

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

## Contenido

---

### [Introducción](#)

### [Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

### [Antecedentes](#)

[Seguridad Wi-Fi 6E](#)

[WPA3](#)

[Conjunto de niveles: modos WPA3](#)

[AP Cisco Catalyst Wi-Fi 6E](#)

[Configuración de seguridad admitida por clientes](#)

### [Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración base](#)

### [Verificación](#)

[Verificación de seguridad](#)

[WPA3 - AES \(CCMP128\) + OWE](#)

[WPA3 - AES \(CCMP128\) + OWE con modo de transición](#)

[WPA3-Personal: AES \(CCMP128\) + SAE](#)

[WPA3-Personal: AES \(CCMP128\) + SAE + FT](#)

[WPA3-Enterprise + AES \(CCMP128\) + 802.1x-SHA256 + FT](#)

[WPA3-Enterprise + cifrado GCMP128 + SUITEB-1X](#)

[Cifrado WPA3-Enterprise + GCMP256 + SUITEB192-1X](#)

[Conclusiones de seguridad](#)

### [Troubleshoot](#)

### [Información Relacionada](#)

---

## 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 (abierto) 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:

**WPA2/WPA3 Encryption**

AES(CCMP128)	<input checked="" type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>	GCMP256	<input type="checkbox"/>

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.

## Protected Management Frame

PMF

Required

Association Comeback Timer\*

1

SA Query Time\*

200

Opciones de PMF

Administración de claves de autenticación

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

## Auth Key Mgmt

SAE  FT + SAE

OWE  FT + 802.1x

802.1x-  
SHA256

Anti Clogging Threshold\*

Max Retries\*

Retransmit Timeout\*

PSK Format

PSK Type

Pre-Shared Key\*

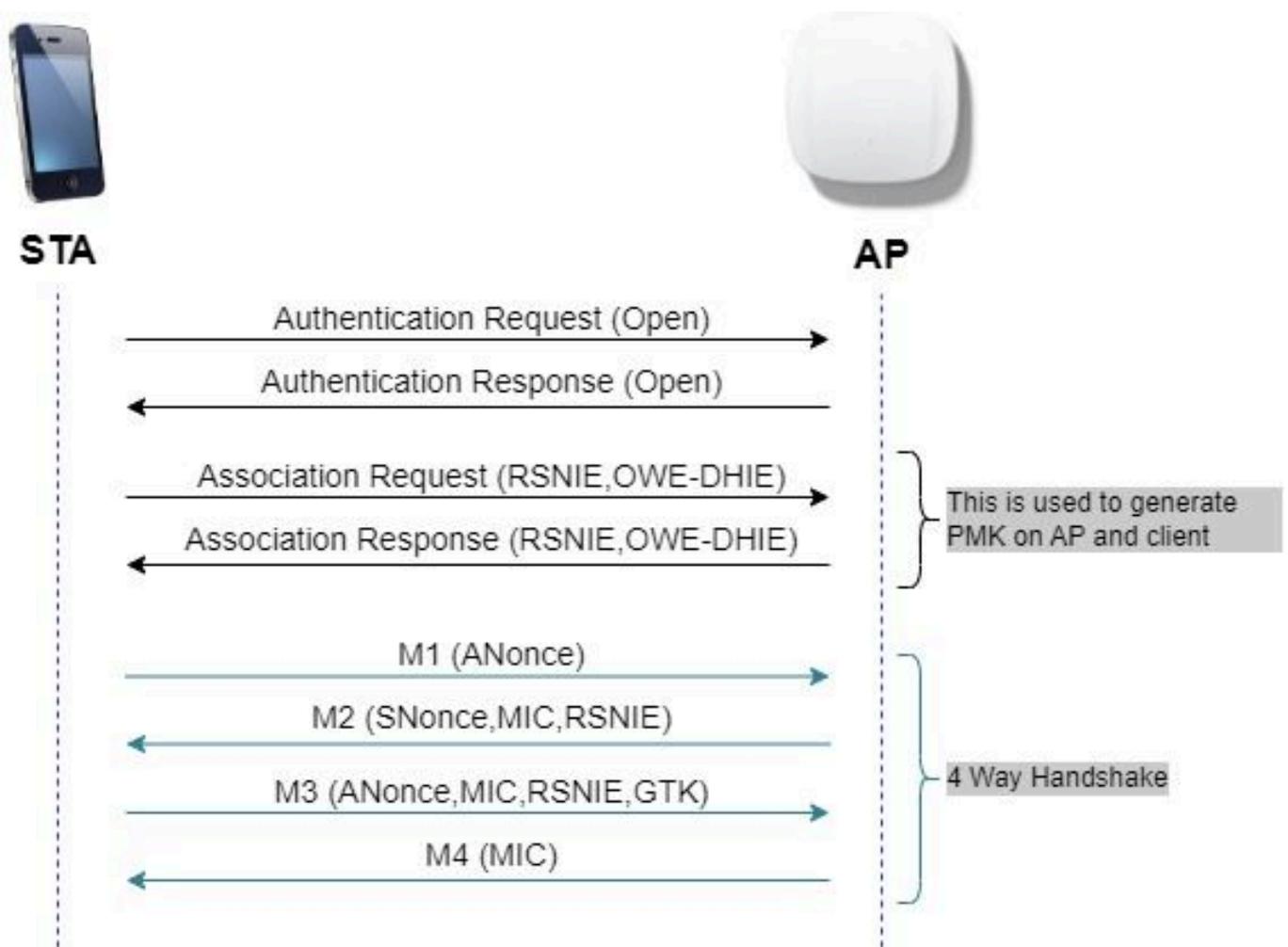
SAE Password Element ⓘ

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.

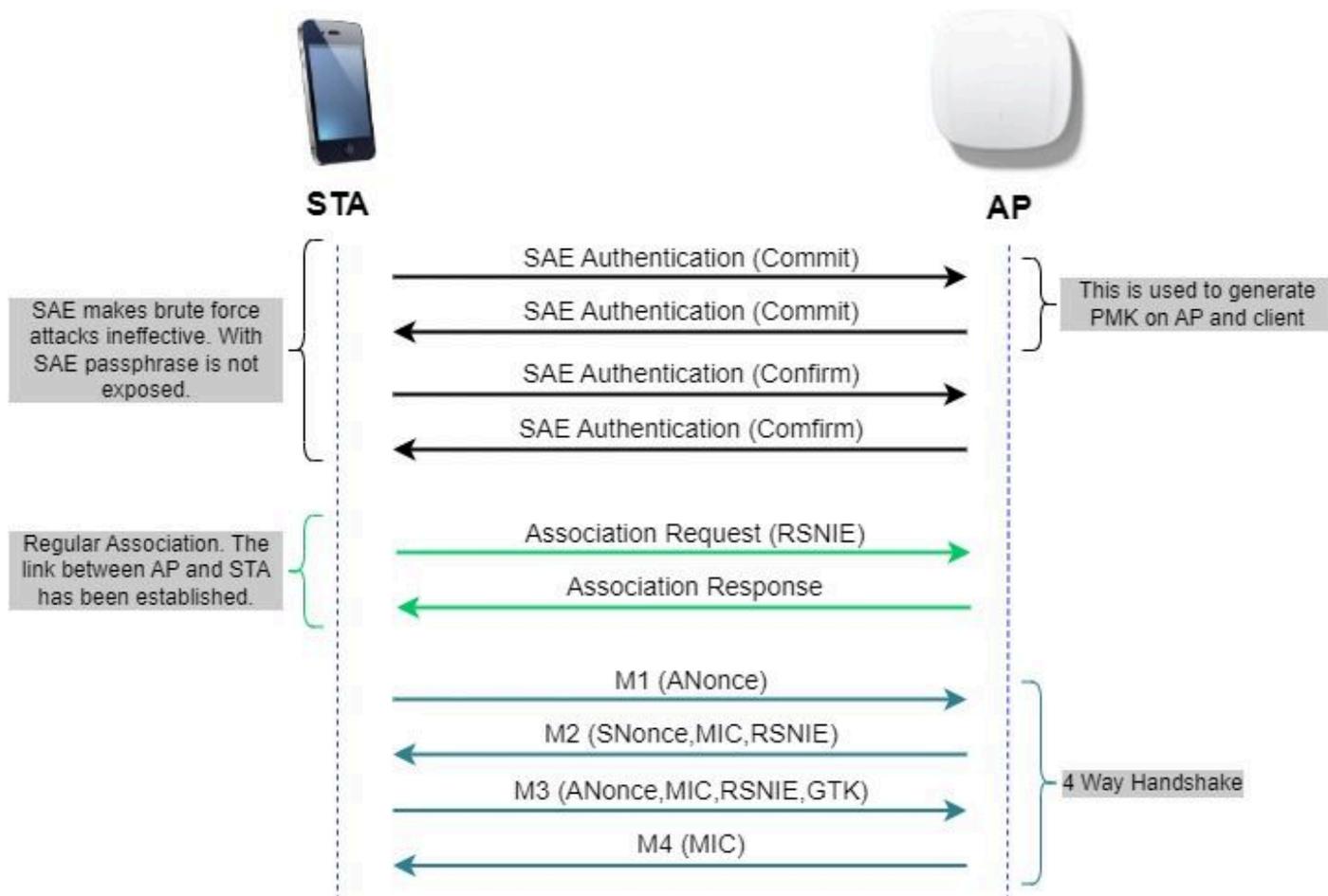
SAE con H2E es obligatorio para WPA3 y Wi-Fi 6E.

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.

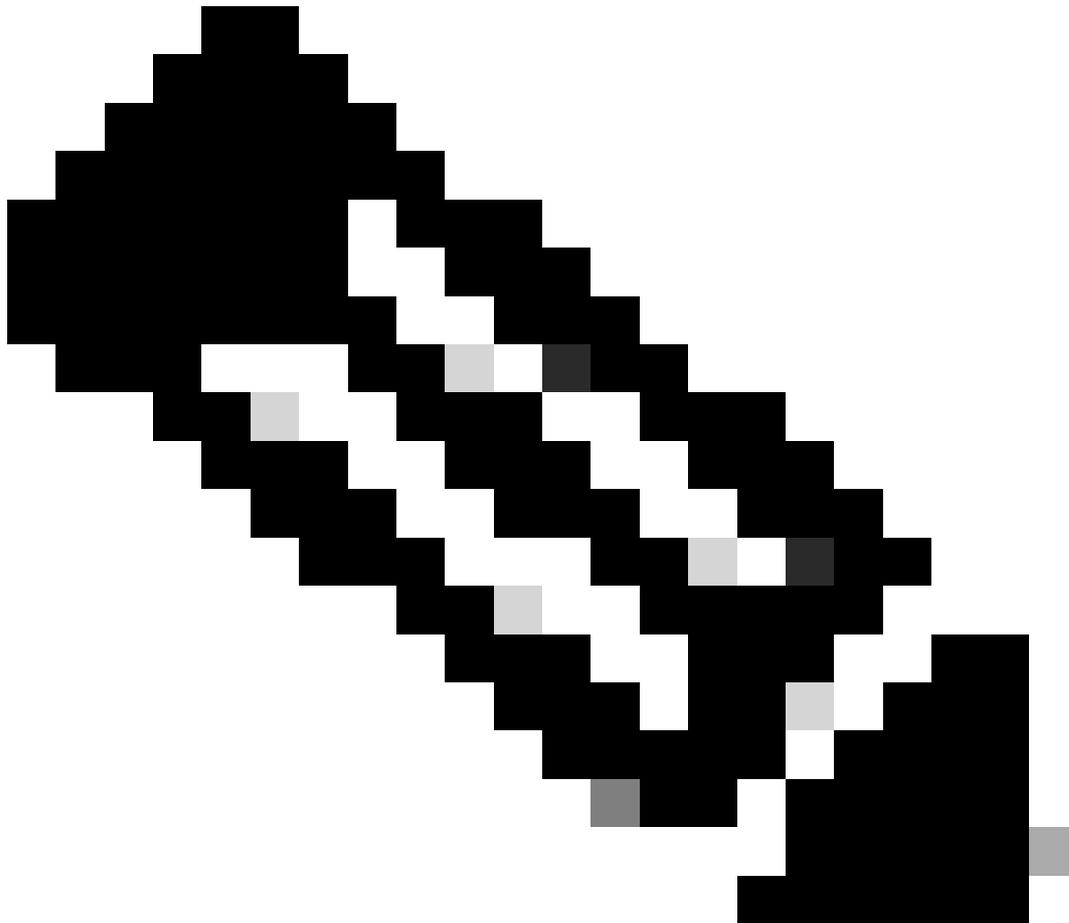
Si STA utiliza Hunting-and-Pecking (HnP), todo el intercambio SAE permanece sin cambios.

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.

---

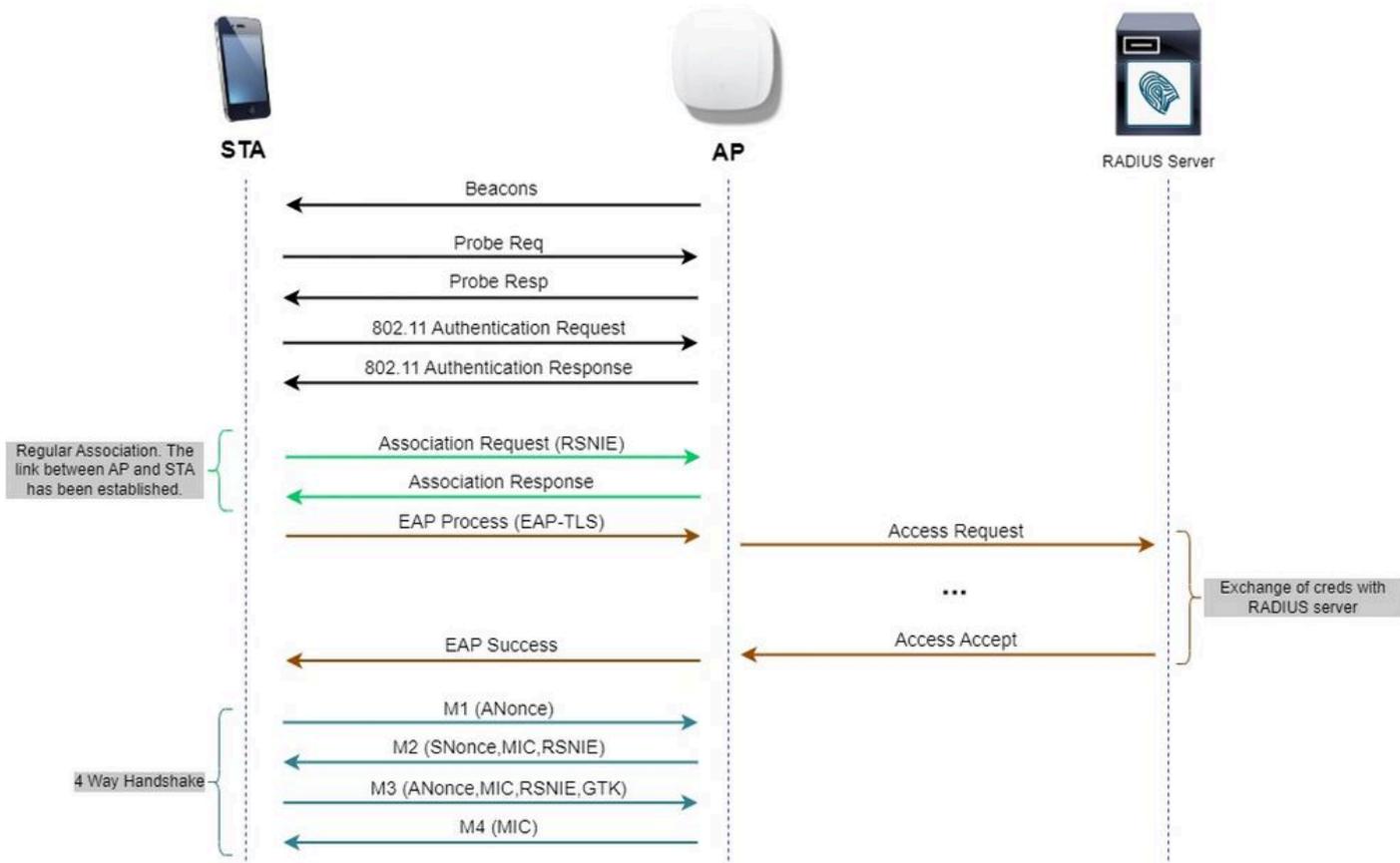


Nota: 6 GHz sólo admite el método PWE SAE de hash a elemento.

