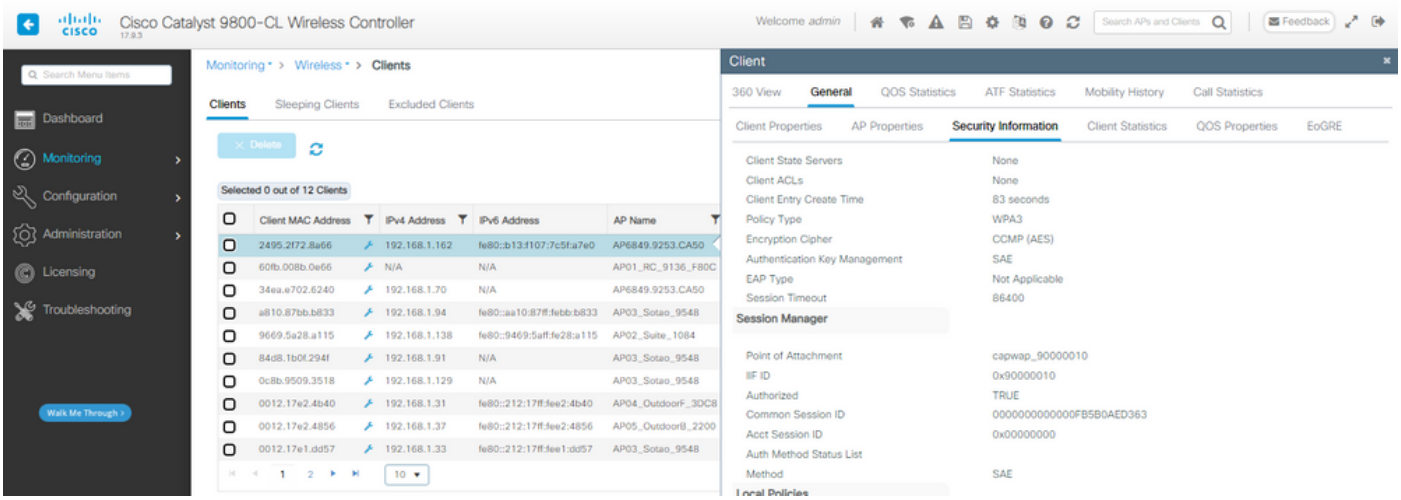


Pixel 6a

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

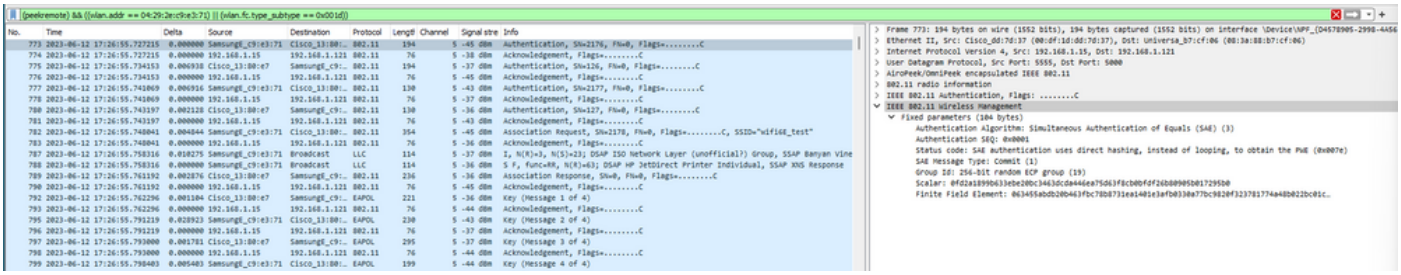


Client-Details in WLC:

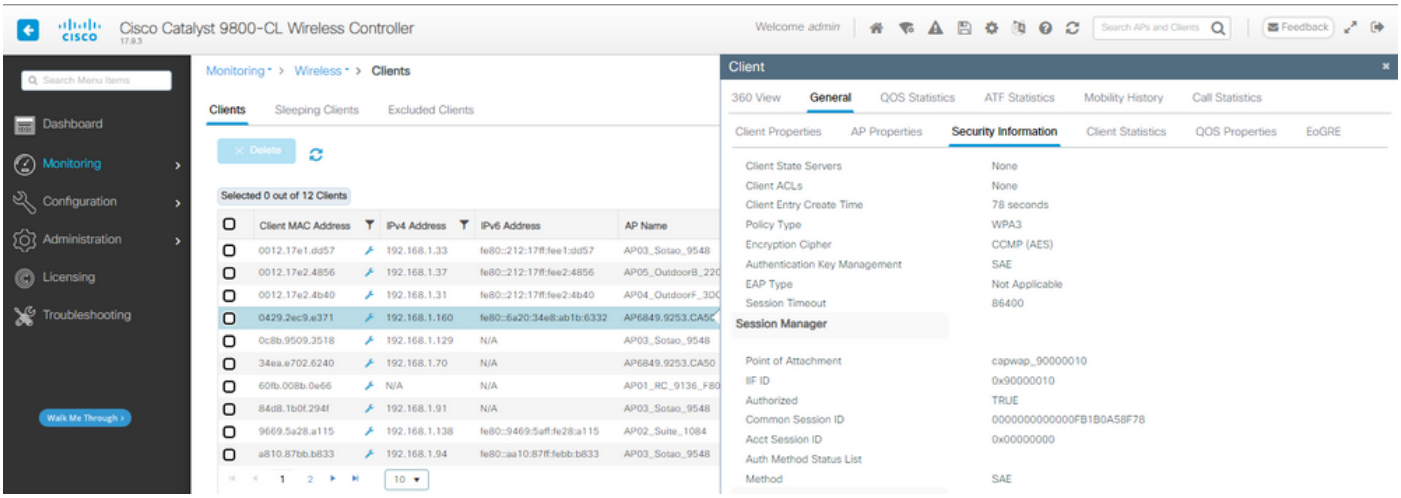


Samsung S23

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

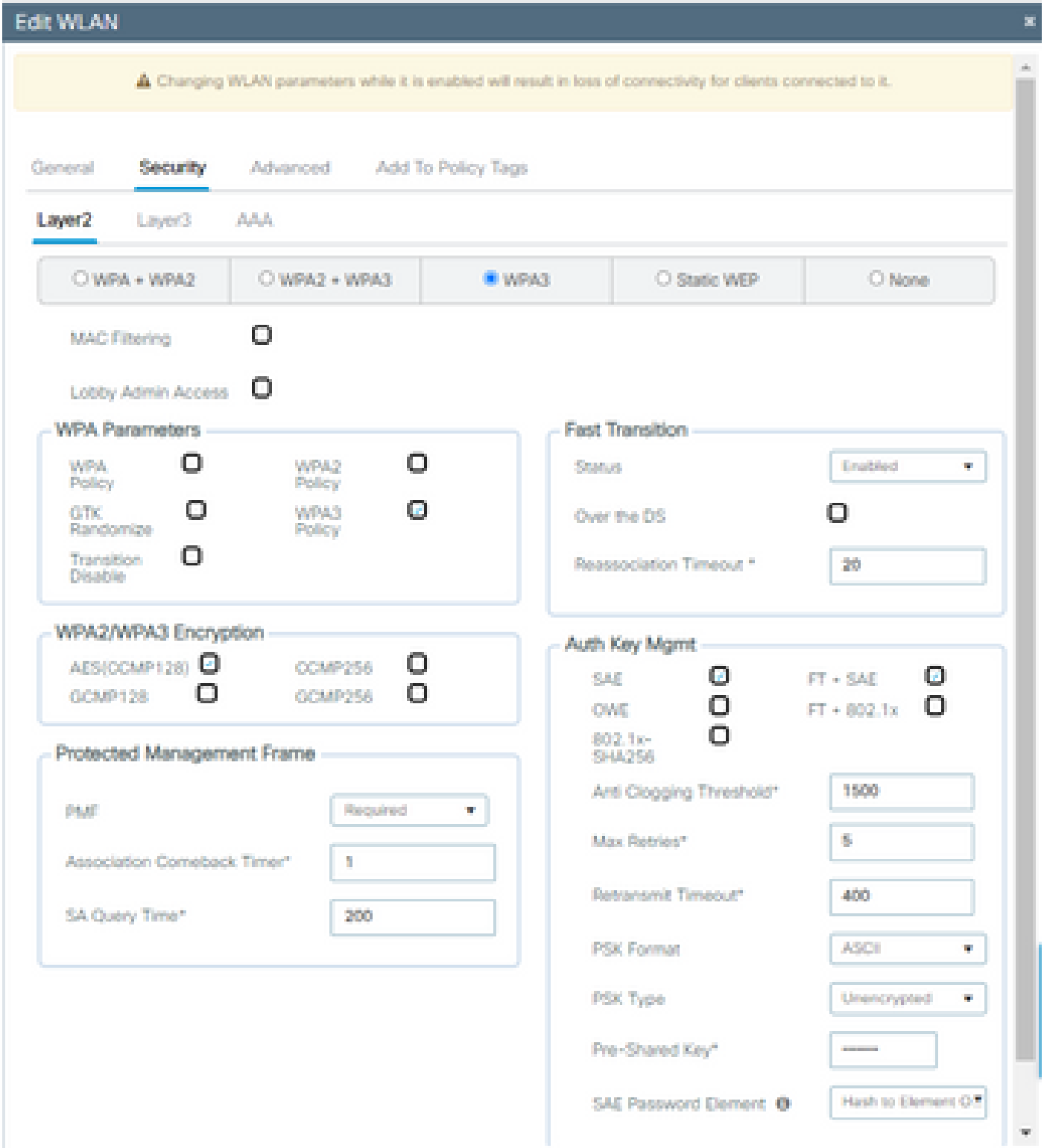


Client-Details in WLC:



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

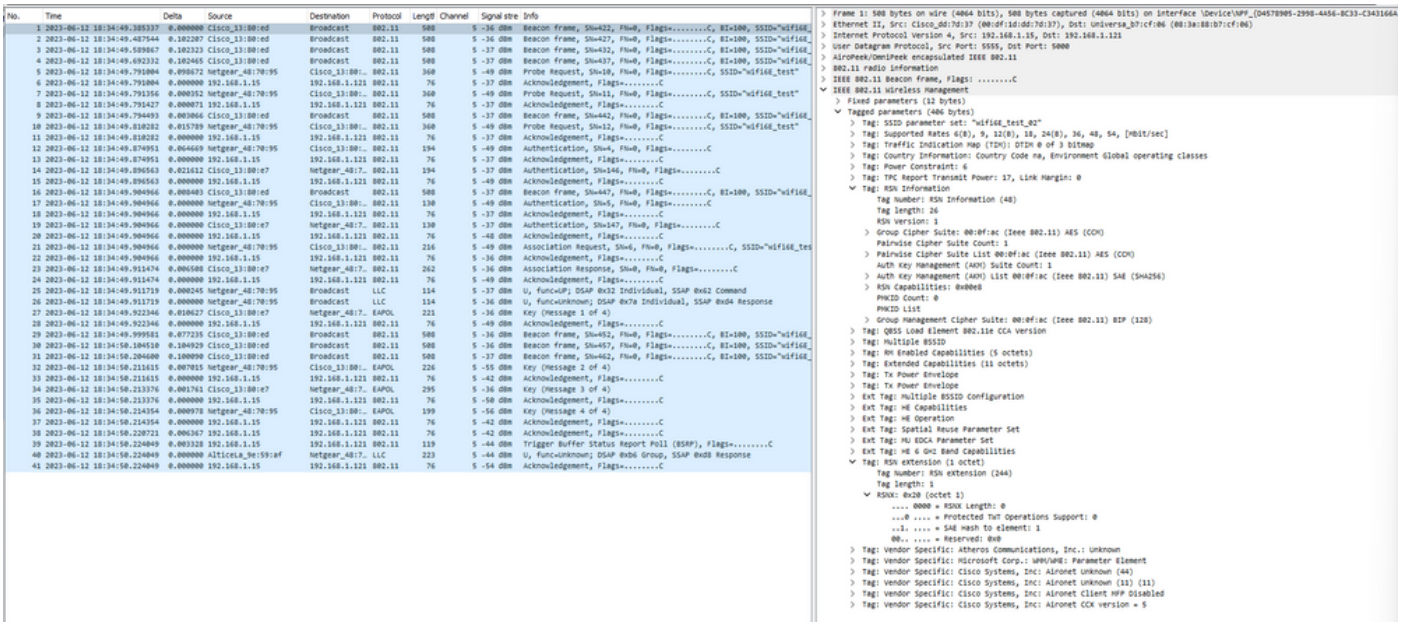
WLAN-Sicherheitskonfiguration:


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

Vorsicht: Bei der Verwaltung von Authentifizierungsschlüsseln kann der WLC FT+SAE auswählen, ohne dass SAE aktiviert ist. Es wurde jedoch beobachtet, dass die Clients keine Verbindung herstellen konnten. Aktivieren Sie immer beide Kontrollkästchen SAE und FT+SAE, wenn Sie SAE mit Fast Transition verwenden möchten.

Auf der WLC-GUI der WLAN-Sicherheitseinstellungen anzeigen:

Verifizierung von Beacons OTA:

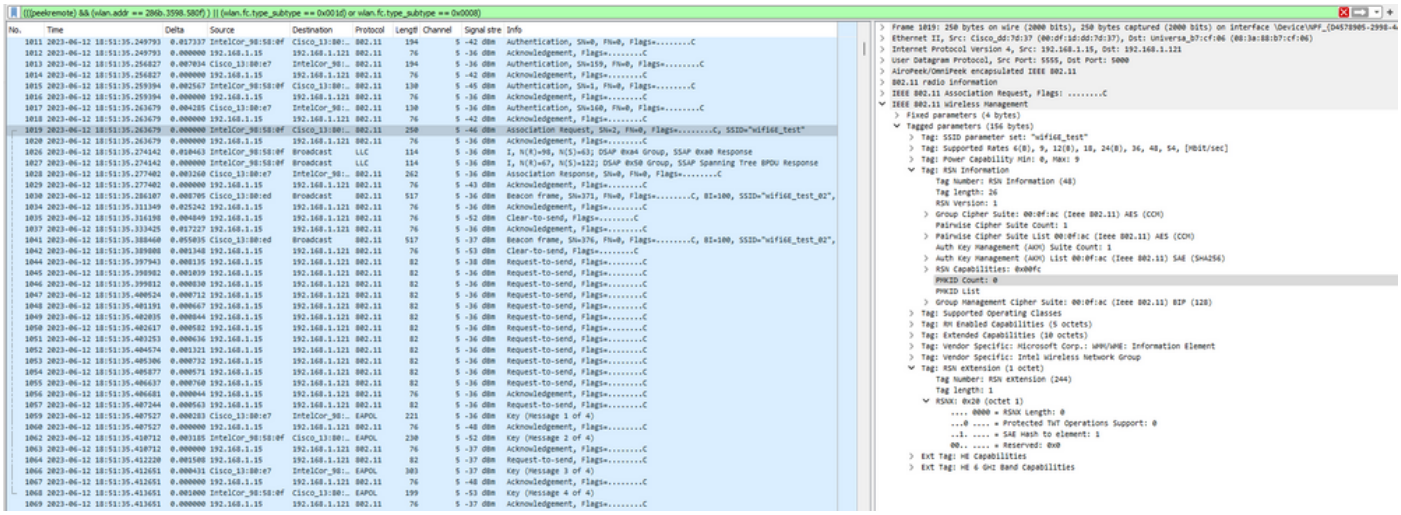


WPA3 SAE + FT Beacons

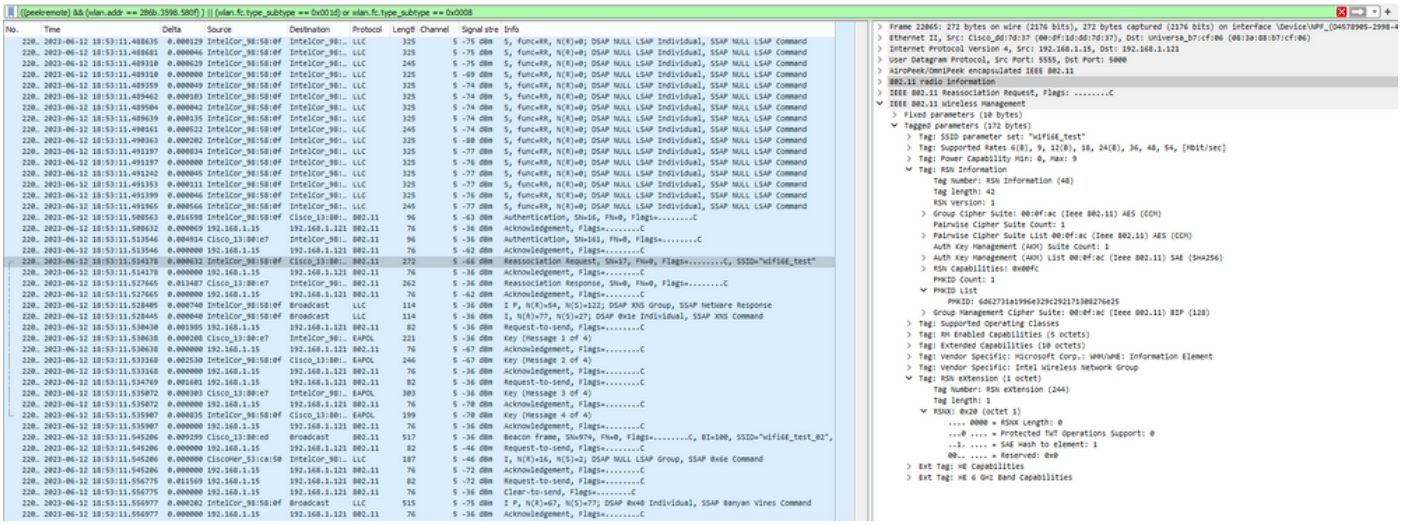
Hier können wir beobachten, wie Wi-Fi 6E-Clients sich verbinden:

Intel AX211

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:

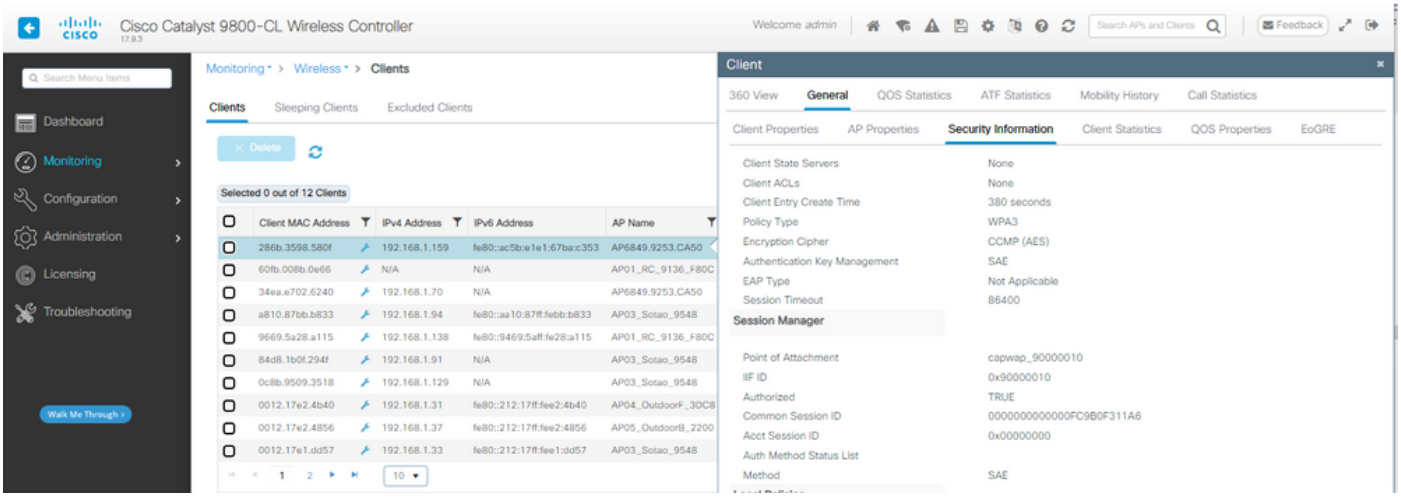


Roaming-Veranstaltung, bei der die PMKID angezeigt wird:



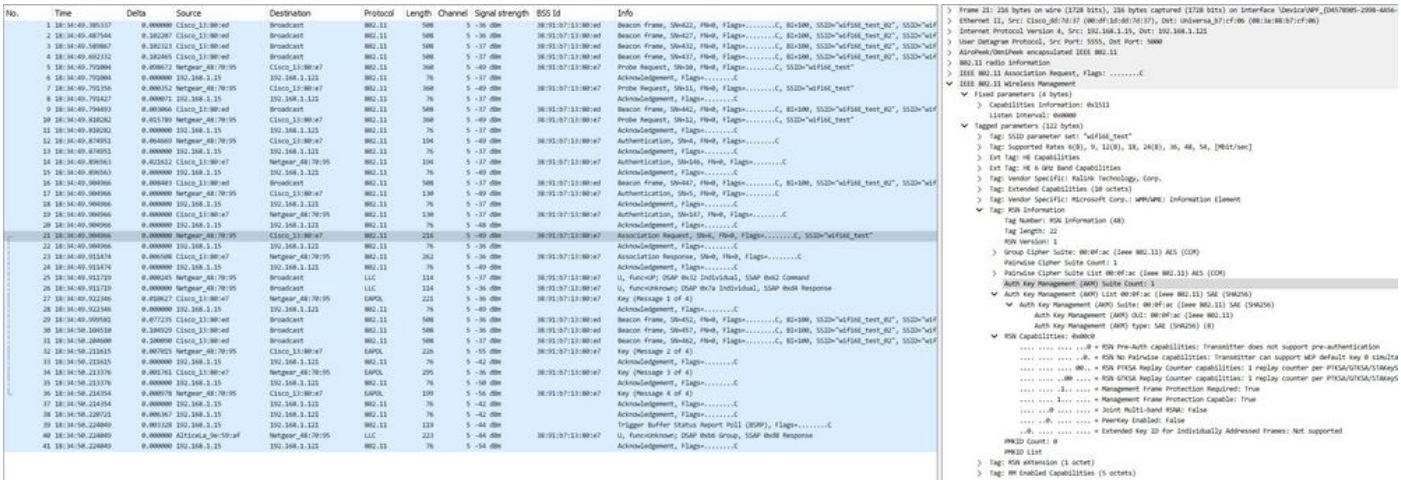
WPA3 SAE + FT-Neuzuordnungsanforderung

Client-Details in WLC:



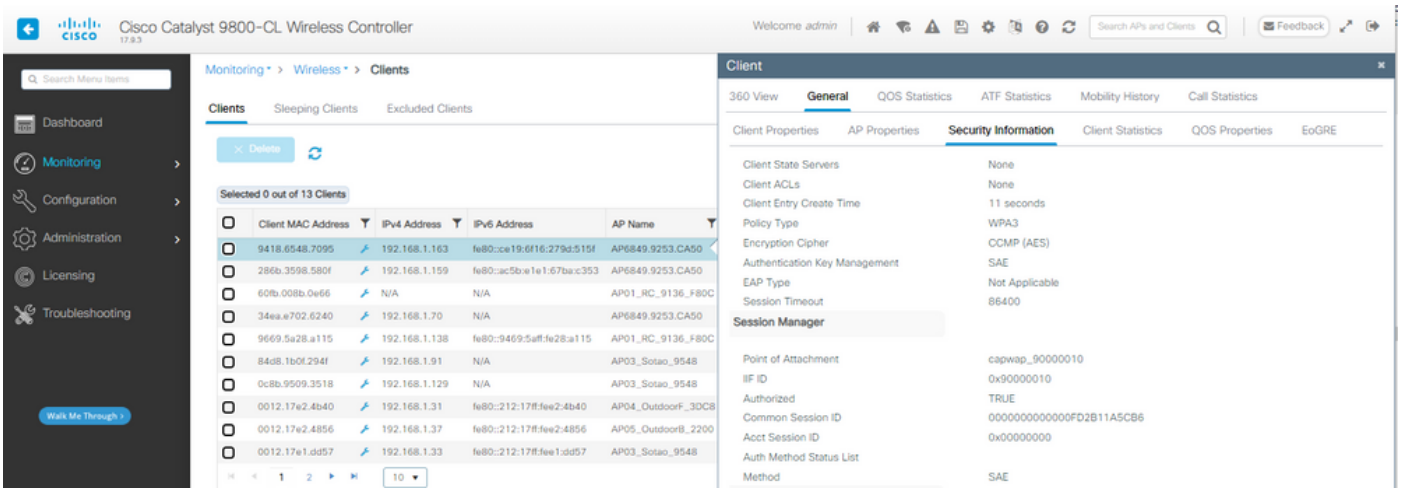
NetGear A8000

Verbindung OTA mit Fokus auf die RSN-Informationen vom Client. Erstverbindung:



SSS

Client-Details in WLC:



Pixel 6a

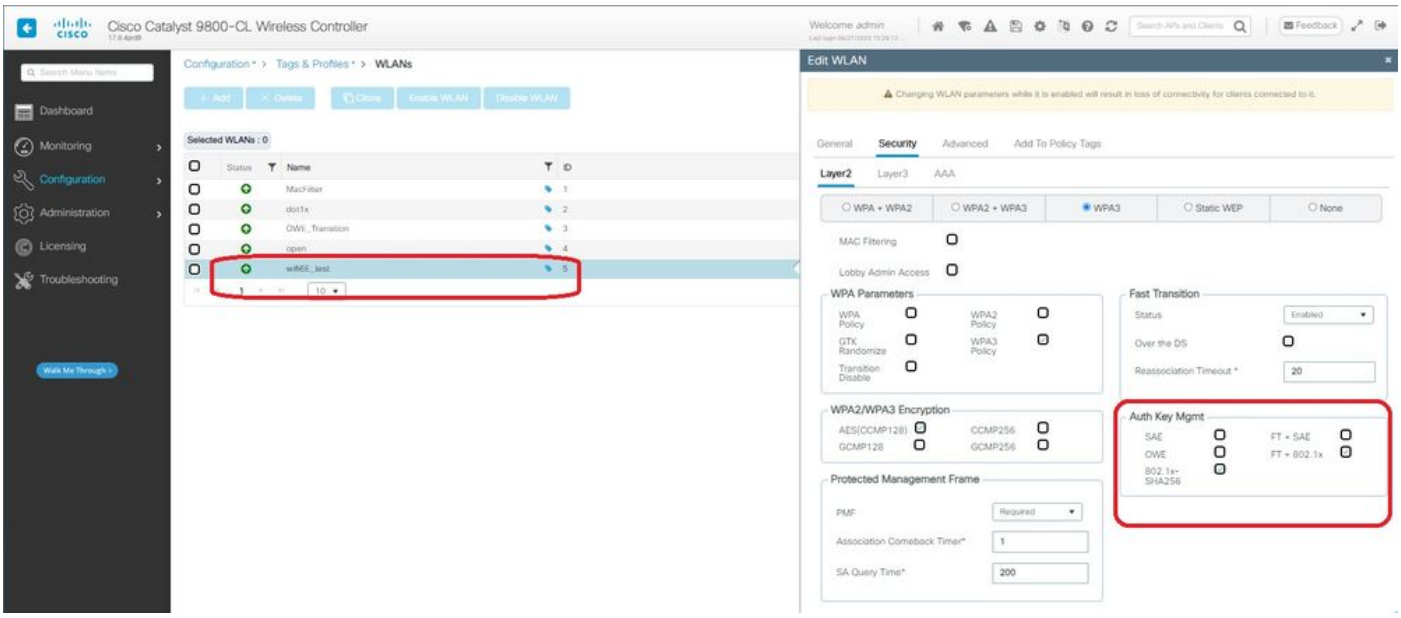
Das Gerät konnte kein Roaming durchführen, wenn FT aktiviert ist.

Samsung S23

Das Gerät konnte kein Roaming durchführen, wenn FT aktiviert ist.

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

WLAN-Sicherheitskonfiguration:



WPA3 Enterprise 802.1x-SHA256 + FTWLAN-Sicherheitskonfiguration

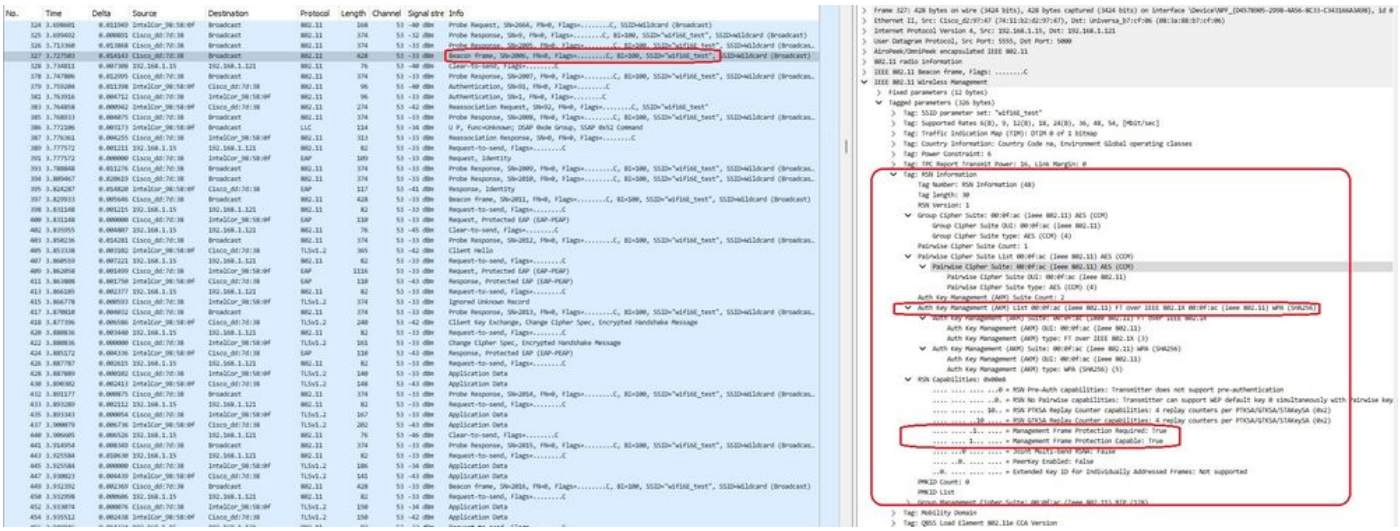
Auf der WLC-GUI der WLAN-Sicherheitseinstellungen anzeigen:

Hier sehen Sie die ISE-Live-Protokolle mit den Authentifizierungen der einzelnen Geräte:

	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-Live-Protokolle

Beacons und OTAs sehen wie folgt aus:

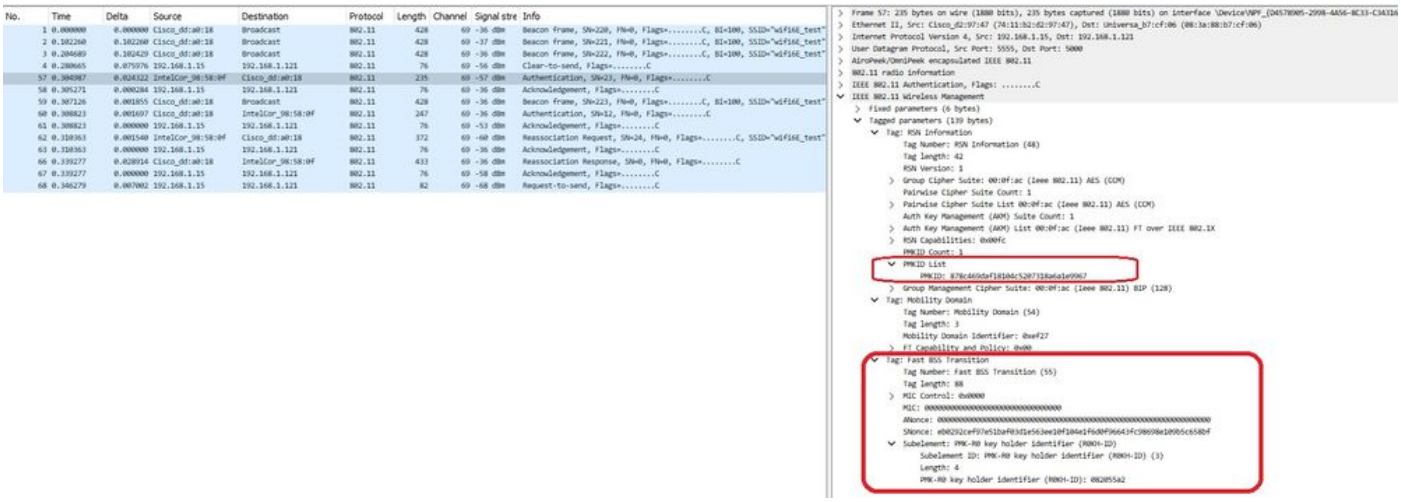


WPA3 Enterprise 802.1x + FT-Beacon

Hier können wir beobachten, wie Wi-Fi 6E-Clients sich verbinden:

Intel AX211

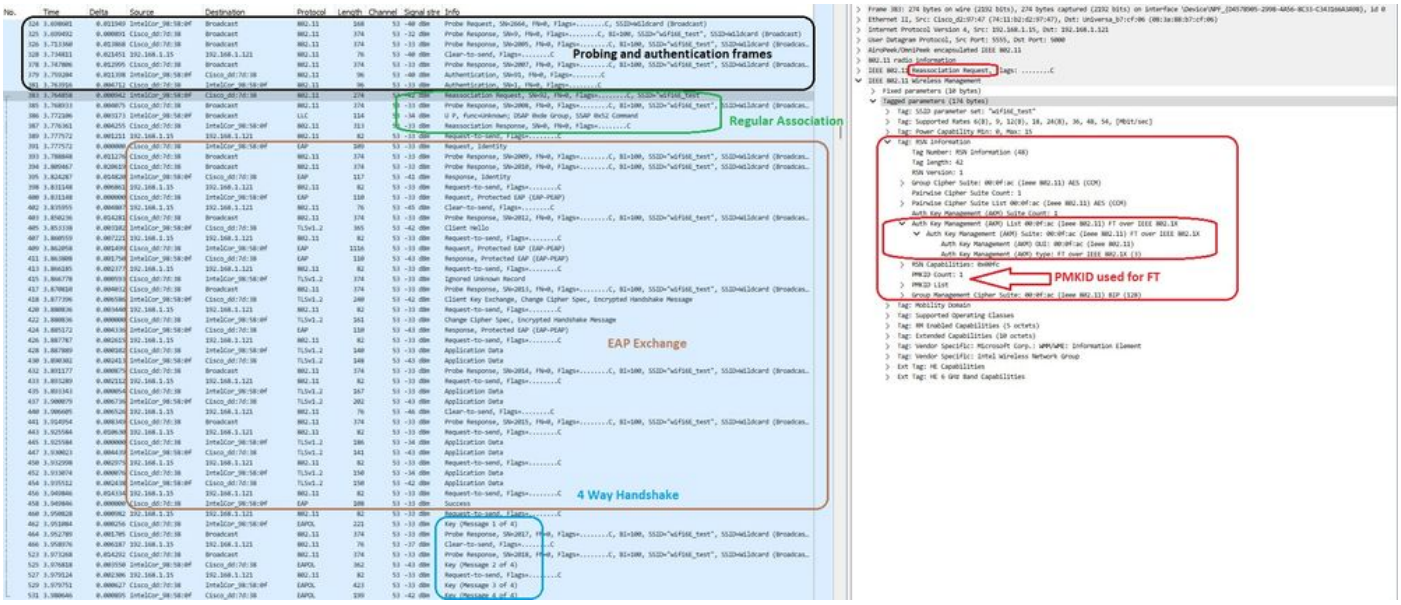
OTA-Verbindung mit Schwerpunkt auf RSN-Informationen des Clients zu einem Roaming-Ereignis:



WPA3 Enterprise 802.1x + FT Roaming-Ereignis

Ein interessantes Verhalten tritt auf, wenn Sie den Client manuell aus dem WLAN löschen (z.B. aus der WLC GUI). Der Client empfängt einen Trennungs-Frame, versucht jedoch, erneut eine Verbindung mit demselben Access Point herzustellen, und verwendet einen Trennungs-Frame, gefolgt von einem vollständigen EAP-Austausch, da die Client-Details vom Access Point/WLC gelöscht wurden.

Das ist im Grunde der gleiche Rahmenaustausch wie in einem neuen Assoziationsprozess. Hier sehen Sie den Frame-Austausch:



WPA3 Enterprise 802.1x + FT AX211-Verbindungsablauf

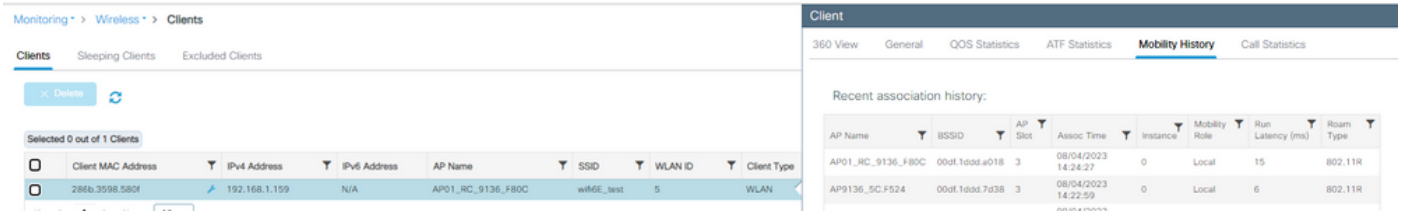
Client-Details in WLC:

Details zum WPA3 Enterprise 802.1x + FT-Client

Dieser Client wurde auch mit FT über den DS getestet und konnte mithilfe von 802.11r Roaming durchführen:

AX211-Roaming mit FT über DS

Außerdem werden die Roaming-Ereignisse der FT angezeigt:



WPA3 Enterprise mit FT

Client-RA-Trace von wlc:

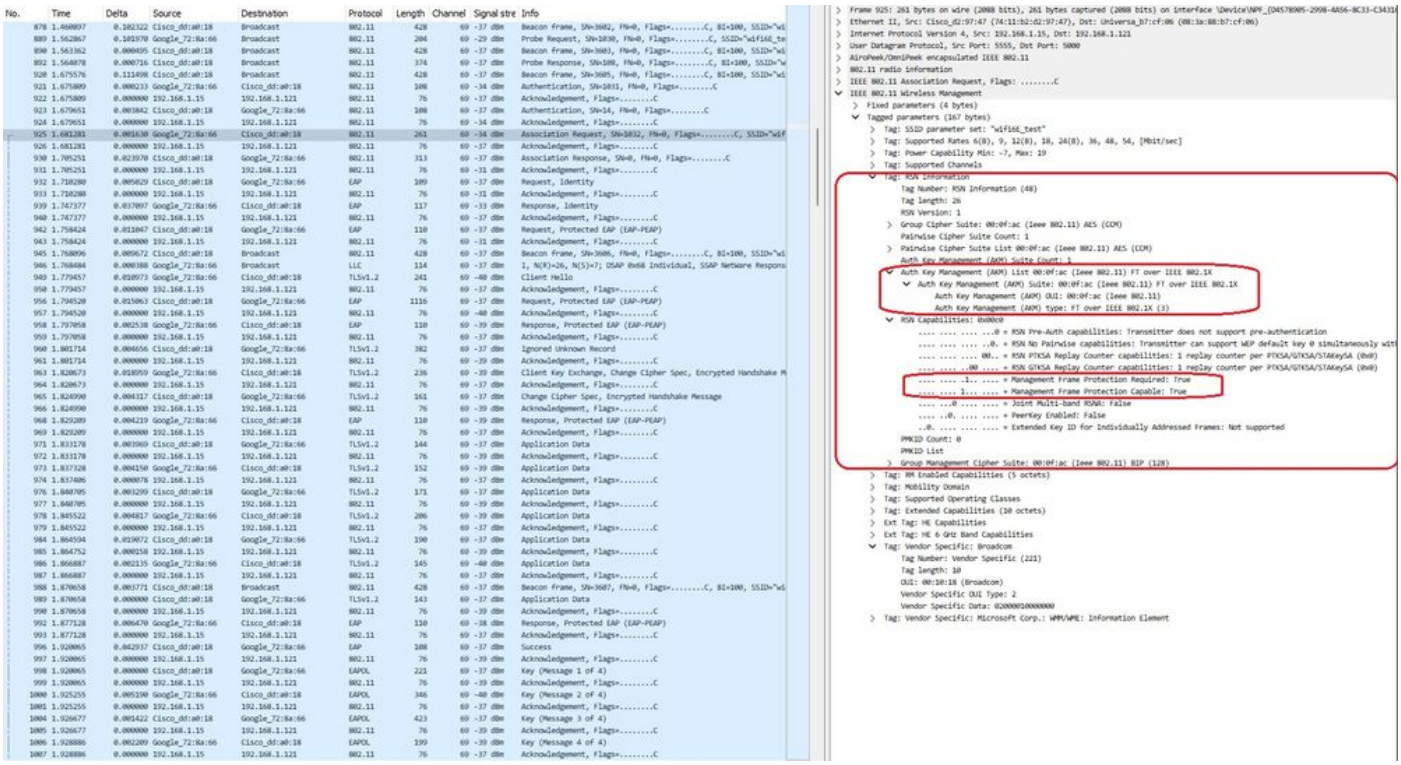
```
Logging display requested on 2023/08/04 14:27:55 (GMT) for Hostname: [eWLC-9800-01], Model: [C9800-CL-K9], Version: [17.09.03], SN: [9RY35HS10G9], MD_SN: [9RY35HS10G9]
2023/08/04 14:22:59.315300237 {wncd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 204b.3598.580f Re-Association received. BSSID 00df.1ddd.7d30, WLAN wifi6E_test, Slot 3 AP 00df.1ddd.7d30, AP9136_5C.F524, old BSSID 00df.1ddd.a010
2023/08/04 14:22:59.316044210 {wncd_x_R0-0}{1}: [dot11] [15210]: (note): MAC: 204b.3598.580f 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.3598.580f 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.3598.580f 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.3598.580f 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.3598.580f 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.3598.580f 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.3598.580f 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.3598.580f ADD MOBILE sent. Client state flags: 0x76 BSSID: MAC: 00df.1ddd.7d38 capwap IFID: 0x9000000d, Add mobiles sent: 1
2023/08/04 14:22:59.321254052 {wncd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 204b.3598.580f 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.3598.580f 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.3598.580f 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.3598.580f 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 14:24:27.919597444 {wncd_x_R0-0}{1}: [dot11] [15210]: (note): MAC: 204b.3598.580f 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.3598.580f 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.3598.580f 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.3598.580f 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.3598.580f 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.3598.580f 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.3598.580f 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.3598.580f 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.3598.580f Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS -> S_CO_DPATH_PLUMB_IN_PROGRESS
2023/08/04 14:24:27.933010101 {wncd_x_R0-0}{1}: [client-orch-state] [15210]: (note): MAC: 204b.3598.580f 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.3598.580f Client state transition: S_CO_IP_LEARN_IN_PROGRESS -> S_CO_RUN
```

NetGear A8000

WPA3-Enterprise wird auf diesem Client nicht unterstützt.

