Configuración y verificación de la seguridad de capa 2 de WLAN Wi-Fi 6E

Contenido

Introducción

Este documento describe cómo configurar la seguridad Wi-Fi 6E WLAN Layer 2 y qué esperar en diferentes clientes.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Controladores de LAN inalámbrica de Cisco (WLC) 9800
- Puntos de acceso (AP) de Cisco compatibles con Wi-Fi 6E.
- Estándar IEEE 802.11ax.
- Herramientas: Wireshark v4.0.6

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC 9800-CL con IOS® XE 17.9.3
- AP C9136, CW9162, CW9164 y CW9166.
- Clientes Wi-Fi 6E:
    - Lenovo X1 Carbon Gen11 con adaptador Intel AX211 Wi-Fi 6 y 6E con controlador versión 22.200.2(1).
    - Adaptador Wi-Fi 6 y 6E Netgear A8000 con controlador v1(0.0.108);
    - Teléfono móvil Pixel 6a con Android 13;
    - Teléfono móvil Samsung S23 con Android 13.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Lo más importante es que Wi-Fi 6E no es un estándar completamente nuevo, sino una extensión. En su base, Wi-Fi 6E es una extensión del estándar inalámbrico Wi-Fi 6 (802.11ax) en la banda de radiofrecuencia de 6 GHz.

Wi-Fi 6E se basa en Wi-Fi 6, que es la última generación del estándar Wi-Fi, pero solo los dispositivos y aplicaciones Wi-Fi 6E pueden funcionar en la banda de 6 GHz.

Seguridad Wi-Fi 6E

Wi-Fi 6E aumenta la seguridad con Wi-Fi Protected Access 3 (WPA3) y Opportunistic Wireless Encryption (OWE), y no hay compatibilidad con versiones anteriores con la seguridad Open (abierta) y WPA2.

WPA3 y Enhanced Open Security son ahora obligatorios para la certificación Wi-Fi 6E y Wi-Fi 6E también requiere Protected Management Frame (PMF) tanto en el punto de acceso como en los clientes.

Al configurar un SSID de 6 GHz, deben cumplirse determinados requisitos de seguridad:

- Seguridad WPA3 de nivel 2 con OWE, SAE u 802.1x-SHA256
- Marco de administración protegido habilitado;

- No se permite ningún otro método de seguridad L2, es decir, no es posible ningún modo mixto.

WPA3

WPA3 está diseñado para mejorar la seguridad Wi-Fi al permitir una mejor autenticación a través de WPA2, proporcionar una mayor resistencia criptográfica y aumentar la resistencia de las redes críticas.

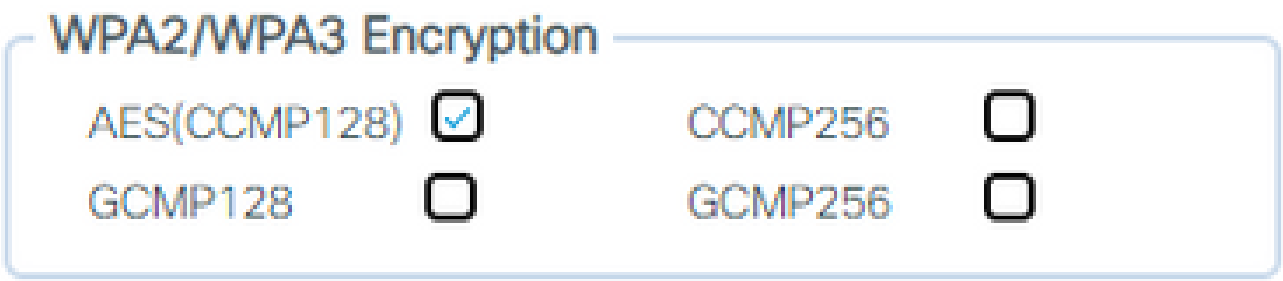
Entre las funciones clave de WPA3 se incluyen:

- Protected Management Frame (PMF) protege las tramas de administración de unidifusión y difusión y cifra las tramas de administración de unidifusión. Esto significa que los sistemas de detección de intrusiones inalámbricas y los sistemas de prevención de intrusiones inalámbricas tienen ahora menos formas de aplicar políticas de cliente por fuerza bruta.
- La autenticación simultánea de iguales (SAE) permite la autenticación basada en contraseña y un mecanismo de acuerdo de clave. Esto protege frente a ataques de fuerza bruta.
- El modo de transición es un modo mixto que permite el uso de WPA2 para conectar clientes que no admiten WPA3.

WPA3 tiene que ver con el desarrollo y la conformidad continuos de la seguridad, así como con la interoperabilidad.
No hay ningún elemento de información que designe WPA3 (igual que WPA2). WPA3 se define mediante combinaciones AKM/Cipher Suite/PMF.

En la configuración WLAN 9800, tiene 4 algoritmos de encriptación WPA3 diferentes que puede utilizar.

Se basan en Galois/Counter Mode Protocol (GCMP) y Counter Mode con Cipher Block Chaining Message Authentication Code Protocol (CCMP): AES (CCMP128), CCMP256, GCMP128 y GCMP256:

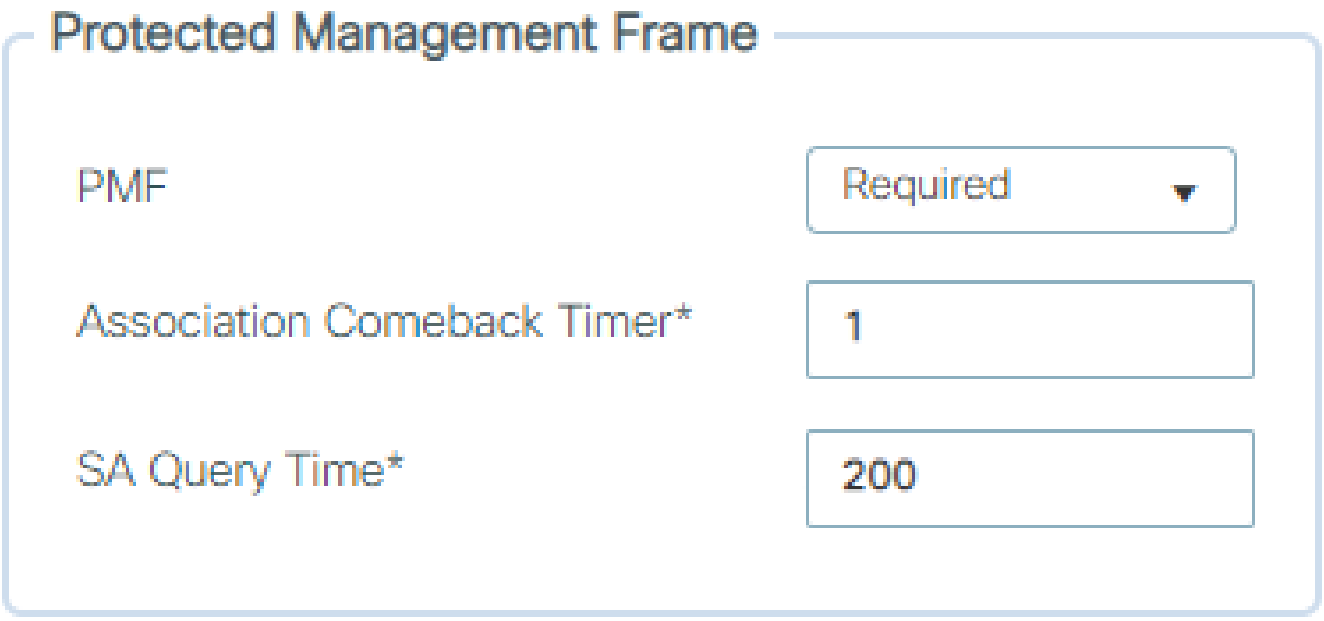


Opciones de encriptación WPA2/3

PMF

El PMF se activa en una WLAN cuando se habilita el PMF.

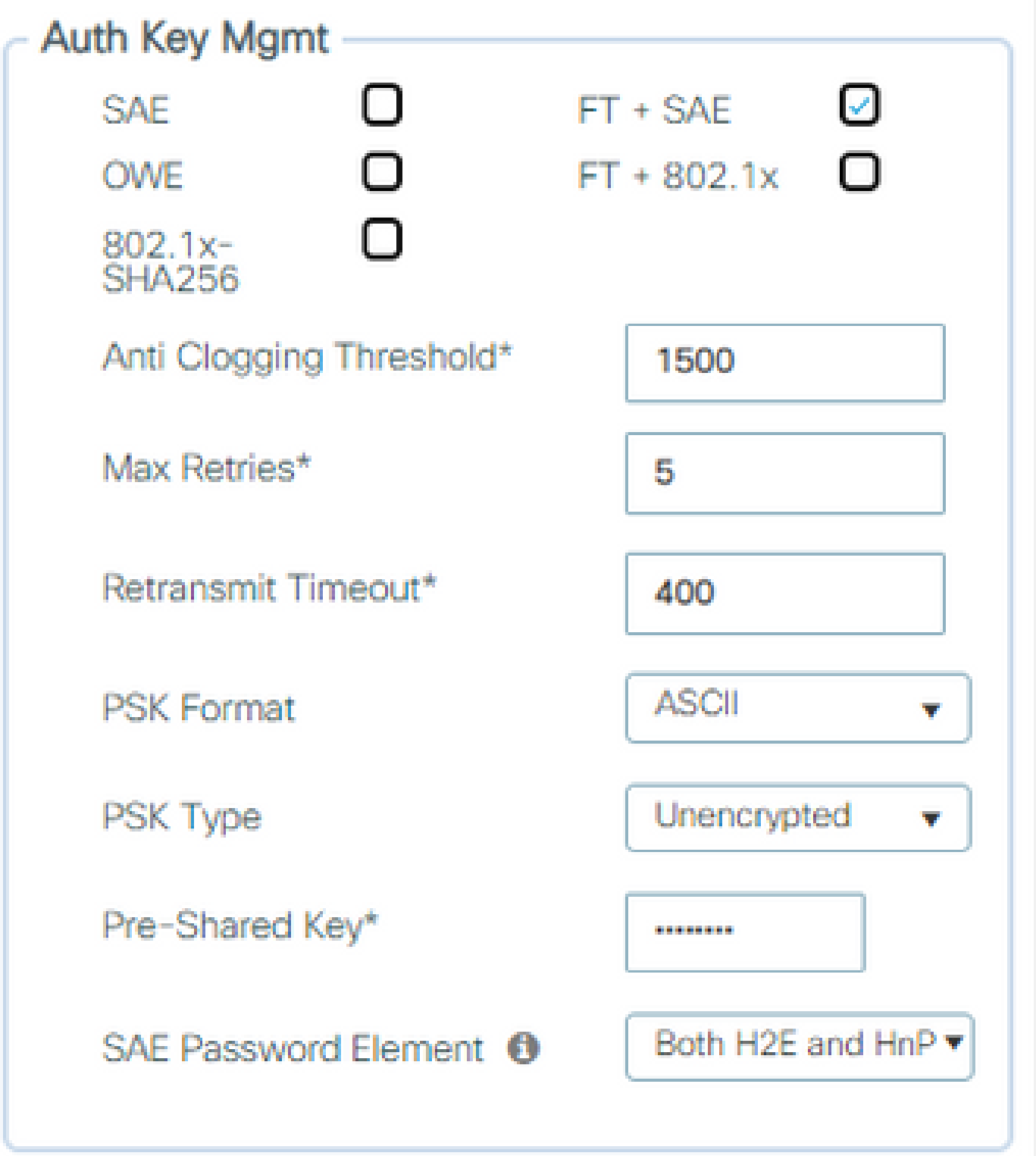
De forma predeterminada, las tramas de administración 802.11 no están autenticadas y, por lo tanto, no están protegidas contra la suplantación. El marco de protección de administración de infraestructura (MFP) y los marcos de administración protegidos (PMF) 802.11w proporcionan protección frente a este tipo de ataques.



Opciones de PMF

Administración de claves de autenticación

Estas son las opciones de AKM disponibles en la versión 17.9.x:

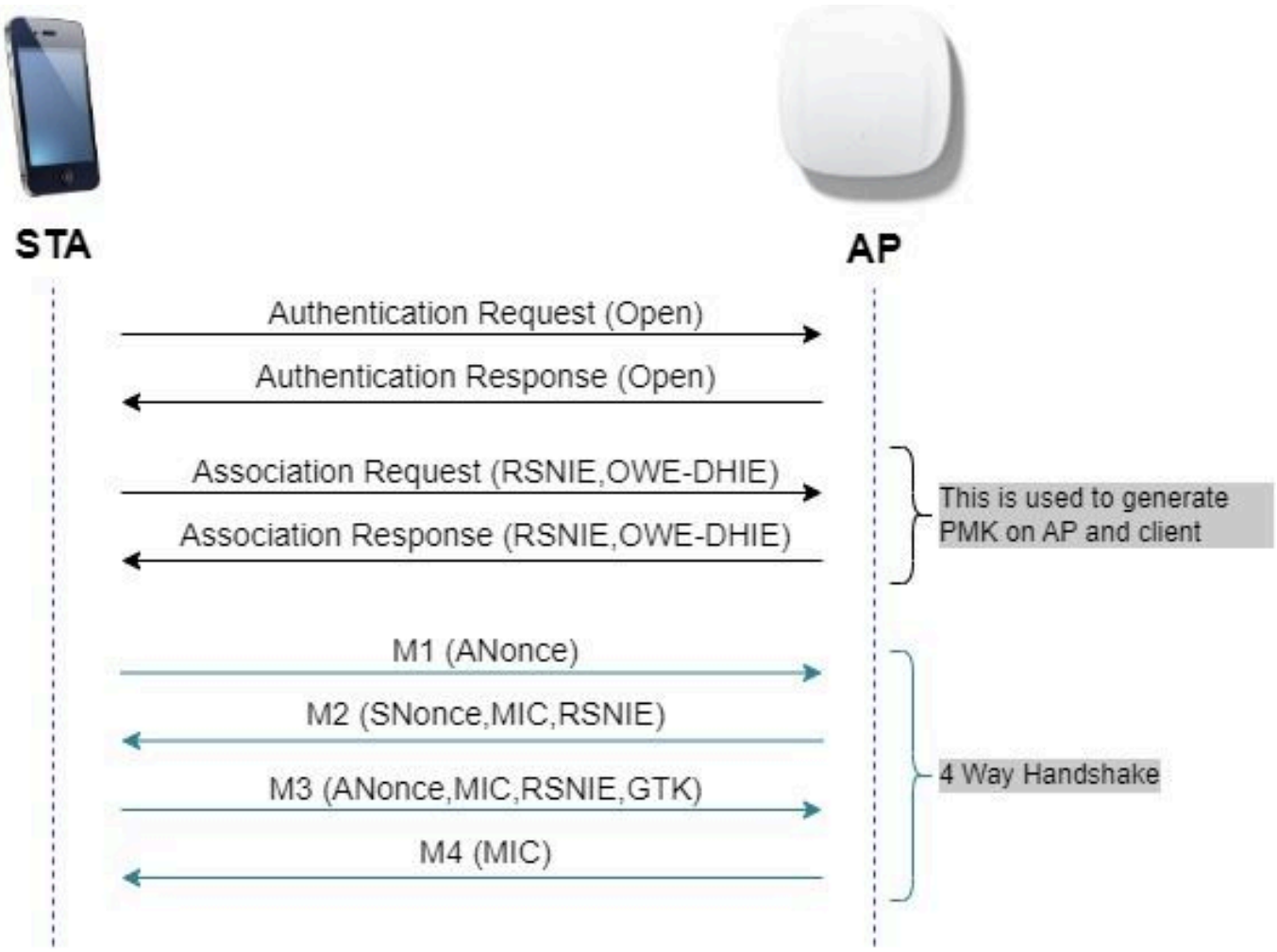


Opciones de AKM

DEBER

El cifrado inalámbrico oportunista (OWE) es una extensión de IEEE 802.11 que proporciona cifrado del medio inalámbrico (IETF RFC 8110). El propósito de la autenticación basada en OWE es evitar la conectividad inalámbrica abierta no segura entre los AP y los clientes. La OWE utiliza la criptografía basada en los algoritmos Diffie-Hellman para configurar el cifrado inalámbrico. Con OWE, el cliente y el AP realizan un intercambio de claves Diffie-Hellman durante el procedimiento de acceso y utilizan el secreto de clave maestra en pares (PMK) resultante con el protocolo de

enlace de 4 vías. El uso de OWE mejora la seguridad de la red inalámbrica en aquellas implementaciones en las que se implementan redes abiertas o compartidas basadas en PSK.



intercambio de tramas OWE

SAE

WPA3 utiliza un nuevo mecanismo de autenticación y administración de claves denominado Autenticación simultánea de iguales. Este mecanismo se mejora aún más mediante el uso de Hash-to-Element (H2E) SAE.

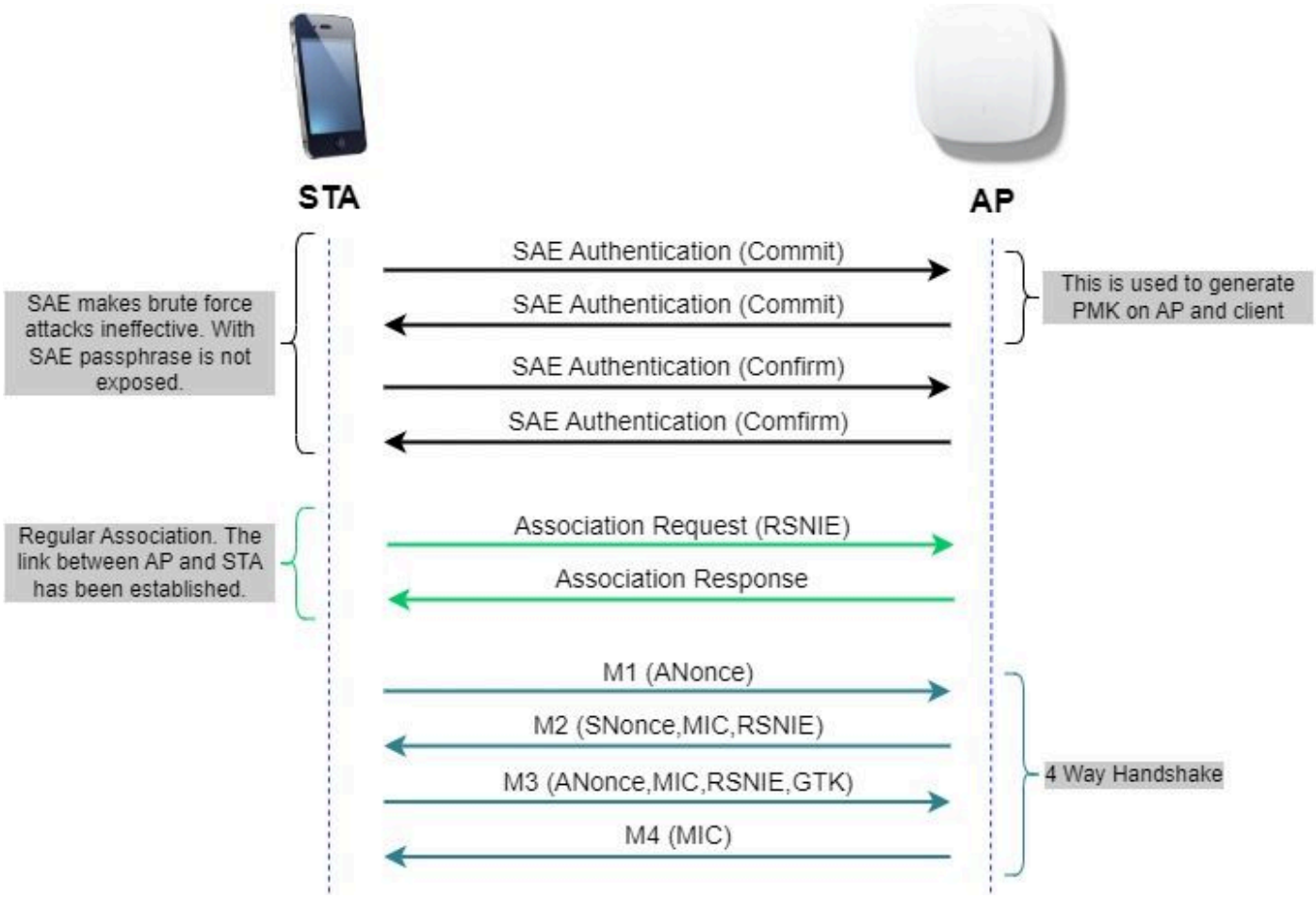
SAE con H2E es obligatorio para WPA3 y Wi-Fi 6E.

SAE emplea una criptografía de logaritmo discreta para realizar un intercambio eficiente de una manera que realiza la autenticación mutua utilizando una contraseña que probablemente sea resistente a un ataque de diccionario sin conexión.

Un ataque de diccionario sin conexión es cuando un adversario intenta determinar una contraseña de red intentando posibles contraseñas sin más interacción de red.

Cuando el cliente se conecta al punto de acceso, realiza un intercambio SAE. Si tienen éxito, crean una clave criptográficamente segura, de la que se deriva la clave de sesión. Básicamente, un cliente y un punto de acceso entran en fases de confirmación y luego confirman.

Una vez que hay un compromiso, el cliente y el punto de acceso pueden entrar en los estados de confirmación cada vez que hay una clave de sesión que se debe generar. El método utiliza la confidencialidad directa, donde un intruso podría descifrar una sola clave, pero no todas las demás.



intercambio de tramas SAE

Hash a elemento (H2E)

Hash-to-Element (H2E) es un nuevo método SAE Password Element (PWE). En este método, el PWE secreto utilizado en el protocolo SAE se genera a partir de una contraseña.