---

### 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

Ideal for Small to Medium-sized deployments	Best In Class, Flexibility		Mission Critical, Performance
 <p><b>CW9162</b></p> <ul style="list-style-type: none"> <li>• 2x2 + 2x2 + 2x2</li> <li>• 2.5 Gbps mGig</li> <li>• Power Options: PoE, DC Power</li> <li>• IoT ready + Bluetooth 5.x</li> <li>• Partial iCAP</li> <li>• USB - 4.5 W</li> </ul> <p><small>Available with IOS-XE 17.9.2</small></p>	 <p><b>CW9164</b></p> <ul style="list-style-type: none"> <li>• 2x2, 4x4, 4x4</li> <li>• 2.5 Gbps mGig</li> <li>• Power Options: PoE, DC Power</li> <li>• IoT Ready + Bluetooth 5.x</li> <li>• Partial iCAP</li> <li>• USB- 4.5 W</li> </ul>	 <p><b>CW9166</b></p> <ul style="list-style-type: none"> <li>• 4x4 + 4x4 + 4x4 (XOR 5/6)</li> <li>• 5 Gbps mGig</li> <li>• Power Options: PoE, DC Power</li> <li>• IoT ready + Bluetooth 5.x</li> <li>• Environmental Sensor</li> <li>• Full Packet Capture (iCAP)</li> <li>• Zero-Wait DFS*</li> <li>• USB - 4.5W</li> </ul>	 <p><b>C9136</b></p> <ul style="list-style-type: none"> <li>• 4x4, 8x8, 4x4 (or) 4x4, 4x4+4x4, 4x4</li> <li>• Dual 5 Gbps mGig, active fail over</li> <li>• PoE Redundancy</li> <li>• IoT ready</li> <li>• Bluetooth 5.x</li> <li>• Environmental Sensor</li> <li>• Full Packet Capture (iCAP)</li> <li>• Zero-Wait DFS*</li> <li>• USB - 9W</li> </ul> <p><small>*Available in Future</small></p>
<p><b>Full radio capability (6 GHz @ LPI) on single 30W PoE+</b></p>			
Dedicated Radio for CleanAir Pro	Same Bracket, Industrial Design	AP Power Optimization	USB

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_eda979fbdede064\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\mtknhvux.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:



None

Enhanced Open

WEP

WPA/WPA2-Personal

WPA3-Personal

WPA/WPA2-Enterprise

WPA3-Enterprise

WPA3-Enterprise 192-bit



CIF



- 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:

**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

Profile Name*	<input type="text" value="wifi_test"/>	<div style="border: 1px solid #ccc; padding: 5px; background-color: #f0f0f0;"> <b>Radio Policy</b> ⓘ           </div> <p style="text-align: right; color: #0070c0; font-size: small;">Show slot configuration</p> <div style="border: 1px solid #add8e6; padding: 5px; margin-bottom: 5px;"> <b>6 GHz</b>            Status <span style="float: right; border: 1px solid green; padding: 2px 5px; color: green; font-weight: bold;">ENABLED</span> <input checked="" type="checkbox"/> <ul style="list-style-type: none"> <li><span style="color: green;">✔</span> WPA2 Disabled</li> <li><span style="color: green;">✔</span> WPA3 Enabled</li> <li><span style="color: green;">✔</span> Dot11ax Enabled</li> </ul> </div> <div style="border: 1px solid #add8e6; padding: 5px; margin-bottom: 5px;"> <b>5 GHz</b>            Status <span style="float: right; border: 1px solid gray; padding: 2px 5px; color: gray; font-weight: bold;">DISABLED</span> <input type="checkbox"/> </div> <div style="border: 1px solid #add8e6; padding: 5px;"> <b>2.4 GHz</b>            Status <span style="float: right; border: 1px solid gray; padding: 2px 5px; color: gray; font-weight: bold;">DISABLED</span> <input type="checkbox"/>             802.11b/g Policy <span style="float: right; border: 1px solid gray; padding: 2px 5px;">802.11b/g ▾</span> </div>
SSID*	<input type="text" value="wifi_test"/>	
WLAN ID*	<input type="text" value="5"/>	
Status	<span style="border: 1px solid green; padding: 2px 5px; color: green; font-weight: bold;">ENABLED</span> <input checked="" type="checkbox"/>	
Broadcast SSID	<span style="border: 1px solid green; padding: 2px 5px; color: green; font-weight: bold;">ENABLED</span> <input checked="" type="checkbox"/>	

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

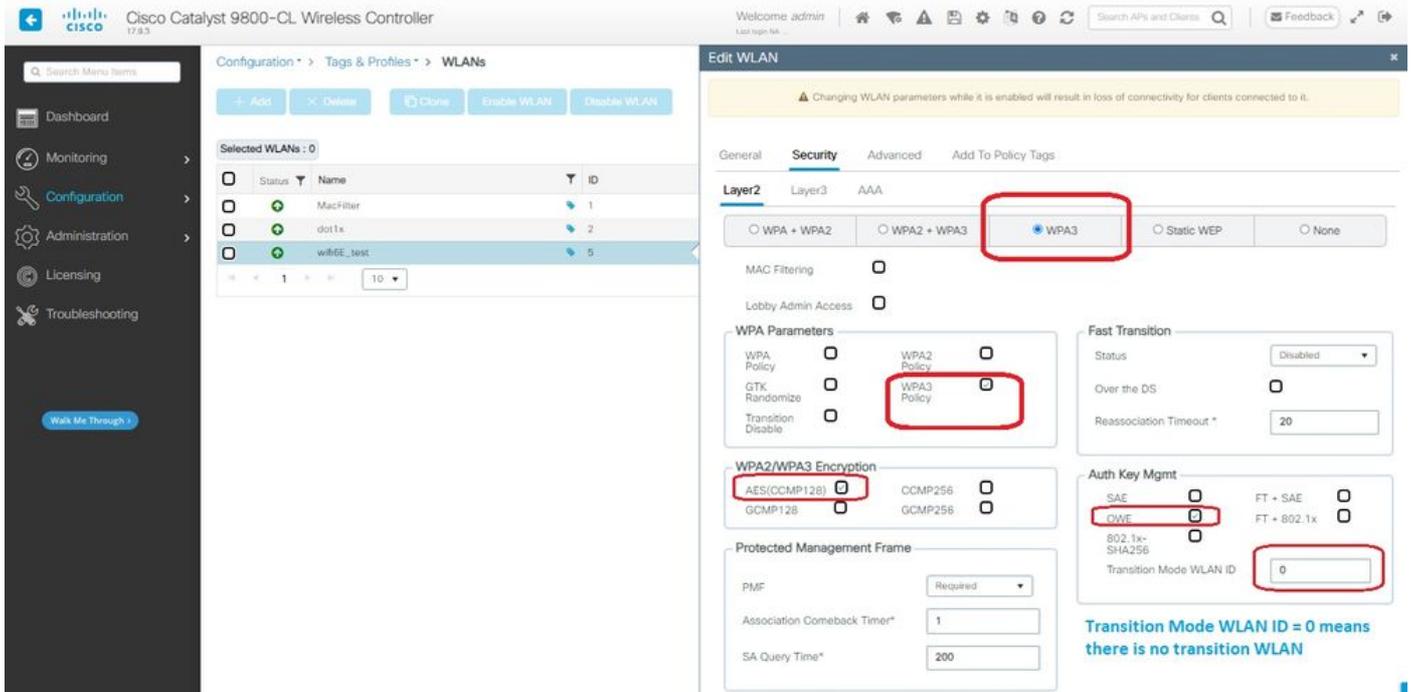


Nota: Aunque no hay clientes que soporten el cifrado GCMP128 + SUITEB-1X al momento de escribir este documento, se probó para observar que se estaba transmitiendo y verificar la información RSN en las balizas.

---

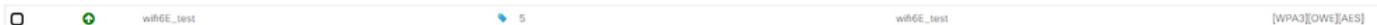
WPA3 - AES (CCPM128) + OWE

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.





No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
930	2023-06-12 14:03:07.117065	0.000000	netgear_48:78195	broadcast	802.11	166		-51 dBm	Probe Request, Sha158a, Fw0, Flags=.....C, SSID="billzar"
931	2023-06-12 14:03:07.117790	0.000021	netgear_48:78195	broadcast	802.11	166		-51 dBm	Probe Request, Sha151a, Fw0, Flags=.....C, SSID="billzar"
932	2023-06-12 14:03:07.118790	0.000006	netgear_48:78195	broadcast	802.11	166		-51 dBm	Probe Request, Sha152a, Fw0, Flags=.....C, SSID="billzar"
933	2023-06-12 14:03:07.119655	0.000003	netgear_48:78195	broadcast	802.11	166		-51 dBm	Probe Request, Sha153a, Fw0, Flags=.....C, SSID="billzar"
934	2023-06-12 14:03:08.445478	1.365423	netgear_48:78195	Cisco_11:00:	802.11	368		-51 dBm	Probe Request, Sha1, Fw0, Flags=.....C, SSID="wifi6_test"
1001	2023-06-12 14:03:08.445478	0.000000	192.168.1.15	192.168.1.121	802.11	76		-36 dBm	Acknowledgment, Flags=.....C
1015	2023-06-12 14:03:08.445484	0.000076	netgear_48:78195	Cisco_11:00:	802.11	368		-52 dBm	Probe Request, Sha2, Fw0, Flags=.....C, SSID="wifi6_test"
1016	2023-06-12 14:03:08.445959	0.000041	192.168.1.15	192.168.1.121	802.11	76		-36 dBm	Acknowledgment, Flags=.....C
1019	2023-06-12 14:03:08.504575	0.015166	netgear_48:78195	Cisco_11:00:	802.11	368		-41 dBm	Probe Request, Sha3, Fw0, Flags=.....C, SSID="wifi6_test"
1020	2023-06-12 14:03:08.504575	0.000000	192.168.1.15	192.168.1.121	802.11	76		-36 dBm	Acknowledgment, Flags=.....C
1024	2023-06-12 14:03:08.718083	0.213580	netgear_48:78195	Cisco_11:00:	802.11	368		-51 dBm	Authentication, Sha1, Fw0, Flags=.....C
1025	2023-06-12 14:03:08.718083	0.000000	Cisco_11:00:	netgear_48:78195	802.11	76		-36 dBm	Acknowledgment, Flags=.....C
1026	2023-06-12 14:03:08.724401	0.006330	Cisco_11:00:	netgear_48:78195	802.11	76		-36 dBm	Authentication, Sha06, Fw0, Flags=.....C
1027	2023-06-12 14:03:08.724401	0.000000	192.168.1.15	192.168.1.121	802.11	76		-36 dBm	Acknowledgment, Flags=.....C
1029	2023-06-12 14:03:08.728164	0.000373	netgear_48:78195	Cisco_11:00:	802.11	368		-51 dBm	Association Request, Sha0, Fw0, Flags=.....C, SSID="wifi6_test"
1030	2023-06-12 14:03:08.728164	0.000000	192.168.1.15	192.168.1.121	802.11	76		-36 dBm	Acknowledgment, Flags=.....C
1044	2023-06-12 14:03:08.736139	0.000285	netgear_48:78195	broadcast	LLC	124		-36 dBm	U, FuncUnknown, DSAP Bcc Group, SSAP Remote Program Load Response
1045	2023-06-12 14:03:08.736139	0.000000	Cisco_11:00:	netgear_48:78195	802.11	259		-36 dBm	Association Response, Sha0, Fw0, Flags=.....C
1046	2023-06-12 14:03:08.739139	0.000000	192.168.1.15	192.168.1.121	802.11	76		-50 dBm	Acknowledgment, Flags=.....C
1047	2023-06-12 14:03:08.739139	0.000000	192.168.1.15	192.168.1.121	802.11	124		-36 dBm	I, P, N(0)S(0), N(1)S(1) DSAP Bcc Group, SSAP Bcc Response
1049	2023-06-12 14:03:08.742139	0.000750	Cisco_11:00:	EAPOL	223			-36 dBm	Key (Message 1 of 4)
1050	2023-06-12 14:03:08.742139	0.000000	192.168.1.15	192.168.1.121	802.11	76		-51 dBm	Acknowledgment, Flags=.....C
1051	2023-06-12 14:03:08.742139	0.000000	netgear_48:78195	Cisco_11:00:	EAPOL	223		-51 dBm	Key (Message 2 of 4)
1052	2023-06-12 14:03:08.742139	0.000000	192.168.1.15	192.168.1.121	802.11	76		-36 dBm	Acknowledgment, Flags=.....C
1053	2023-06-12 14:03:08.751342	0.000000	Cisco_11:00:	EAPOL	235			-36 dBm	Key (Message 1 of 4)
1054	2023-06-12 14:03:08.751342	0.000000	192.168.1.15	192.168.1.121	802.11	76		-50 dBm	Acknowledgment, Flags=.....C
1055	2023-06-12 14:03:08.751342	0.000000	netgear_48:78195	Cisco_11:00:	EAPOL	199		-51 dBm	Key (Message 4 of 4)
1056	2023-06-12 14:03:08.751342	0.000000	192.168.1.15	192.168.1.121	802.11	76		-43 dBm	Acknowledgment, Flags=.....C
1057	2023-06-12 14:03:08.757481	0.006139	Cisco_11:00:	EAPOL	187			-51 dBm	I, P, N(0)S(0), N(1)S(1) DSAP Bcc Individual, SSAP Bcc Command
1058	2023-06-12 14:03:08.757481	0.000000	192.168.1.15	192.168.1.121	802.11	76		-51 dBm	Acknowledgment, Flags=.....C
1059	2023-06-12 14:03:08.757481	0.000000	192.168.1.15	192.168.1.121	802.11	119		-43 dBm	Trigger Buffer Status Report Poll (BSRP), Flags=.....C
1063	2023-06-12 14:03:08.798068	0.041187	192.168.1.15	192.168.1.121	802.11	119		-43 dBm	Trigger Buffer Status Report Poll (BSRP), Flags=.....C
1064	2023-06-12 14:03:08.808063	0.014595	netgear_48:78195	PhyMgmt_16	LLC	227		-41 dBm	I, N(0)S(0), N(1)S(1) DSAP Pktnbr (IC955) Active Station List Maintenance
1065	2023-06-12 14:03:08.808063	0.000000	192.168.1.15	192.168.1.121	802.11	76		-41 dBm	Acknowledgment, Flags=.....C
1066	2023-06-12 14:03:08.808063	0.000000	192.168.1.15	192.168.1.121	802.11	119		-42 dBm	Trigger Buffer Status Report Poll (BSRP), Flags=.....C
1068	2023-06-12 14:03:08.808063	0.000000	netgear_48:78195	PhyMgmt_16	LLC	199		-38 dBm	I, P, N(0)S(0), N(1)S(1) DSAP Bcc Group, SSAP Bcc Command
1126	2023-06-12 14:03:08.820643	0.000000	192.168.1.15	192.168.1.121	802.11	76		-36 dBm	Key (Message 1 of 4)
1130	2023-06-12 14:03:08.829249	0.000000	netgear_48:78195	broadcast	LLC	444		-36 dBm	U, FuncUnknown, DSAP Bcc Group, SSAP Bcc Command
1131	2023-06-12 14:03:08.829249	0.000000	192.168.1.15	192.168.1.121	802.11	76		-42 dBm	Acknowledgment, Flags=.....C
1132	2023-06-12 14:03:08.829249	0.000000	netgear_48:78195	PhyMgmt_16	LLC	199		-37 dBm	I, N(0)S(0), N(1)S(1) DSAP Bcc Group, SSAP Bcc Response
1133	2023-06-12 14:03:08.829249	0.000000	192.168.1.15	192.168.1.121	802.11	76		-36 dBm	Key (Message 4 of 4)
1134	2023-06-12 14:03:08.829249	0.000000	netgear_48:78195	broadcast	LLC	442		-36 dBm	I, P, N(0)S(0), N(1)S(1) DSAP Bcc Individual, SSAP Bcc Response
1135	2023-06-12 14:03:08.829249	0.000000	192.168.1.15	192.168.1.121	802.11	76		-41 dBm	U, FuncUnknown, DSAP Bcc Individual, SSAP Bcc Response
1144	2023-06-12 14:03:08.917921	0.000000	192.168.1.15	192.168.1.121	802.11	76		-41 dBm	Acknowledgment, Flags=.....C
1146	2023-06-12 14:03:08.917921	0.000000	Cisco_11:00:	netgear_48:78195	802.11	265		-37 dBm	I, N(0)S(0), N(1)S(1) DSAP Bcc MS-511 Manufacturing Message Service Ind
1148	2023-06-12 14:03:08.921977	0.000456	Cisco_11:00:	netgear_48:78195	802.11	118		-36 dBm	Action, Sha1, Fw0, Flags=.....C
1149	2023-06-12 14:03:08.921977	0.000000	192.168.1.15	192.168.1.121	802.11	76		-51 dBm	Acknowledgment, Flags=.....C

## Detalles del cliente en WLC:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The 'Client' tab is selected, displaying details for client 9418.6548.7095. The client is associated with MAC address 9418.6548.7095, IP address 192.168.1.163, and is connected to AP6849.9253.CA50. The client state is 'Servers: None', and it is using CCMP (AES) encryption. The session timeout is set to 86400 seconds.