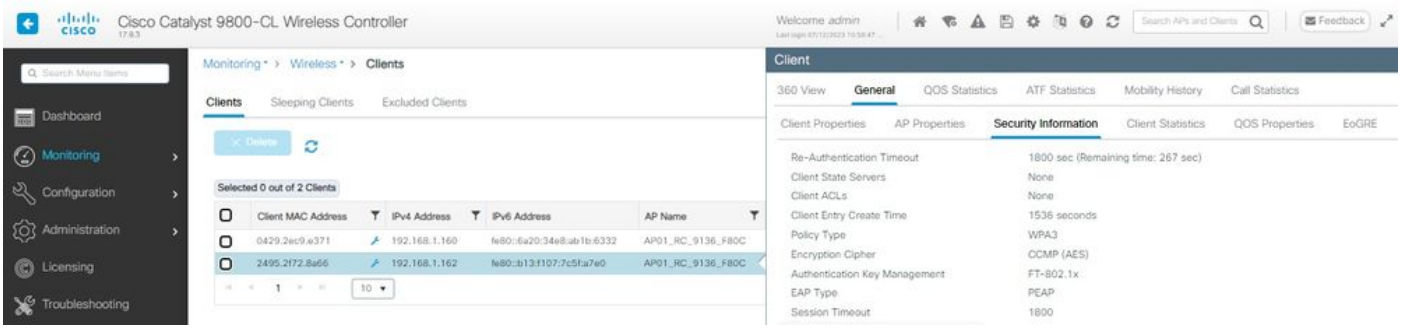
Pixel 6a

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:



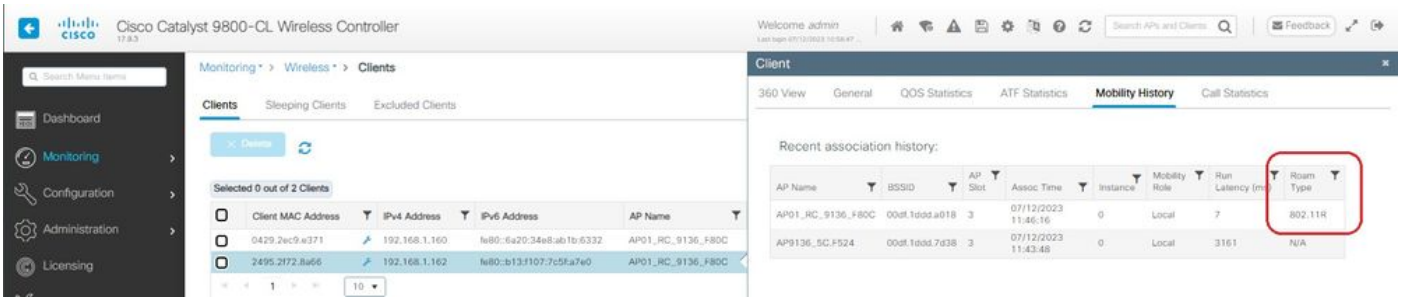
WPA3 Enterprise 802.1x + FT Pixel6a-Zuordnung

Client-Details in WLC:



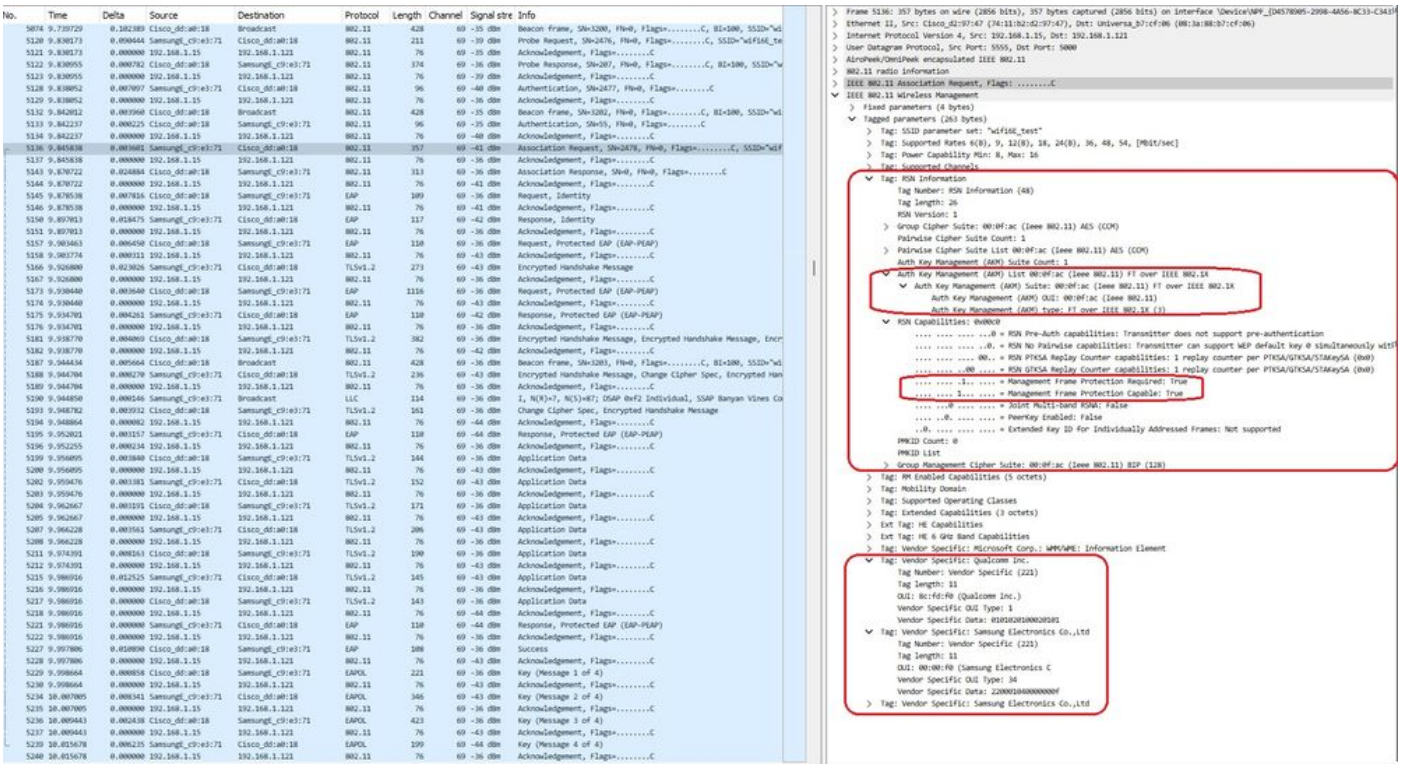
Details zum WPA3 Enterprise 802.1x + FT Pixel6a-Client

Konzentrieren Sie sich auf den Roamingtyp Over the Air (Über das Flugzeug), wo Sie den Roamingtyp 802.11R sehen können:



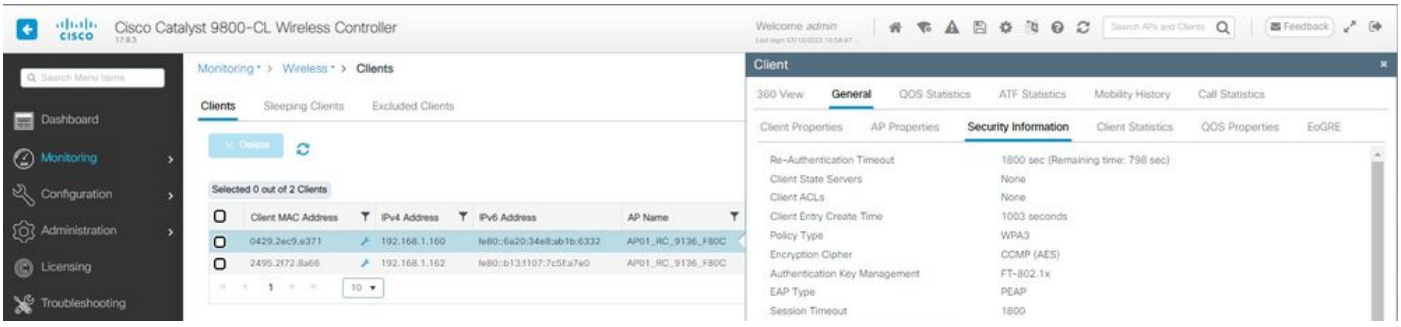
Samsung S23

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:



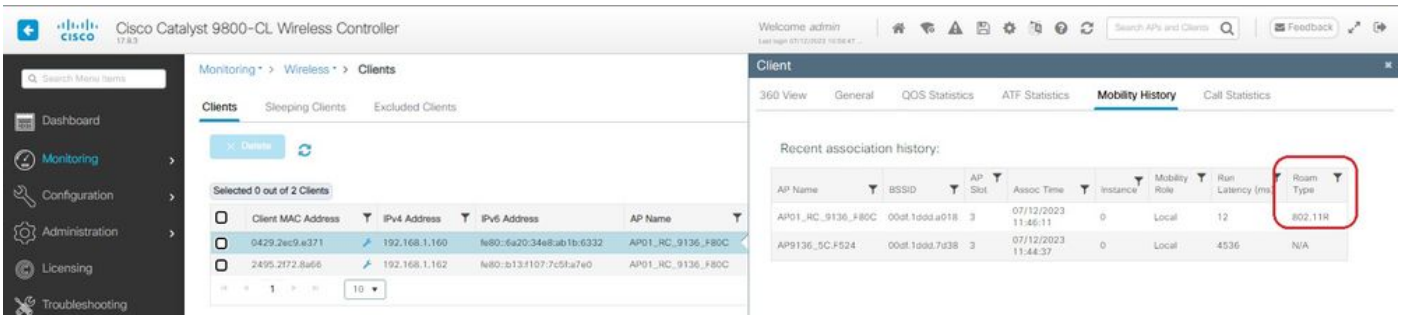
S23 FToTA Roaming-Veranstaltung

Client-Details in WLC:



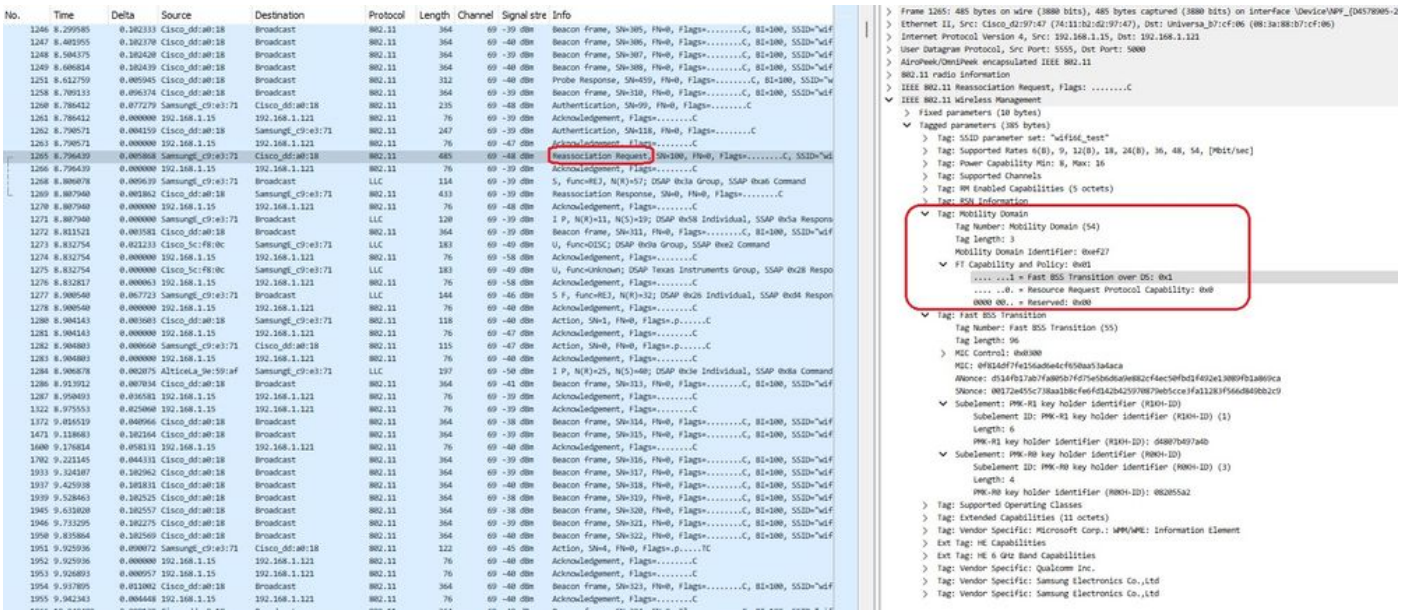
S23-Clienteigenschaften

Konzentrieren Sie sich auf den Roamingtyp Over the Air (Über das Flugzeug), wo Sie den Roamingtyp 802.11R sehen können:



S23 Roaming-Typ 802.11R

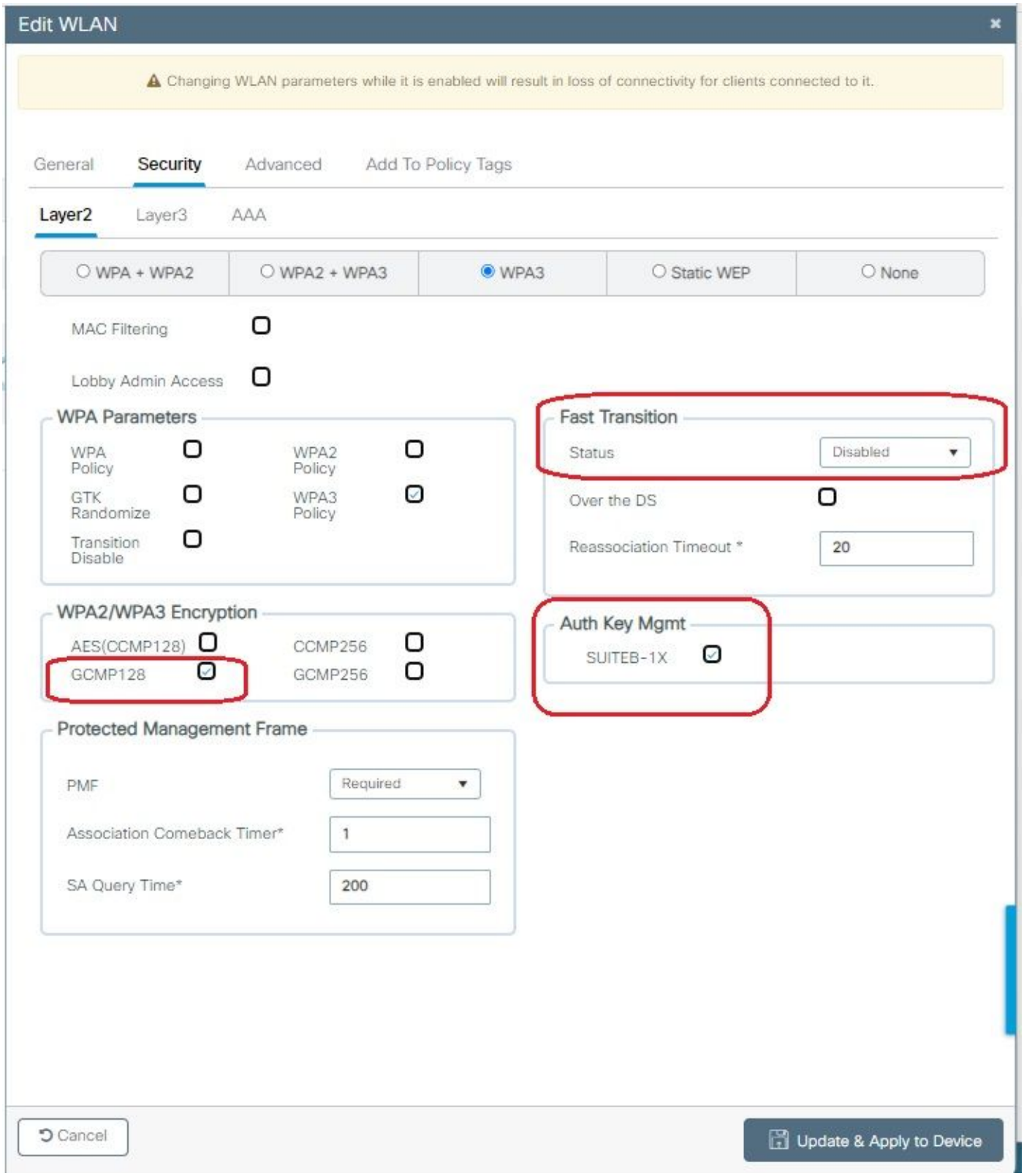
Dieser Client wurde auch mit FT über den DS getestet und konnte mithilfe von 802.11r Roaming durchführen:



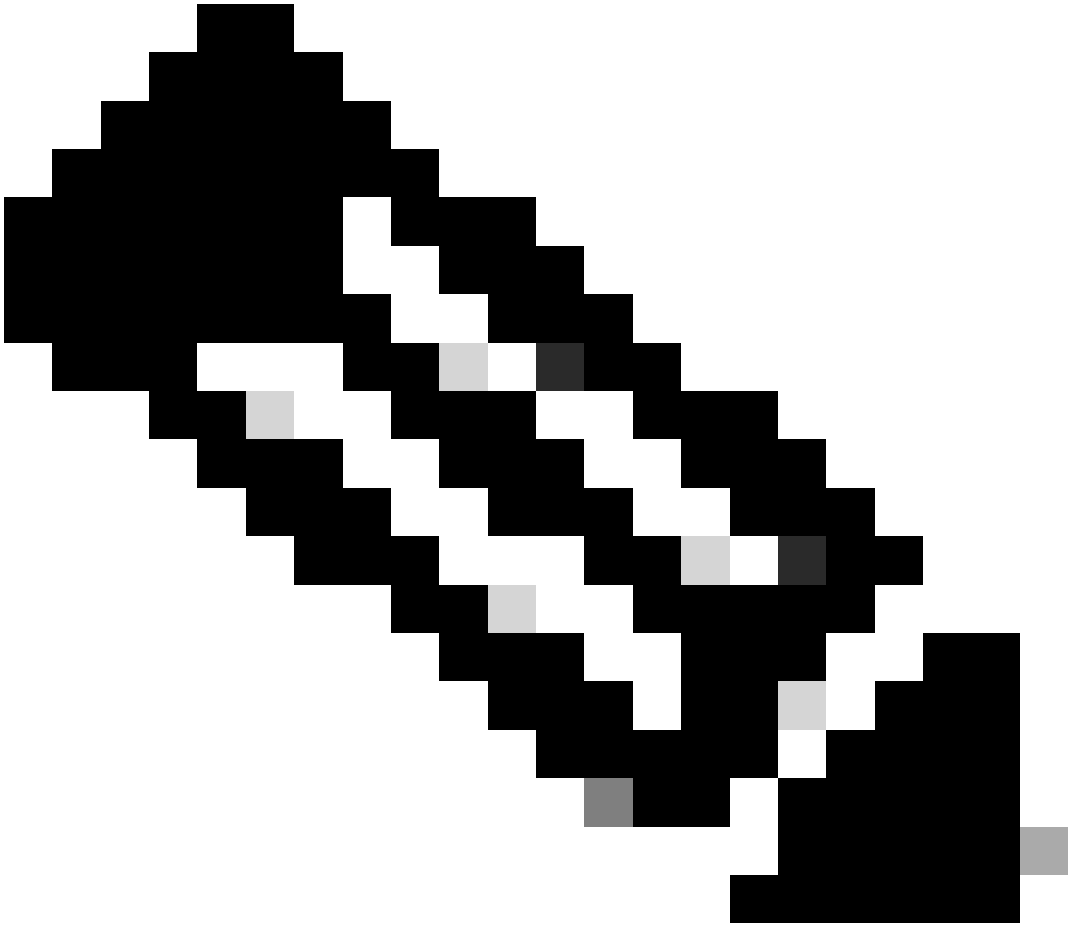
S23 Roaming-FToDS-Pakete

WPA3-Enterprise + GCMP128-Chiffre + SUITEB-1X

WLAN-Sicherheitskonfiguration:



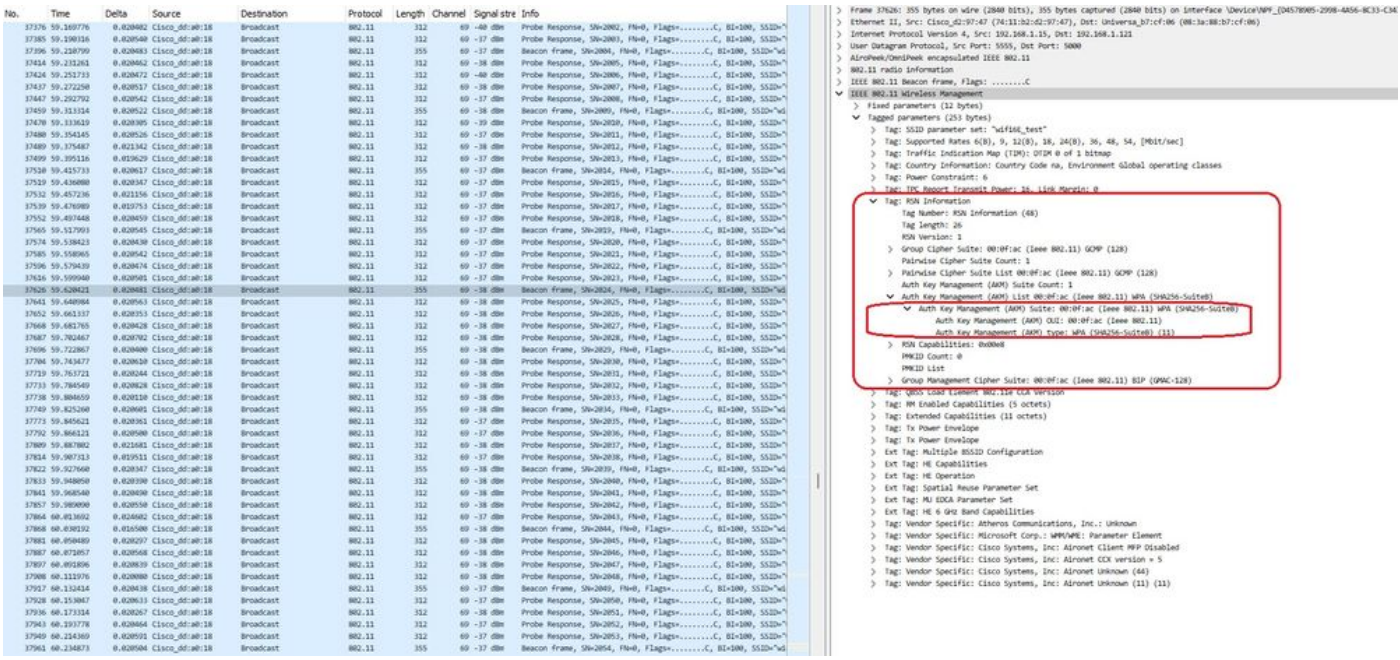
WPA3 Enterprise Suite B-1X - Sicherheitskonfiguration



Hinweis: FT wird in SUITEB-1X nicht unterstützt

Auf der WLC-GUI der WLAN-Sicherheitseinstellungen anzeigen:

Verifizierung von Beacons OTA:

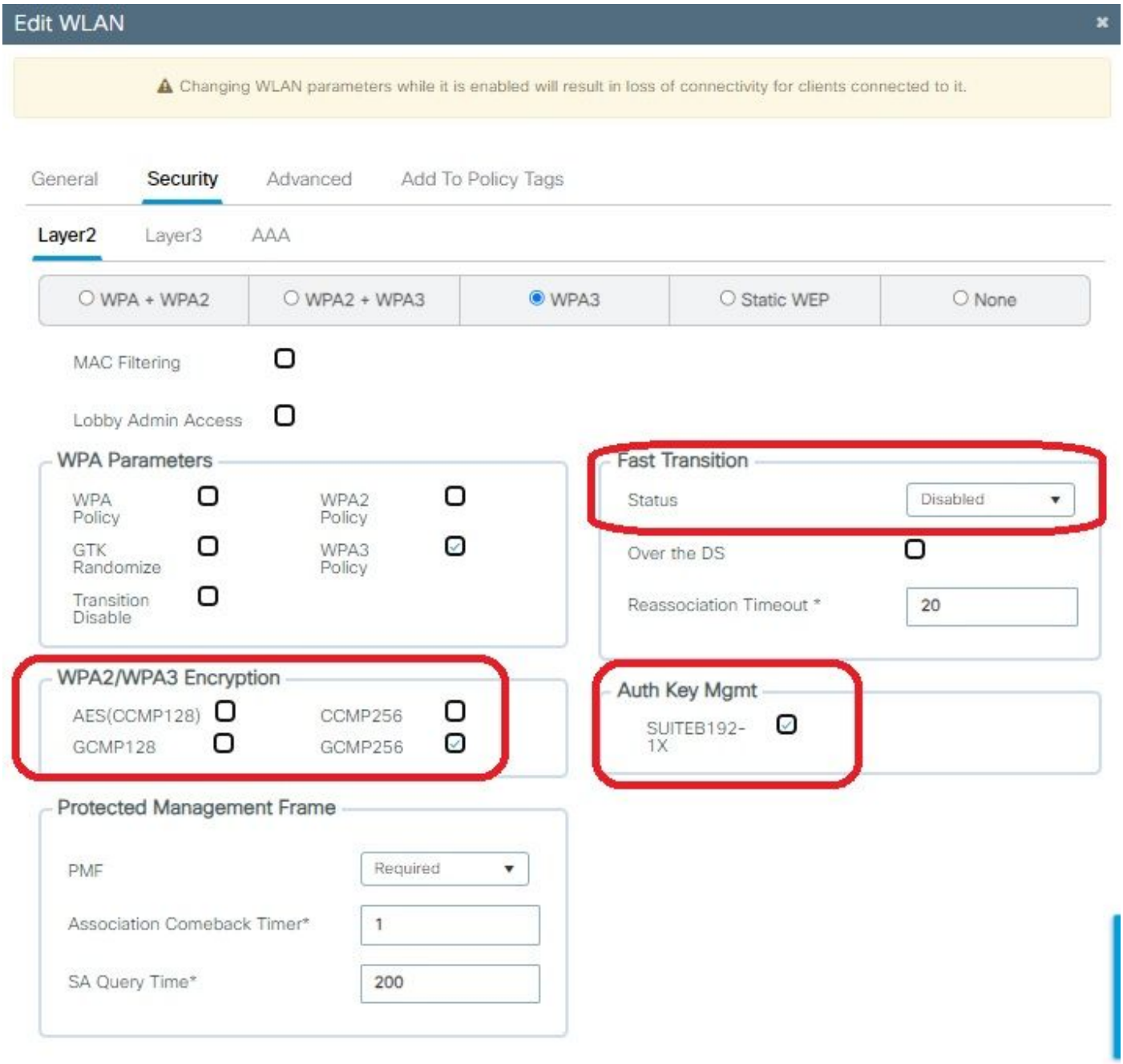


WPA3 Enterprise Suite B-1X Beacon

Keiner der getesteten Clients konnte sich mit SuiteB-1X mit dem WLAN verbinden. Dies bestätigt, dass keiner dieser Clients diese Sicherheitsmethode unterstützt.

WPA3-Enterprise + GCMP256-Chiffre + SUITEB192-1X

WLAN-Sicherheitskonfiguration:



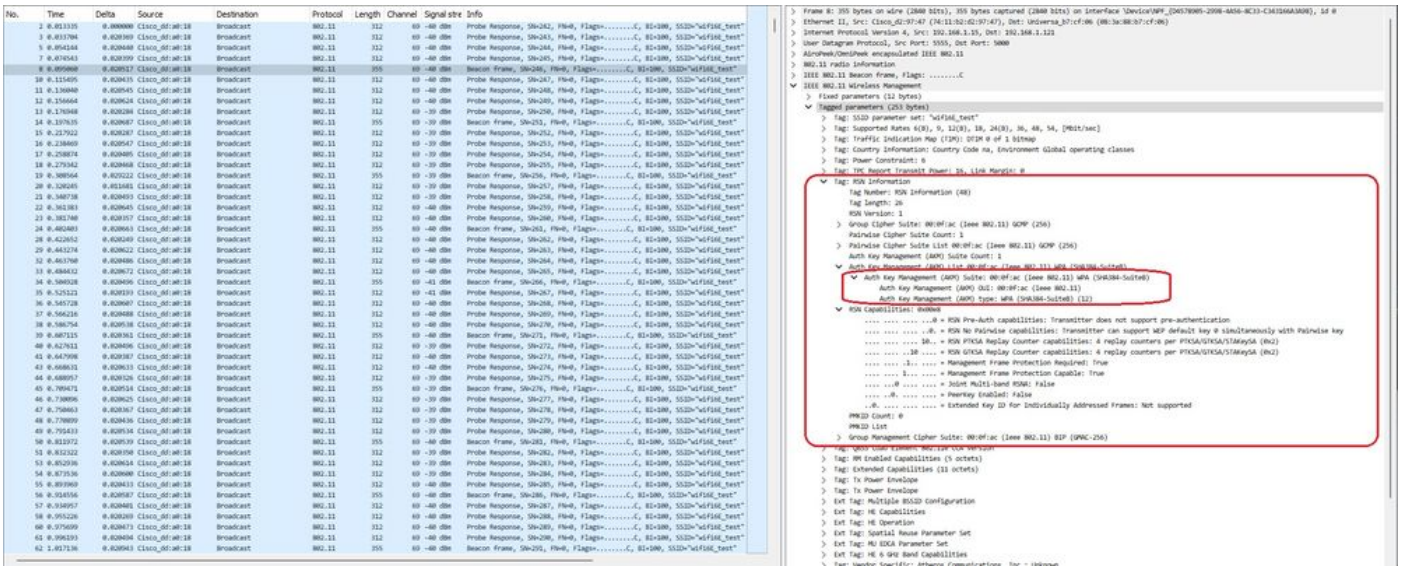
WPA3 Enterprise SUITEB192-1x Sicherheitseinstellungen

Hinweis: FT wird von GCMP256+SUITEB192-1X nicht unterstützt.

Liste der WLANs auf der WLC-GUI:

WLAN für Tests

Verifizierung von Beacons OTA:

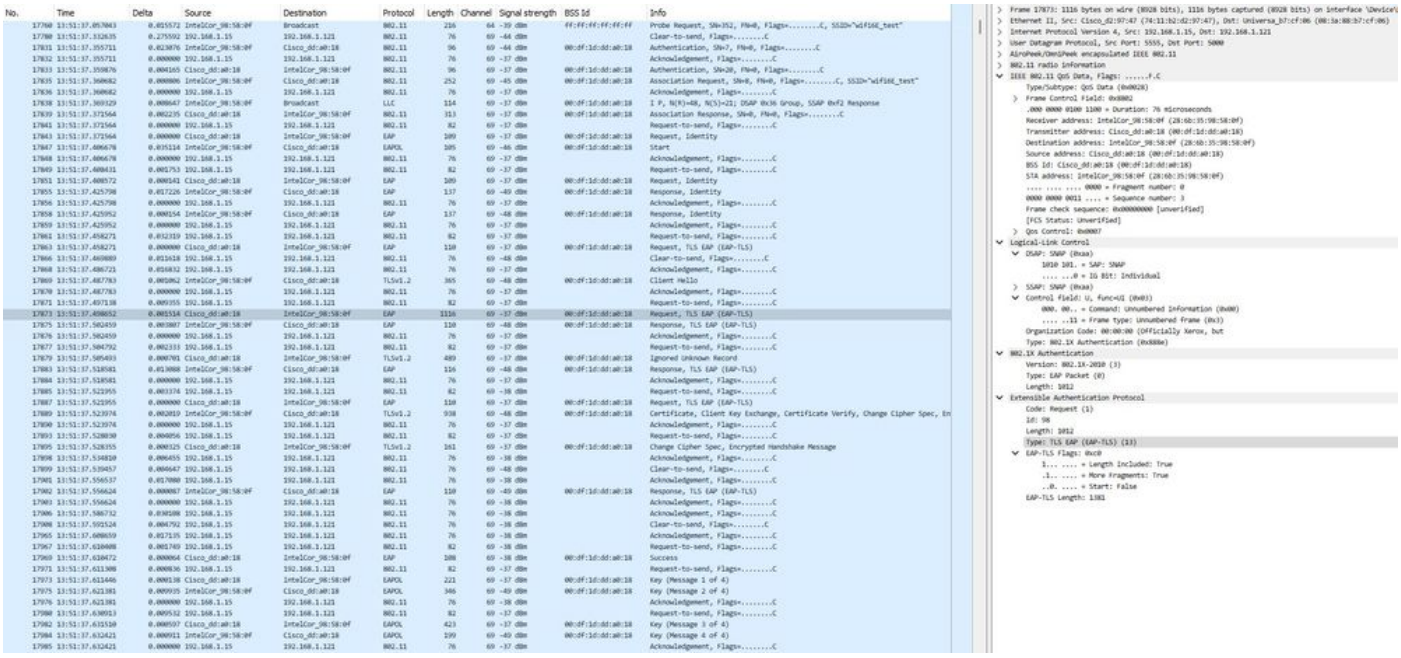


WPA3 Enterprise SUITEB192-1x Beacons

Hier können wir beobachten, wie Wi-Fi 6E-Clients sich verbinden:

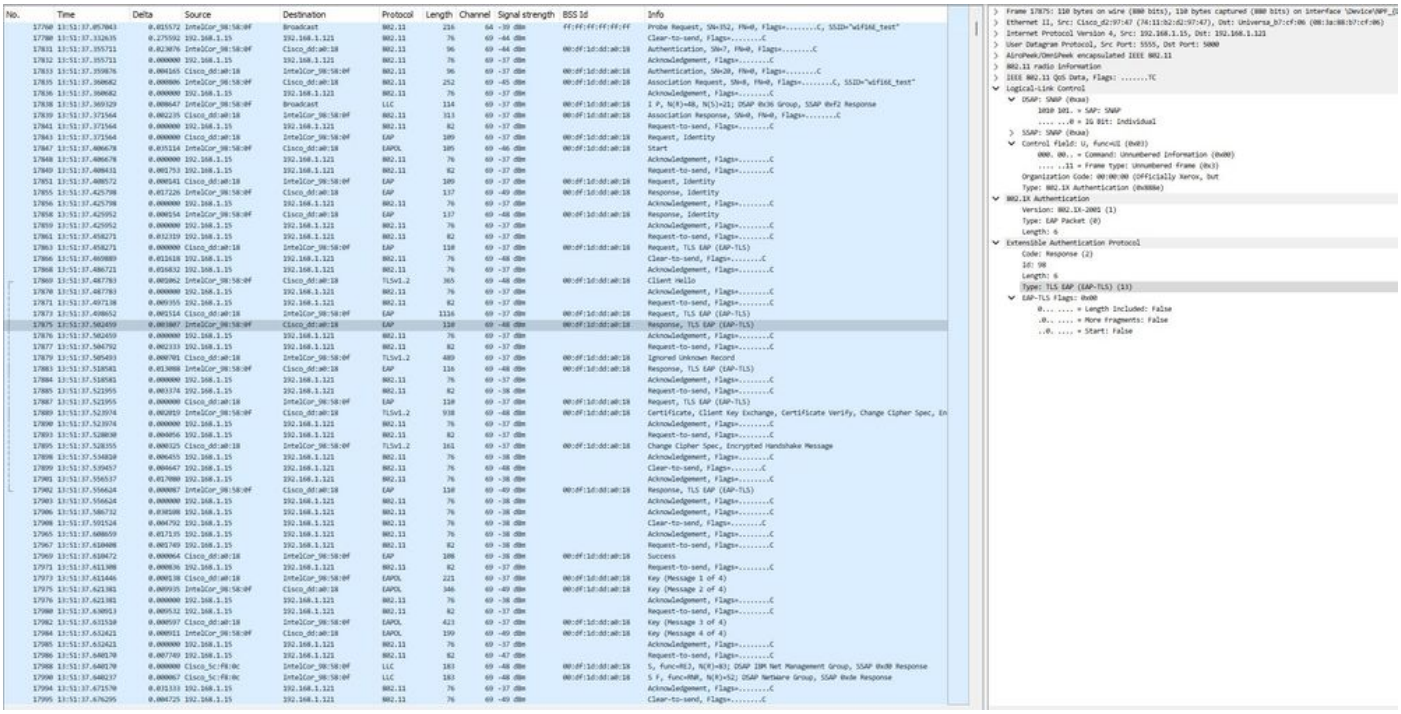
Intel AX211

Verbindung OTA mit Fokus auf RSN-Informationen vom Client:



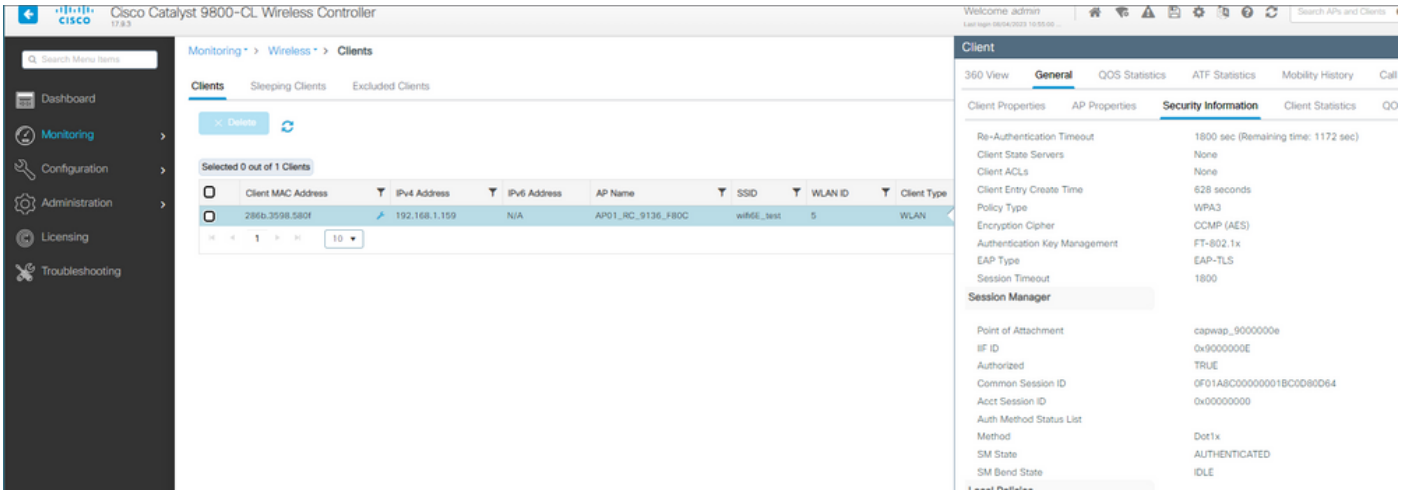
WPA3 Enterprise mit EAP-TLS-Zuordnung mit Intel AX211-Client und RSN-Info

Und der EAP-TLS-Austausch:



WPA3 Enterprise mit EAP-TLS-Zuordnung mit Intel AX211-Client und EAP-TLS-Fokus

Client-Details in WLC:



WPA3 Enterprise mit EAP-TLS-Clientdetails

NetGear A8000

WPA3-Enterprise wird auf diesem Client nicht unterstützt.

Pixel 6a

Zum Zeitpunkt der Erstellung dieses Dokuments war dieser Client nicht in der Lage, mithilfe von EAP-TLS eine Verbindung zu WPA3 Enterprise herzustellen.

Dies war ein kundenseitiges Problem, das derzeit bearbeitet wird, und sobald es gelöst ist, wird dieses Dokument aktualisiert werden.

Samsung S23

Zum Zeitpunkt der Erstellung dieses Dokuments war dieser Client nicht in der Lage, mithilfe von EAP-TLS eine Verbindung zu WPA3 Enterprise herzustellen.

Dies war ein kundenseitiges Problem, das derzeit bearbeitet wird, und sobald es gelöst ist, wird dieses Dokument aktualisiert werden.

Sicherheitsschlussfolgerungen

Nach allen vorherigen Tests sind folgende Schlussfolgerungen zu ziehen:

Protokolle	Verschlüsselung	AKM	AKM-Verschlüsselung	EAP-Methode	FT-OverTA	FT-OVER-DS	Intel AX211
SCHULD	AES-CCMP128	SCHULD	N.	N.	NA	NA	Unterst
SAE	AES-CCMP128	SAE (nur H2E)	SHA 256	N.	Unterstützt	Unterstützt	Unterst nur H2 und FT oTA
Unternehmen	AES-CCMP128	802.1x-SHA256	SHA 256	PEAP/FAST/TLS	Unterstützt	Unterstützt	Unterst SHA25 und FT oTA/oD Nicht unterst EAP-F
Unternehmen	GMP 128	Suite B-1x	SHA256-Suite B	PEAP/FAST/TLS	Nicht unterstützt	Nicht unterstützt	Nicht unterst
Unternehmen	GMP 256	Suite B-192	SHA384-Suite B	TLS	Nicht unterstützt	Nicht unterstützt	k. A.

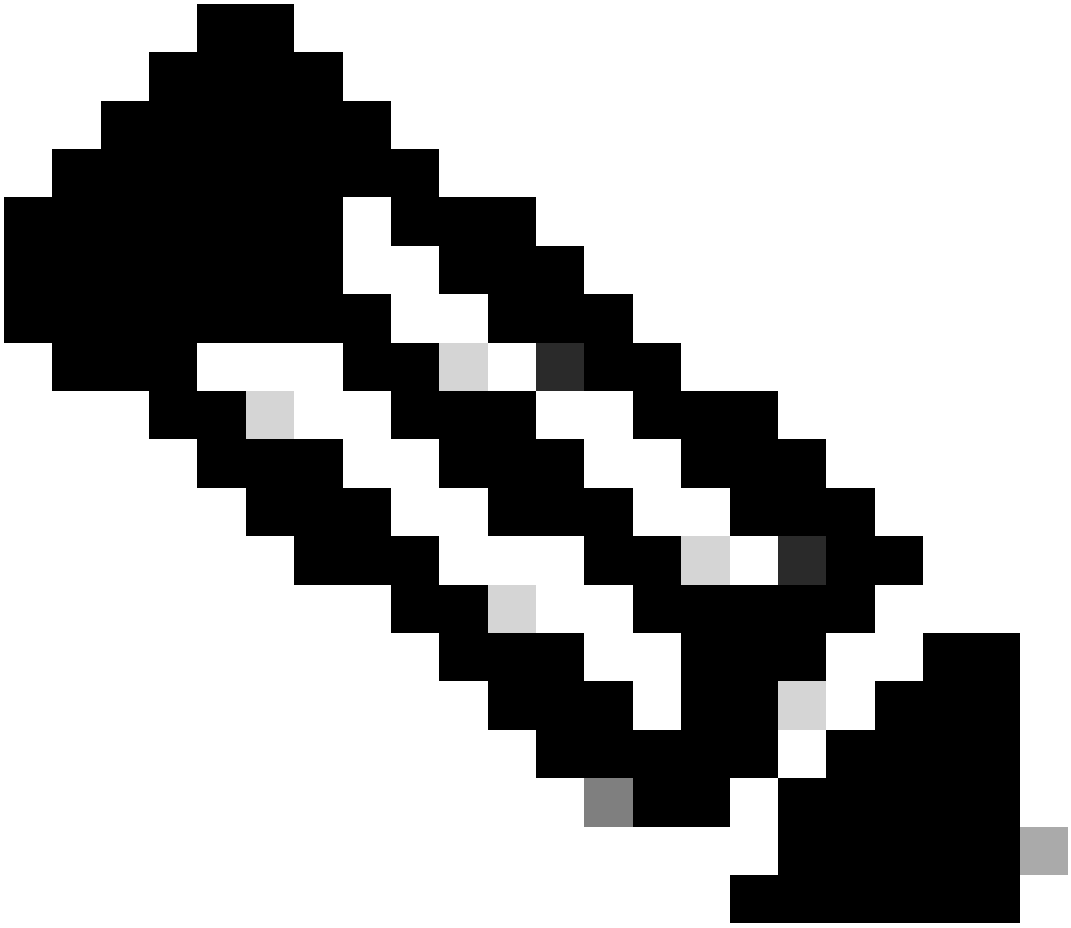
Fehlerbehebung

Die in diesem Dokument verwendete Fehlerbehebung basiert auf dem Online-Dokument:

Fehlerbehebung bei COS-APs

Die allgemeine Richtlinie für die Fehlerbehebung besteht darin, die RA-Ablaufverfolgung im Debugmodus vom WLC mithilfe der Client-MAC-Adresse zu erfassen. Dabei wird sichergestellt, dass der Client die Verbindung über die Geräte-MAC herstellt und keine randomisierte MAC-Adresse.

Für die Fehlerbehebung per Funk wird empfohlen, AP im Sniffer-Modus zu verwenden, um den Datenverkehr auf dem Kanal des Client-AP zu erfassen.



Hinweis: Lesen Sie Wichtige Informationen zu Debug-Befehlen, bevor Sie Debug-Befehle verwenden.

Zugehörige Informationen

Was ist Wi-Fi 6E?

Was ist Wi-Fi 6 im Vergleich zu Wi-Fi 6E?

Wi-Fi 6E - Informationen auf einen Blick

Wi-Fi 6E: Das nächste große Kapitel im Wi-Fi-Whitepaper

Cisco Live - Architektur eines Wireless-Netzwerks der nächsten Generation mit Catalyst Wi-Fi 6E Access Points

Software-Konfigurationsleitfaden für Cisco Catalyst Wireless Controller der Serie 9800 17.9.x

WPA3-Bereitstellungsleitfaden

Informationen zu dieser Übersetzung

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