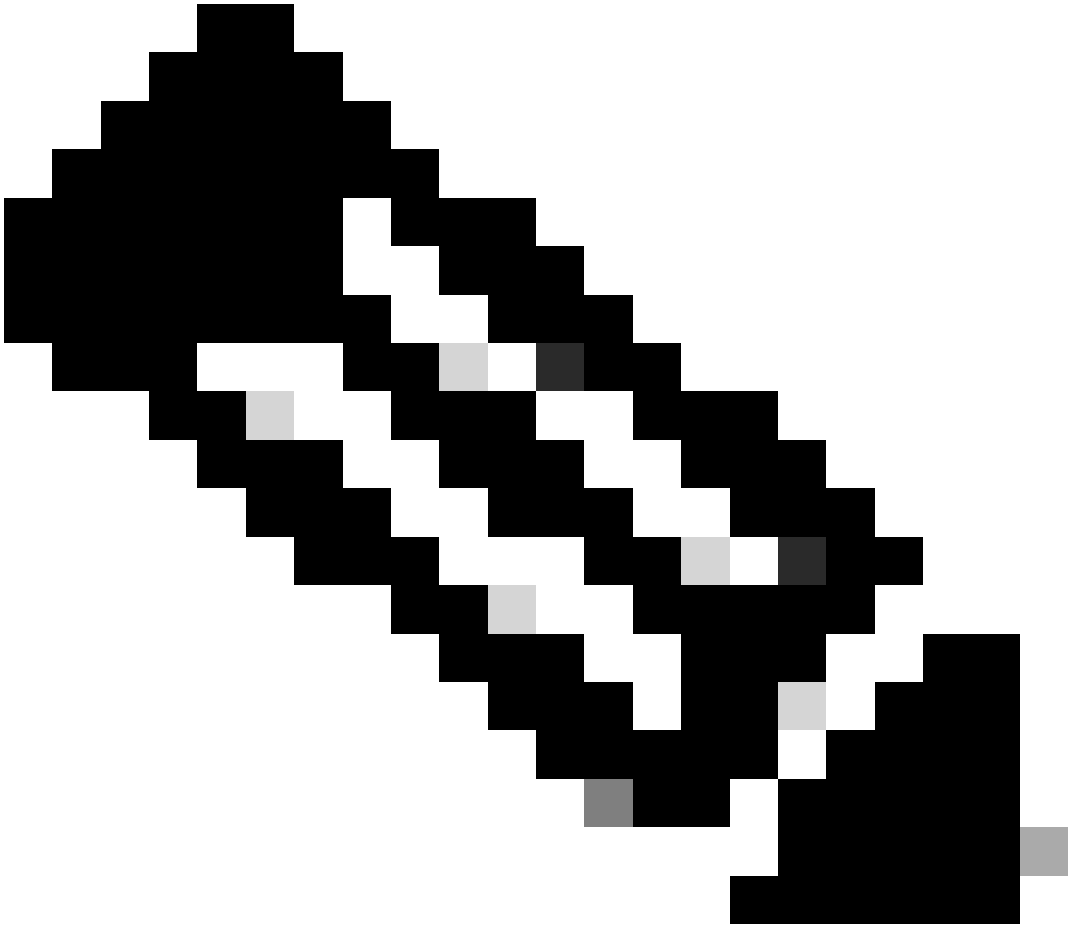
Cuando una estación (STA) que soporta H2E inicia SAE con un AP, verifica si AP soporta H2E. Si la respuesta es sí, el AP utiliza el H2E para derivar el PWE usando un valor de código de estado recién definido en el mensaje de confirmación SAE.

Si STA utiliza Hunting-and-Pecking (HnP), todo el intercambio SAE permanece sin cambios.

Mientras se utiliza el H2E, la derivación PWE se divide en estos componentes:

- Derivación de un elemento intermediario secreto (PT) de la contraseña. Esto se puede realizar sin conexión cuando la contraseña se configura inicialmente en el dispositivo para cada grupo admitido.
- Derivación del PWE del PT almacenado. Esto depende del grupo negociado y de las

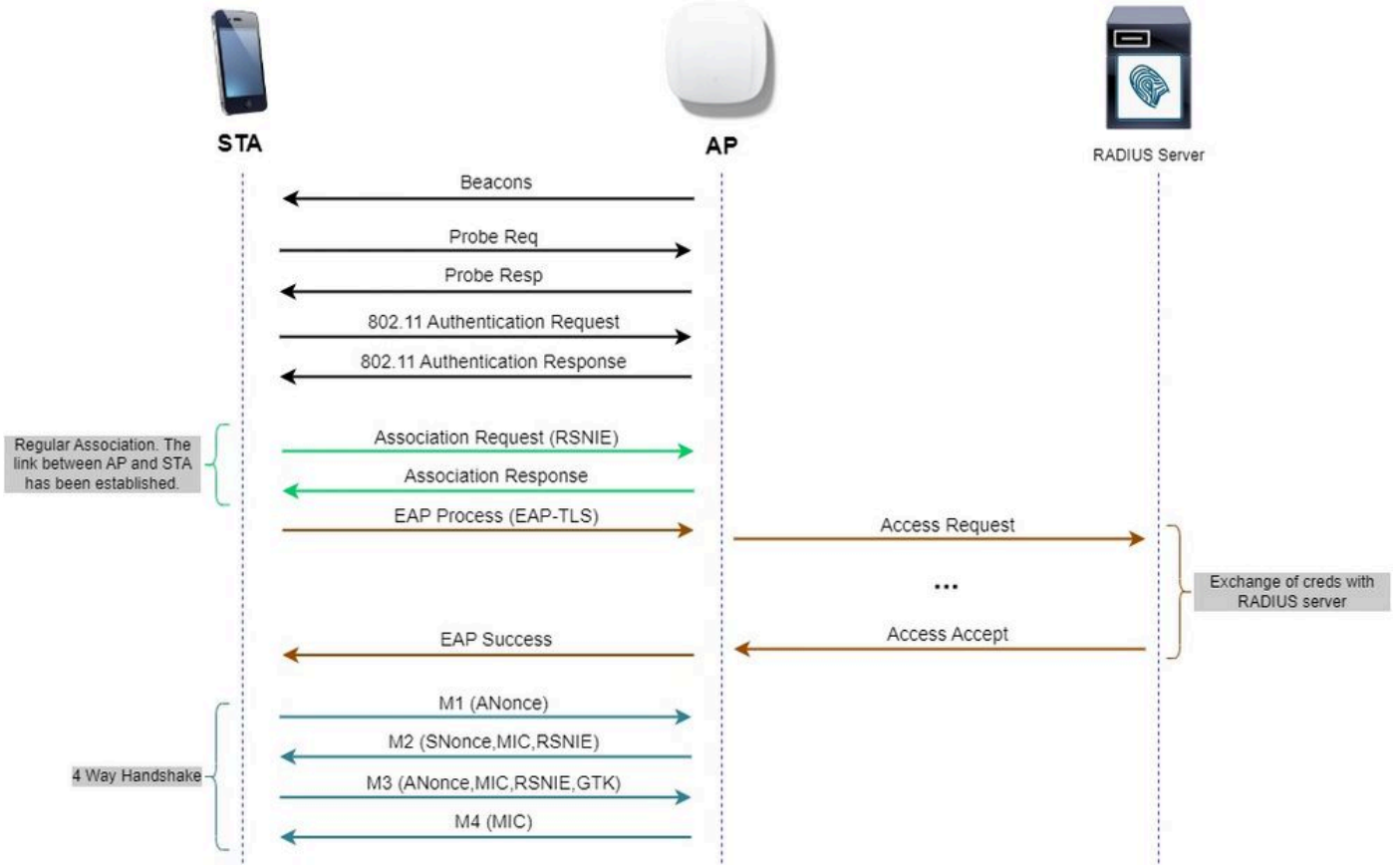
direcciones MAC de los peers. Esto se realiza en tiempo real durante el intercambio SAE.



Nota: 6 GHz sólo admite el método PWE SAE de hash a elemento.

WPA-Enterprise (802.1x)

WPA3-Enterprise es la versión más segura de WPA3 y utiliza una combinación de nombre de usuario y contraseña con 802.1X para la autenticación de usuarios con un servidor RADIUS. De forma predeterminada, WPA3 utiliza encriptación de 128 bits, pero también introduce una encriptación de 192 bits configurable opcionalmente, que proporciona protección adicional a cualquier red que transmita datos confidenciales.



Flujo de diagrama de WPA3 Enterprise

Conjunto de niveles: modos WPA3

- WPA3-Personal
  - Modo sólo WPA3-Personal
    - PMF requerido
  - Modo de transición WPA3-Personal
    - Reglas de configuración: en un punto de acceso, siempre que se active WPA2-Personal, el modo de transición WPA3-Personal también se debe habilitar de forma predeterminada, a menos que el administrador lo invalide explícitamente para funcionar en el modo WPA2-Personal only

- WPA3 Enterprise
  - Modo sólo WPA3-Enterprise
    - El PMF se negociará para todas las conexiones WPA3
  - Modo de transición WPA3-Enterprise
    - El PMF se negociará para una conexión WPA3
    - PMF opcional para una conexión WPA2
  - WPA3-Enterprise suite-B modo "192 bits" alineado con el algoritmo de seguridad nacional comercial (CNSA)
    - Más que solo para el gobierno federal
    - Conjuntos de cifrado criptográfico coherentes para evitar errores de configuración

- Adición de GCMP y ECCP para funciones de cifrado y hash mejoradas (SHA384)
- PMF requerido

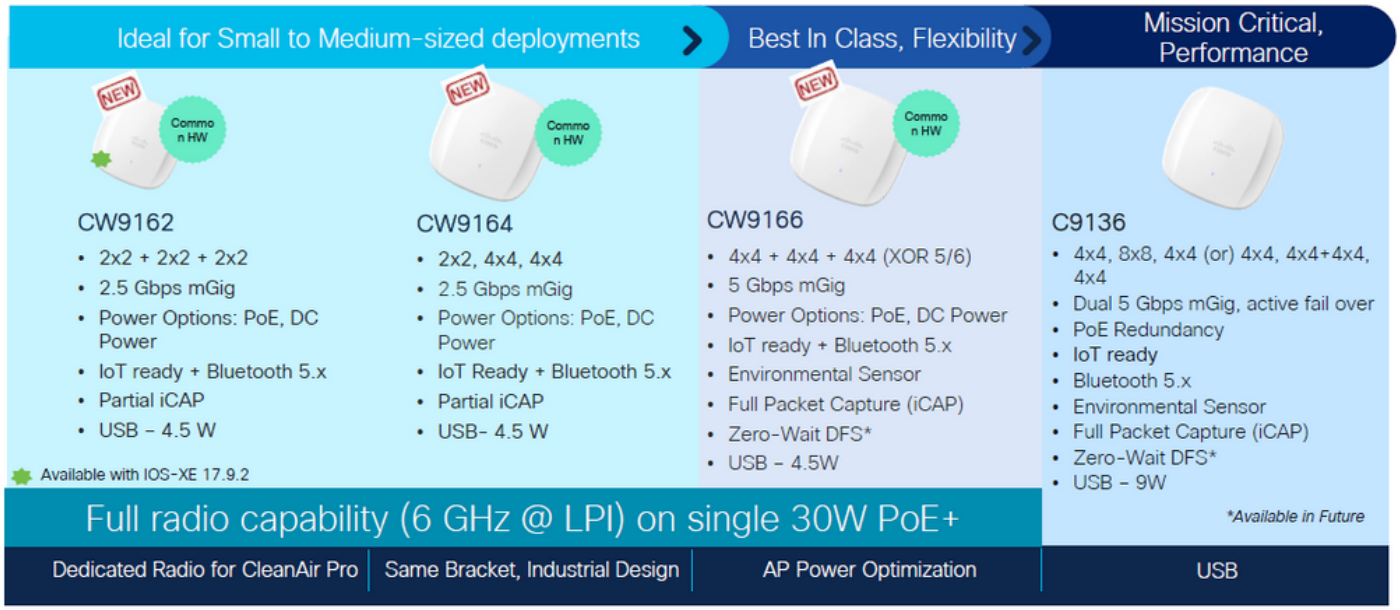
- La seguridad WPA3 de 192 bits será exclusiva para EAP-TLS, que requerirá certificados tanto en el solicitante como en el servidor RADIUS.

- Para utilizar WPA3 Enterprise de 192 bits, los servidores RADIUS deben utilizar uno de los cifrados EAP permitidos:

  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Para obtener más información sobre la implementación de WPA3 en las WLAN de Cisco, incluida la matriz de compatibilidad de seguridad del cliente, no dude en consultar la Guía de implementación de WPA3.

AP Cisco Catalyst Wi-Fi 6E



Puntos de acceso Wi-Fi 6E

Configuración de seguridad admitida por clientes

Puede encontrar qué producto admite WPA3-Enterprise utilizando la página web de WiFi Alliance buscador de productos.

En los dispositivos Windows, puede verificar cuáles son las configuraciones de seguridad admitidas por el adaptador mediante el comando "netsh wlan show drivers".

Aquí puede ver el resultado del 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
```

Resultado de Windows de _netsh wlan show driver_ para el cliente AX211

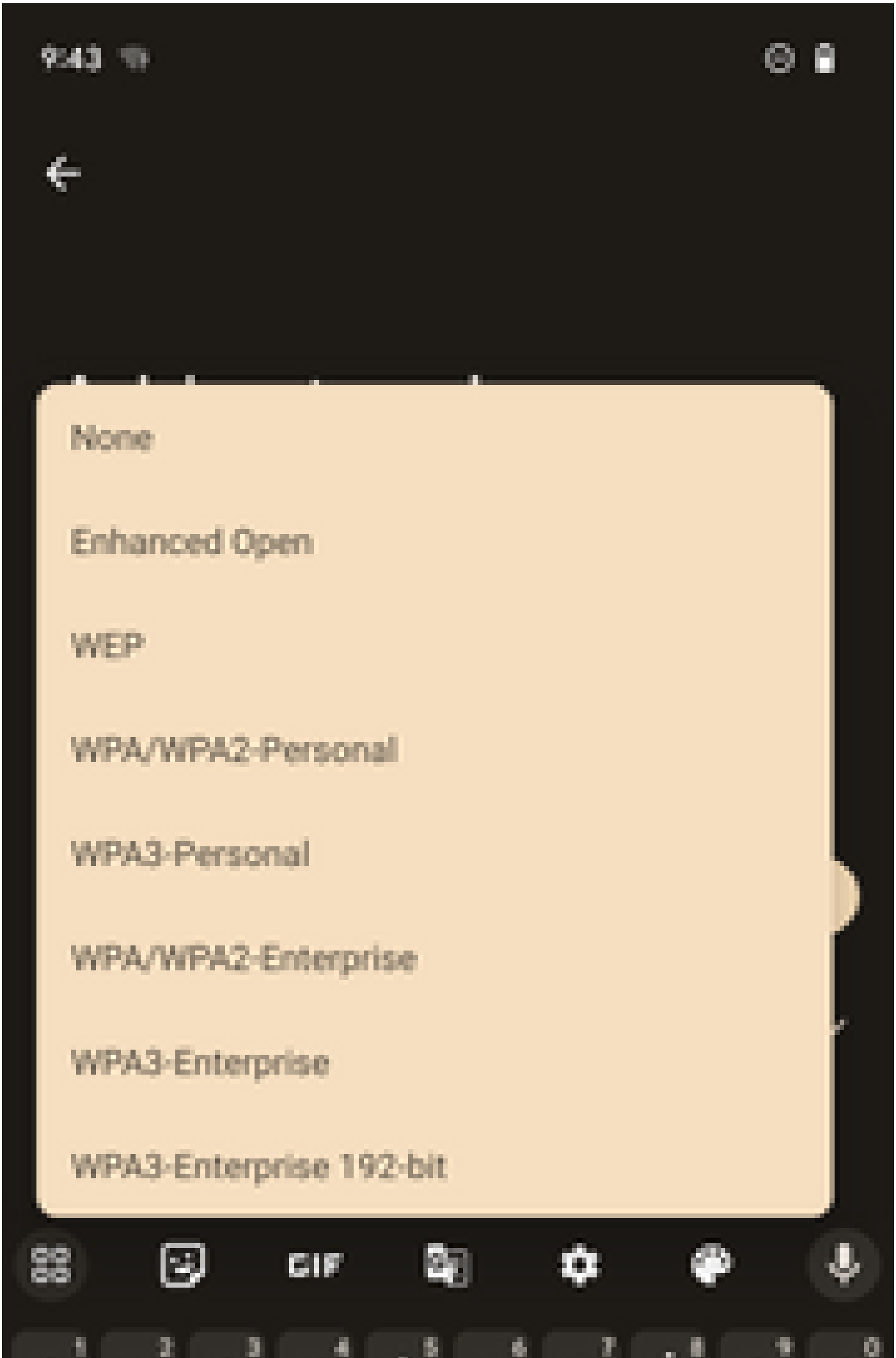
Netgear A8000:

```
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)
```

Resultado de Windows de _netsh wlan show driver_ para el cliente Netgear A8000s

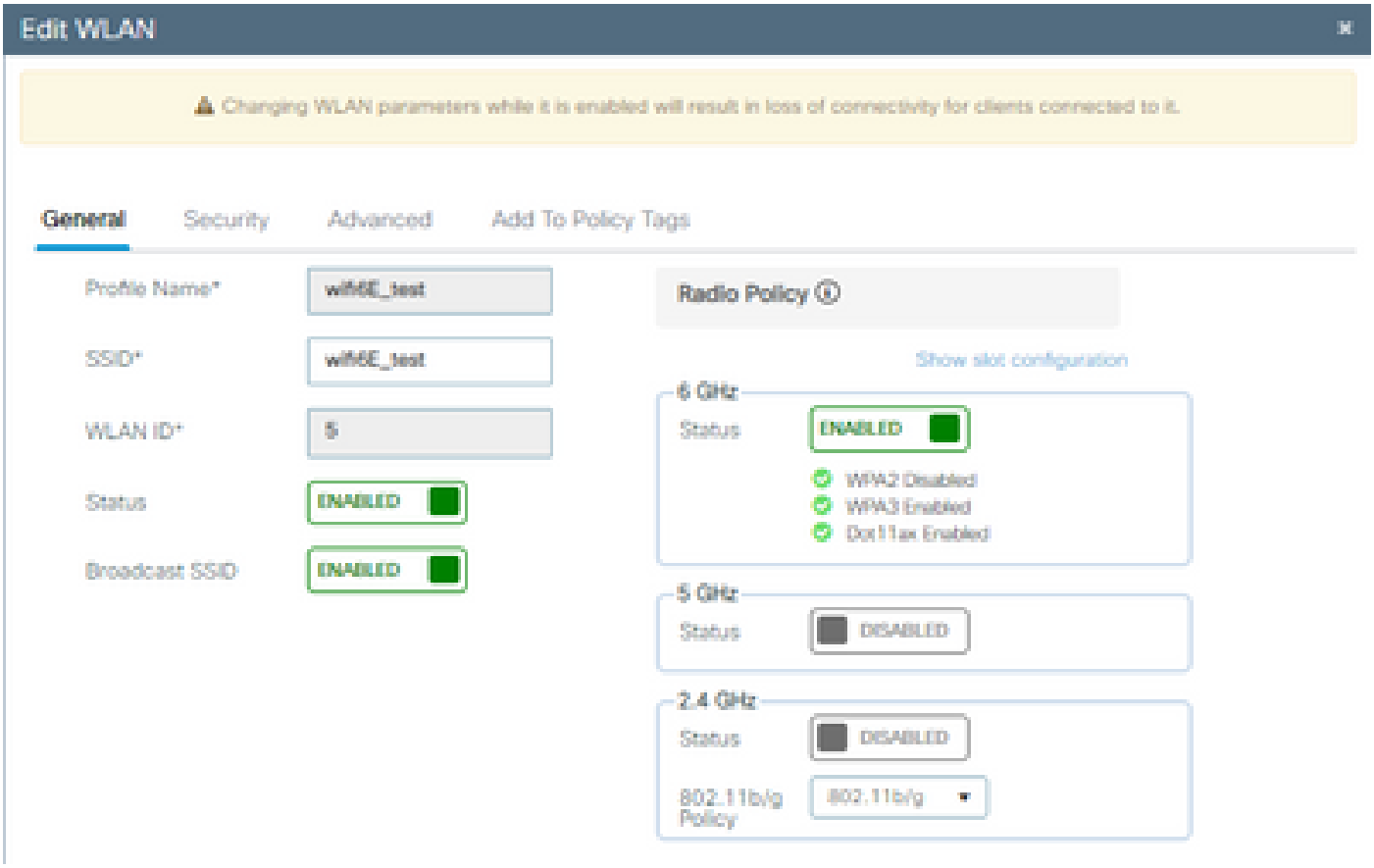
Android Pixel 6a:


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

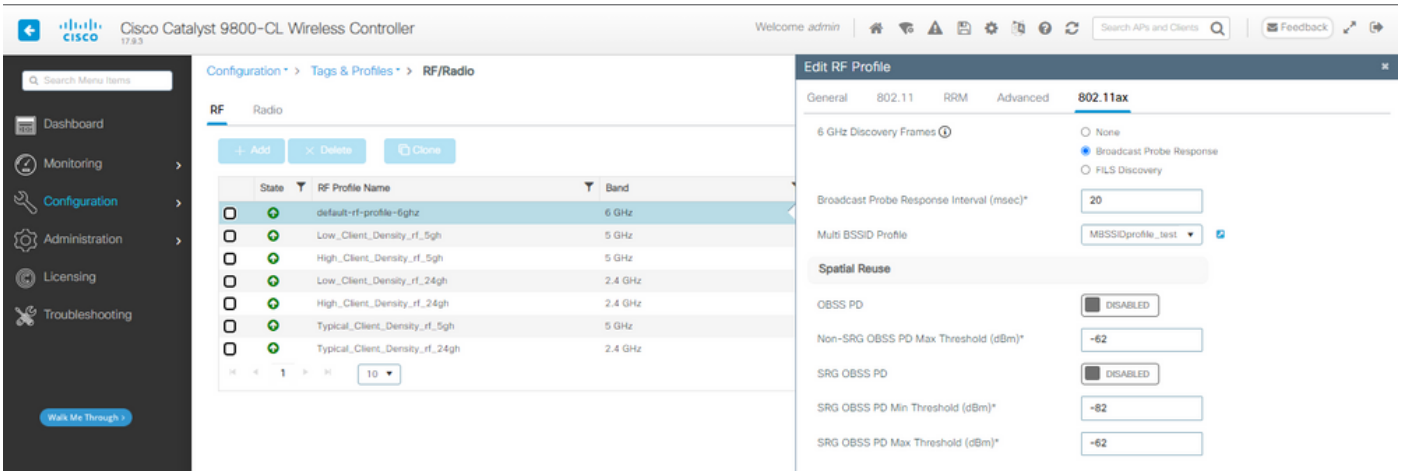
- WPA3 + cifrado AES + AKM 802.1x-SHA256 (FT)
- WPA3 + cifrado AES + AKM OWE
- WPA3 + cifrado AES + AKM SAE (FT)
- WPA3 + cifrado CCMP256 + AKM SUITEB192-1X
- WPA3 + cifrado GCMP128 + SUITEB-1X AKM
- WPA3 + cifrado GCMP256 + AKM SUITEB192-1X

Configuración base

La WLAN se configuró con el método de detección de política de radio y UPR (Respuesta de sondeo de difusión) solo de 6 GHz:



Configuración de base WLAN



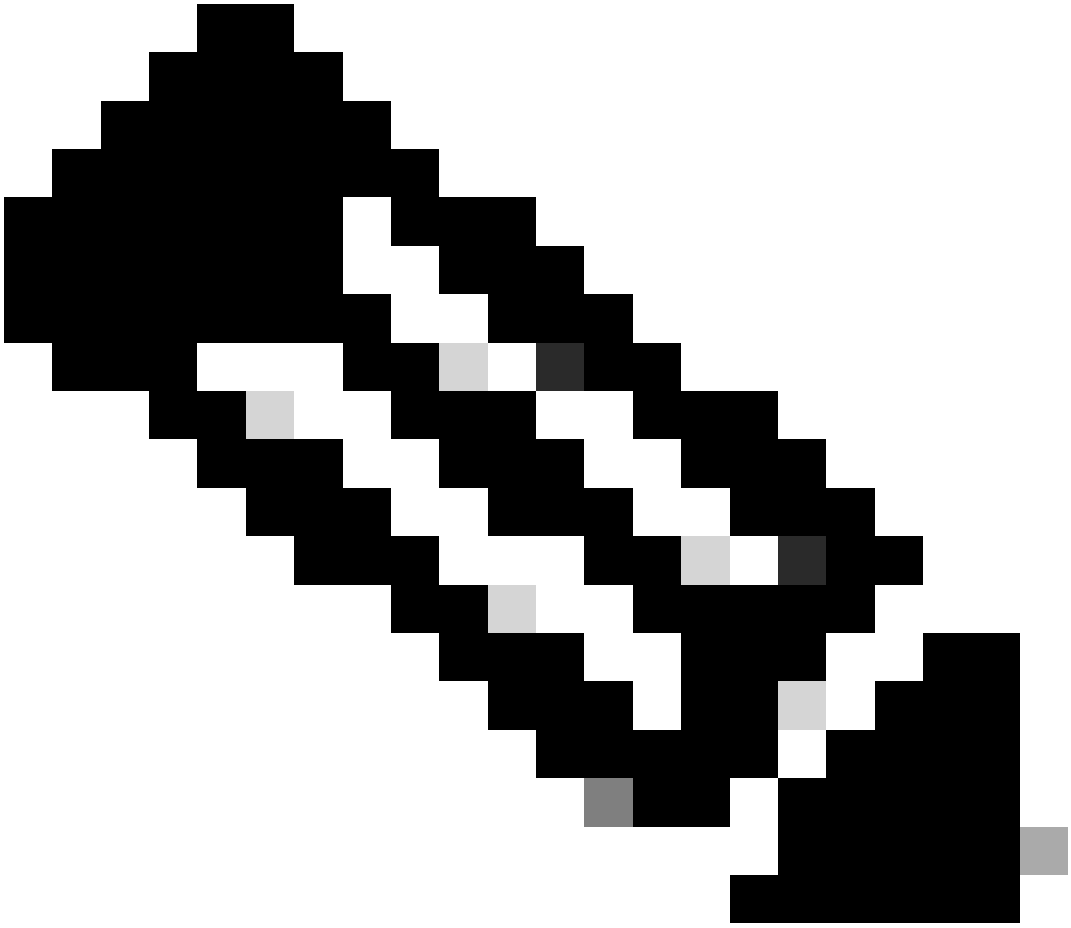
Configuración del perfil de RF de 6 GHz

Verificación

Verificación de seguridad

En esta sección se presenta la fase de asociación de cliente y configuración de seguridad mediante las siguientes combinaciones de protocolos WPA3:

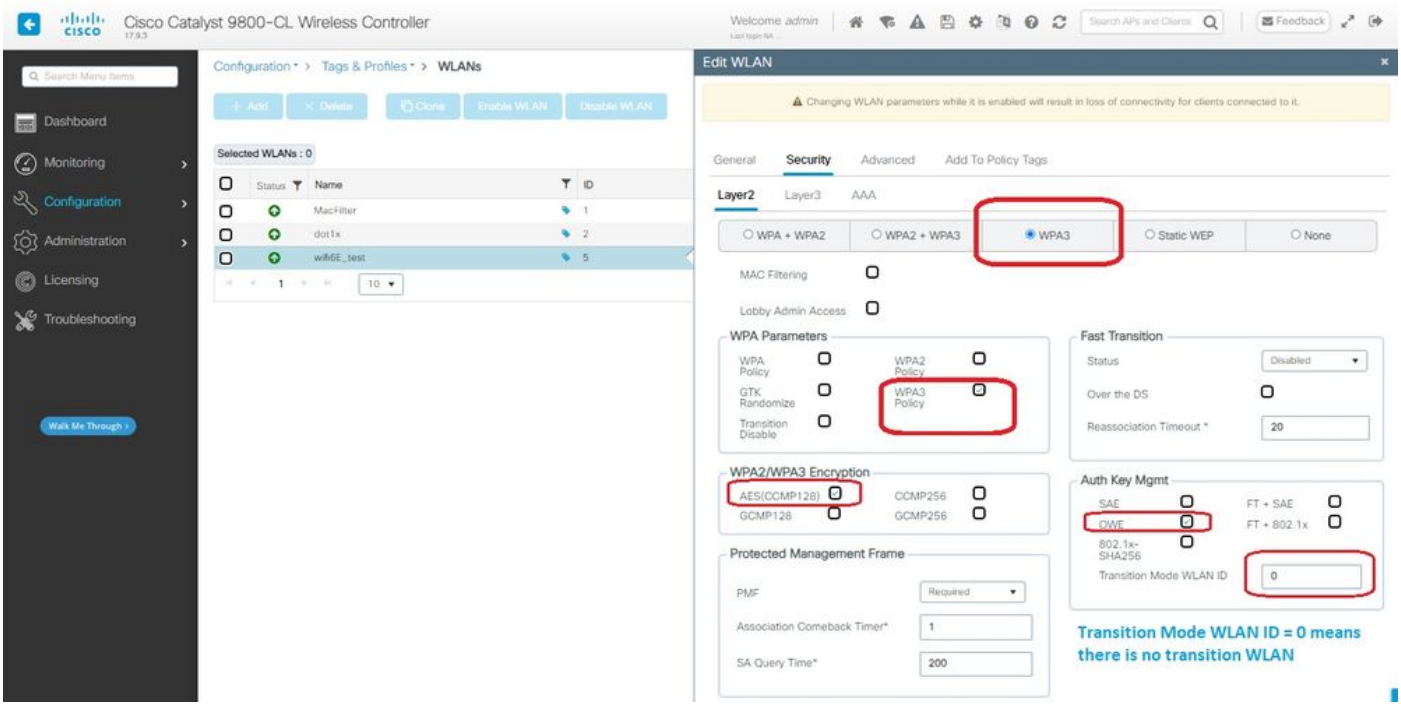
- WPA3- AES (CCMP128) + OWE
  - Modo de transición OWE
- WPA3-Personal
  - AES (CCMP128) + SAE
- WPA3 Enterprise
  - AES (CCMP128) + 802.1x-SHA256
  - AES (CCMP128) + 802.1x-SHA256 + FT
  - Cifrado GCMP128 + SUITEB-1X
  - Cifrado GCMP256 + SUITEB192-1X



Nota: Aunque no hay clientes que soporten el cifrado GCMP128 + SUITEB-1X al momento de escribir este documento, se probó para observar que se estaba transmitiendo y verificar la información RSN en las balizas.

WPA3 - AES (CCPM128) + OWE

Esta es la configuración de Seguridad WLAN:



Configuración de seguridad OWE

Ver en WLC GUI de los ajustes de seguridad WLAN:

Parámetros de seguridad WLAN en la GUI del WLC

Aquí podemos observar el proceso de conexión de clientes Wi-Fi 6E:

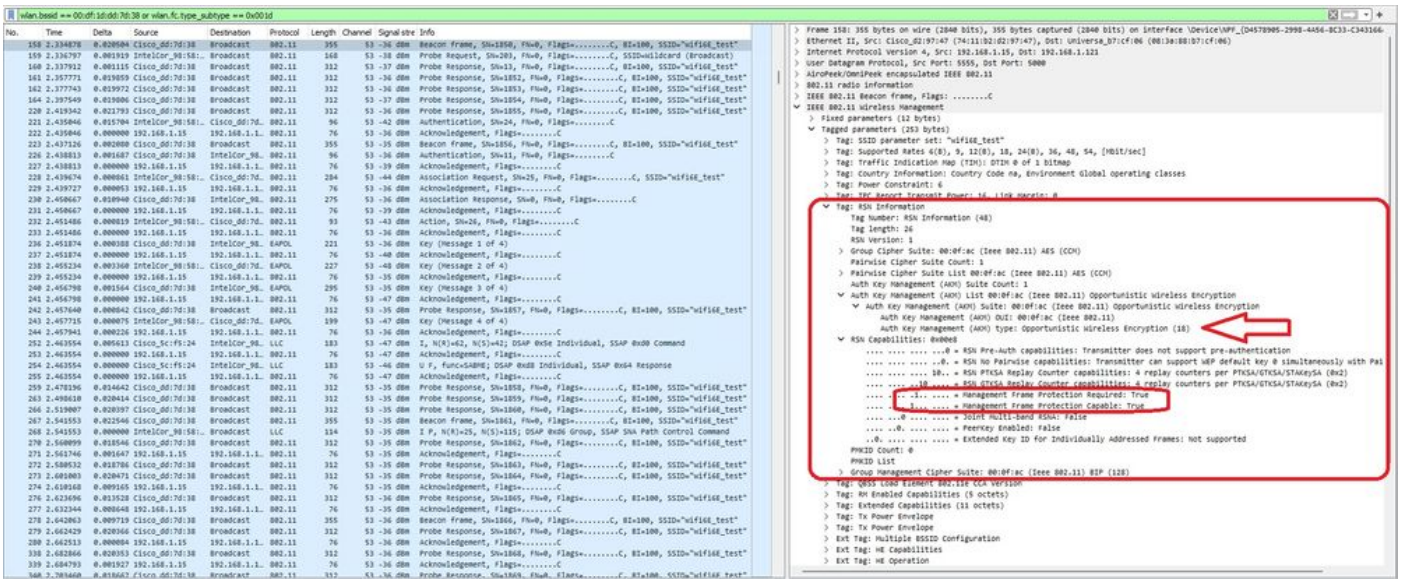
Intel AX211

Aquí mostramos el proceso de conexión completo del cliente Intel AX211.

Descubrimiento de OWE

Aquí se pueden ver las balizas OTA. El AP anuncia el soporte para OWE usando el selector de conjunto AKM para OWE bajo el elemento de información RSN.

Puede ver el valor 18 (00-0F-AC:18) del tipo de conjunto AKM que indica el soporte de OWE.



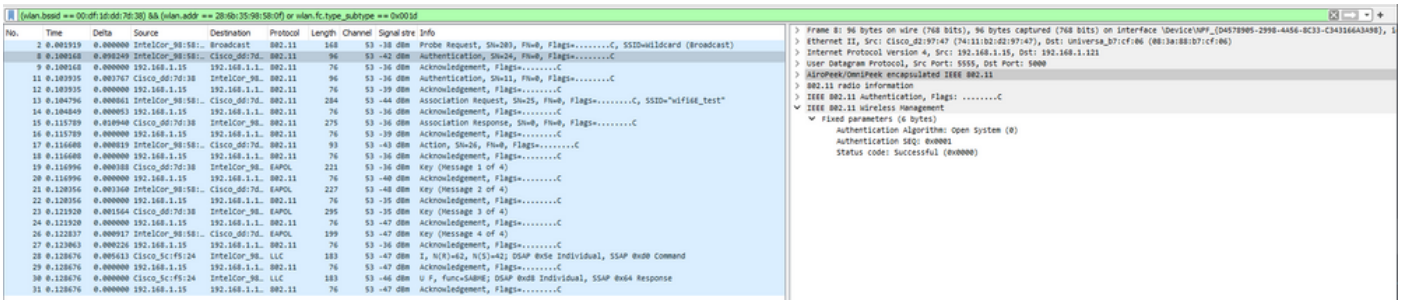
trama de baliza OWE

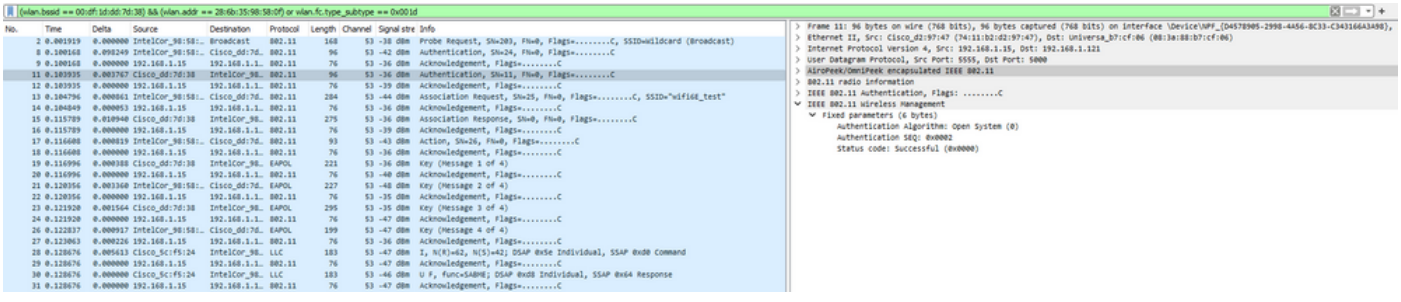
Si observa el campo de capacidades RSN, puede ver que AP anuncia capacidades de protección de tramas de administración (MFP) y bit requerido de MFP establecido en 1.

Asociación OWE

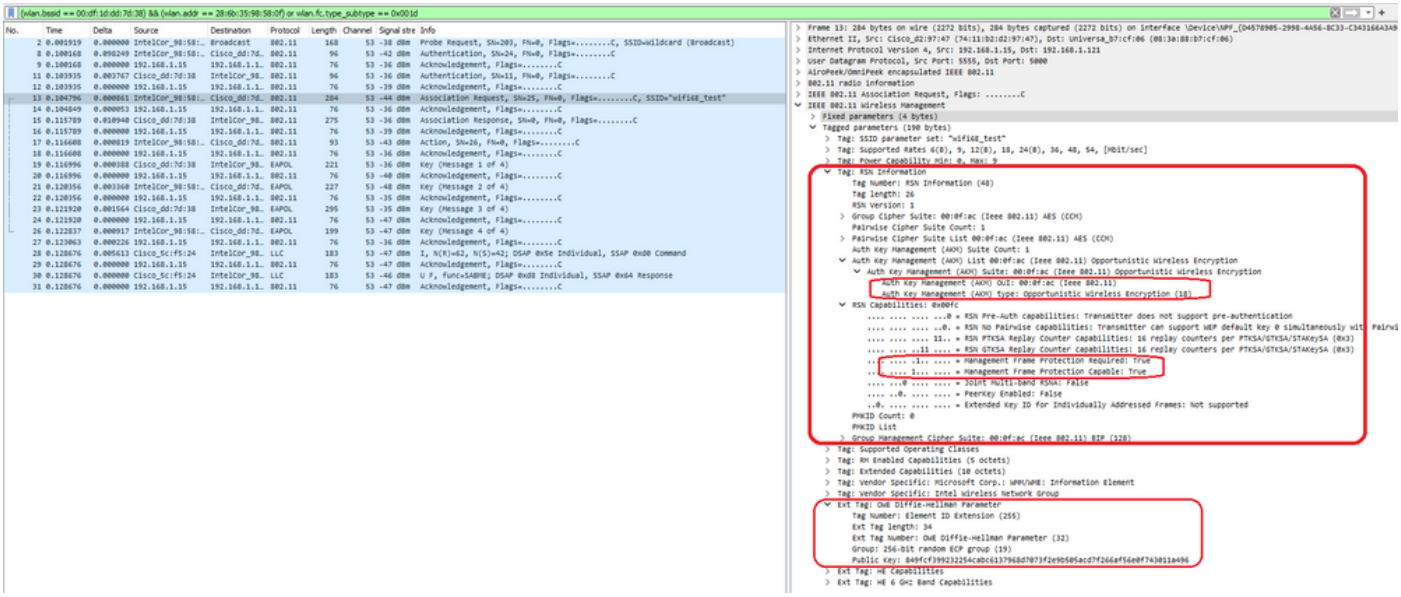
Puede ver el UPR enviado en modo de difusión y luego la asociación misma.

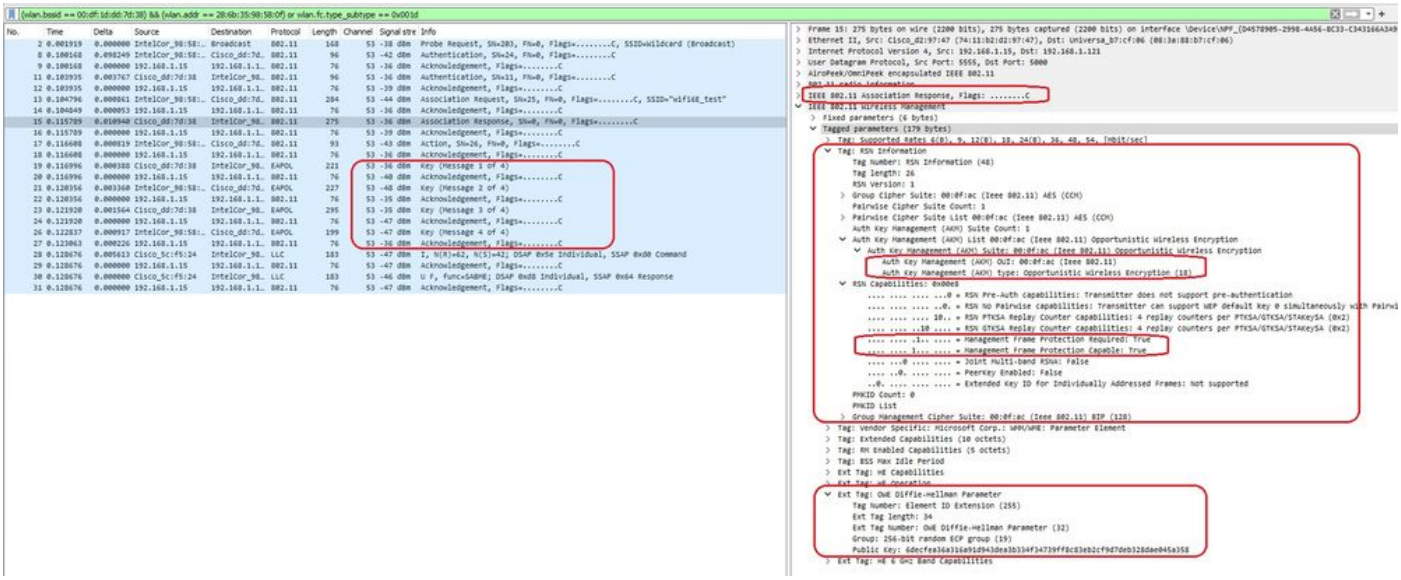
El OWE comienza con la solicitud y respuesta de autenticación OPEN:





Luego, un cliente que quiera hacer OWE debe indicar OWE AKM en la trama RSN IE of Association Request e incluir el elemento de parámetro Diffie Helman (DH):

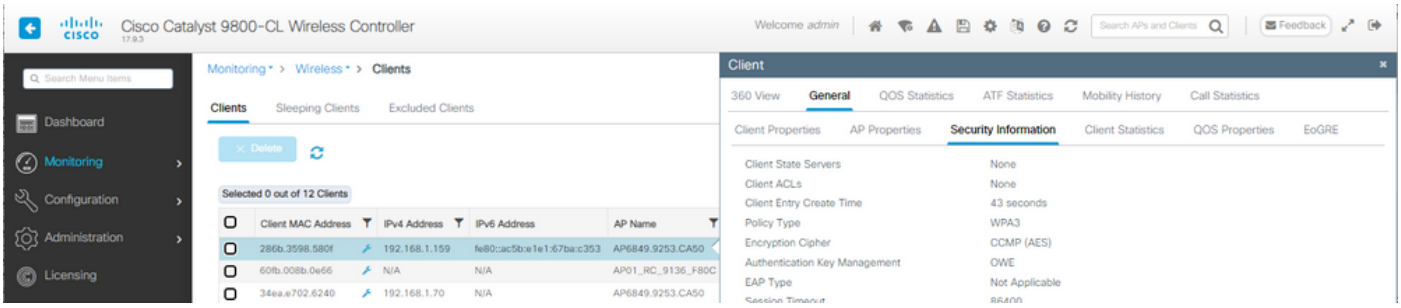




Respuesta de OWE Association

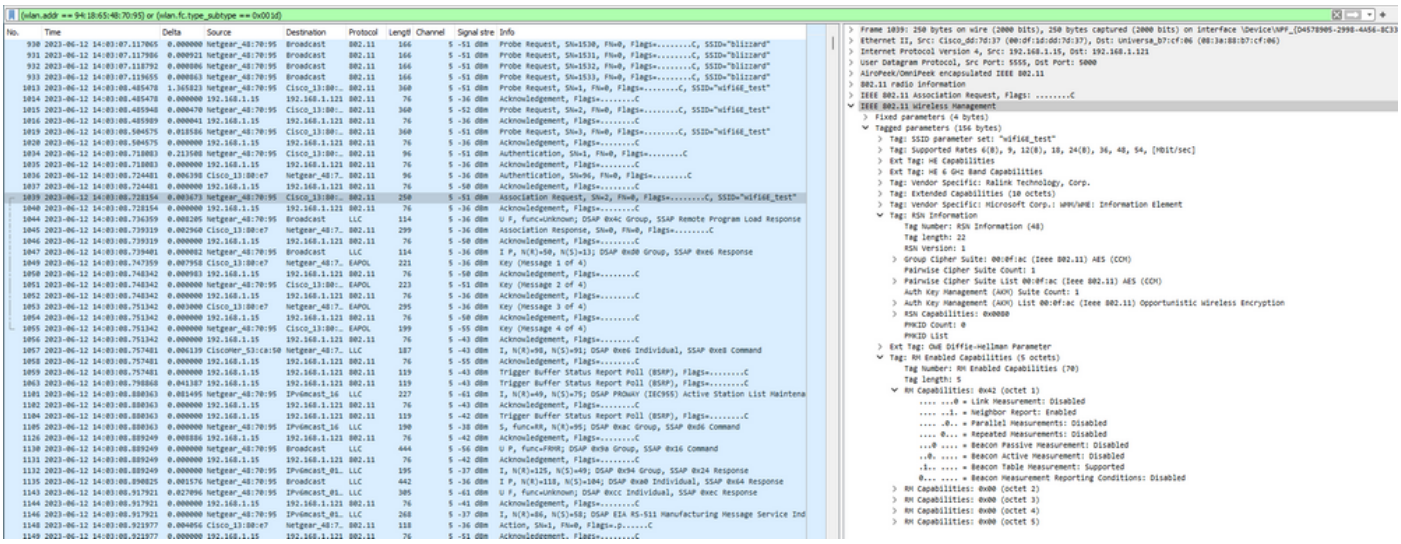
Después de la respuesta de asociación, podemos ver el protocolo de enlace de 4 vías y el cliente pasa al estado conectado.

Aquí usted puede ver los detalles del cliente en la GUI del WLC:

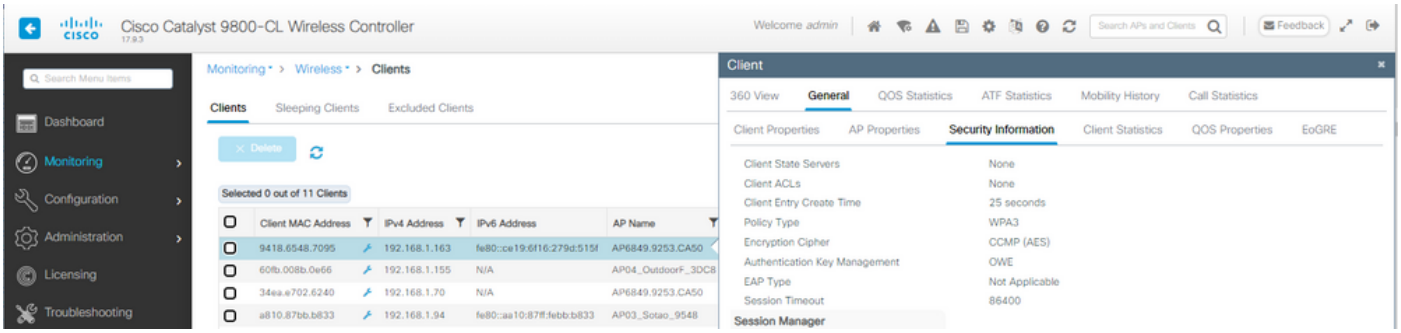


NetGear A8000

Conexión OTA con enfoque en la información RSN del cliente:

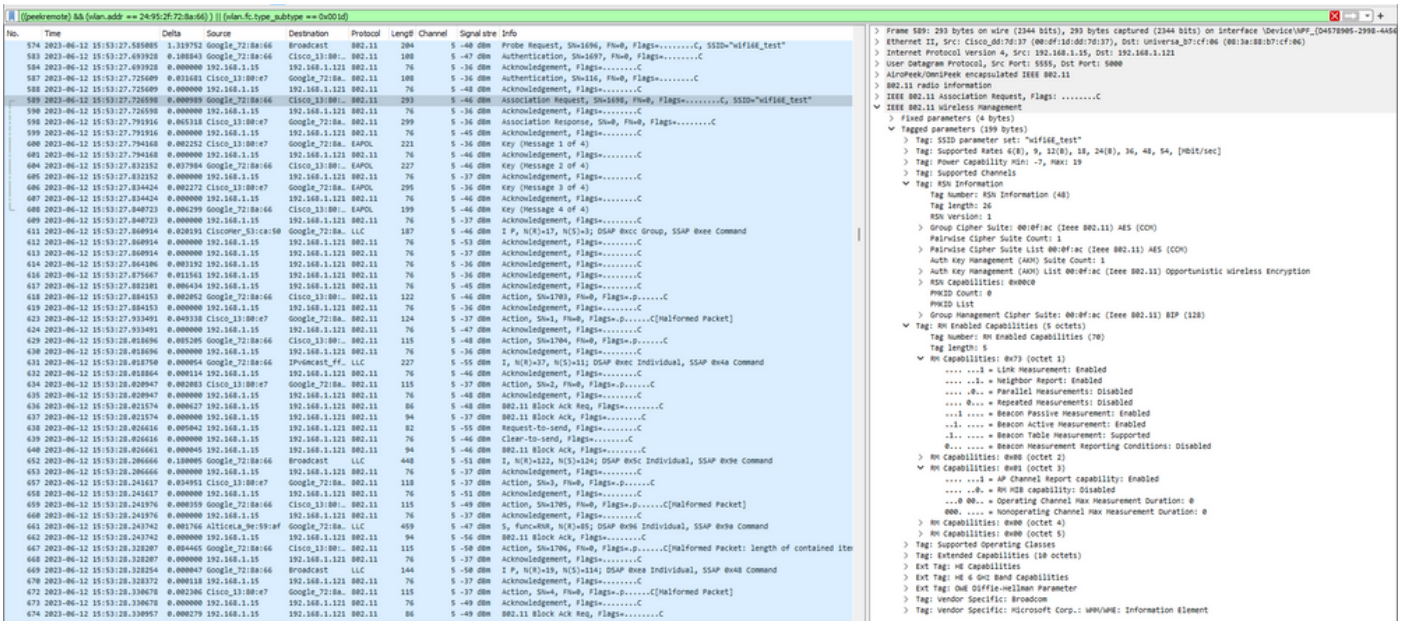


Detalles del cliente en WLC:

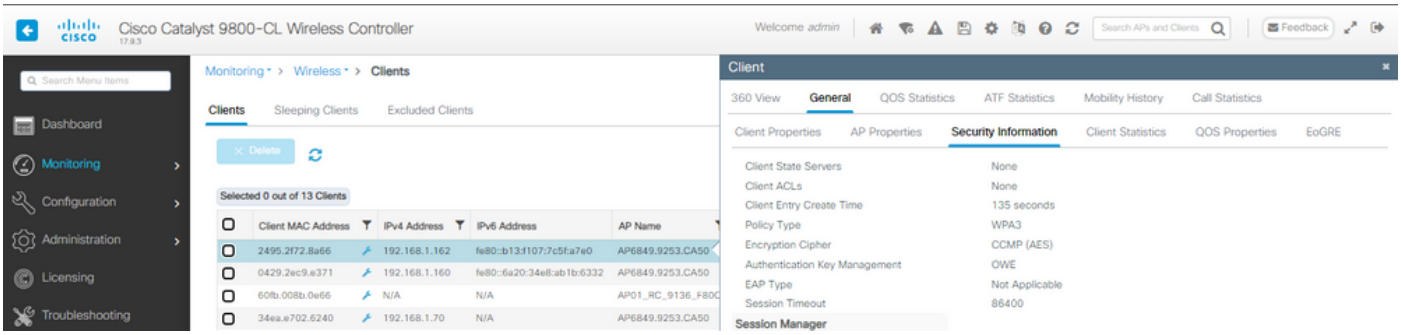


Píxel 6a

Conexión OTA con enfoque en la información RSN del cliente:

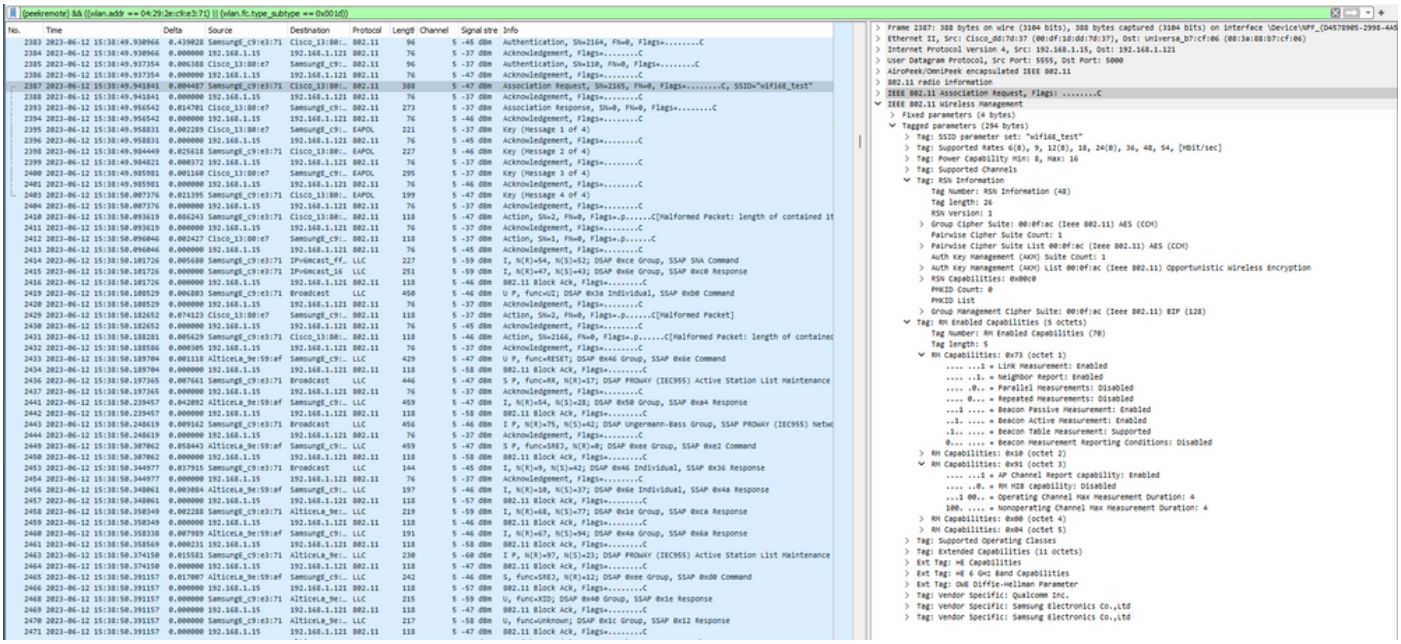


Detalles del cliente en WLC:

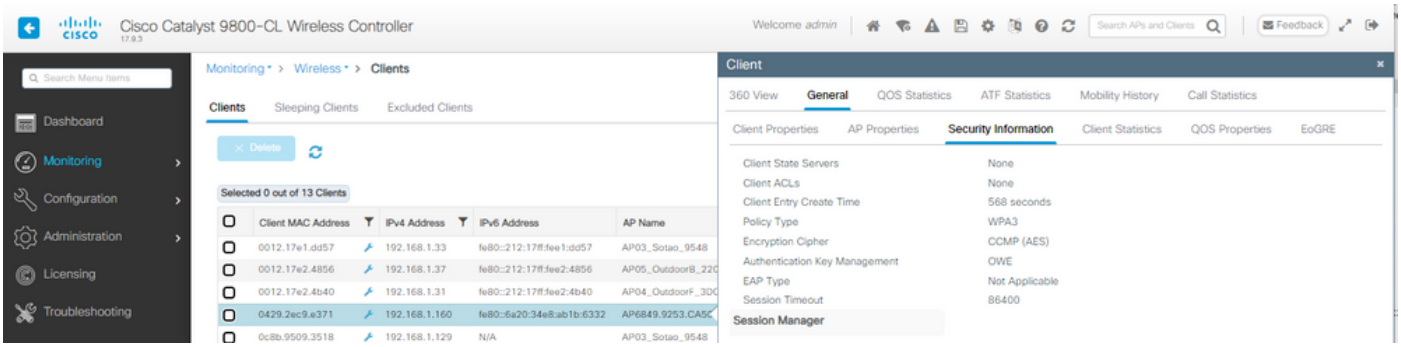


Samsung S23

Conexión OTA con enfoque en la información RSN del cliente:



Detalles del cliente en WLC:

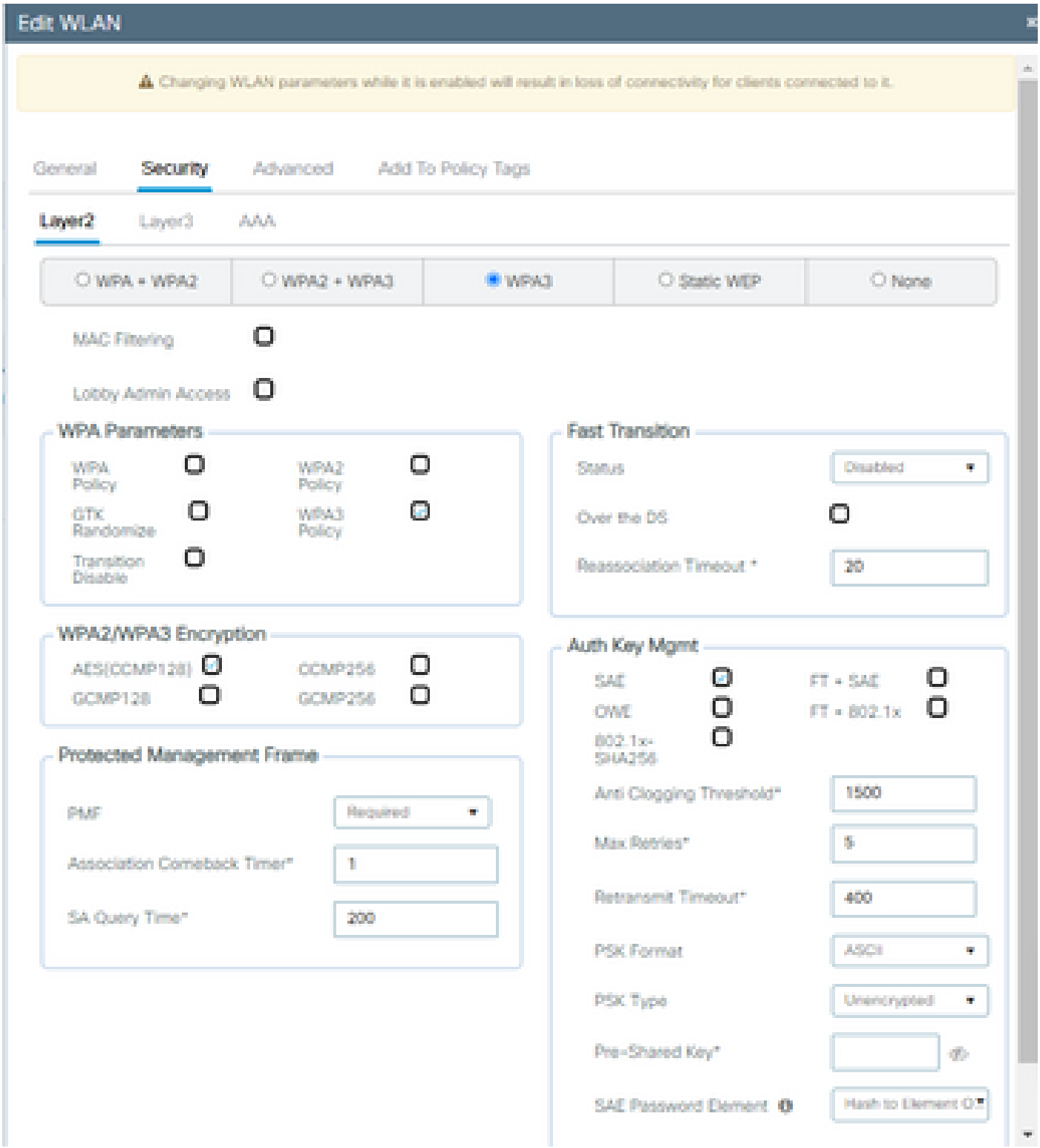


WPA3 - AES (CCPM128) + OWE con modo de transición

Configuración y resolución de problemas detallados del modo de transición OWE disponibles en este documento: [Configure Enhanced Open SSID with Transition Mode - OWE].

WPA3-Personal: AES (CCMP128) + SAE

Configuración de seguridad WLAN:

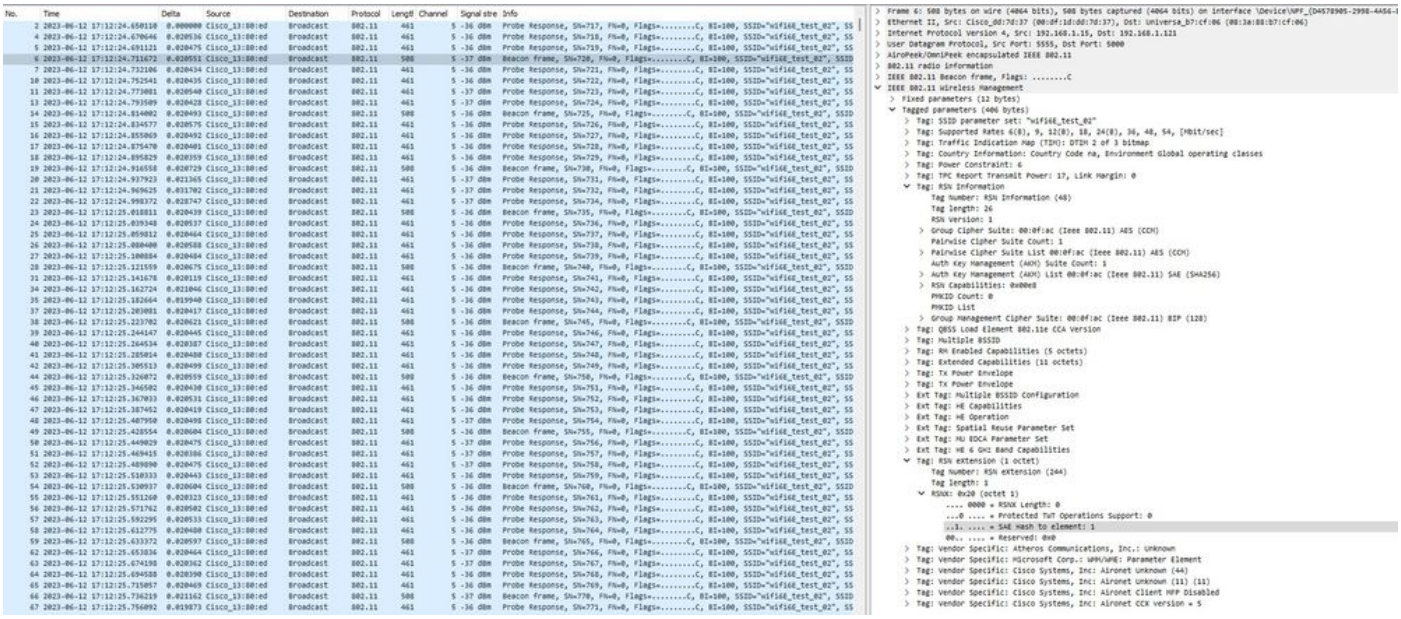


Configuración de WPA3 SAE

Nota: Tenga en cuenta que la política de radio de 6 GHz no permite la búsqueda y el rastreo. Al configurar una WLAN de sólo 6 GHz, debe seleccionar H2E SAE Password Element (Elemento de contraseña SAE H2E).

Ver en WLC GUI de los ajustes de seguridad WLAN:

Verificación de las balizas OTA:

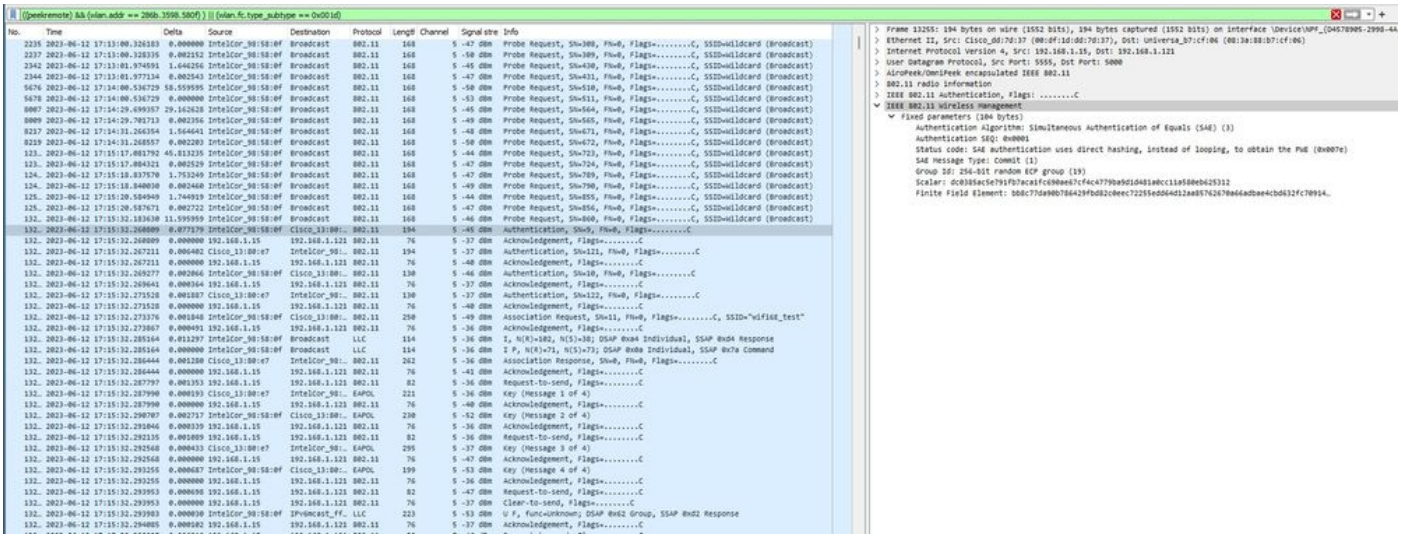


Indicadores WPA3 SAE

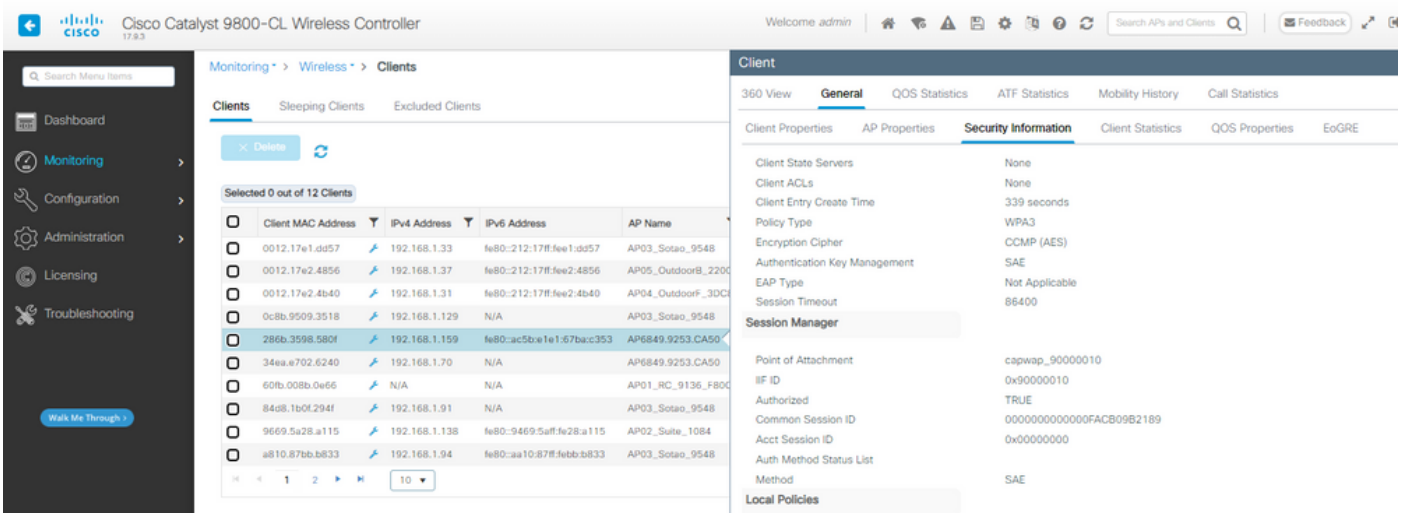
Aquí podemos observar clientes Wi-Fi 6E asociando:

Intel AX211

Conexión OTA con enfoque en la información RSN del cliente:

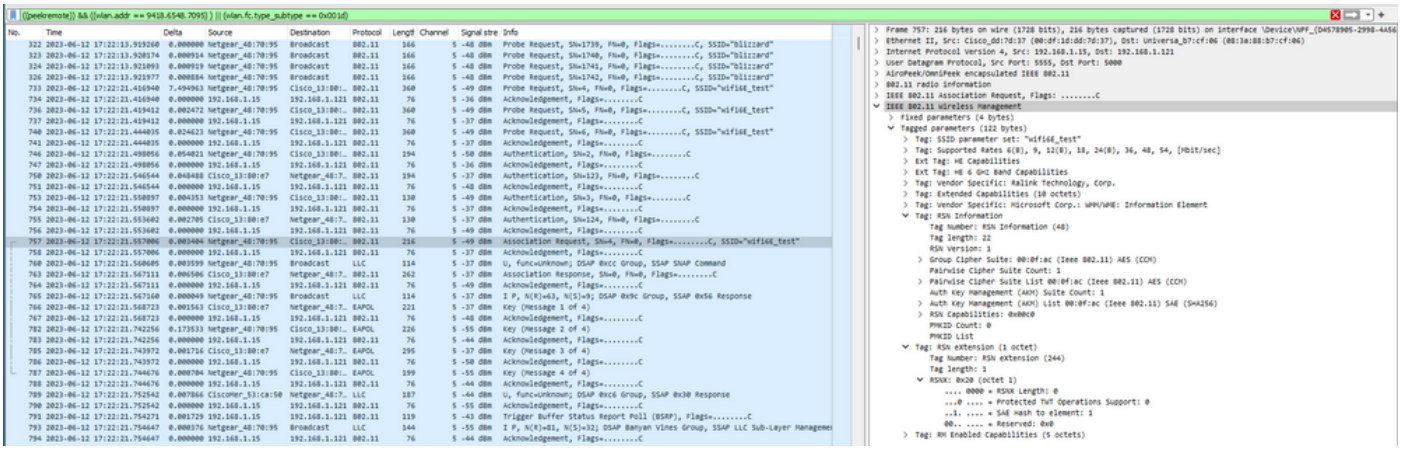


Detalles del cliente en WLC:

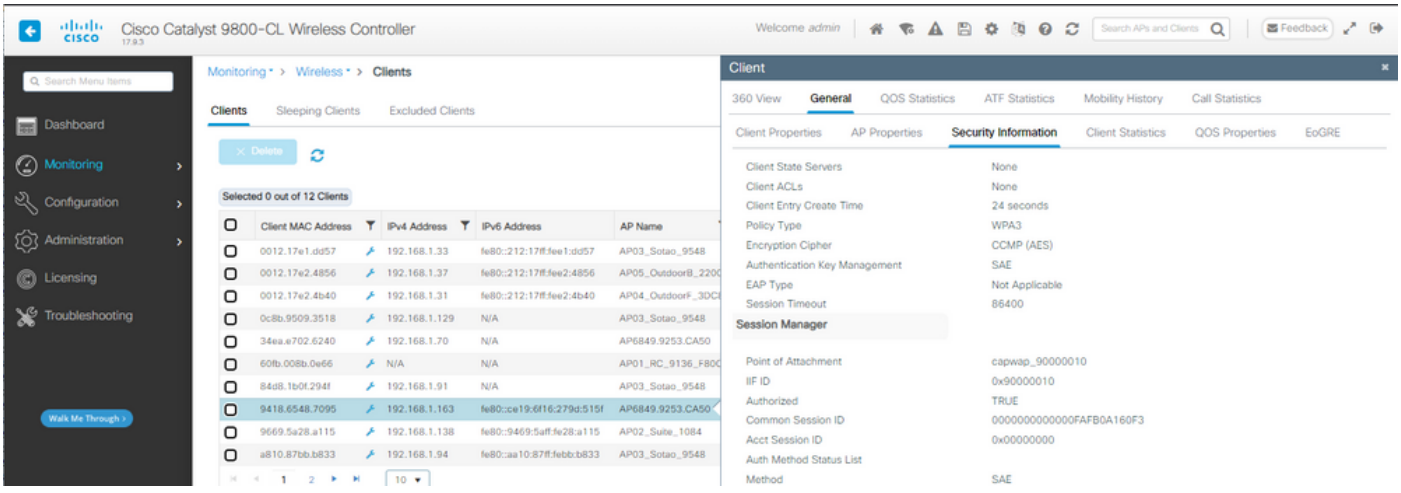


NetGear A8000

Conexión OTA con enfoque en la información RSN del cliente:

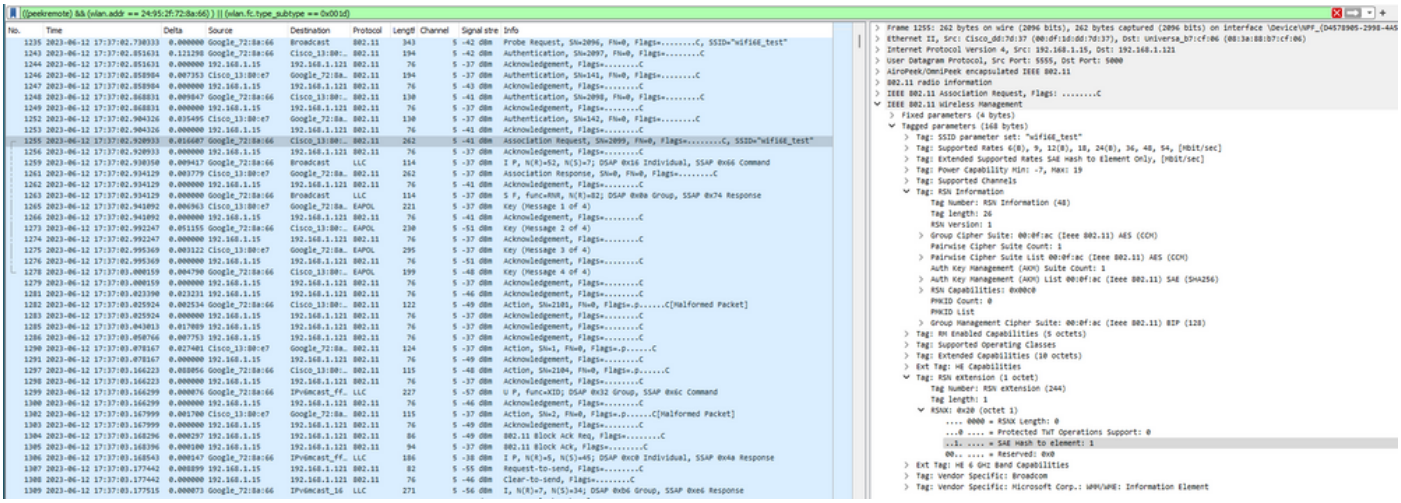


Detalles del cliente en WLC:

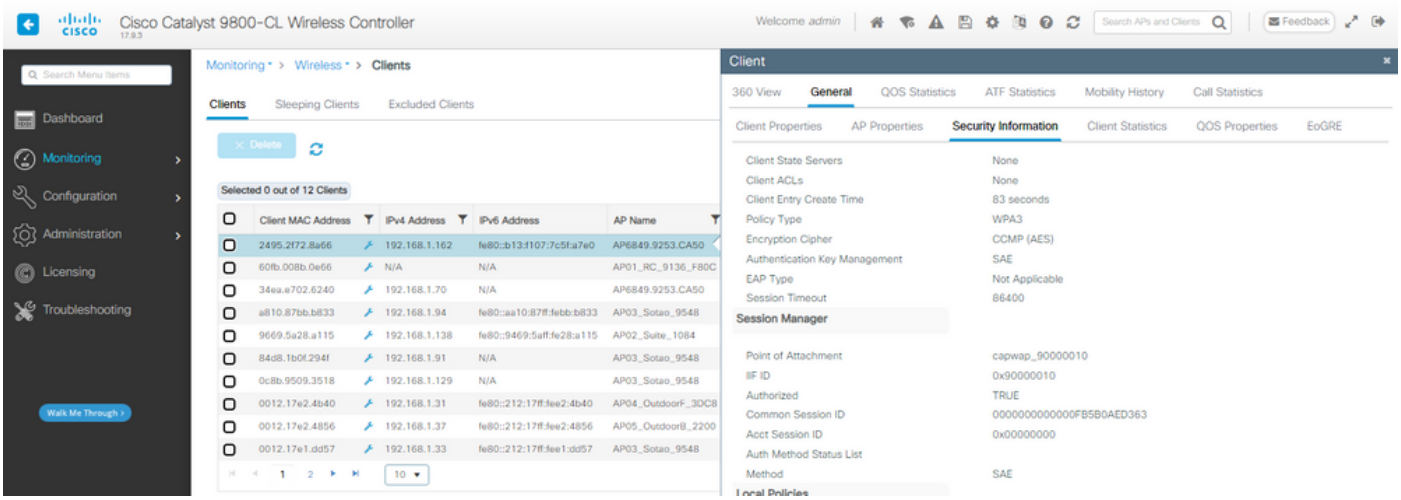


Píxel 6a

Conexión OTA con enfoque en la información RSN del cliente:

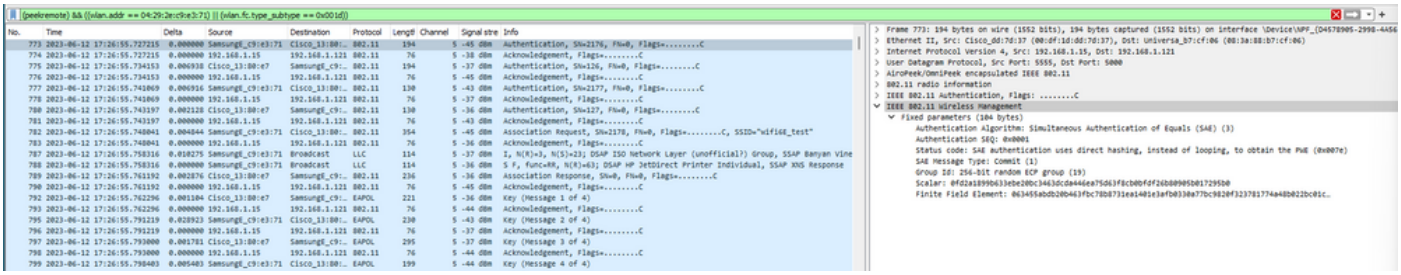


Detalles del cliente en WLC:

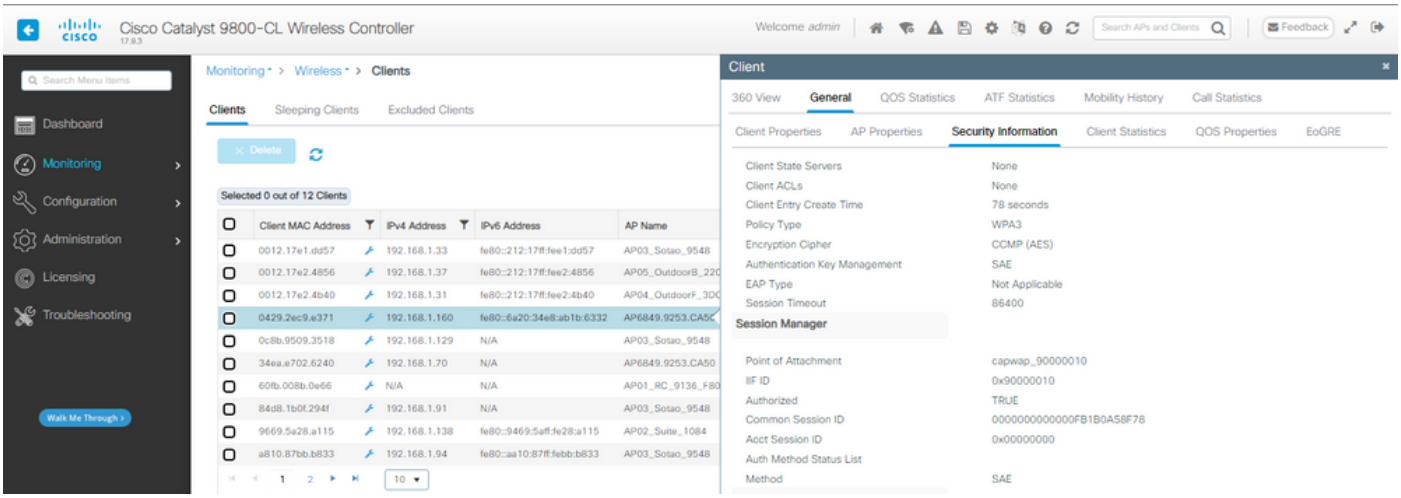


Samsung S23

Conexión OTA con enfoque en la información RSN del cliente:

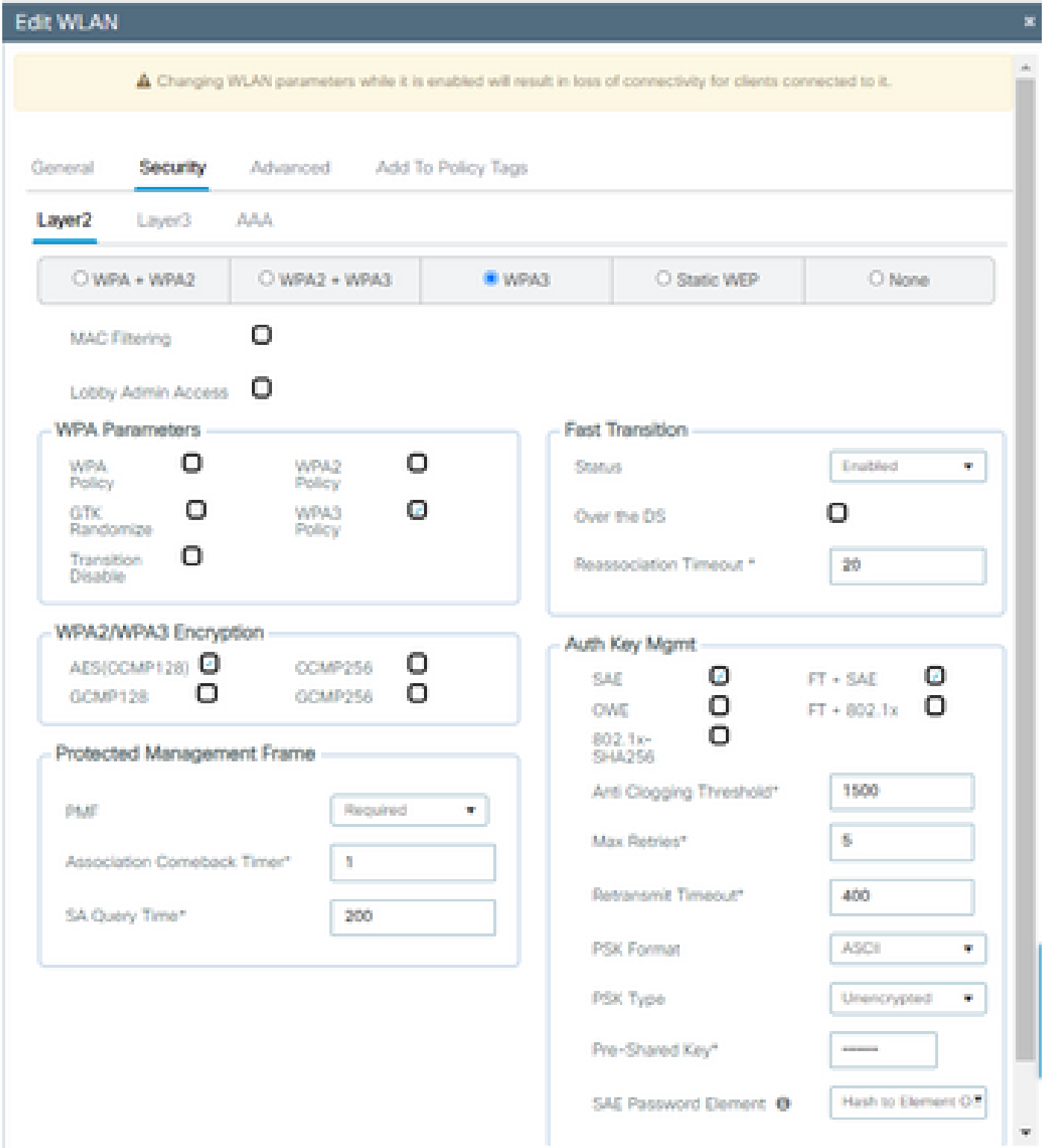


Detalles del cliente en WLC:



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

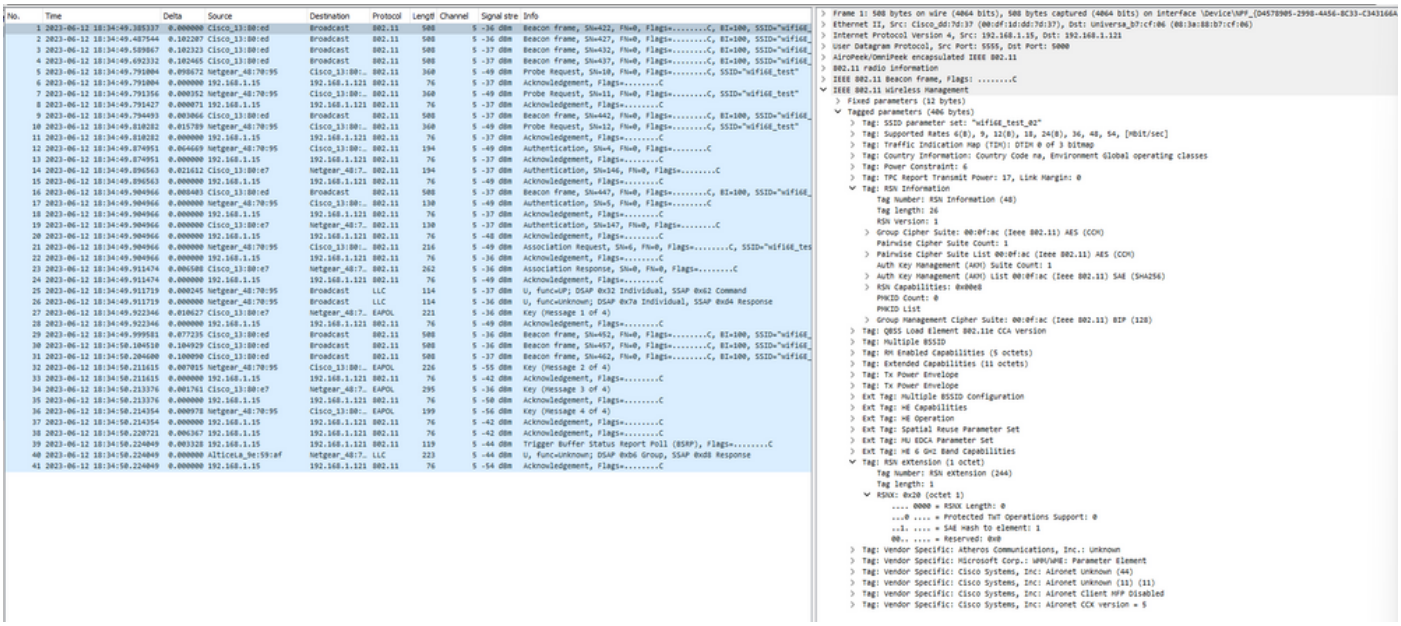
Configuración de seguridad WLAN:


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

Precaución: En la Administración de claves de autenticación, el WLC permite seleccionar FT+SAE sin SAE habilitado, sin embargo se observó que los clientes no pudieron conectarse. Active siempre ambas casillas de verificación SAE y FT+SAE si desea utilizar SAE con Fast Transition.

Ver en WLC GUI de los ajustes de seguridad WLAN:

Verificación de las balizas OTA:

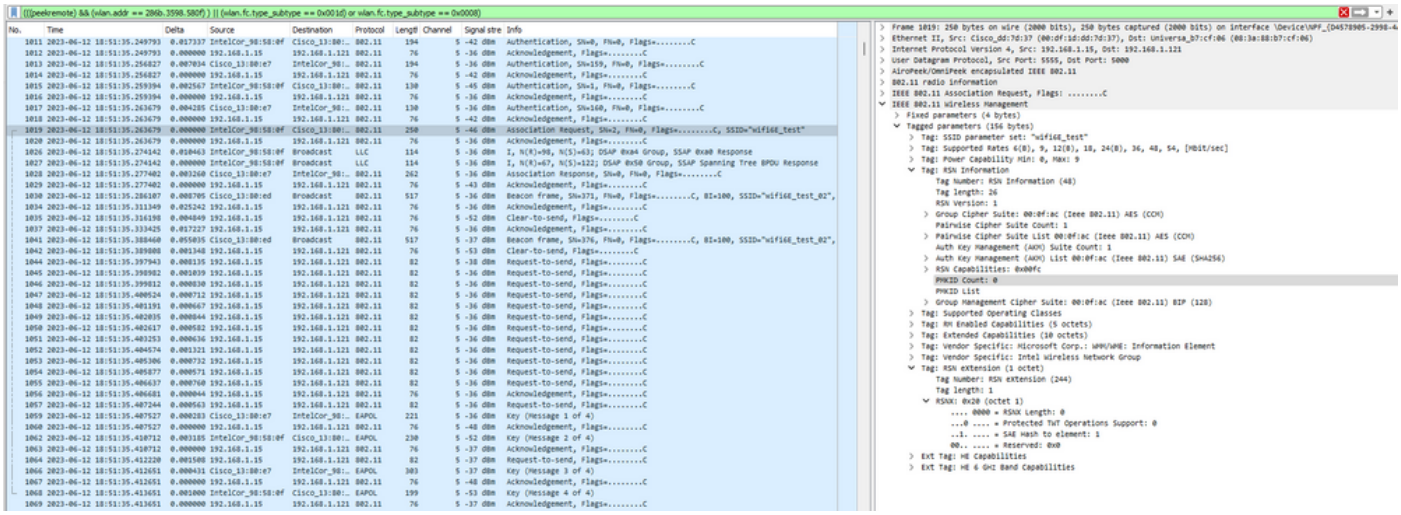


Indicadores WPA3 SAE + FT

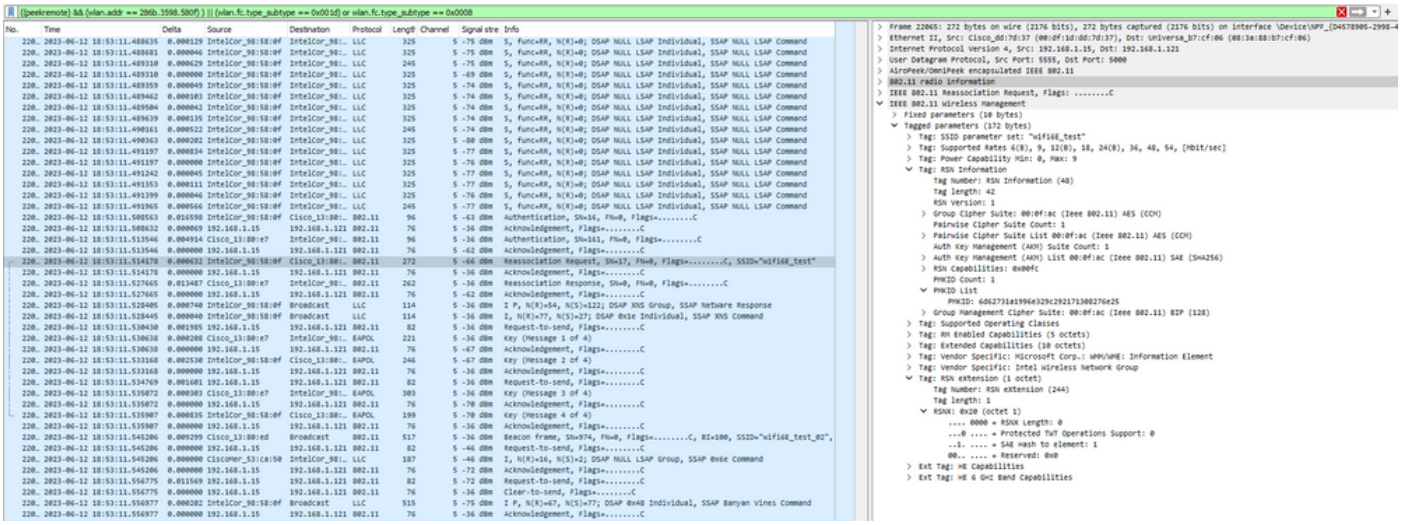
Aquí podemos observar clientes Wi-Fi 6E asociando:

Intel AX211

Conexión OTA con enfoque en la información RSN del cliente:

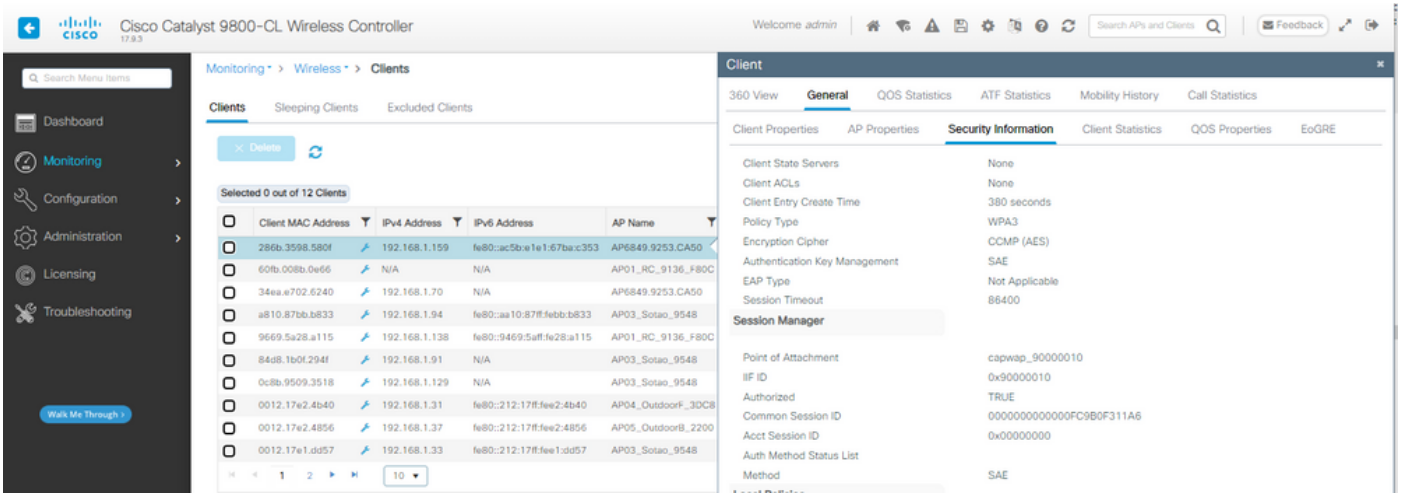


Evento de itinerancia en el que puede ver PMKID:



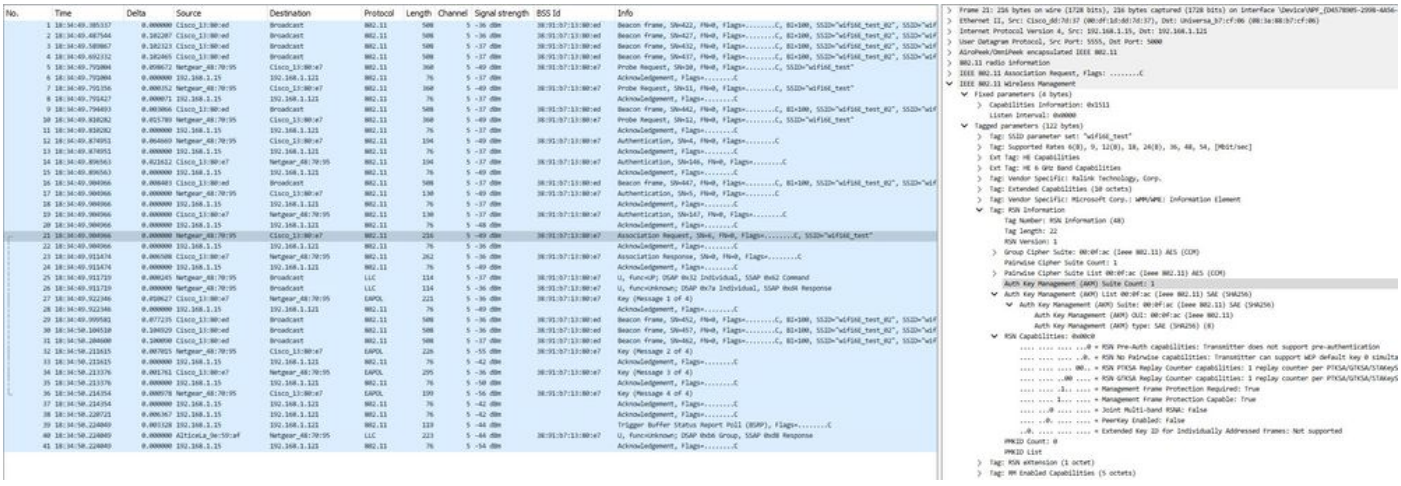
WPA3 SAE + FT Solicitud de reasociación

Detalles del cliente en WLC:



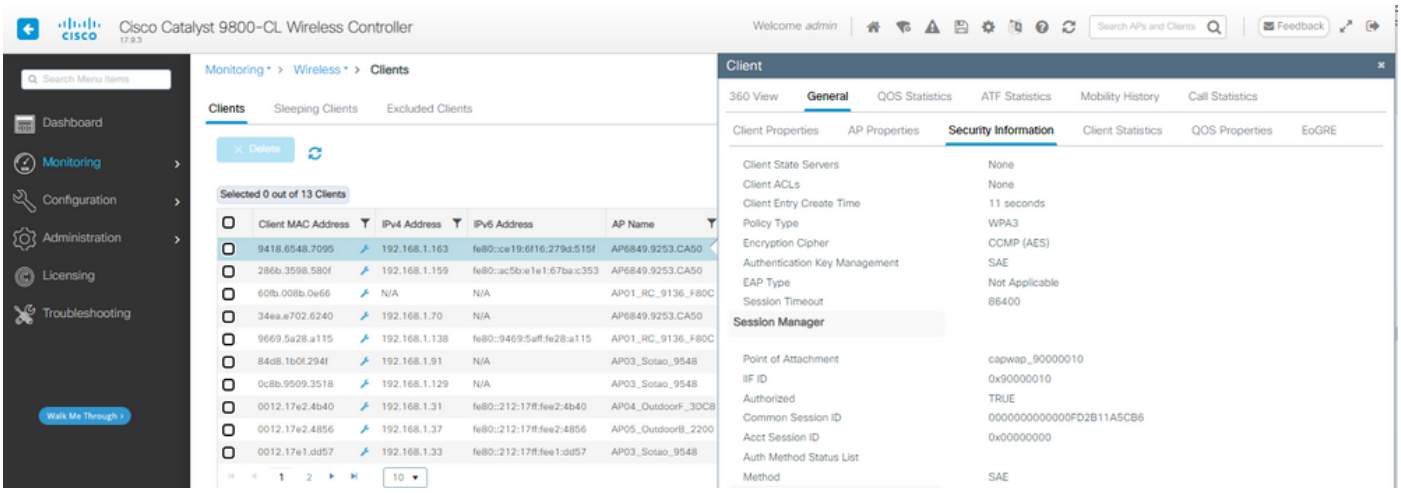
NetGear A8000

Conexión OTA con enfoque en la información RSN del cliente. Conexión inicial:



ssss

Detalles del cliente en WLC:



Píxel 6a

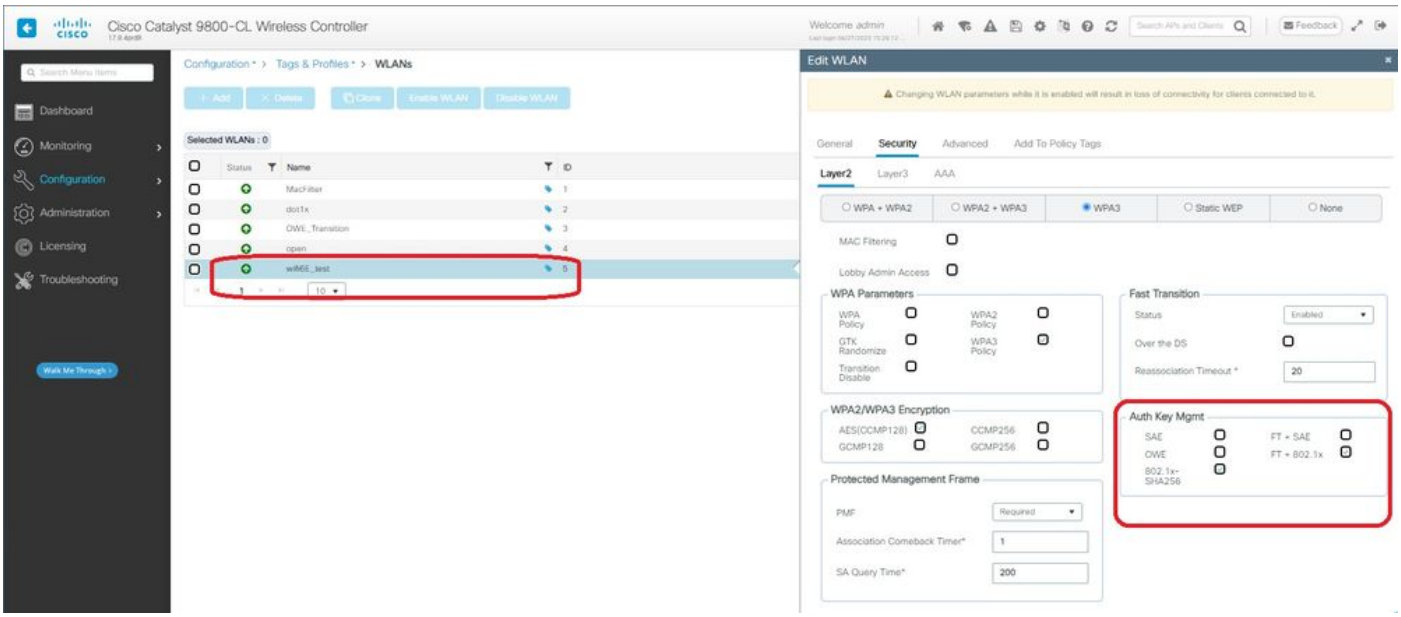