## Píxel 6a

## Conexión OTA con enfoque en la información RSN del cliente:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info	
504	2023-06-12 15:53:27.559885	0.000000	google_72:8a:66	netgear_48:78195	Cisco_11:00:	802.11	108		-47 dBm	Authentication, Sha1097, Fw0, Flags=.....C, SSID="wifi6_test"
505	2023-06-12 15:53:27.559885	0.000000	192.168.1.15	192.168.1.121	802.11	108		-36 dBm	Acknowledgment, Flags=.....C	
506	2023-06-12 15:53:27.559885	0.000000	192.168.1.15	192.168.1.121	802.11	108		-36 dBm	Authentication, Sha1098, Fw0, Flags=.....C	
507	2023-06-12 15:53:27.559885	0.000000	192.168.1.15	192.168.1.121	802.11	76		-48 dBm	Acknowledgment, Flags=.....C	
509	2023-06-12 15:53:27.574598	0.000939	google_72:8a:66	Cisco_11:00:	802.11	293		-46 dBm	Association Request, Sha0698, Fw0, Flags=.....C, SSID="wifi6_test"	
510	2023-06-12 15:53:27.574598	0.000000	192.168.1.15	192.168.1.121	802.11	76		-36 dBm	Acknowledgment, Flags=.....C	
518	2023-06-12 15:53:27.791916	0.061118	Cisco_11:00:	google_72:8a:66	EAPOL	239		-36 dBm	Key (Message 1 of 4)	
519	2023-06-12 15:53:27.791916	0.000000	192.168.1.15	192.168.1.121	802.11	76		-45 dBm	Acknowledgment, Flags=.....C	
600	2023-06-12 15:53:27.794140	0.002312	Cisco_11:00:	google_72:8a:66	EAPOL	223		-36 dBm	Key (Message 1 of 4)	
601	2023-06-12 15:53:27.794140	0.000000	192.168.1.15	192.168.1.121	802.11	76		-46 dBm	Acknowledgment, Flags=.....C	
604	2023-06-12 15:53:27.832152	0.037884	google_72:8a:66	Cisco_11:00:	EAPOL	227		-46 dBm	Key (Message 2 of 4)	
605	2023-06-12 15:53:27.832152	0.000000	192.168.1.15	192.168.1.121	802.11	76		-36 dBm	Key (Message 1 of 4)	
606	2023-06-12 15:53:27.832152	0.000000	192.168.1.15	192.168.1.121	802.11	76		-46 dBm	Acknowledgment, Flags=.....C	
607	2023-06-12 15:53:27.834424	0.000000	192.168.1.15	192.168.1.121	802.11	76		-46 dBm	Key (Message 4 of 4)	
609	2023-06-12 15:53:27.840723	0.000000	192.168.1.15	192.168.1.121	802.11	76		-37 dBm	Acknowledgment, Flags=.....C	
611	2023-06-12 15:53:27.868914	0.028191	Cisco_11:00:	google_72:8a:66	EAPOL	187		-46 dBm	I, P, N(0)S(0), N(1)S(1) DSAP Bcc Group, SSAP Bcc Command	
612	2023-06-12 15:53:27.868914	0.000000	192.168.1.15	192.168.1.121	802.11	76		-53 dBm	Acknowledgment, Flags=.....C	
613	2023-06-12 15:53:27.868914	0.000000	192.168.1.15	192.168.1.121	802.11	76		-37 dBm	Acknowledgment, Flags=.....C	
614	2023-06-12 15:53:27.864306	0.001192	192.168.1.15	192.168.1.121	802.11	76		-36 dBm	Acknowledgment, Flags=.....C	
615	2023-06-12 15:53:27.875667	0.011561	192.168.1.15	192.168.1.121	802.11	76		-36 dBm	Acknowledgment, Flags=.....C	
617	2023-06-12 15:53:27.882181	0.006434	192.168.1.15	192.168.1.121	802.11	76		-45 dBm	Acknowledgment, Flags=.....C	
618	2023-06-12 15:53:27.884415	0.002652	google_72:8a:66	Cisco_11:00:	802.11	122		-36 dBm	Action, Sha1709, Fw0, Flags=.....C	
619	2023-06-12 15:53:27.884415	0.000000	192.168.1.15	192.168.1.121	802.11	76		-46 dBm	Acknowledgment, Flags=.....C	
621	2023-06-12 15:53:27.933021	0.049318	Cisco_11:00:	google_72:8a:66	EAPOL	124		-37 dBm	Action, Sha1, Fw0, Flags=.....C [Malformed Packet]	
622	2023-06-12 15:53:27.933021	0.000000	192.168.1.15	192.168.1.121	802.11	76		-47 dBm	Acknowledgment, Flags=.....C	
623	2023-06-12 15:53:28.018306	0.085285	google_72:8a:66	Cisco_11:00:	802.11	115		-48 dBm	Action, Sha1704, Fw0, Flags=.....C	
624	2023-06-12 15:53:28.018306	0.000000	192.168.1.15	192.168.1.121	802.11	76		-36 dBm	Acknowledgment, Flags=.....C	
631	2023-06-12 15:53:28.018306	0.000000	192.168.1.15	192.168.1.121	802.11	76		-46 dBm	Acknowledgment, Flags=.....C	
632	2023-06-12 15:53:28.018306	0.000000	192.168.1.15	192.168.1.121	802.11	76		-46 dBm	Acknowledgment, Flags=.....C	
634	2023-06-12 15:53:28.020947	0.002603	Cisco_11:00:	google_72:8a:66	EAPOL	115		-37 dBm	Action, Sha2, Fw0, Flags=.....C	
635	2023-06-12 15:53:28.020947	0.000000	192.168.1.15	192.168.1.121	802.11	76		-48 dBm	Acknowledgment, Flags=.....C	
636	2023-06-12 15:53:28.021574	0.000627	192.168.1.15	192.168.1.121	802.11	76				

## Samsung S23

## Conexión OTA con enfoque en la información RSN del cliente:

## Detalles del cliente en WLC:

## WPA3 - AES (CCMP128) + 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:

### 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

#### Fast Transition

Status

Over the DS

Reassociation Timeout \*

#### WPA2/WPA3 Encryption

AES(OCMP128)  OCMP256

GCMP128  GCMP256

#### Protected Management Frame

PMF

Association Comeback Timer\*

SA Query Time\*

#### Auth Key Mgmt

SAE  FT - SAE

ONE  FT - 802.1x

802.1x-SHA256

Anti Clogging Threshold\*

Max Retries\*

Retransmit Timeout\*

PSK Format

PSK Type

Pre-Shared Key\*

SAE Password Element ⓘ

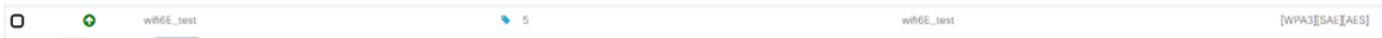
Configuración de WPA3 SAE



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:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
2	2023-06-12 17:12:24.459118	0.00000	Cisco_13:180E:0F	Broadcast	802.11	463	5.36 dBm	Probe Response, Shw733, Fwub, Flags:.....C, B1=100, SSID="WiFi6E_Test_02", SS	<pre> Frame 6: 508 bytes on wire (4064 bits), 508 bytes captured (4064 bits) on interface Vdeice\NPF_{04578995-2998-4464-4 Ethernet II, Src: Cisco_02:00:0C:70:1B:37, Dst: Unicast_Broadcast (08:00:00:00:00:00) Internet Protocol version 4, Src: 192.168.1.13, Dst: 192.168.1.11 User Datagram Protocol, Src Port: 5555, Dst Port: 5000 AirPeeek/OmniPeek encapsulated IEEE 802.11 IEEE 802.11 radio information IEEE 802.11 Beacon frame, Flags:.....C IEEE 802.11 wireless management Fixed parameters (12 bytes) Tagged parameters (406 bytes) Tag: SSI parameter set "WiFi6E_Test_02" Tag: Supported rates (3), 5, 11M; 18, 24M; 36, 48, 54, 72Mbit/sec Tag: Traffic Indication Map (TIM): OTF# 2 of 3 bitmaps Tag: Country Information: Country code is, Environment global operating classes Tag: Power Constraints: 0 Tag: TPC Report Transm Power: 17, Link Margin: 0 Tag: RSN Information Tag number: RSN Information (48) Tag length: 36 RSN version: 1 Group Cipher Suite: 000fac (IEEE 802.11) AES (CCM) Pairwise Cipher Suite Count: 1 Pairwise Cipher Suite List: 000fac (IEEE 802.11) AES (CCM) Auth Key Management (AKM) Suite Count: 1 Auth Key Management (AKM) List: 000fac (IEEE 802.11) SAE (SHA256) RSN Capabilities: 00000 PMKID Count: 0 PMKID List Group Management Cipher Suite: 000fac (IEEE 802.11) GCM (128) Tag: QSS Load Element 000fac (CCM version) Tag: Multiple BSSIDs Tag: M Enabled Capabilities (5 octets) Tag: Extended Capabilities (11 octets) Tag: TX Power Envelope Tag: TX Power Envelope Ext Tag: Multiple BSSID Configuration Ext Tag: HE Capabilities Ext Tag: HE Capabilities Ext Tag: HE Capabilities Ext Tag: Spatial Reuse Parameter Set Ext Tag: MU-EDCA Parameter Set Ext Tag: HE Capabilities Tag: RSN extension (1 octet) Tag number: RSN extension (244) RSN: 0x20 (test 1) .... 0000 = RSN Length: 0 .... 0 = Protected Test Operations Support: 0 .... = SAE mesh to element: 1 </pre>

### Indicadores WPA3 SAE

Aqui podemos observar clientes Wi-Fi 6E asociando:

Intel AX211

Conexión OTA con enfoque en la información RSN del cliente:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
2235	2023-06-12 17:15:00.328310	0.00000	IntelCor_9E:18:5E:0F	Broadcast	802.11	168	5.47 dBm	Probe Request, Shw389, Fwub, Flags:.....C, SSID=Wildcard (Broadcast)	<pre> Frame 1225: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits) on interface Vdeice\NPF_{04578995-2998-4464-4 Ethernet II, Src: Cisco_02:00:0C:70:1B:37, Dst: Unicast_Broadcast (08:00:00:00:00:00) Internet Protocol version 4, Src: 192.168.1.13, Dst: 192.168.1.11 User Datagram Protocol, Src Port: 5555, Dst Port: 5000 AirPeeek/OmniPeek encapsulated IEEE 802.11 IEEE 802.11 authentication, Flags:.....C IEEE 802.11 wireless management Fixed parameters (184 bytes) Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (1) Authentication SAE: 0x0001 Status code: SAE authentication via direct hashing, instead of looping, to obtain the PMK (0000E) SAE message type: Commit (1) Group ID: 254-011 random (0) group (19) Scalar: dc0385cfe797f2ac1f608e87c4c779a0d104818a3808e425312 Finite Field Element: 58c775a078e6249b0212ec7275ed66d42a85726786a48eac6d032f70934. </pre>

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:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1235	2023-06-12 17:37:02.738033	0.000000	Google_7218a-66	Cisco_31180-1	Broadcast	802.11	343	-42 dBm	Probe Request, S/W=99, P/W=0, Flags=.....C, SSID="wifi6_test"
1243	2023-06-12 17:37:02.855163	0.117100	Google_7218a-66	Cisco_31180-1	Authentication	Sw=2097, P/W=0, Flags=.....C	194	-42 dBm	Authentication, Sw=2097, P/W=0, Flags=.....C
1244	2023-06-12 17:37:02.855163	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1246	2023-06-12 17:37:02.859394	0.007353	Cisco_31180-1	Google_7218a-66	Authentication	Sw=141, P/W=0, Flags=.....C	194	-37 dBm	Authentication, Sw=141, P/W=0, Flags=.....C
1247	2023-06-12 17:37:02.859394	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1248	2023-06-12 17:37:02.868831	0.009467	Google_7218a-66	Cisco_31180-1	Authentication	Sw=2098, P/W=0, Flags=.....C	198	-41 dBm	Authentication, Sw=2098, P/W=0, Flags=.....C
1249	2023-06-12 17:37:02.868831	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1250	2023-06-12 17:37:02.904326	0.035495	Cisco_31180-1	Google_7218a-66	Authentication	Sw=142, P/W=0, Flags=.....C	198	-37 dBm	Authentication, Sw=142, P/W=0, Flags=.....C
1251	2023-06-12 17:37:02.904326	0.000000	192.168.1.15	192.168.1.121	802.11	76	-41 dBm	Acknowledgment, Flags=.....C	
1255	2023-06-12 17:37:02.929933	0.016467	Google_7218a-66	Cisco_31180-1	Association Request	Sw=2099, P/W=0, Flags=.....C, SSID="wifi6_test"	262	-41 dBm	Association Request, Sw=2099, P/W=0, Flags=.....C, SSID="wifi6_test"
1256	2023-06-12 17:37:02.929933	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1259	2023-06-12 17:37:02.930808	0.000917	Google_7218a-66	Broadcast	LLC	114	-49 dBm	I P, N(=)S(=), N(S)=23; OSPF v2 Network Layer (unofficial) Group, SSAP Banyan Vlan	
1261	2023-06-12 17:37:02.934129	0.003759	Cisco_31180-1	Google_7218a-66	Association Response	Sw=0, P/W=0, Flags=.....C	262	-37 dBm	Association Response, Sw=0, P/W=0, Flags=.....C
1262	2023-06-12 17:37:02.934129	0.000000	192.168.1.15	192.168.1.121	802.11	76	-41 dBm	Acknowledgment, Flags=.....C	
1263	2023-06-12 17:37:02.934129	0.000000	Google_7218a-66	Broadcast	LLC	114	-37 dBm	S P, Func=0x, N(=)S(=); OSPF v2 Group, SSAP Bn2 Response	
1265	2023-06-12 17:37:02.943892	0.000363	Cisco_31180-1	Google_7218a-66	EAPOL	223	-37 dBm	Key (message 1 of 4)	
1266	2023-06-12 17:37:02.943892	0.000000	192.168.1.15	192.168.1.121	802.11	76	-41 dBm	Acknowledgment, Flags=.....C	
1273	2023-06-12 17:37:02.992247	0.051155	Google_7218a-66	Cisco_31180-1	EAPOL	238	-51 dBm	Key (message 2 of 4)	
1274	2023-06-12 17:37:02.992247	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1275	2023-06-12 17:37:02.995369	0.003122	Cisco_31180-1	Google_7218a-66	EAPOL	295	-37 dBm	Key (message 3 of 4)	
1276	2023-06-12 17:37:02.995369	0.000000	192.168.1.15	192.168.1.121	802.11	76	-51 dBm	Acknowledgment, Flags=.....C	
1278	2023-06-12 17:37:03.000159	0.004790	Google_7218a-66	Cisco_31180-1	EAPOL	199	-48 dBm	Key (message 4 of 4)	
1279	2023-06-12 17:37:03.000159	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1281	2023-06-12 17:37:03.021709	0.021231	192.168.1.15	192.168.1.121	802.11	76	-46 dBm	Acknowledgment, Flags=.....C	
1282	2023-06-12 17:37:03.025924	0.002534	Google_7218a-66	Cisco_31180-1	Action	Sw=2101, P/W=0, Flags=.....C (Malformed Packet)	122	-49 dBm	Action, Sw=2101, P/W=0, Flags=.....C (Malformed Packet)
1283	2023-06-12 17:37:03.025924	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1284	2023-06-12 17:37:03.040493	0.017809	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1286	2023-06-12 17:37:03.046766	0.007793	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1290	2023-06-12 17:37:03.078167	0.027401	Cisco_31180-1	Google_7218a-66	Action	Sw=1, P/W=0, Flags=.....C	124	-37 dBm	Action, Sw=1, P/W=0, Flags=.....C
1291	2023-06-12 17:37:03.078167	0.000000	192.168.1.15	192.168.1.121	802.11	76	-49 dBm	Acknowledgment, Flags=.....C	
1297	2023-06-12 17:37:03.166223	0.088956	Google_7218a-66	Cisco_31180-1	Action	Sw=2104, P/W=0, Flags=.....C	115	-48 dBm	Action, Sw=2104, P/W=0, Flags=.....C
1298	2023-06-12 17:37:03.166223	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
1299	2023-06-12 17:37:03.166229	0.000076	Google_7218a-66	IPv6cast	LLC	227	-57 dBm	I P, Func=0x; OSPF v2 Group, SSAP Bn2 Command	
1300	2023-06-12 17:37:03.166229	0.000000	192.168.1.15	192.168.1.121	802.11	76	-49 dBm	Acknowledgment, Flags=.....C	
1302	2023-06-12 17:37:03.167399	0.001700	Cisco_31180-1	Google_7218a-66	Action	Sw=2, P/W=0, Flags=.....C (Malformed Packet)	115	-37 dBm	Action, Sw=2, P/W=0, Flags=.....C (Malformed Packet)
1303	2023-06-12 17:37:03.167399	0.000000	192.168.1.15	192.168.1.121	802.11	76	-49 dBm	Acknowledgment, Flags=.....C	
1304	2023-06-12 17:37:03.167399	0.000000	192.168.1.15	192.168.1.121	802.11	82	-49 dBm	802.11 Block Ack Req, Flags=.....C	
1305	2023-06-12 17:37:03.167399	0.000000	192.168.1.15	192.168.1.121	802.11	94	-37 dBm	802.11 Block Ack, Flags=.....C	
1306	2023-06-12 17:37:03.168543	0.000347	Cisco_31180-1	IPv6cast	LLC	186	-38 dBm	I P, N(=)S(=), N(S)=45; OSPF v2 Group, SSAP Bn2 Response	
1307	2023-06-12 17:37:03.177442	0.000000	192.168.1.15	192.168.1.121	802.11	82	-49 dBm	Request-to-send, Flags=.....C	
1308	2023-06-12 17:37:03.177442	0.000000	192.168.1.15	192.168.1.121	802.11	76	-46 dBm	Clear-to-send, Flags=.....C	
1309	2023-06-12 17:37:03.177515	0.000073	Google_7218a-66	IPv6cast	LLC	271	-56 dBm	I, N(=)S(=), N(S)=34; OSPF v2 Group, SSAP Bn2 Response	

```

> Frame 1255: 262 bytes on wire (2096 bits), 262 bytes captured (2096 bits) on interface VdeviceVAP_04578905-2998-445
> Ethernet II, Src: Cisco_G0/16:17 (00:0f:1d:0d:7d:37), Dst: Univers_07:cf:06 (08:0a:8b:07:cf:06)
> Internet Protocol version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5858, Dst Port: 5800
> Airopeek/OmniPeek encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
  > fixed parameters (4 bytes)
  > Tagged parameters (168 bytes)
    > Tag: SSID parameter Set: "wifi6_test"
    > Tag: Supported rates (0), 9, 12.0, 18, 24.0, 36, 48, 54, [Mbit/sec]
    > Tag: Extended Supported Rates SAE mesh to element only, [Mbit/sec]
    > Tag: Power Capability MIM: -7, MIM: 19
    > Tag: Supported Channels
    > Tag: SSN Information
      Tag Number: SSN Information (48)
      Tag Length: 26
      SSN Version: 1
      > Group Cipher Suite: 00:0fac (IEEE 802.11) AES (CCM)
      Pairwise Cipher Suite Count: 1
      Pairwise Cipher Suite List 00:0fac (IEEE 802.11) AES (CCM)
      Auth Key Management (AKM) Suite Count: 1
      Auth Key Management (AKM) List 00:0fac (IEEE 802.11) SAE (SHA256)
      > Tag: Supported Channels
      > SSN Capabilities: 00000
      PMKID Count: 0
      PMKID List:
      > Group Management Cipher Suite: 00:0fac (IEEE 802.11) BIP (128)
      > Tag: W enabled capabilities (5 octets)
      > Tag: Supported Operating Classes
      > Tag: Extended capabilities (18 octets)
      > Ext Tag: HE Capabilities
      > Tag: SSN extension (1 octet)
      Tag Number: SSN extension (244)
      Tag Length: 1
      > SSN: 0xae (octet 1)
        ..... 0000 = SSN length: 0
        ..... 0000 = Protected TWT element Support: 0
        ..... 0000 = reserved: 000
        ..... 0000 = SAE mesh to element: 1
    > Ext Tag: HE 4 oct Band Capabilities
    > Tag: vendor specific: Broadcom
    > Tag: vendor specific: Microsoft Corp.: WPA/WPE: Information Element
  
```

## Detalles del cliente en WLC:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller interface. The main content area displays a list of clients under the 'Monitoring' tab. One client is selected, and its details are shown in the 'Security Information' panel on the right.

Client MAC Address	IPv4 Address	IPv6 Address	AP Name
2495.2f72.8a66	192.168.1.162	fe80::b13:1107:7c5fa7e0	AP6849_9253_CA50
60fb.008b.0e66	N/A	N/A	AP01_RC_9136_F80C
34ea.e702.6240	192.168.1.70	N/A	AP6849_9253_CA50
a810.87bb.b833	192.168.1.94	fe80::a10:87f:febb:b833	AP03_Sotao_9548
9669.5a28.a115	192.168.1.138	fe80::9669:5aff:fa28:a115	AP02_Sotao_1084
8408.1b01.294f	192.168.1.91	N/A	AP03_Sotao_9548
0c8b.9509.3518	192.168.1.129	N/A	AP03_Sotao_9548
0012.17e2.4b40	192.168.1.31	fe80::212:17f:fe2:4b40	AP04_OutdoorF_3DC8
0012.17e2.4856	192.168.1.37	fe80::212:17f:fe2:4856	AP05_OutdoorF_2200
0012.17e1.dd57	192.168.1.133	fe80::212:17f:fe1:dd57	AP03_Sotao_9548

The 'Security Information' panel for the selected client shows the following details:

- Client State Servers: None
- Client ACLs: None
- Client Entry Create Time: B3 seconds
- Policy Type: WPA3
- Encryption Cipher: CCMP (AES)
- Authentication Key Management: SAE
- EAP Type: Not Applicable
- Session Timeout: 86400
- Point of Attachment: capwap\_90000010
- IF ID: 0x90000010
- Authorized: TRUE
- Common Session ID: 000000000000FB58AED363
- Acct Session ID: 0x00000000
- Auth Method Status List: SAE
- Method: SAE

## Samsung S23

## Conexión OTA con enfoque en la información RSN del cliente:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
773	2023-06-12 17:26:55.727215	0.000000	Samsung_C9-0371	Cisco_31180-1	Authentication	Sw=2176, P/W=0, Flags=.....C	194	-45 dBm	Authentication, Sw=2176, P/W=0, Flags=.....C
774	2023-06-12 17:26:55.727215	0.000000	192.168.1.15	192.168.1.121	802.11	76	-38 dBm	Acknowledgment, Flags=.....C	
775	2023-06-12 17:26:55.734513	0.000038	Cisco_31180-1	Samsung_C9-0371	Authentication	Sw=2176, P/W=0, Flags=.....C	194	-37 dBm	Authentication, Sw=2176, P/W=0, Flags=.....C
776	2023-06-12 17:26:55.734513	0.000000	192.168.1.15	192.168.1.121	802.11	76	-45 dBm	Acknowledgment, Flags=.....C	
777	2023-06-12 17:26:55.742869	0.000316	Samsung_C9-0371	Cisco_31180-1	Authentication	Sw=2177, P/W=0, Flags=.....C	198	-43 dBm	Authentication, Sw=2177, P/W=0, Flags=.....C
778	2023-06-12 17:26:55.742869	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
780	2023-06-12 17:26:55.743197	0.000228	Cisco_31180-1	Samsung_C9-0371	Authentication	Sw=2177, P/W=0, Flags=.....C	198	-36 dBm	Authentication, Sw=2177, P/W=0, Flags=.....C
781	2023-06-12 17:26:55.743197	0.000000	192.168.1.15	192.168.1.121	802.11	76	-43 dBm	Acknowledgment, Flags=.....C	
782	2023-06-12 17:26:55.748094	0.004544	Samsung_C9-0371	Cisco_31180-1	Association Request	Sw=2178, P/W=0, Flags=.....C, SSID="wifi6_test"	354	-45 dBm	Association Request, Sw=2178, P/W=0, Flags=.....C, SSID="wifi6_test"
783	2023-06-12 17:26:55.748094	0.000000	192.168.1.15	192.168.1.121	802.11	76	-36 dBm	Acknowledgment, Flags=.....C	
787	2023-06-12 17:26:55.758131	0.010275	Samsung_C9-0371	Broadcast	LLC	114	-36 dBm	I, N(=)S(=), N(S)=23; OSPF v2 Network Layer (unofficial) Group, SSAP Banyan Vlan	
788	2023-06-12 17:26:55.758131	0.000000	Samsung_C9-0371	Broadcast	LLC	114	-36 dBm	S P, Func=0x, N(=)S(=); OSPF v2 Printer Individual, SSAP Bn2 Response	
789	2023-06-12 17:26:55.763192	0.002876	Cisco_31180-1	Samsung_C9-0371	Association Response	Sw=0, P/W=0, Flags=.....C	236	-36 dBm	Association Response, Sw=0, P/W=0, Flags=.....C
790	2023-06-12 17:26:55.763192	0.000000	192.168.1.15	192.168.1.121	802.11	76	-44 dBm	Acknowledgment, Flags=.....C	
792	2023-06-12 17:26:55.762296	0.001184	Cisco_31180-1	Samsung_C9-0371	EAPOL	223	-36 dBm	Key (message 1 of 4)	
793	2023-06-12 17:26:55.762296	0.000000	192.168.1.15	192.168.1.121	802.11	76	-44 dBm	Acknowledgment, Flags=.....C	
795	2023-06-12 17:26:55.791219	0.028823	Samsung_C9-0371	Cisco_31180-1	EAPOL	238	-43 dBm	Key (message 2 of 4)	
796	2023-06-12 17:26:55.791219	0.000000	192.168.1.15	192.168.1.121	802.11	76	-37 dBm	Acknowledgment, Flags=.....C	
797	2023-06-12 17:26:55.793800	0.001781	Cisco_31180-1	Samsung_C9-0371	EAPOL	295	-37 dBm	Key (message 3 of 4)	
798	2023-06-12 17:26:55.793800	0.000000	192.168.1.15	192.168.1.121	802.11	76	-44 dBm	Acknowledgment, Flags=.....C	
799	2023-06-12 17:26:55.798403	0.000483	Samsung_C9-0371	Cisco_31180-1	EAPOL	199	-46 dBm	Key (message 4 of 4)	

```

> Frame 773: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits) on interface VdeviceVAP_04578905-2998-445
> Ethernet II, Src: Cisco_G0/16:17 (00:0f:1d:0d:7d:37), Dst: Univers_07:cf:06 (08:0a:8b:07:cf:06)
> Internet Protocol version 4, Src: 192.168.1.15, Dst: 192.168.1.121
> User Datagram Protocol, Src Port: 5858, Dst Port: 5800
> Airopeek/OmniPeek encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Authentication, Flags: .....C
  > fixed parameters (184 bytes)
    Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)
    Authentication SEQ: 00000
    Status code: SAE Authentication uses direct hashing, instead of looping, to obtain the PMK (00000)
    SAE Message Type: COMMIT (1)
    Group ID: 254-011 random ECP group (19)
    Scalar: 00c21890e130e20c4630c044e7501f6c0b0f2620890508129508
    Finite Field Element: 0014546db2080430c70d781e4481e8f803
```

Cisco Catalyst 9800-CL Wireless Controller

Welcome admin

Search APs and Clients

Feedback

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Delete

Selected 0 out of 12 Clients

	Client MAC Address	IPv4 Address	IPv6 Address	AP Name
<input type="checkbox"/>	0012.17e1.dd57	192.168.1.33	fe80::212:17ff:fee1:dd57	AP03_Sotao_9548
<input type="checkbox"/>	0012.17e2.4856	192.168.1.37	fe80::212:17ff:fee2:4856	AP05_OutdoorB_220
<input type="checkbox"/>	0012.17e2.4b40	192.168.1.31	fe80::212:17ff:fee2:4b40	AP04_OutdoorF_300
<input type="checkbox"/>	0429.2ec9.e371	192.168.1.160	fe80::6a20:34e8:ab1b:6332	AP6849.9253.CA50
<input type="checkbox"/>	0c8b.9509.3518	192.168.1.129	N/A	AP03_Sotao_9548
<input type="checkbox"/>	34ea.e702.6240	192.168.1.70	N/A	AP6849.9253.CA50
<input type="checkbox"/>	60fb.008b.0e66	N/A	N/A	AP01_RC_9136_F80
<input type="checkbox"/>	84d8.1b0f.294f	192.168.1.91	N/A	AP03_Sotao_9548
<input type="checkbox"/>	9669.5a28.a115	192.168.1.138	fe80::9469:5aff:fe28:a115	AP02_Suite_1084
<input type="checkbox"/>	a810.87bb.b833	192.168.1.94	fe80::aa10:87ff:febb:b833	AP03_Sotao_9548

Client

360 View General QoS Statistics ATF Statistics Mobility History Call Statistics

Client Properties AP Properties Security Information Client Statistics QoS Properties EoGRE