El dispositivo no pudo desplazarse cuando FT está habilitado.

Samsung S23

El dispositivo no pudo desplazarse cuando FT está habilitado.

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

Configuración de seguridad WLAN:



Configuración de seguridad WPA3 Enterprise 802.1x-SHA256 + FTWLAN

Ver en WLC GUI de los ajustes de seguridad WLAN:

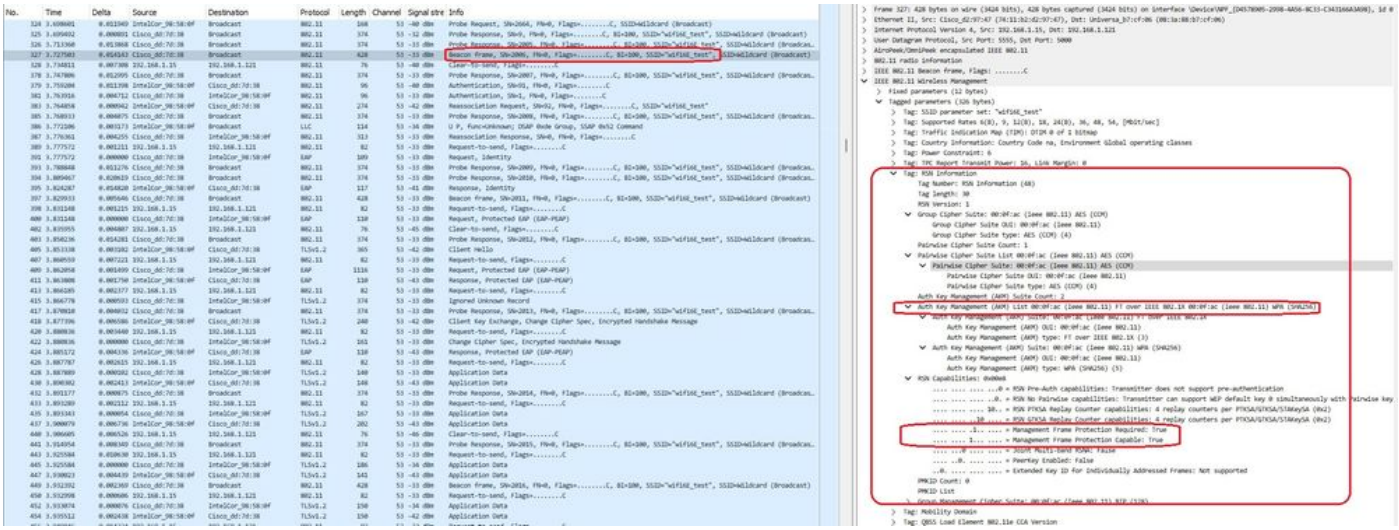
Aquí podemos ver los registros en directo de ISE que muestran las autenticaciones procedentes

de cada dispositivo:

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authenticat...	Authorizati...	Authorizati...	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

registros en vivo de ISE

Las balizas OTA se ven así:

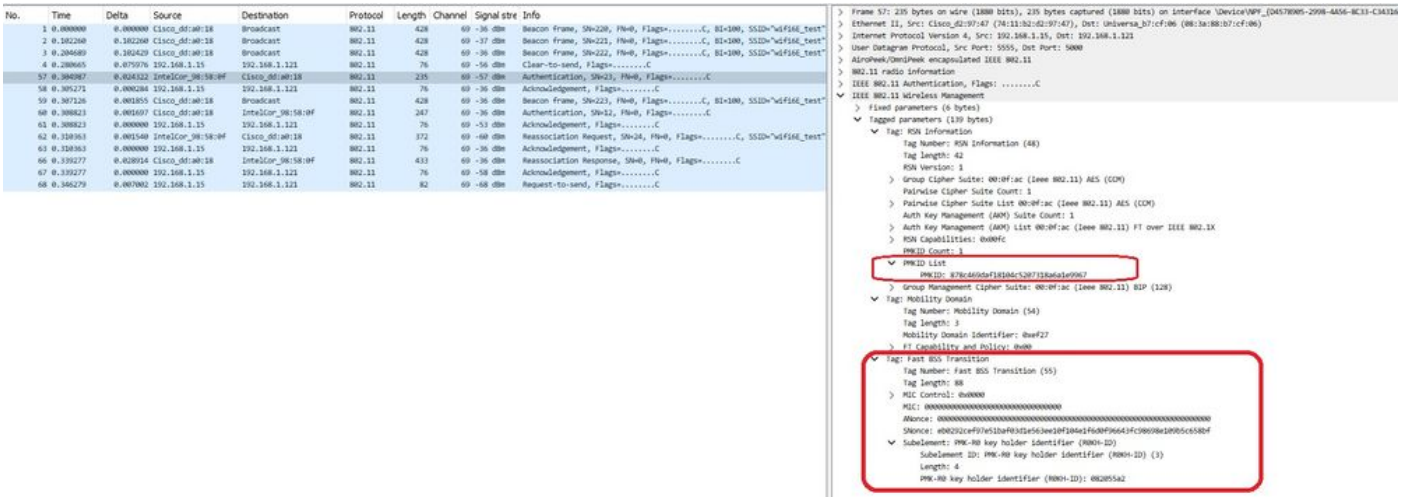


Baliza WPA3 Enterprise 802.1x +FT

Aquí podemos observar clientes Wi-Fi 6E asociando:

Intel AX211

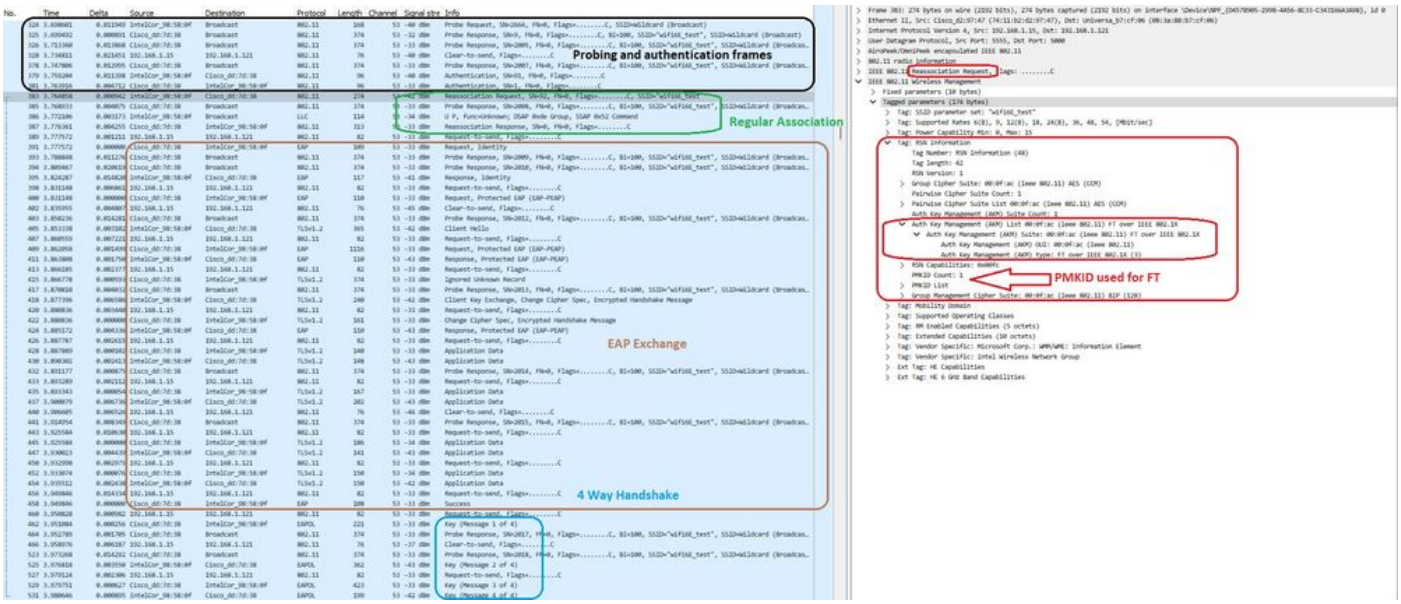
Conexión OTA con enfoque en la información RSN del cliente en un evento de roaming:



WPA3 Enterprise 802.1x + evento de roaming de la DF

Un comportamiento interesante ocurre si usted elimina manualmente el cliente de la WLAN (de la GUI del WLC por ejemplo). El cliente recibe una trama de desasociación pero intenta volver a conectarse al mismo AP y utiliza una trama de reasociación seguida por un intercambio EAP completo porque los detalles del cliente se eliminaron del AP/WLC.

Se trata básicamente del mismo intercambio de tramas que en un nuevo proceso de asociación. Aquí puede ver el intercambio de tramas:



Flujo de conexión WPA3 Enterprise 802.1x + FT Ax211

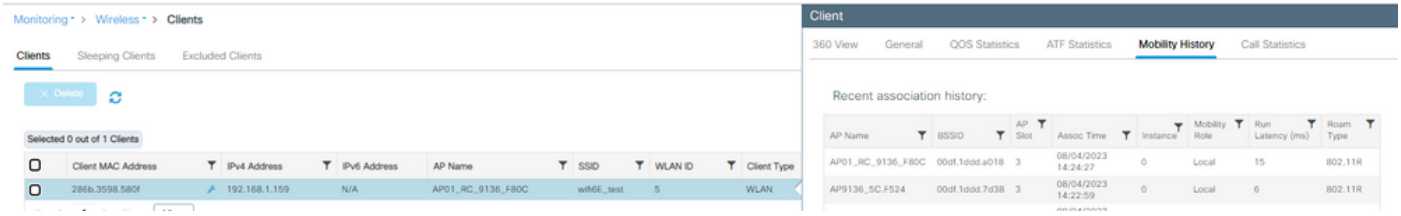
Detalles del cliente en WLC:

Detalles del cliente WPA3 Enterprise 802.1x + FT

Este cliente también se probó con FT en la DS y pudo desplazarse usando 802.11r:

Itinerancia AX211 con FT sobre DS

También podemos ver los eventos de itinerancia de FT:



WPA3 Enterprise con FT

Y el cliente traza desde wlc:

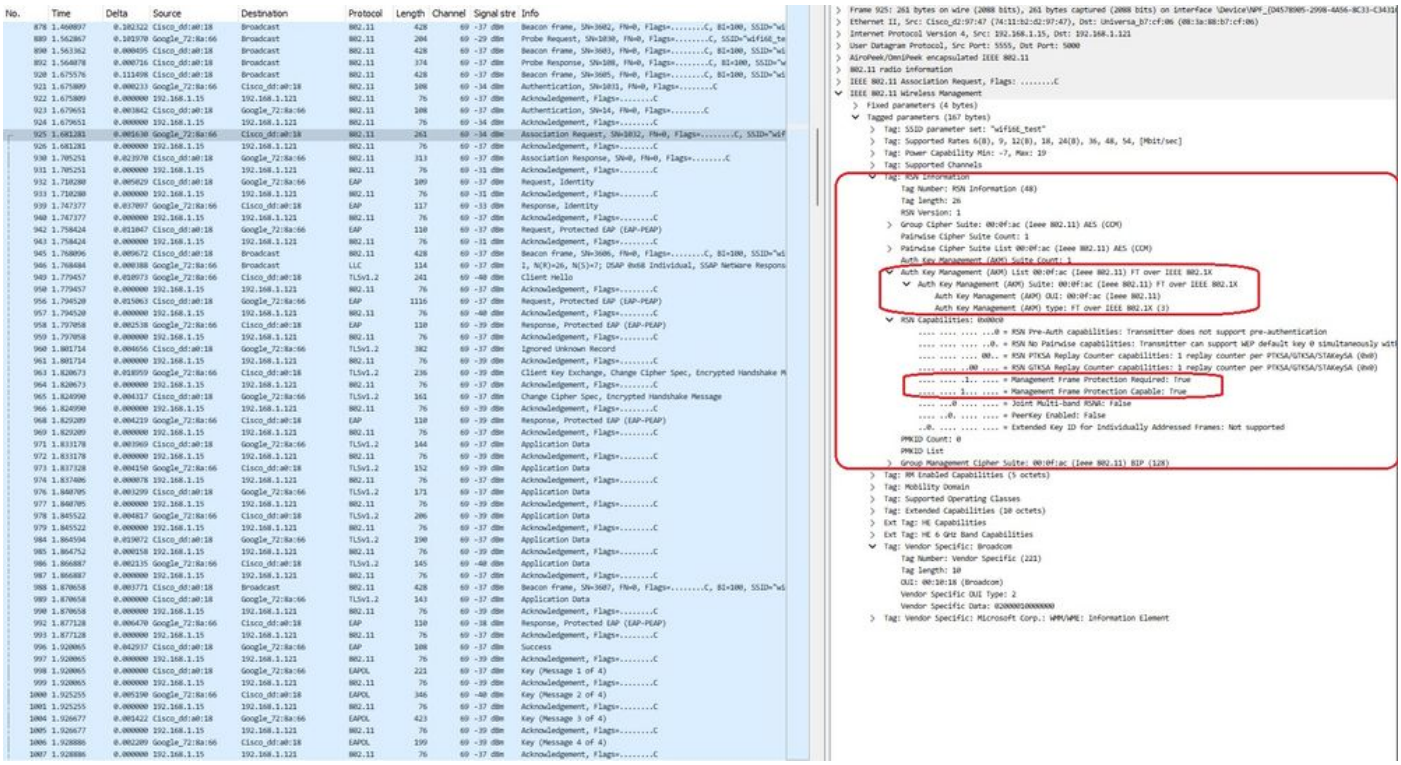
```
Logging display requested on 2023/08/04 14:27:55 (GMT) for Hostname: [eWLC-9800-01], Model: [C9800-CL-K9], Version: [17.09.03], SN: [9RY35HS10G9], MD_SN: [9RY35HS10G9]
2023/08/04 14:22:59.315300237 {wncd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 204b.3590.580f Re-Association received. BSSID 00df.1ddd.7d30, WLAN wifi6E_test, Slot 3 AP 00df.1ddd.7d30, AP9136_5C.F524, old BSSID 00df.1ddd.a018
2023/08/04 14:22:59.316044120 {wncd_x_R0-0}{1}: [dot11] [15210]: (note): MAC: 204b.3590.580f Association success. AID 33, Roaming = True, WGB = False, 11z = 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.a018 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.a018 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 14:22:59.321264052 {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.a018, 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, 11z = 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.a018 capwap IFID: 0x9000000e, Add mobiles sent: 1
2023/08/04 14:24:27.931505071 {wncd_x_R0-0}{1}: [client-orch-sm] [15210]: (note): MAC: 204b.3590.580f Mobility discovery triggered. Client mode: Local
2023/08/04 14:24:27.931511962 {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.a018 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 A8000