Client State Servers None

Client ACLs None

Client Entry Create Time 78 seconds

Policy Type WPA3

Encryption Cipher CCMP (AES)

Authentication Key Management SAE

EAP Type Not Applicable

Session Timeout 86400

Session Manager

Point of Attachment capwap\_90000010

IF ID 0x90000010

Authorized TRUE

Common Session ID 000000000000FB1B0A58F78

Acct Session ID 0x00000000

Auth Method Status List

Method SAE

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

Configuración de seguridad 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

Fast Transition

Status  ▾  
 Over the DS   
 Reassociation Timeout \*

WPA2/WPA3 Encryption

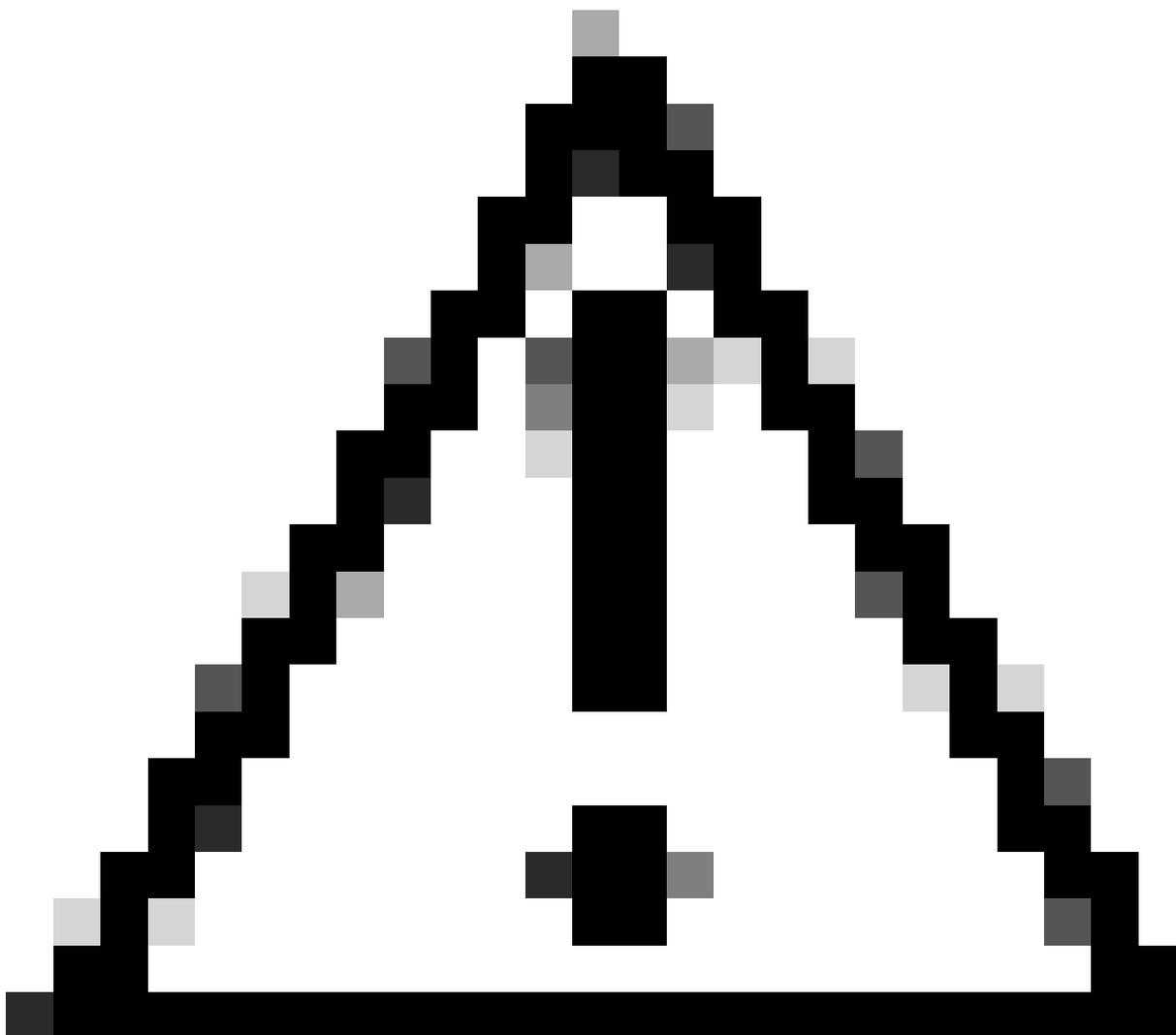
AES(OCMP128)  CCMP256   
 GCMP128  GCMP256

Auth Key Mgmt

SAE  FT + SAE   
 OWE  FT + 802.1x   
 802.1x-SHA256   
 Anti Clogging Threshold\*   
 Max Retries\*   
 Retransmit Timeout\*   
 PSK Format  ▾  
 PSK Type  ▾  
 Pre-Shared Key\*   
 SAE Password Element ⓘ  ▾

Protected Management Frame

PMF  ▾  
 Association Comeback Timer\*   
 SA Query Time\*



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:

wifGE\_test 5 wifGE\_test [WPA3][SAE][FT + SAE][AES][FT Enabled]

Verificación de las balizas OTA:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1	2023-06-12 18:34:49.35337	0.000000	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=22, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
2	2023-06-12 18:34:49.42754	0.102287	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
3	2023-06-12 18:34:49.50957	0.102287	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=23, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
4	2023-06-12 18:34:49.62332	0.102465	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
5	2023-06-12 18:34:49.79180	0.099672	Netgear_48:78:35	Cisco_13:180:e7	802.11	360	5	-49 dBm	Probe Request, S/W=8, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
6	2023-06-12 18:34:49.79180	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
7	2023-06-12 18:34:49.79180	0.000000	192.168.1.15	192.168.1.121	802.11	360	5	-49 dBm	Probe Request, S/W=1, F/W=, Flags=.....C, SSID="wifi6_test"
8	2023-06-12 18:34:49.79180	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
9	2023-06-12 18:34:49.79493	0.003066	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=22, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
10	2023-06-12 18:34:49.81282	0.015789	Netgear_48:78:35	Cisco_13:180:e7	802.11	360	5	-49 dBm	Probe Request, S/W=1, F/W=, Flags=.....C, SSID="wifi6_test"
11	2023-06-12 18:34:49.81282	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
12	2023-06-12 18:34:49.87491	0.000000	192.168.1.15	192.168.1.121	802.11	194	5	-49 dBm	Authentication, S/W=, F/W=, Flags=.....C
13	2023-06-12 18:34:49.87491	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
14	2023-06-12 18:34:49.89653	0.021812	Cisco_13:180:e7	Netgear_48:78:35	802.11	194	5	-37 dBm	Authentication, S/W=54, F/W=, Flags=.....C
15	2023-06-12 18:34:49.89653	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Acknowledgment, Flags=.....C
16	2023-06-12 18:34:49.90496	0.000000	Cisco_13:180:e7	Eurocast	802.11	588	5	-37 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
17	2023-06-12 18:34:49.90496	0.000000	Netgear_48:78:35	Cisco_13:180:e7	802.11	130	5	-49 dBm	Authentication, S/W=, F/W=, Flags=.....C
18	2023-06-12 18:34:49.90496	0.000000	192.168.1.15	192.168.1.121	802.11	130	5	-37 dBm	Authentication, S/W=, F/W=, Flags=.....C
19	2023-06-12 18:34:49.90496	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Association Request, S/W=, F/W=, Flags=.....C, SSID="wifi6_test"
20	2023-06-12 18:34:49.90496	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Association Request, S/W=, F/W=, Flags=.....C, SSID="wifi6_test"
21	2023-06-12 18:34:49.90496	0.000000	Netgear_48:78:35	Cisco_13:180:e7	802.11	216	5	-49 dBm	Association Request, S/W=, F/W=, Flags=.....C, SSID="wifi6_test"
22	2023-06-12 18:34:49.90496	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
23	2023-06-12 18:34:49.91174	0.005180	Cisco_13:180:e7	Netgear_48:78:35	802.11	262	5	-36 dBm	Association Response, S/W=, F/W=, Flags=.....C
24	2023-06-12 18:34:49.91174	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Acknowledgment, Flags=.....C
25	2023-06-12 18:34:49.91174	0.000000	Netgear_48:78:35	Eurocast	802.11	114	5	-37 dBm	u, func=unknown; DSAP 0x12 Individual, SSAP 0x02 Command
26	2023-06-12 18:34:49.91174	0.000000	Netgear_48:78:35	Eurocast	802.11	114	5	-36 dBm	u, func=unknown; DSAP 0x7a Individual, SSAP 0x0a Response
27	2023-06-12 18:34:49.92236	0.010267	Cisco_13:180:e7	Netgear_48:78:35	EAPOL	221	5	-36 dBm	Key (Message 1 of 4)
28	2023-06-12 18:34:49.92236	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-49 dBm	Acknowledgment, Flags=.....C
29	2023-06-12 18:34:49.99951	0.077235	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
30	2023-06-12 18:34:50.10458	0.104029	Cisco_13:180:e7	Eurocast	802.11	588	5	-36 dBm	Beacon frame, S/W=27, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
31	2023-06-12 18:34:50.20400	0.100000	Cisco_13:180:e7	Eurocast	802.11	588	5	-46 dBm	Beacon frame, S/W=22, F/W=, Flags=.....C, B=100, SSID="wifi6_test"
32	2023-06-12 18:34:50.21161	0.007615	Netgear_48:78:35	Cisco_13:180:e7	EAPOL	226	5	-55 dBm	Key (Message 2 of 4)
33	2023-06-12 18:34:50.21161	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
34	2023-06-12 18:34:50.21161	0.000000	Netgear_48:78:35	Eurocast	802.11	296	5	-49 dBm	Key (Message 3 of 4)
35	2023-06-12 18:34:50.21376	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-58 dBm	Acknowledgment, Flags=.....C
36	2023-06-12 18:34:50.21454	0.000000	Netgear_48:78:35	Cisco_13:180:e7	EAPOL	199	5	-56 dBm	Key (Message 4 of 4)
37	2023-06-12 18:34:50.22346	0.000000	Netgear_48:78:35	Eurocast	802.11	114	5	-43 dBm	Key (Message 1 of 4)
38	2023-06-12 18:34:50.22346	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
39	2023-06-12 18:34:50.22872	0.006367	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
40	2023-06-12 18:34:50.22849	0.003128	192.168.1.15	192.168.1.121	802.11	119	5	-44 dBm	Trigger Buffer Status Report Poll (BSRP), Flags=.....C
41	2023-06-12 18:34:50.22849	0.000000	Netgear_48:78:35	Eurocast	802.11	221	5	-44 dBm	u, func=unknown; DSAP 0x0b Group, SSAP 0x0b Response
42	2023-06-12 18:34:50.22849	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-54 dBm	Acknowledgment, Flags=.....C

Indicadores WPA3 SAE + FT

Aquí podemos observar clientes Wi-Fi 6E asociando:

Intel AX211

Conexión OTA con enfoque en la información RSN del cliente:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
1811	2023-06-12 18:51:39.24979	0.021337	IntelCor_98:53:8f	Cisco_13:180:e7	802.11	194	5	-42 dBm	Authentication, S/W=, F/W=, Flags=.....C
1812	2023-06-12 18:51:39.24979	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1813	2023-06-12 18:51:39.254827	0.007634	Cisco_13:180:e7	IntelCor_98:53:8f	802.11	194	5	-36 dBm	Authentication, S/W=59, F/W=, Flags=.....C
1814	2023-06-12 18:51:39.254827	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
1815	2023-06-12 18:51:39.259394	0.002567	IntelCor_98:53:8f	Cisco_13:180:e7	802.11	130	5	-46 dBm	Authentication, S/W=, F/W=, Flags=.....C
1816	2023-06-12 18:51:39.259394	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1817	2023-06-12 18:51:39.263479	0.004235	Cisco_13:180:e7	IntelCor_98:53:8f	802.11	130	5	-36 dBm	Authentication, S/W=50, F/W=, Flags=.....C
1818	2023-06-12 18:51:39.263479	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-42 dBm	Acknowledgment, Flags=.....C
1819	2023-06-12 18:51:39.263479	0.000000	IntelCor_98:53:8f	Cisco_13:180:e7	802.11	250	5	-46 dBm	Association Request, S/W=, F/W=, Flags=.....C, SSID="wifi6_test"
1820	2023-06-12 18:51:39.263479	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1826	2023-06-12 18:51:39.271442	0.018463	IntelCor_98:53:8f	Broadcast	LLC	114	5	-36 dBm	I, H(K)=, N(S)=; DSAP 0x0a Group, SSAP 0x0a Response
1827	2023-06-12 18:51:39.271442	0.000000	IntelCor_98:53:8f	Broadcast	LLC	114	5	-36 dBm	I, H(K)=, N(S)=; DSAP 0x0a Group, SSAP 0x0a Response
1828	2023-06-12 18:51:39.277402	0.000000	192.168.1.15	192.168.1.121	802.11	262	5	-36 dBm	Association Response, S/W=, F/W=, Flags=.....C
1829	2023-06-12 18:51:39.277402	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-43 dBm	Acknowledgment, Flags=.....C
1830	2023-06-12 18:51:39.281817	0.003705	Cisco_13:180:e7	Broadcast	802.11	517	5	-36 dBm	Beacon frame, S/W=71, F/W=, Flags=.....C, B=100, SSID="wifi6_test_02"
1834	2023-06-12 18:51:39.311349	0.025242	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1835	2023-06-12 18:51:39.311349	0.000449	192.168.1.15	192.168.1.121	802.11	76	5	-52 dBm	Clear-to-send, Flags=.....C
1842	2023-06-12 18:51:39.339808	0.001348	192.168.1.15	192.168.1.121	802.11	76	5	-53 dBm	Clear-to-send, Flags=.....C
1844	2023-06-12 18:51:39.339808	0.000135	192.168.1.15	192.168.1.121	802.11	82	5	-38 dBm	Request-to-send, Flags=.....C
1845	2023-06-12 18:51:39.339808	0.001839	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1846	2023-06-12 18:51:39.339808	0.000030	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1847	2023-06-12 18:51:39.400924	0.000712	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1848	2023-06-12 18:51:39.401191	0.000667	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1849	2023-06-12 18:51:39.402035	0.000044	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1850	2023-06-12 18:51:39.402035	0.000000	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1851	2023-06-12 18:51:39.402035	0.000036	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1852	2023-06-12 18:51:39.406474	0.001321	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1853	2023-06-12 18:51:39.406474	0.000732	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1854	2023-06-12 18:51:39.406877	0.000071	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1855	2023-06-12 18:51:39.406877	0.000769	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1856	2023-06-12 18:51:39.406877	0.000044	192.168.1.15	192.168.1.121	802.11	76	5	-36 dBm	Acknowledgment, Flags=.....C
1857	2023-06-12 18:51:39.407244	0.000563	192.168.1.15	192.168.1.121	802.11	82	5	-36 dBm	Request-to-send, Flags=.....C
1859	2023-06-12 18:51:39.407327	0.000023	Cisco_13:180:e7	IntelCor_98:53:8f	EAPOL	221	5	-52 dBm	Key (Message 1 of 4)
1860	2023-06-12 18:51:39.407327	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-48 dBm	Acknowledgment, Flags=.....C
1862	2023-06-12 18:51:39.420712	0.003185	IntelCor_98:53:8f	Cisco_13:180:e7	EAPOL	230	5	-56 dBm	Key (Message 2 of 4)
1863	2023-06-12 18:51:39.420712	0.000000	192.168.1.15	192.168.1.121	802.11	76	5	-37 dBm	Acknowledgment, Flags=.....C
1864	2023-06-12 18:51:39.421220	0.002180	192.168.1.15	192.168					



## Detalles del cliente en WLC:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The main panel displays a list of clients under 'Monitoring > Wireless > Clients'. One client is selected, and its details are shown in the 'Client' pane on the right. The 'Security Information' tab is active, showing the following settings:

- Client State Servers: None
- Client ACLs: None
- Client Entry Create Time: 11 seconds
- Policy Type: WPA3
- Encryption Cipher: CCMP (AES)
- Authentication Key Management: SAE
- EAP Type: Not Applicable
- Session Timeout: 86400
- Session Manager:
  - Point of Attachment: capwap\_90000010
  - IF ID: 0x90000010
  - Authorized: TRUE
  - Common Session ID: 0000000000000FD2B11A5CB6
  - Acct Session ID: 0x00000000
  - Auth Method Status List: SAE
  - Method: SAE

## 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:

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI in the 'Edit WLAN' configuration page. The 'Security' tab is selected, and the 'Auth Key Mgmt' section is highlighted with a red box. The configuration is as follows:

- General: WPA3 (selected)
- Layer2: WPA3 (selected)
- WPA Parameters:
  - WPA Policy: WPA3
  - GTK Randomize: Disabled
  - Transition: Disabled
- WPA2/WPA3 Encryption:
  - AES(CCMP128): Enabled
  - GCMP128: Disabled
  - CCMP256: Disabled
  - GCMP256: Disabled
- Protected Management Frame: Required
- Association Comeback Timer: 1
- SA Query Time: 200
- Fast Transition: Enabled
  - Over the OS: Disabled
  - Reassociation Timeout: 20
- Auth Key Mgmt (highlighted):
  - SAE: Enabled
  - FT + SAE: Enabled
  - OWE: Disabled
  - FT + 802.1x: Disabled
  - 802.1x-SHA256: Disabled

Configuración de seguridad WPA3 Enterprise 802.1x-SHA256 + FTWLAN

Ver en WLC GUI de los ajustes de seguridad WLAN:

The screenshot shows the bottom status bar of the WLC GUI, displaying the WLAN configuration: [WPA3][FT + 802.1x][AES][PMF 802.1x][FT Enabled]

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



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:

The image shows a Wireshark packet capture of a WLAN re-association and authentication process. The capture is divided into several sections:

- Probing and authentication frames:** Shows the initial probe requests and responses, including authentication and association request frames.
- Regular Association:** Shows the successful completion of the association process.
- EAP Exchange:** Shows the EAP exchange, including the EAP-Request/Protected EAP (PEAP) frame and the EAP-Response/Protected EAP (PEAP) frame. A red box highlights the PMKID used for FT in the EAP exchange.
- 4 Way Handshake:** Shows the 4-way handshake process, including the EAP-Request/Protected EAP (PEAP) frame and the EAP-Response/Protected EAP (PEAP) frame.

Flujo de conexión WPA3 Enterprise 802.1x + FT Ax211

Detalles del cliente en WLC:

The screenshot shows the Cisco WLC GUI with the following details for the client:

- Client Properties:** Client MAC Address: 266b.3598.580f, IPv4 Address: 192.168.1.150, IPv6 Address: 2001:8a0:rb91:1c00:c07a:1190:8069:7398, AP Name: AP9136\_5C-F524, SSID: wlan1
- Security Information:**
  - Re-Authentication Timeout: 1800 sec (Remaining time: 462 sec)
  - Client State Servers: None
  - Client ACLs: None
  - Client Entry Create Time: 1338 seconds
  - Policy Type: WPA3
  - Encryption Cipher: CCMP (AES)
  - Authentication Key Management: FT-802.1x
  - EAP Type: PEAP
  - Session Timeout: 1800

Detalles del cliente WPA3 Enterprise 802.1x + FT

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

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
3028	16.492589	0.182243	Cisco_Sc180:8c	Broadcast	802.11	364	69	-36	dtm Beacon Frame, Src=8c, Pkts, Flags.....C, B1=80, SSID=WiFi
3029	16.504273	0.120828	Cisco_Sc180:8c	Broadcast	802.11	364	69	-36	dtm Beacon Frame, Src=8c, Pkts, Flags.....C, B1=80, SSID=WiFi
3030	16.564794	0.059523	IntelCor_98158:0f	Broadcast	802.11	328	69	-45	dtm Probe Request, Src=27, Pkts, Flags.....C, SSID=8c1dca2c (E
3031	16.564794	0.000000	Cisco_Sc180:8c	Broadcast	802.11	368	69	-38	dtm Probe Response, Src=8c, Pkts, Flags.....C, B1=80, SSID=WiFi
3079	16.695629	0.013635	Cisco_Sc180:8c	Broadcast	802.11	364	69	-38	dtm Beacon Frame, Src=8c, Pkts, Flags.....C, B1=80, SSID=WiFi
3088	16.702455	0.000220	IntelCor_98158:0f	Cisco_Sc180:8c	802.11	235	69	-46	dtm Authentication, Src=11, Pkts, Flags.....C
3089	16.701542	0.000087	192.168.1.121	192.168.1.121	802.11	76	69	-39	dtm Acknowledgment, Flags.....C
3092	16.706278	0.004736	Cisco_Sc180:8c	IntelCor_98158:0f	802.11	247	69	-38	dtm Authentication, Src=15, Pkts, Flags.....C
3093	16.706278	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-39	dtm Acknowledgment, Flags.....C
3098	16.709897	0.000000	IntelCor_98158:0f	Cisco_Sc180:8c	802.11	372	69	-48	dtm Association Request, Src=27, Pkts, Flags.....C, SSID=WiFi
3099	16.709827	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-38	dtm Acknowledgment, Flags.....C
3105	16.718126	0.000020	Cisco_Sc180:8c	IntelCor_98158:0f	802.11	433	69	-39	dtm Association Response, Src=8c, Pkts, Flags.....C
3108	16.731226	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-41	dtm Acknowledgment, Flags.....C
3109	16.727450	0.000220	IntelCor_98158:0f	192.168.1.121	223	69	-59	dtm I P, N(R)=8, N(S)=102; DSAP SNAP Group, SSAP Bk2 Response	
3109	16.727457	0.000188	192.168.1.15	192.168.1.121	802.11	76	69	-47	dtm Acknowledgment, Flags.....C
3109	16.727457	0.013376	IntelCor_98158:0f	Broadcast	LLC	525	69	-59	dtm U P, func=0x0a; DSAP Bk0 Individual, SSAP Bk2 Command
3109	16.728833	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags.....C
3099	16.742984	0.000071	Cisco_Sc180:8c	IntelCor_98158:0f	LLC	383	69	-50	dtm I P, N(R)=8, N(S)=102; DSAP Upperman-Basis Individual, SSAP B
3100	16.742984	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-53	dtm Acknowledgment, Flags.....C
3101	16.742984	0.000000	Cisco_Sc180:8c	IntelCor_98158:0f	LLC	383	69	-50	dtm I, N(R)=8, N(S)=75; DSAP SNAP Individual, SSAP Bk7 Command
3102	16.742984	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-53	dtm Acknowledgment, Flags.....C
3106	16.768980	0.012522	IntelCor_98158:0f	192.168.1.121	223	69	-59	dtm I P, N(R)=8, N(S)=101; DSAP Bk0 Individual, SSAP Bk2 Respons	
3107	16.768833	0.000124	192.168.1.15	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags.....C
3109	16.772475	0.003842	Cisco_Sc180:8c	IntelCor_98158:0f	802.11	118	69	-48	dtm Action, Src=27, Pkts, Flags.....C
3110	16.772475	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-52	dtm Acknowledgment, Flags.....C
3111	16.773242	0.000000	IntelCor_98158:0f	Broadcast	LLC	179	69	-59	dtm I P, N(R)=8, N(S)=101; DSAP SNAP Group, SSAP 150 Network Layer
3114	16.773242	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags.....C
3115	16.773436	0.000204	IntelCor_98158:0f	Cisco_Sc180:8c	802.11	118	69	-48	dtm Action, Src=11, Pkts, Flags.....C [Malformed Packet]
3116	16.773436	0.000000	192.168.1.121	192.168.1.121	802.11	76	69	-41	dtm Acknowledgment, Flags.....C
3120	16.779112	0.000000	AttiLoca_98159:af	IntelCor_98158:0f	LLC	223	69	-49	dtm U, func=0x0a; DSAP Bk02 Group, SSAP Bk2a Command
3122	16.779545	0.001433	IntelCor_98158:0f	192.168.1.121	802.11	118	69	-48	dtm Action, Src=27, Pkts, Flags.....C
3123	16.779545	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-52	dtm Acknowledgment, Flags.....C
3124	16.779599	0.001854	IntelCor_98158:0f	Cisco_Sc180:8c	802.11	118	69	-48	dtm Action, Src=8c, Pkts, Flags.....C [Malformed Packet]: length
3125	16.779599	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags.....C
3128	16.781489	0.003858	AttiLoca_98159:af	IntelCor_98158:0f	LLC	197	69	-49	dtm U P, func=0x0e; DSAP Bk0e Individual, SSAP Bk0c Command
3132	16.781489	0.000000	IntelCor_98158:0f	AttiLoca_98159:af	LLC	222	69	-58	dtm U, func=0x0a; DSAP Bk0c Group, SSAP Bk0d Command
3133	16.781489	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47	dtm Acknowledgment, Flags.....C
3136	16.790825	0.000000	IntelCor_98158:0f	192.168.1.121	223	69	-59	dtm I P, N(R)=8, N(S)=101; DSAP SNAP Group, SSAP 150 Network Layer	
3137	16.790815	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47	dtm Acknowledgment, Flags.....C
3140	16.793424	0.002599	IntelCor_98158:0f	Broadcast	LLC	525	69	-58	dtm I, N(R)=8, N(S)=22; DSAP HP Extended LLC Group, SSAP NetWare
3141	16.793477	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-47	dtm Acknowledgment, Flags.....C
3144	16.793774	0.000027	IntelCor_98158:0f	Broadcast	LLC	179	69	-58	dtm U, func=0x02; N(R)=0; DSAP Bk0 Individual, SSAP Bk2 Respons
3145	16.793849	0.000075	192.168.1.15	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags.....C
3149	16.794563	0.000714	IntelCor_98158:0f	192.168.1.121	802.11	183	69	-48	dtm I P, N(R)=12, N(S)=113; DSAP Bk0c Group, SSAP Bk70 Respons
3150	16.794620	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags.....C
3154	16.794928	0.000000	IntelCor_98158:0f	192.168.1.121	223	69	-58	dtm I P, func=0x03; N(R)=0; DSAP Bk0c Group, SSAP Bk76 Respons	
3155	16.794909	0.000004	192.168.1.15	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags.....C
3158	16.795624	0.000824	IntelCor_98158:0f	192.168.1.121	223	69	-58	dtm U P, func=0x0a; DSAP MALL SSAP Individual, SSAP Banyan View	
3220	16.795959	0.000000	192.168.1.15	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags.....C
3248	16.797085	0.000000	IntelCor_98158:0f	192.168.1.121	223	69	-58	dtm U, func=0x09; N(R)=0; DSAP Bk0c Group, SSAP Bk72 Respons	
3262	16.795852	0.000007	192.168.1.15	192.168.1.121	802.11	76	69	-48	dtm Acknowledgment, Flags.....C

Itinerancia AX211 con FT sobre DS

También podemos ver los eventos de itinerancia de FT:

Monitoring > Wireless > Clients

Clients Sleeping Clients Excluded Clients

Selected 0 out of 1 Clients

Client MAC Address	IPv4 Address	IPv6 Address	AP Name	SSID	WLAN ID	Client Type
286b.3598.580f	192.168.1.159	N/A	AP01_RC_9136_F80C	wifi6_test	5	WLAN

Client

360 View General QOS Statistics ATF Statistics **Mobility History** Call Statistics

Recent association history:

AP Name	BSSID	AP Slot	Assoc Time	Instance	Mobility Role	Run Latency (ms)	Roam Type
AP01_RC_9136_F80C	00d1.1d8d.a018	3	08/04/2023 14:24:27	0	Local	15	802.11R
AP9136_5C_F524	00d1.1d8d.7d38	3	08/04/2023 14:22:59	0	Local	6	802.11R

WPA3 Enterprise con FT

Y el cliente traza desde wlc:

```

Logging display requested on 2023/08/04 14:27:55 (GMT) for Hostname: [wMCO-9800-01], Model: [C9500-CL-F91, Version: [17.09.03], SN: [59Y358S1909], MD_SN: [59Y358S1909]
2023/08/04 14:22:59.31858237 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Re-Association Received. BSSID 00d1.1d8d.7d38, WLAN wifi6_test, Slot 3 AP 00d1.1d8d.7d38, AP9136_5C_F524, old BSSID 00d1.1d8d.a018
2023/08/04 14:22:59.31858237 [wMCO_R_0-0] (1): [dot11] [15218]: (note) MAC: 286b.3598.580f Association success. Aid 33, Roaming = True, WCB = False, llw = True, llw = True Fast Roam = True
2023/08/04 14:22:59.31849811 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Delete mobile payload sent for BSSID: 00d1.1d8d.a018 WTP mac: 00d1.1d8d.a018 slot id: 3
2023/08/04 14:22:59.31849811 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Mobility discovery triggered. Client mode: Local
2023/08/04 14:22:59.32104197 [wMCO_R_0-0] (1): [client-auth] [15218]: (note) MAC: 286b.3598.580f Add mobile sent. Client state flags: 0x71 BSSID: MAC: 00d1.1d8d.7d38 capwap IFF: 0x00000000, Add mobiles sent: 1
2023/08/04 14:22:59.32104197 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Mobility discovery triggered. Client mode: Local
2023/08/04 14:22:59.32104197 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Delete mobile payload sent for BSSID: 00d1.1d8d.7d38 WTP mac: 00d1.1d8d.7d38 slot id: 3
2023/08/04 14:22:59.32104197 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Re-Association Received. BSSID 00d1.1d8d.a018, WLAN wifi6_test, Slot 3 AP 00d1.1d8d.a018, AP01_RC_9136_F80C, old BSSID 00d1.1d8d.7d38
2023/08/04 14:22:59.32104197 [wMCO_R_0-0] (1): [client-auth] [15218]: (note) MAC: 286b.3598.580f Add mobile sent. Client state flags: 0x71 BSSID: MAC: 00d1.1d8d.7d38 capwap IFF: 0x00000000, Add mobiles sent: 1
2023/08/04 14:22:59.32104197 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS --> S_CO_DEATH_PLUMB_IN_PROGRESS
2023/08/04 14:22:59.32146355 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_DEATH_PLUMB_IN_PROGRESS --> S_CO_LP_LEARN_IN_PROGRESS
2023/08/04 14:22:59.32146355 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_LP_LEARN_IN_PROGRESS --> S_CO_RRM
2023/08/04 14:24:17.91858521 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_LP_LEARN_IN_PROGRESS --> S_CO_LP_LEARN_IN_PROGRESS
2023/08/04 14:24:17.91858521 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Association success. Aid 33, Roaming = True, WCB = False, llw = True, llw = True Fast Roam = True
2023/08/04 14:24:17.91858521 [wMCO_R_0-0] (1): [client-auth] [15218]: (note) MAC: 286b.3598.580f Delete mobile payload sent for BSSID: 00d1.1d8d.7d38 WTP mac: 00d1.1d8d.7d38 slot id: 3
2023/08/04 14:24:17.91858521 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Mobility discovery triggered. Client mode: Local
2023/08/04 14:24:17.91858521 [wMCO_R_0-0] (1): [client-auth] [15218]: (note) MAC: 286b.3598.580f Add mobile sent. Client state flags: 0x71 BSSID: MAC: 00d1.1d8d.a018 capwap IFF: 0x00000000, Add mobiles sent: 1
2023/08/04 14:24:17.91858521 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Mobility discovery triggered. Client mode: Local
2023/08/04 14:24:17.91858521 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Delete mobile payload sent for BSSID: 00d1.1d8d.7d38 WTP mac: 00d1.1d8d.7d38 slot id: 3
2023/08/04 14:24:17.91858521 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Re-Association Received. BSSID 00d1.1d8d.a018, WLAN wifi6_test, Slot 3 AP 00d1.1d8d.a018, AP01_RC_9136_F80C, old BSSID 00d1.1d8d.7d38
2023/08/04 14:24:17.91858521 [wMCO_R_0-0] (1): [client-auth] [15218]: (note) MAC: 286b.3598.580f Add mobile sent. Client state flags: 0x71 BSSID: MAC: 00d1.1d8d.a018 capwap IFF: 0x00000000, Add mobiles sent: 1
2023/08/04 14:24:17.91858521 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_MOBILITY_DISCOVERY_IN_PROGRESS --> S_CO_DEATH_PLUMB_IN_PROGRESS
2023/08/04 14:24:17.91858521 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_DEATH_PLUMB_IN_PROGRESS --> S_CO_LP_LEARN_IN_PROGRESS
2023/08/04 14:24:17.91858521 [wMCO_R_0-0] (1): [client-orch-stm] [15218]: (note) MAC: 286b.3598.580f Client state transition: S_CO_LP_LEARN_IN_PROGRESS --> S_CO_RRM

```

NetGear A8000

WPA3-Enterprise no se admite en este cliente.