WPA3-Enterprise no se admite en este cliente.

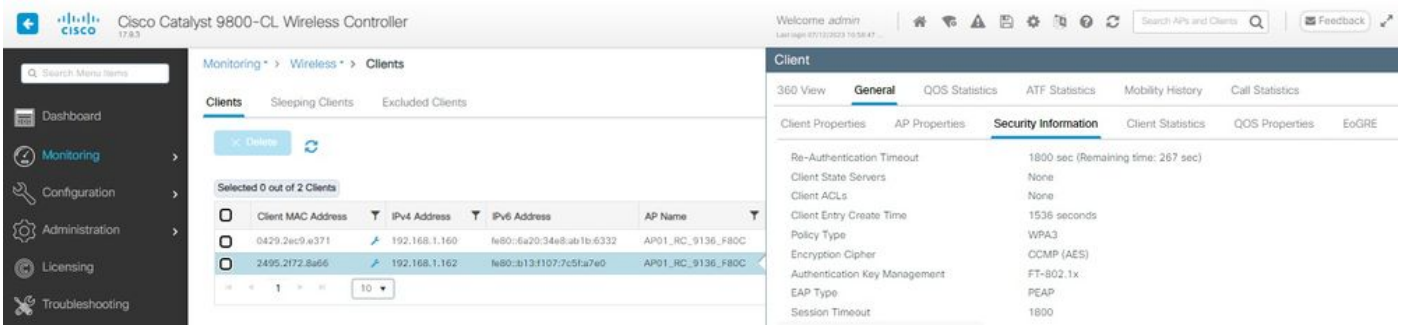
Píxel 6a

Conexión OTA con enfoque en la información RSN del cliente:



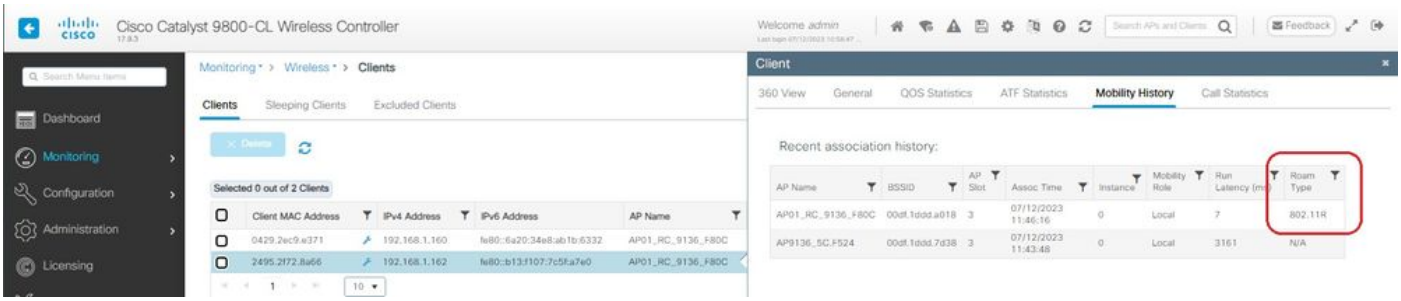
Asociación WPA3 Enterprise 802.1x + FT Pixel6a

Detalles del cliente en WLC:



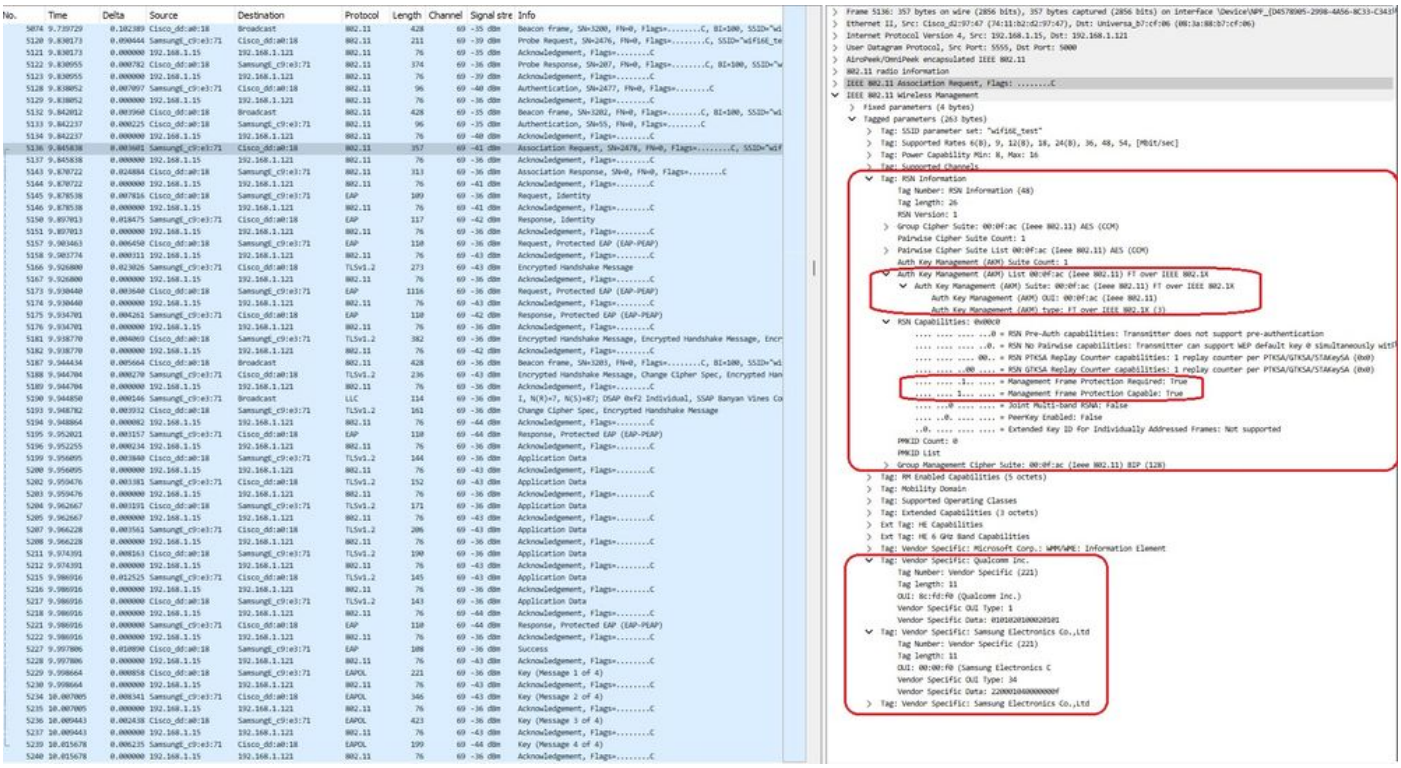
Detalles del cliente WPA3 Enterprise 802.1x + FT Pixel6a

Céntrese en el tipo de itinerancia "Over the Air", donde se puede ver el tipo de itinerancia 802.11R:



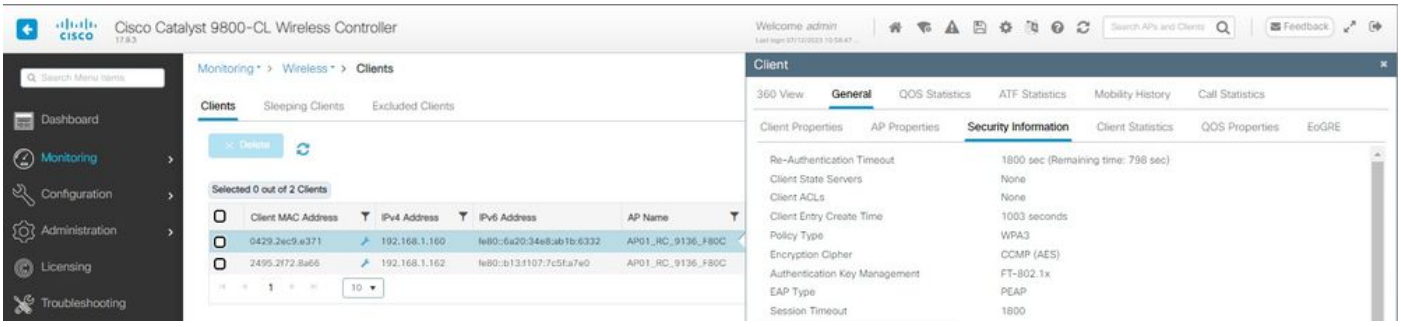
Samsung S23

Conexión OTA con enfoque en la información RSN del cliente:



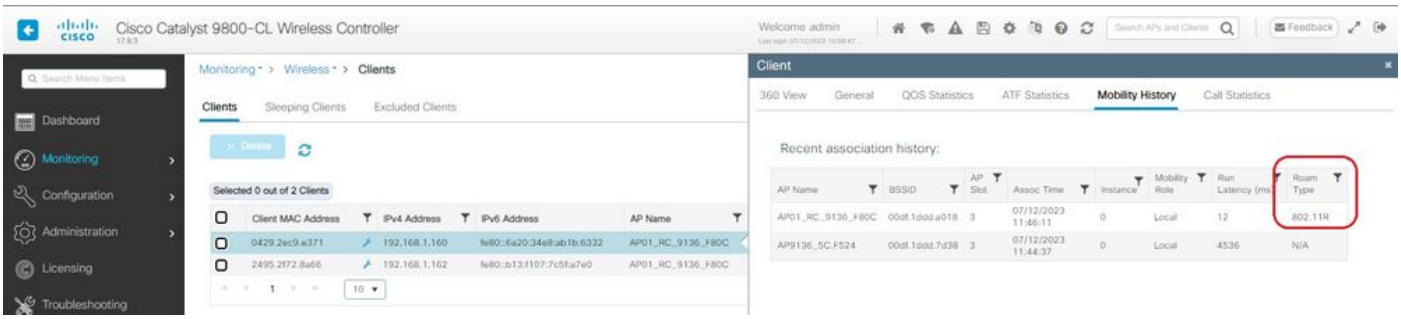
S23 Evento de roaming FToTA

Detalles del cliente en WLC:



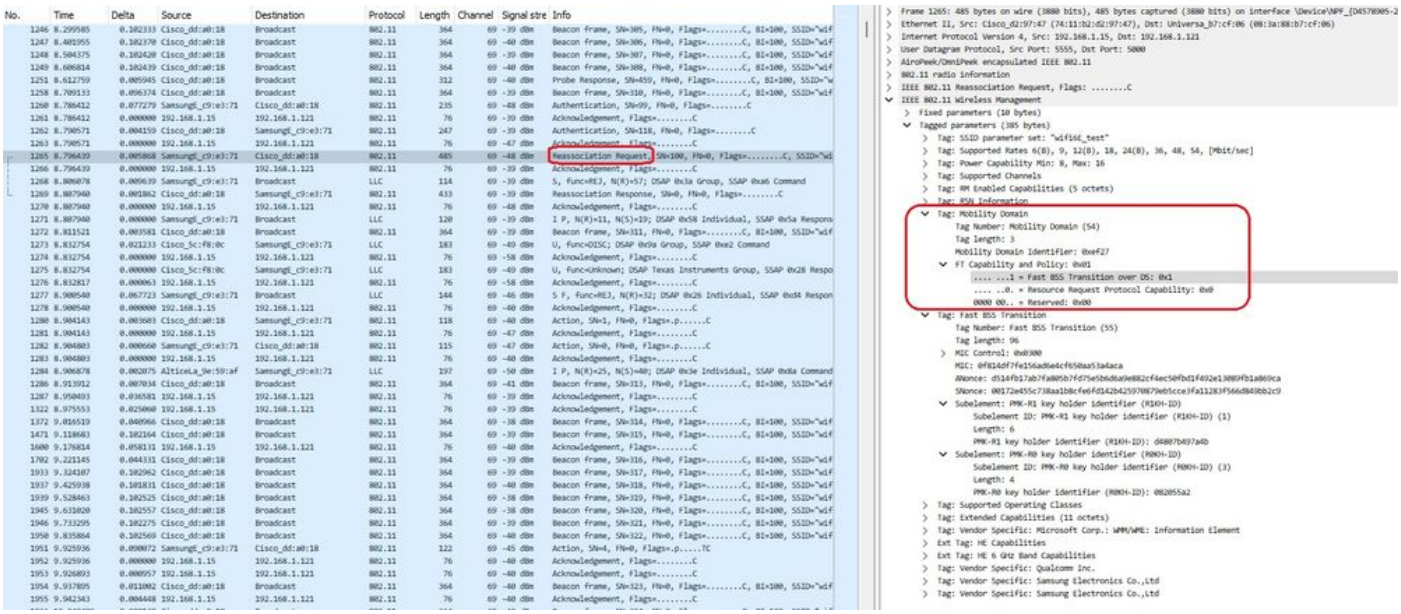
Propiedades del cliente S23

Céntrese en el tipo de itinerancia "Over the Air", donde se puede ver el tipo de itinerancia 802.11R:



S23 Roaming type 802.11R

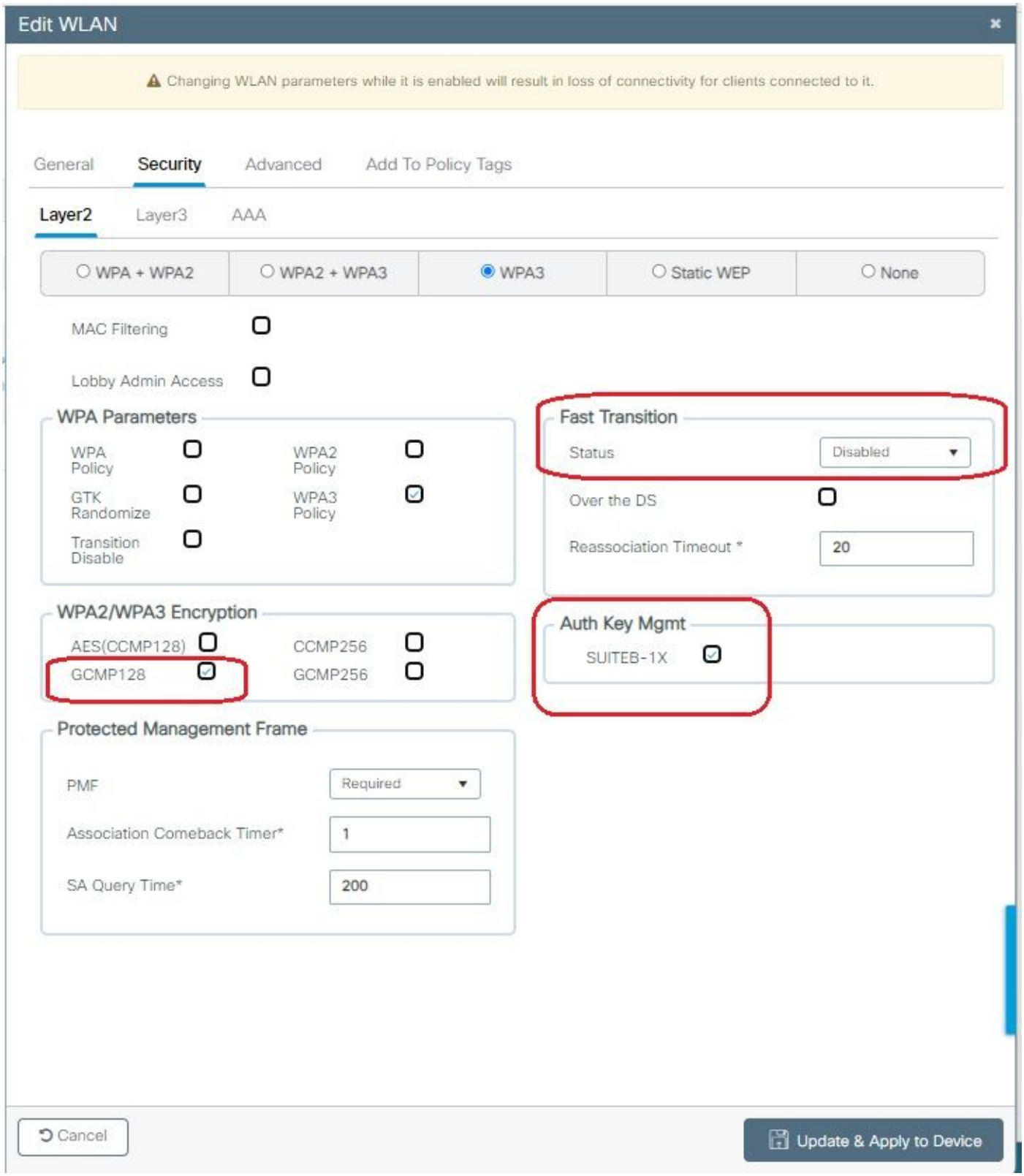
Este cliente también se probó con FT en la DS y pudo desplazarse usando 802.11r:



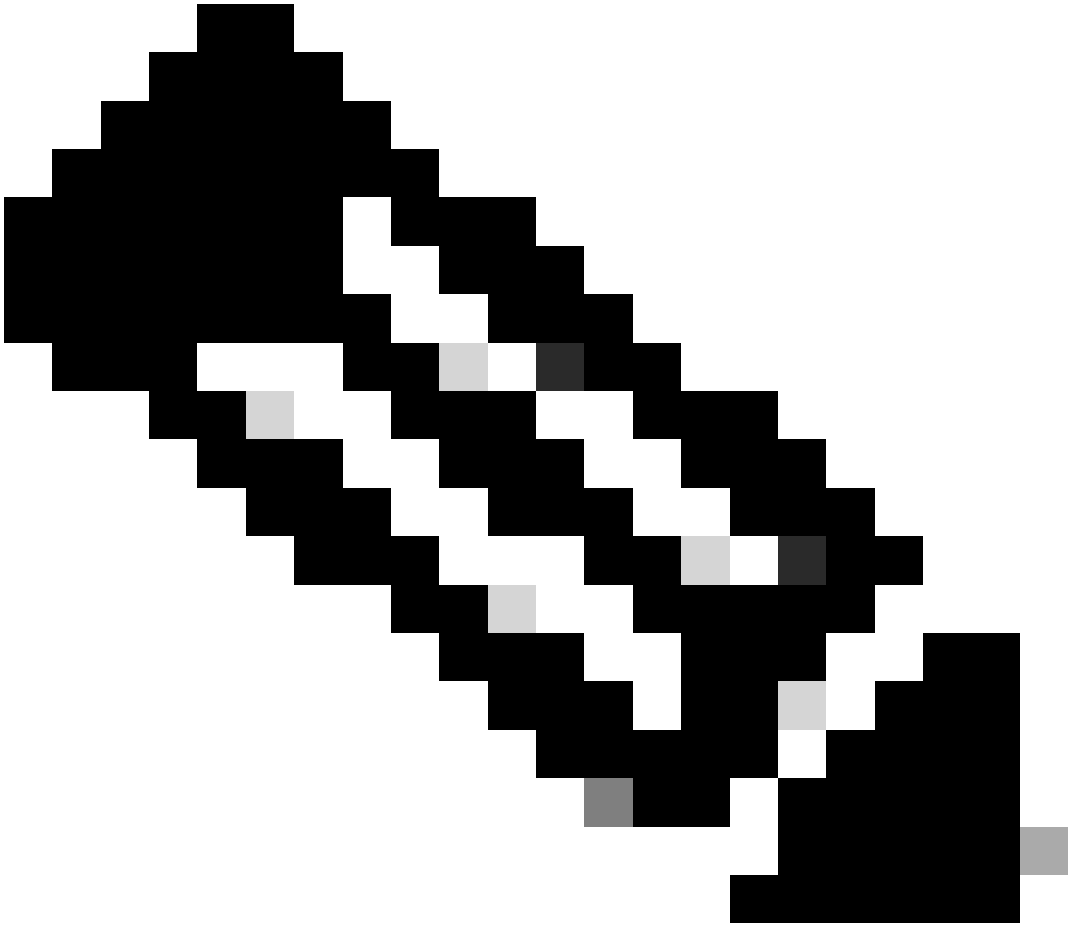
Paquetes FToDS de roaming S23

WPA3-Enterprise + cifrado GCMP128 + SUITEB-1X

Configuración de seguridad WLAN:



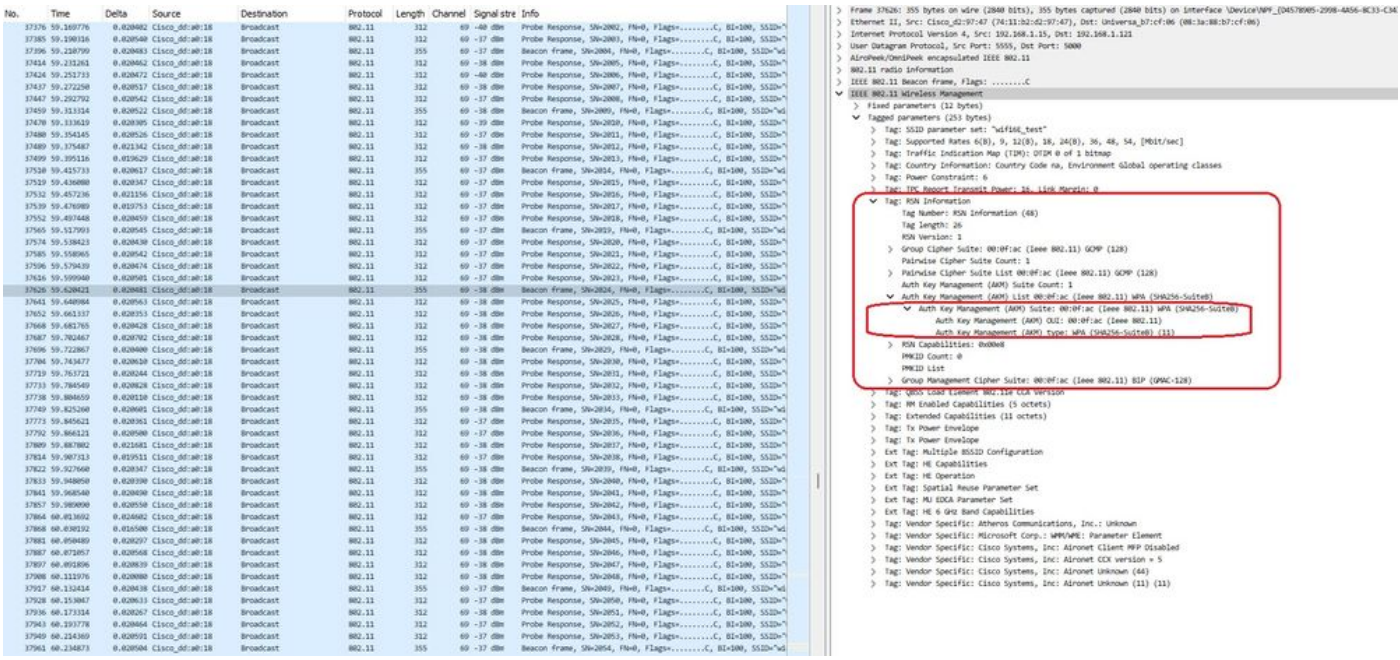
Configuración de seguridad de WPA3 Enterprise SuiteB-1X