Píxel 6a

Conexión OTA con enfoque en la información RSN del cliente:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
878	1.408897	0.302322	Cisco_05:0a:08:13:18	Broadcast	802.11	428	69	-17	dbm
879	1.408907	0.120370	Cisco_05:0a:08:13:18	Broadcast	802.11	204	69	-29	dbm
880	1.561362	0.000405	Cisco_05:0a:08:13:18	Broadcast	802.11	428	69	-17	dbm
882	1.564878	0.000716	Cisco_05:0a:08:13:18	Broadcast	802.11	374	69	-17	dbm
928	1.675576	0.114498	Cisco_05:0a:08:13:18	Broadcast	802.11	428	69	-17	dbm
932	1.675989	0.000217	Cisco_05:0a:08:13:18	Cisco_05:0a:08:13:18	802.11	308	69	-14	dbm
932	1.675989	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-17	dbm
923	1.679651	0.003842	Cisco_05:0a:08:13:18	Broadcast	802.11	108	69	-17	dbm
924	1.679651	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-14	dbm
925	1.682824	0.000000	192.168.1.15	192.168.1.122	802.11	284	69	-14	dbm
926	1.682121	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-17	dbm
930	1.782511	0.023970	Cisco_05:0a:08:13:18	Google_72:8a:96	802.11	313	69	-17	dbm
931	1.782511	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-13	dbm
932	1.782629	0.000620	Cisco_05:0a:08:13:18	Google_72:8a:96	EAP	309	69	-17	dbm
933	1.782629	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-11	dbm
939	1.747377	0.017007	Google_72:8a:96	Cisco_05:0a:08:13:18	EAP	117	69	-13	dbm
940	1.747377	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-17	dbm
942	1.784248	0.012047	Cisco_05:0a:08:13:18	Google_72:8a:96	EAP	110	69	-17	dbm
943	1.784248	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-11	dbm
945	1.788896	0.005672	Cisco_05:0a:08:13:18	Broadcast	802.11	428	69	-17	dbm
946	1.788896	0.000180	Google_72:8a:96	Cisco_05:0a:08:13:18	LIC	124	69	-17	dbm
949	1.794517	0.018971	Google_72:8a:96	Cisco_05:0a:08:13:18	802.11	241	69	-48	dbm
950	1.794517	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-17	dbm
956	1.794529	0.015081	Cisco_05:0a:08:13:18	Google_72:8a:96	EAP	1116	69	-17	dbm
957	1.794529	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-48	dbm
958	1.797058	0.002520	Google_72:8a:96	Cisco_05:0a:08:13:18	EAP	110	69	-17	dbm
959	1.797058	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-17	dbm
960	1.801724	0.004656	Cisco_05:0a:08:13:18	Google_72:8a:96	802.11	382	69	-17	dbm
961	1.801724	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-19	dbm
963	1.820673	0.001870	Google_72:8a:96	Cisco_05:0a:08:13:18	802.11	238	69	-17	dbm
964	1.820673	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-17	dbm
965	1.820990	0.004317	Cisco_05:0a:08:13:18	Google_72:8a:96	802.11	161	69	-17	dbm
966	1.820990	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-19	dbm
968	1.820990	0.004229	Google_72:8a:96	Cisco_05:0a:08:13:18	EAP	110	69	-19	dbm
969	1.820990	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-17	dbm
971	1.831178	0.003960	Cisco_05:0a:08:13:18	Google_72:8a:96	802.11	144	69	-17	dbm
972	1.831178	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-19	dbm
973	1.831728	0.004210	Google_72:8a:96	Cisco_05:0a:08:13:18	802.11	132	69	-19	dbm
974	1.831728	0.000078	192.168.1.15	192.168.1.122	802.11	76	69	-17	dbm
976	1.840795	0.003200	Cisco_05:0a:08:13:18	Google_72:8a:96	802.11	171	69	-17	dbm
977	1.840795	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-19	dbm
978	1.845522	0.004817	Google_72:8a:96	Cisco_05:0a:08:13:18	802.11	206	69	-19	dbm
979	1.845522	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-17	dbm
984	1.848494	0.012072	Cisco_05:0a:08:13:18	Google_72:8a:96	802.11	190	69	-17	dbm
985	1.848494	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-19	dbm
986	1.866887	0.002115	Google_72:8a:96	Cisco_05:0a:08:13:18	802.11	145	69	-48	dbm
987	1.866887	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-17	dbm
988	1.870058	0.003771	Cisco_05:0a:08:13:18	Broadcast	802.11	428	69	-17	dbm
989	1.870058	0.000000	192.168.1.15	192.168.1.122	802.11	243	69	-17	dbm
990	1.870058	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-19	dbm
992	1.877128	0.006470	Google_72:8a:96	Cisco_05:0a:08:13:18	EAP	110	69	-18	dbm
993	1.877128	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-17	dbm
996	1.920065	0.002917	Cisco_05:0a:08:13:18	Google_72:8a:96	802.11	108	69	-17	dbm
997	1.920065	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-19	dbm
998	1.920065	0.000000	Cisco_05:0a:08:13:18	Google_72:8a:96	EAPOL	223	69	-17	dbm
999	1.920065	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-19	dbm
1000	1.920255	0.000200	Google_72:8a:96	Cisco_05:0a:08:13:18	EAPOL	346	69	-48	dbm
1001	1.920255	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-17	dbm
1004	1.920677	0.003422	Cisco_05:0a:08:13:18	Google_72:8a:96	EAPOL	423	69	-17	dbm
1005	1.920677	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-19	dbm
1006	1.920886	0.003200	Google_72:8a:96	Cisco_05:0a:08:13:18	EAPOL	199	69	-19	dbm
1007	1.920886	0.000000	192.168.1.15	192.168.1.122	802.11	76	69	-17	dbm

```

> Frame 925: 261 bytes on wire (2088 bits), 261 bytes captured (2088 bits) on interface DeviceWPF_04578005-2998-4006-8C31-C3A13
> Ethernet II, Src: Cisco_05:0a:08:13:18:00:00:00:00:00:00, Dst: Indefina_07:cf:8e:0e:1a:3a:00:07:cf:8e
> Internet Protocol Version 4, Src: 192.168.1.15, Dst: 192.168.1.122
> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
> AirFlow/OutStream encapsulated IEEE 802.11
> IEEE 802.11 radio information
> IEEE 802.11 Association Request, Flags: .....C
> IEEE 802.11 Wireless Management
> Fixed parameters (4 bytes)
  > Tagged parameters (167 bytes)
    > Tag: SSID parameter set: "wifi6e_test"
    > Tag: Supported Rates (6R): 9, 12(R), 18, 24(R), 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability Mtr: 9, Max: 29
    > Tag: Supported Channels
  > Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag Length: 28
    RSN Version: 1
    > Group Cipher Suite: 00:0f:ac (See IEEE 802.11 AES (CCM))
    Pairwise Cipher Suite Count: 1
    Pairwise Cipher Suite List: 00:0f:ac (See IEEE 802.11 AES (CCM))
    Auth Key Management (AKM) Suite Count: 1
    Auth Key Management (AKM) List: 00:0f:ac (See IEEE 802.11 FT over IEEE 802.1X)
    Auth Key Management (AKM) OUI: 00:0f:ac (See IEEE 802.11)
    Auth Key Management (AKM) type: FT over IEEE 802.1X (1)
  > RSN Capabilities: 00:00
    .....0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
    .....0 = RSN No Pairwise capabilities: Transmitter can support MP default key 0 simultaneously w/ft
    .....0 = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/TKkeySA (0x0)
    .....00 = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/TKkeySA (0x0)
    .....1 = Management frame Protection Required: True
    .....1 = Management frame Protection Capable: True
    .....0 = 32bit M211-band RSN: False
    .....0 = Perkey Enabled: False
    ..... = Extended key ID for Individually Addressed Frames: Not supported
  PMSN Count: 0
  PMSN List
  > Group Management Cipher Suite: 00:0f:ac (See IEEE 802.11 GIP (128))
  > Tag: W Enabled Capabilities (5 octets)
  > Tag: Mobility domain
  > Tag: Supported Operating Classes
  > Tag: Extended Capabilities (20 octets)
  > Ext Tag: HE Capabilities
  > Ext Tag: HE 4-0 Band Capabilities
  > Tag: Vendor Specific: Broadcom
    Tag Number: Vendor Specific (221)
    Tag Length: 10
    OUI: 00:13:18 (Broadcom)
    Vendor Specific OUI Type: 2
    Vendor Specific Data: 00000000000000
  > Tag: Vendor Specific: Microsoft Corp.: WPVUE: Information Element
  
```

Asociación WPA3 Enterprise 802.1x + FT Pixel6a

Detalles del cliente en WLC:

Client Properties | AP Properties | **Security Information** | Client Statistics | QoS Properties | EoGRE

- Re-Authentication Timeout: 1800 sec (Remaining time: 267 sec)
- Client State Servers: None
- Client ACLs: None
- Client Entry Create Time: 1536 seconds
- Policy Type: WPA3
- Encryption Cipher: CCMP (AES)
- Authentication Key Management: FT-802.1x
- EAP Type: PEAP
- Session Timeout: 1800

Detalles del cliente WPA3 Enterprise 802.1x + FT Pixel6a

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

Recent association history:

AP Name	BSSID	AP Slot	Assoc Time	Instance	Mobility Role	Run Latency (ms)	Room Type
AP01_RC_9136_F80C	00d11dad a018	3	07/12/2023 11:46:16	0	Local	7	802.11R
AP9136_SC_F524	00d11dad 7a38	3	07/12/2023 11:43:48	0	Local	3161	N/A

Samsung S23

Conexión OTA con enfoque en la información RSN del cliente:





### 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	<input type="checkbox"/>	WPA2 Policy	<input type="checkbox"/>
GTK Randomize	<input type="checkbox"/>	WPA3 Policy	<input checked="" type="checkbox"/>
Transition Disable	<input type="checkbox"/>		

**Fast Transition**

Status

Over the DS

Reassociation Timeout \*

**WPA2/WPA3 Encryption**

AES(CCMP128)	<input type="checkbox"/>	CCMP256	<input type="checkbox"/>
GCMP128	<input checked="" type="checkbox"/>	GCMP256	<input type="checkbox"/>

**Auth Key Mgmt**

SUITEB-1X

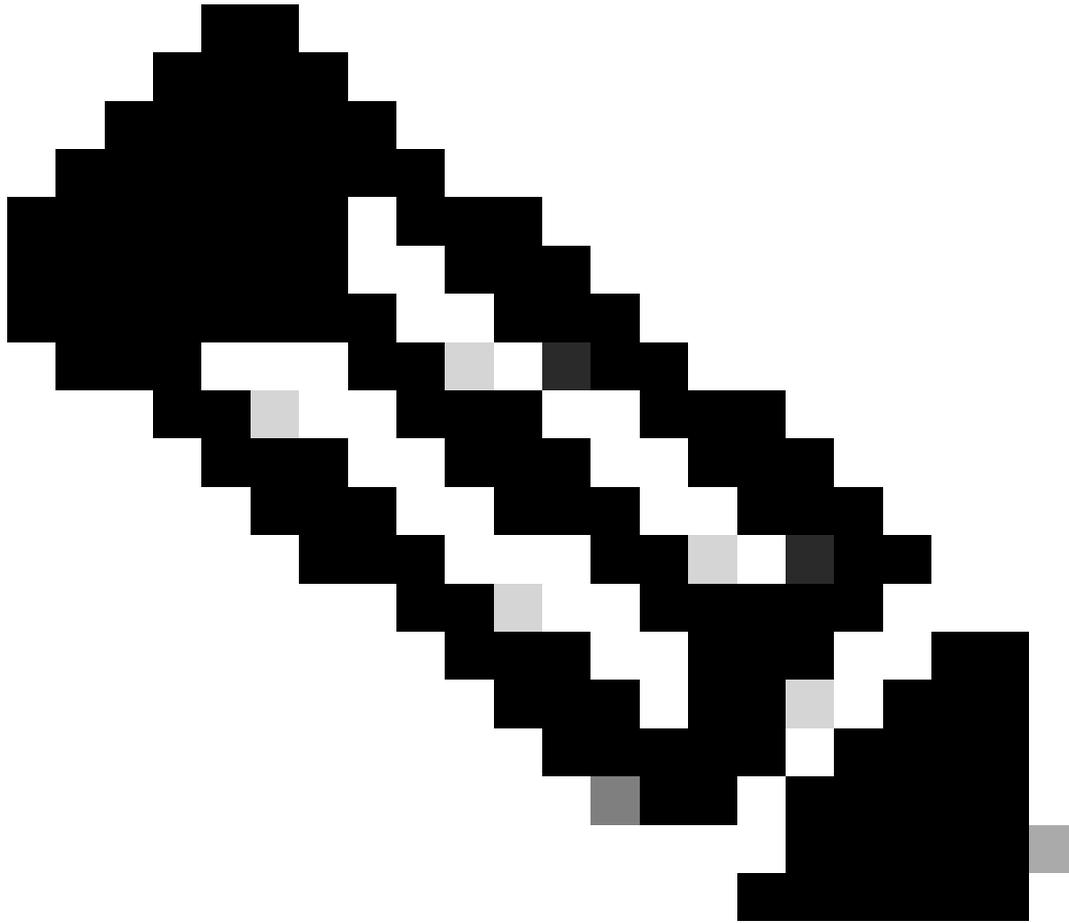
**Protected Management Frame**

PMF

Association Comeback Timer\*

SA Query Time\*

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:

□ w66E\_test 5 w66E\_test [WPA3][SUITEB-1X][GCMP128]

Verificación de las balizas OTA:

No.	Time	Delta	Source	Destination	Protocol	Length	Channel	Signal	Info
37376	59.189776	0.820482	Cisco_05:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2802, Fw=0, Flags=.....C, B=100, SSID=...	> frame 37626: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface 'Device\NPF_{04576965-2998-4456-8C13-C4}
37385	59.190516	0.820498	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2803, Fw=0, Flags=.....C, B=100, SSID=...	> Ethernet II, Src: Cisco_02:00:07 (74:11:32:02:07:47), Dst: Unknown_07:c7:0e (08:00:00:07:c7:0e)
37396	59.191709	0.820481	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2804, Fw=0, Flags=.....C, B=100, SSID=...	> Internet Protocol Version 4, Src: 192.168.1.121, Dst: 192.168.1.121
37414	59.192161	0.820462	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2805, Fw=0, Flags=.....C, B=100, SSID=...	> User Datagram Protocol, Src Port: 5555, Dst Port: 5000
37424	59.192713	0.820472	Cisco_05:00:18	Broadcast	802.11	312	69 -48 dbm	Probe Response, SW=2806, Fw=0, Flags=.....C, B=100, SSID=...	> AlohaPdu/OnStream encapsulated IEEE 802.11
37437	59.192759	0.820457	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2807, Fw=0, Flags=.....C, B=100, SSID=...	> IEEE 802.11 radio information
37447	59.192792	0.820442	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2808, Fw=0, Flags=.....C, B=100, SSID=...	> IEEE 802.11 Beacon frame, Flags: .....C
37459	59.193134	0.820522	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2809, Fw=0, Flags=.....C, B=100, SSID=...	> IEEE 802.11 Wireless Management
37470	59.193629	0.820399	Cisco_05:00:18	Broadcast	802.11	312	69 -39 dbm	Probe Response, SW=2809, Fw=0, Flags=.....C, B=100, SSID=...	> Fixed parameters (12 bytes)
37480	59.194345	0.820501	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2811, Fw=0, Flags=.....C, B=100, SSID=...	> Tagged parameters (213 bytes)
37489	59.195487	0.821342	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2812, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: SSID parameter set: "wifi6_test"
37499	59.195516	0.821929	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2813, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Supported Rates (6B), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]
37520	59.195713	0.820467	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2814, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Traffic Indication Map (TIM): OPM # of 1 bitmap
37529	59.196080	0.820431	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2815, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Country Information: Country Code not, Environment Global operating classes
37532	59.195726	0.821156	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2816, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Power Constraint: 6
37539	59.197089	0.821751	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2817, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: TX Report Transmit Power: 36, L100 Operate: 0
37552	59.197468	0.820499	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2818, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: RSN Information
37565	59.197993	0.820501	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2819, Fw=0, Flags=.....C, B=100, SSID=...	> Tag Number: RSN Information (64)
37574	59.198423	0.820438	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2820, Fw=0, Flags=.....C, B=100, SSID=...	> Tag Length: 26
37585	59.198865	0.820542	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2821, Fw=0, Flags=.....C, B=100, SSID=...	> RSN Version: 1
37596	59.199439	0.820474	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2822, Fw=0, Flags=.....C, B=100, SSID=...	> Group Cipher Suite: 00000000 (IEEE 802.11) GCM (128)
37606	59.199949	0.820499	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2823, Fw=0, Flags=.....C, B=100, SSID=...	> Pairwise Cipher Suite Count: 1
37626	59.202621	0.820481	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2824, Fw=0, Flags=.....C, B=100, SSID=...	> Pairwise Cipher Suite List 00000000 (IEEE 802.11) GCM (128)
37641	59.204964	0.820561	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2825, Fw=0, Flags=.....C, B=100, SSID=...	> Auth Key Management (AKM) Suite Count: 1
37652	59.206137	0.820351	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2826, Fw=0, Flags=.....C, B=100, SSID=...	> Auth Key Management (AKM) List 00000000 (IEEE 802.11) WPA (SHA256-SuiteB)
37668	59.207165	0.820492	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2827, Fw=0, Flags=.....C, B=100, SSID=...	> Auth Key Management (AKM) Suite: 00000000 (IEEE 802.11) WPA (SHA256-SuiteB)
37687	59.210487	0.820792	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2828, Fw=0, Flags=.....C, B=100, SSID=...	> Auth Key Management (AKM) Suite: 00000000 (IEEE 802.11) WPA (SHA256-SuiteB)
37696	59.212867	0.820408	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2829, Fw=0, Flags=.....C, B=100, SSID=...	> RSN Capabilities: 0x0000
37704	59.214777	0.820430	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2830, Fw=0, Flags=.....C, B=100, SSID=...	> PMKID Count: 0
37719	59.215721	0.820241	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2831, Fw=0, Flags=.....C, B=100, SSID=...	> PMKID List
37733	59.218459	0.820628	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2832, Fw=0, Flags=.....C, B=100, SSID=...	> Group Management Cipher Suite: 00000000 (IEEE 802.11) GCM (128)
37738	59.218659	0.820180	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2833, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: QoS Class Information: Not present
37749	59.223200	0.820495	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2834, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: WPA Enabled Capabilities (5 octets)
37775	59.240621	0.820492	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2835, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Extended Capabilities (1 octets)
37792	59.246211	0.820508	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2836, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Tx Power Envelope
37809	59.247802	0.821481	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2837, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Tx Power Envelope
37814	59.247813	0.821551	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2838, Fw=0, Flags=.....C, B=100, SSID=...	> Ext Tag: Multiple BSSID Configuration
37822	59.247960	0.820347	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2839, Fw=0, Flags=.....C, B=100, SSID=...	> Ext Tag: HE Capabilities
37833	59.248050	0.820398	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2840, Fw=0, Flags=.....C, B=100, SSID=...	> Ext Tag: HE Operation
37841	59.248540	0.820490	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2841, Fw=0, Flags=.....C, B=100, SSID=...	> Ext Tag: SpatialReuse Parameter Set
37857	59.249090	0.820509	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2842, Fw=0, Flags=.....C, B=100, SSID=...	> Ext Tag: HE 4 GHz Band Capabilities
37864	00.013602	0.820402	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2843, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Vendor Specific: Atheros Communications, Inc.: Unknown
37868	00.018192	0.820508	Cisco_05:00:18	Broadcast	802.11	355	69 -38 dbm	Beacon frame, SW=2844, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled
37881	00.019489	0.820297	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2845, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCK version = 5
37887	00.019787	0.820498	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2846, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (64)
37897	00.021806	0.820489	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2847, Fw=0, Flags=.....C, B=100, SSID=...	> Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)
37908	00.211976	0.820880	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2848, Fw=0, Flags=.....C, B=100, SSID=...	
37927	00.212414	0.820438	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2849, Fw=0, Flags=.....C, B=100, SSID=...	
37928	00.213087	0.820611	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2850, Fw=0, Flags=.....C, B=100, SSID=...	
37936	00.213114	0.820287	Cisco_05:00:18	Broadcast	802.11	312	69 -38 dbm	Probe Response, SW=2851, Fw=0, Flags=.....C, B=100, SSID=...	
37943	00.213778	0.820464	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2852, Fw=0, Flags=.....C, B=100, SSID=...	
37949	00.214369	0.820593	Cisco_05:00:18	Broadcast	802.11	312	69 -17 dbm	Probe Response, SW=2853, Fw=0, Flags=.....C, B=100, SSID=...	
37961	00.214873	0.820594	Cisco_05:00:18	Broadcast	802.11	355	69 -17 dbm	Beacon frame, SW=2854, Fw=0, Flags=.....C, B=100, SSID=...	

```

> Tag: RSN Information
  Tag Number: RSN Information (64)
  Tag Length: 26
  RSN Version: 1
  > Group Cipher Suite: 00000000 (IEEE 802.11) GCM (128)
  > Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List 00000000 (IEEE 802.11) GCM (128)
  > Auth Key Management (AKM) Suite Count: 1
  > Auth Key Management (AKM) List 00000000 (IEEE 802.11) WPA (SHA256-SuiteB)
  > Auth Key Management (AKM) Suite: 00000000 (IEEE 802.11) WPA (SHA256-SuiteB)
  > Auth Key Management (AKM) Type: WPA (SHA256-SuiteB) (11)
  > RSN Capabilities: 0x0000
  PMKID Count: 0
  PMKID List
  > Group Management Cipher Suite: 00000000 (IEEE 802.11) GCM (128)
  > Tag: QoS Class Information: Not present
  > Tag: WPA Enabled Capabilities (5 octets)
  > Tag: Extended Capabilities (1 octets)
  > Tag: Tx Power Envelope
  > Tag: Tx Power Envelope
  > Ext Tag: Multiple BSSID Configuration
  > Ext Tag: HE Capabilities
  > Ext Tag: HE Operation
  > Ext Tag: SpatialReuse Parameter Set
  > Ext Tag: HE 4 GHz Band Capabilities
  > Tag: Vendor Specific: Atheros Communications, Inc.: Unknown
  > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Client MFP Disabled
  > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet CCK version = 5
  > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (64)
  > Tag: Vendor Specific: Cisco Systems, Inc.: Aironet Unknown (11) (11)

```

### 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:

⚠ 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

Fast Transition

Status   
Over the DS   
Reassociation Timeout \*

WPA2/WPA3 Encryption

AES(CCMP128)  CCMP256   
GCMP128  GCMP256

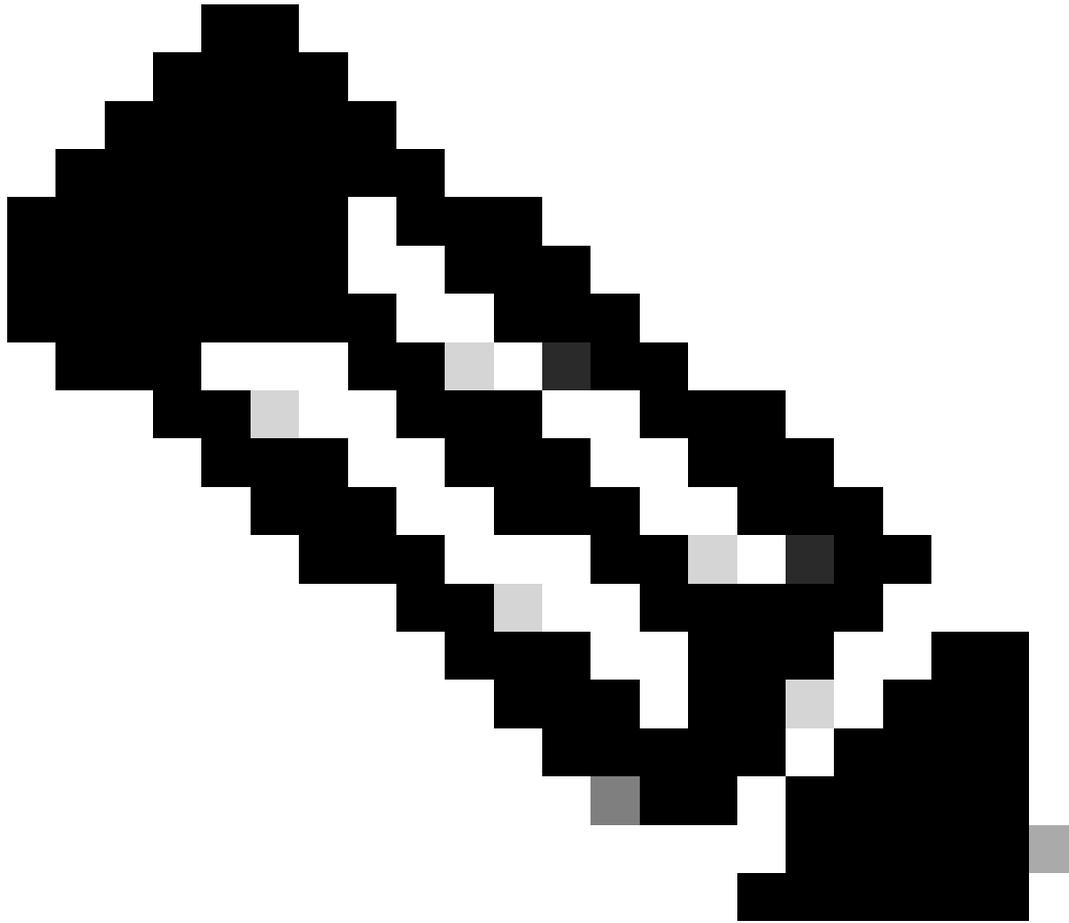
Auth Key Mgmt

SUITEB192-1X

Protected Management Frame

PMF   
Association Comeback Timer\*   
SA Query Time\*

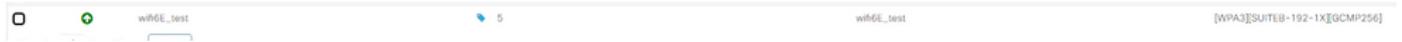
Parámetros de seguridad de WPA3 Enterprise SUITEB192-1x



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:





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/Go 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 Supported
Empresa	GCMP256	SuiteB-192	SHA384-SuiteB	TLS	Not Supported	Not Supported	NA/TBD	NA/TBD

## Troubleshoot

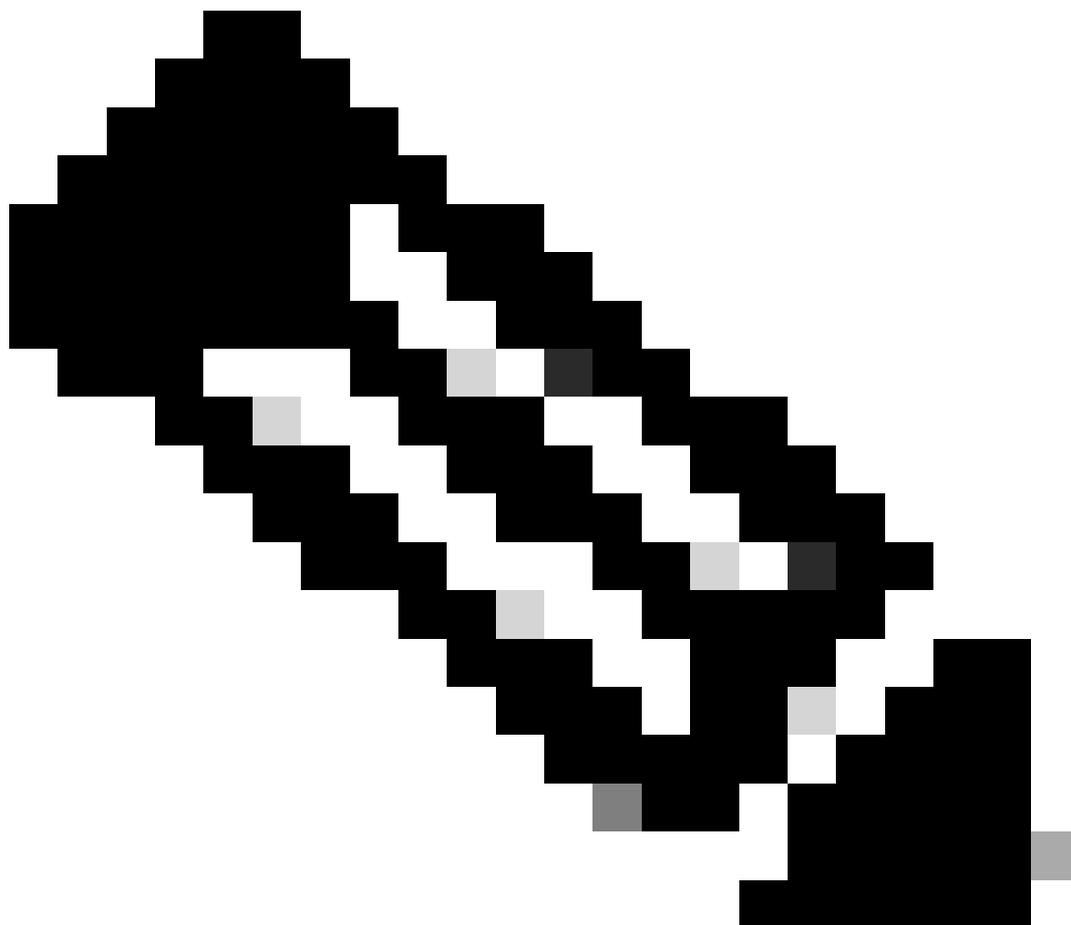
La solución de problemas utilizada en este documento se basó en el documento en línea:

[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 Debug](#) antes 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).