Nota: FT no es compatible con SUITEB-1X

Ver en WLC GUI de los ajustes de seguridad WLAN:

Verificación de las balizas OTA:

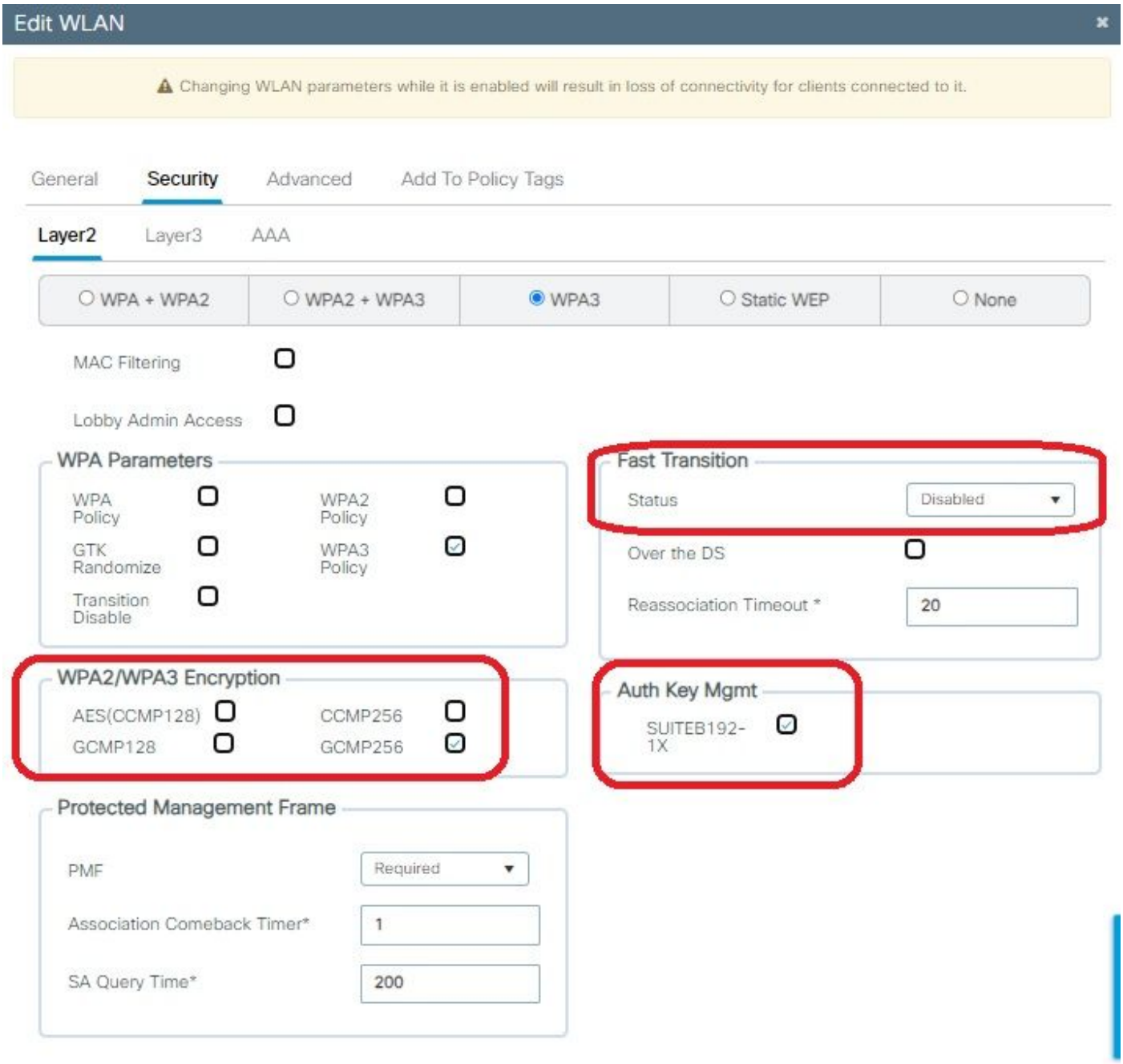


WPA3 Enterprise SuiteIndicador B-1X

Ninguno de los clientes probados pudo conectarse a la WLAN mediante SuiteB-1X, lo que confirma que ninguno admite este método de seguridad.

Cifrado WPA3-Enterprise + GCMP256 + SUITEB192-1X

Configuración de seguridad WLAN:



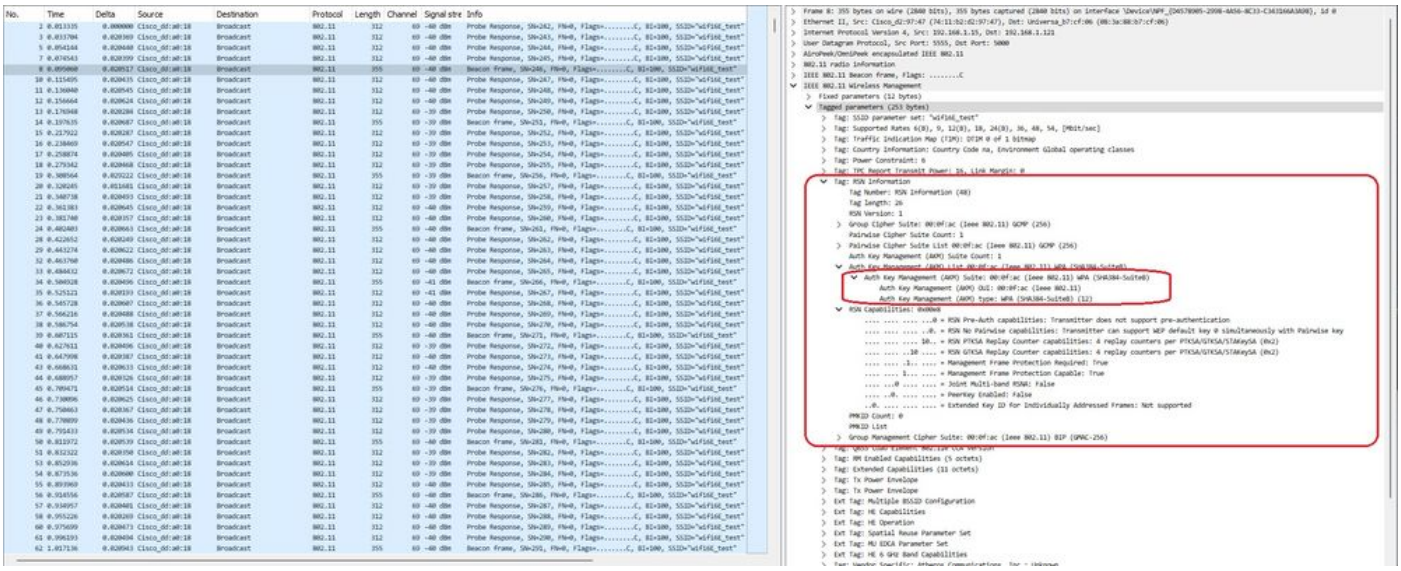
Parámetros de seguridad de WPA3 Enterprise SUITEB192-1x

Nota: FT no es compatible con GCMP256+SUITEB192-1X.

WLAN en la lista WLANs de la GUI del WLC:

WLAN utilizada para las pruebas

Verificación de las balizas OTA:

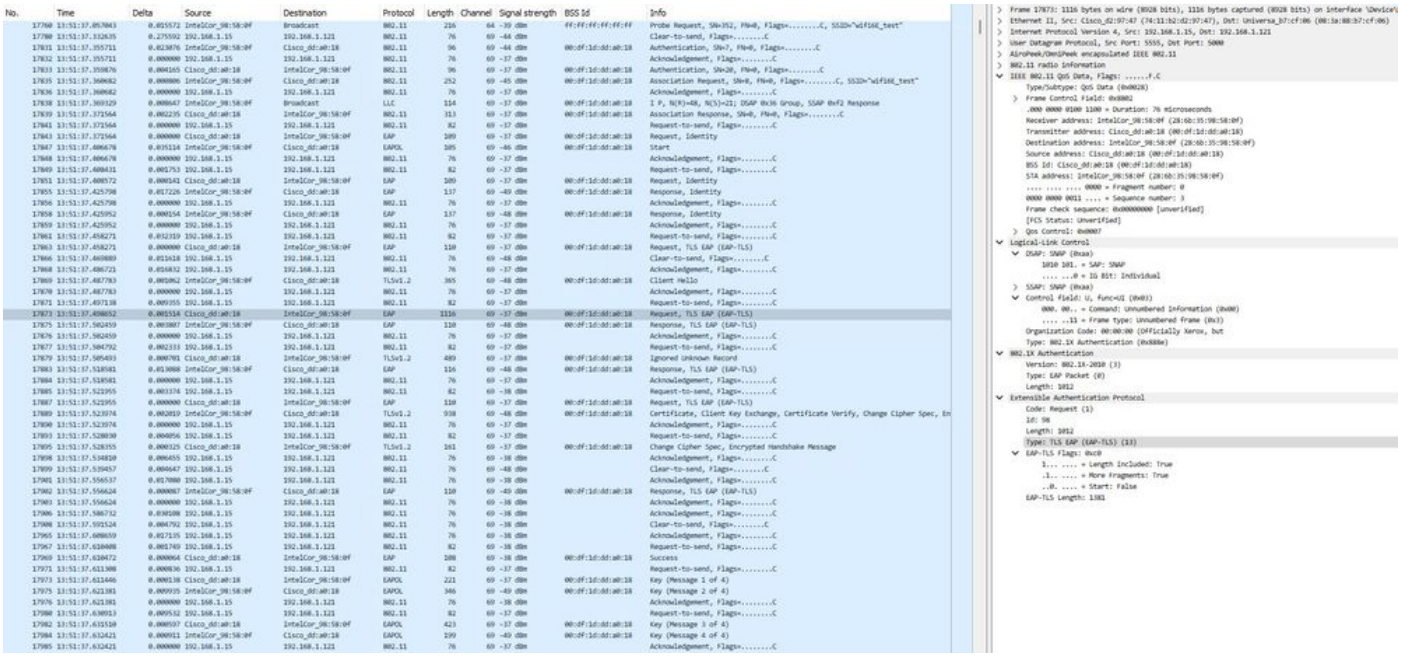


Balizas WPA3 Enterprise SUITEB192-1x

Aquí podemos observar clientes Wi-Fi 6E asociando:

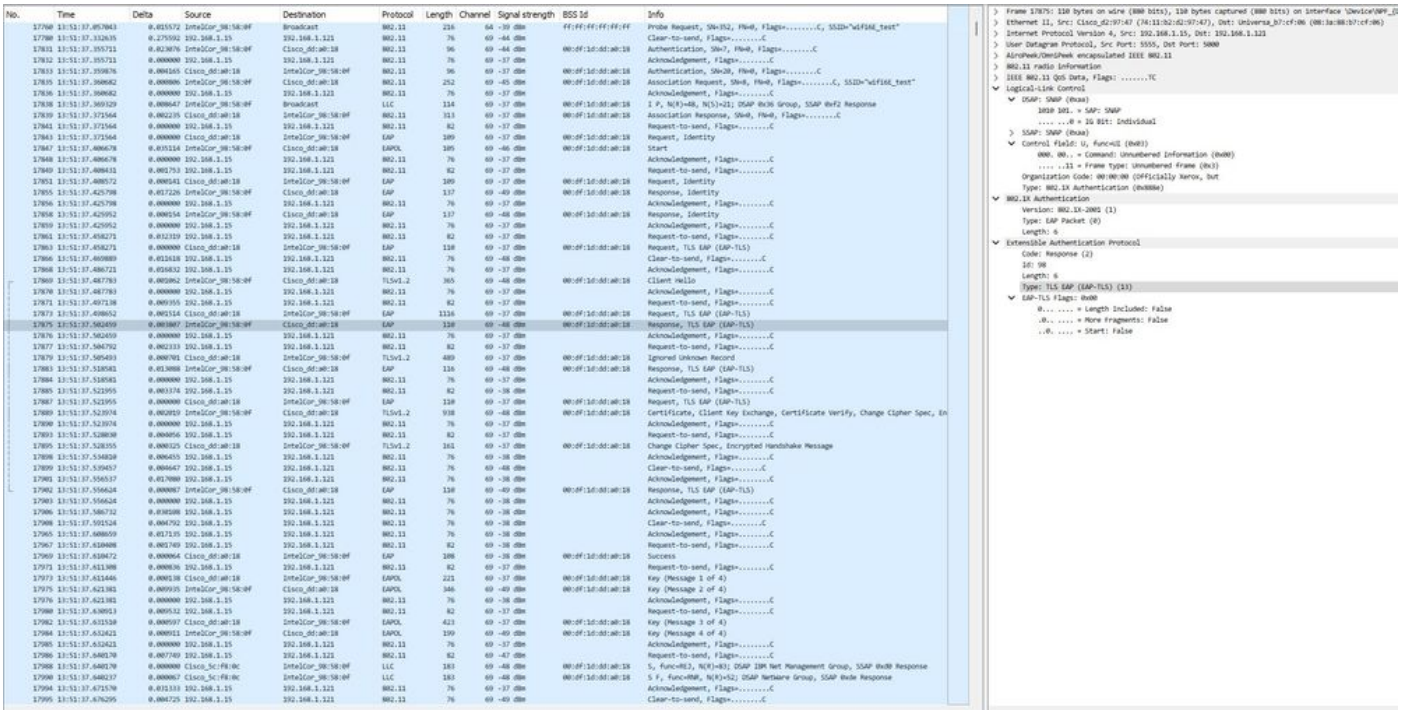
Intel AX211

Conexión OTA con enfoque en la información RSN del cliente:



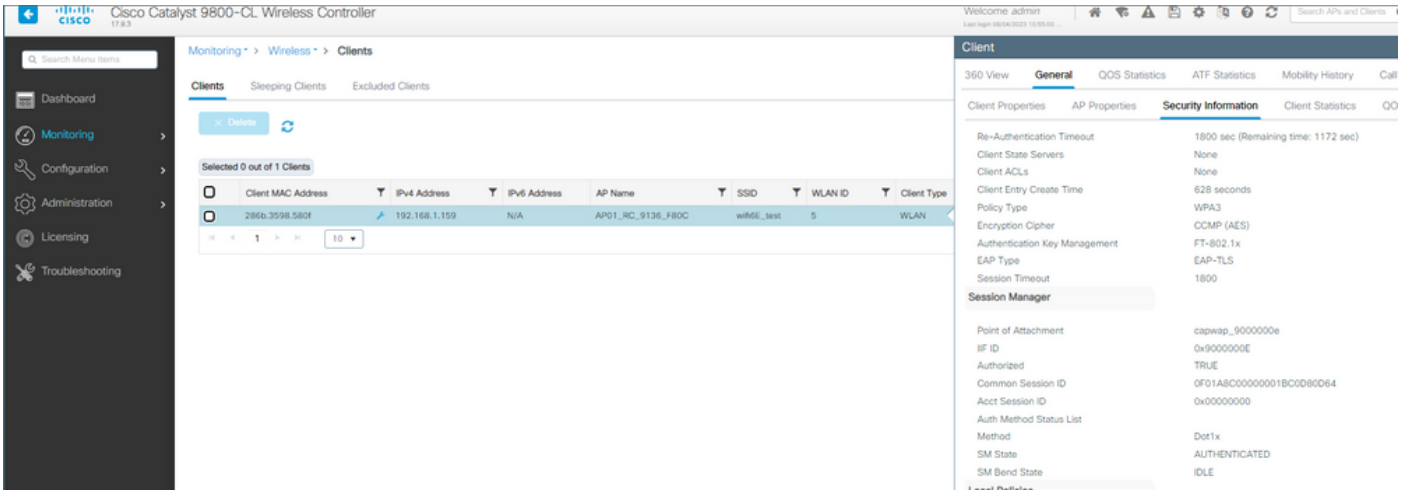
WPA3 Enterprise con asociación EAP-TLS con cliente Intel AX211 e información RSN

Y el intercambio EAP-TLS:



WPA3 Enterprise con asociación EAP-TLS con cliente Intel AX211 y enfoque EAP-TLS

Detalles del cliente en WLC:



WPA3 Enterprise con detalles del cliente EAP-TLS

NetGear A8000

WPA3-Enterprise no se admite en este cliente.

Píxel 6a

En la fecha de escritura de este documento, este cliente no podía conectarse a WPA3 Enterprise mediante EAP-TLS.

Se trataba de un problema relacionado con el cliente que se estaba tratando y, tan pronto como se resolviera, se actualizaría el presente documento.

Samsung S23

En la fecha de escritura de este documento, este cliente no podía conectarse a WPA3 Enterprise mediante EAP-TLS.

Se trataba de un problema relacionado con el cliente que se estaba tratando y, tan pronto como se resolviera, se actualizaría el presente documento.

Conclusiones de seguridad

Después de todas las pruebas anteriores, estas son las conclusiones resultantes:

Protocolo	Cifrado	AKM	Cifrado AKM	Método EAP	FT-OverTA	FT-OverDS	Intel AX211	Samsung/Goo Android
DEBER	AES-CCMP128	DEBER	NA.	NA.	NA	NA	Supported	Supported
SAE	AES-CCMP128	SAE (sólo H2E)	SHA256	NA.	Supported	Supported	Compatible: sólo H2E y FT-TA	Compatible: s H2E. Error de FT. Error de FT-o
Empresa	AES-CCMP128	802.1x-SHA256	SHA256	PEAP/FAST/TLS	Supported	Supported	Compatible: SHA256 y FT-TA/oDS No compatible: EAP-FAST	Compatible: SHA256 y FT-TA, FT-oDS (S23) No compatible EAP-FAST, F oDS (Pixel6a)
Empresa	GCMP128	SuiteB-1x	SHA256-SuiteB	PEAP/FAST/TLS	Not Supported	Not Supported	Not Supported	Not Supporte
Empresa	GCMP256	SuiteB-192	SHA384-SuiteB	TLS	Not Supported	Not Supported	NA/TBD	NA/TBD

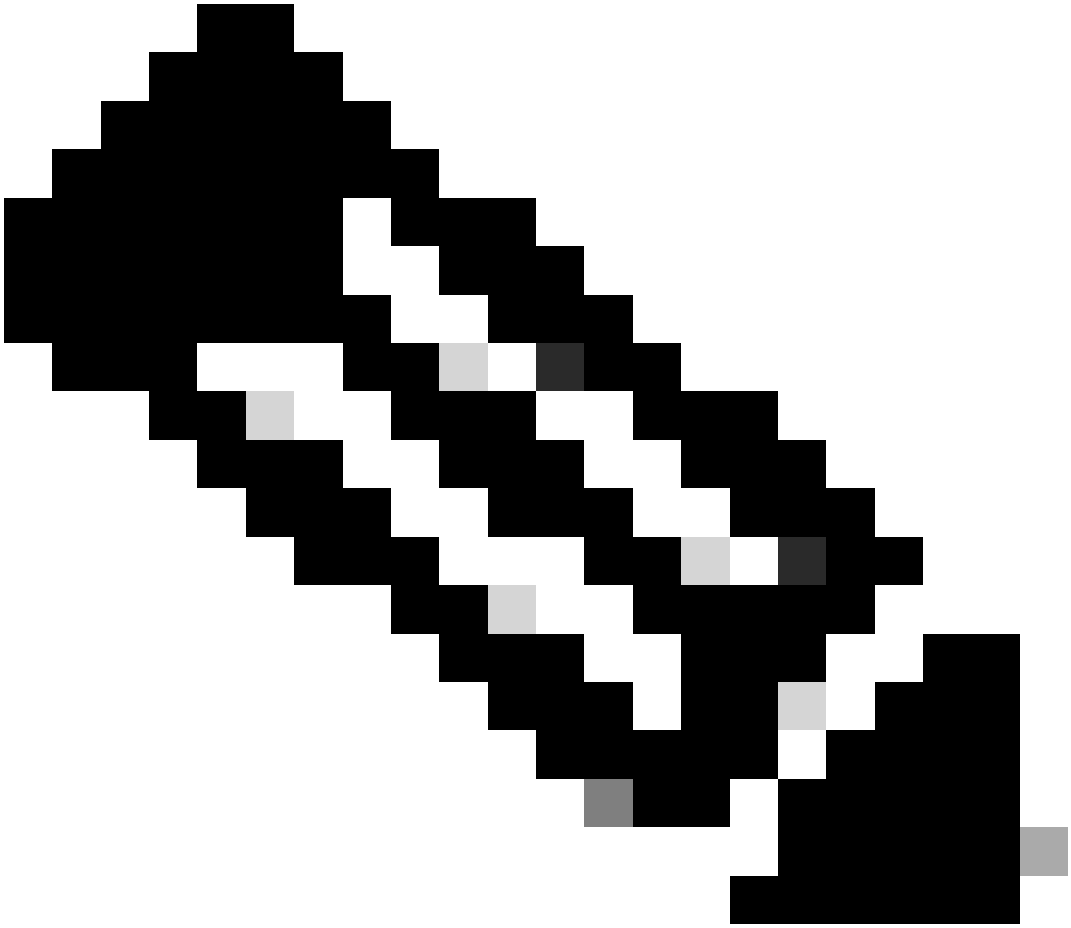
Troubleshoot

La solución de problemas utilizada en este documento se basó en el documento en línea:

Solucionar problemas de COS AP

La pauta general para la resolución de problemas es recolectar el seguimiento de RA en el modo de depuración del WLC usando la dirección MAC del cliente asegurándose de que el cliente se conecte usando la MAC del dispositivo y no una dirección MAC aleatoria.

Para la resolución de problemas por el aire, la recomendación es utilizar el AP en el modo del sabueso que captura el tráfico en el canal del AP que sirve al cliente.



Nota: Consulte Información Importante sobre los Comandos Debugantes de utilizar los comandos debug.

Información Relacionada

¿Qué es Wi-Fi 6E?

¿Qué es Wi-Fi 6 frente a Wi-Fi 6E?

Guía rápida de Wi-Fi 6E

Wi-Fi 6E: el siguiente gran capítulo del informe técnico sobre Wi-Fi

Cisco Live - Arquitectura de la red inalámbrica de última generación con puntos de acceso Catalyst Wi-Fi 6E

Guía de configuración del software del controlador inalámbrico Cisco Catalyst serie 9800 17.9.x

Guía de implementación de WPA3

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).