Comprender el flujo de cifrado inalámbrico oportunista

Contenido

Introducción

Este documento describe el flujo de transición de OWE y cómo funciona en el controlador de LAN inalámbrica (WLC) Catalyst 9800.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cómo configurar el 9800 WLC, el punto de acceso (AP) para el funcionamiento básico
- Cómo configurar los perfiles de política y WLAN.

Componentes Utilizados

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

- C9800-80, Cisco IOS® XE 17.12.4 y también probado en Cisco IOS® XE 17.9.6
- Modelo de punto de acceso: C9136I, verificado tanto en modo de conexión local como flexible.

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.

Descripción

- OWE (cifrado inalámbrico oportunista) es una extensión de IEEE 802.11 que proporciona cifrado para el medio inalámbrico. 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 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 pares resultante con el intercambio de señales 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.

Pasos

1. Configure una WLAN ABIERTA sin ningún tipo de encriptación/seguridad y habilite la difusión.
2. Configure otro SSID con la configuración de seguridad OWE y asigne el número de ID de WLAN ABIERTA en el modo de transición-wlan-id. Deshabilite la opción de difusión de SSID en este SSID de transición OWE.
3. Asigne el número de ID de WLAN de transición de OWE en el campo "transición-modo-wlan-id" de WLAN ABIERTA.

Detalles de Lab Repro

- Nombre de SSID abierto: ABIERTO
- Nombre de SSID de transición OWE: Transición a OWE
- BSSID de OPEN-OWE: 40:ce:24:dd:2e:87
- BSSID de transición a OWE: 40:ce:24:dd:2e:8f

FLUJO DE DEUDA

1. Los indicadores se pueden difundir para OPEN SSID. Puede verlo por su nombre SSID en AIR PCAP.
2. También podemos ver el SSID habilitado de seguridad oculta con el nombre "Comodín" en lugar de su propio nombre SSID en AIR PCAP.
3. Una vez que los clientes reciben la trama de baliza para OPEN SSID, si tiene o soporta OWE, puede comenzar a enviar la solicitud de sondeo a OWE SSID de transición (que es ese SSID habilitado para seguridad en lugar de OPEN SSID).
4. Los clientes compatibles con OWE pueden obtener una respuesta de sondeo de SSID de transición.
5. La autenticación OPEN puede ocurrir entre el cliente y el AP.
6. El cliente puede enviar la solicitud de asociación al AP con los detalles del intercambio de claves DH y utilizar el secreto del par resultante para el intercambio de señales de 4 vías.
7. El AP puede enviar una respuesta de asociación.
8. El intercambio de señales de cuatro vías puede ocurrir entre el AP y el dispositivo del cliente.
9. Después de una correcta administración de claves, la PSK L2 puede ser exitosa.
10. El cliente puede obtener IP de DHCP, ARP, etc.
11. El cliente puede pasar al estado RUN.
12. Si los dispositivos cliente que no son compatibles con OWE, puede enviar una solicitud de sondeo al SSID ABIERTO y puede obtener directamente IP de la que puede pasar al estado EJECUCIÓN.

Marco de baliza original

- Aquí, AIR PCAP muestra que, el SSID "OPEN-OWE" difusión (Marco de baliza). que contiene detalles de transición de SSID y se denomina "OWE-Transition".

Imagen-1: Trama de baliza de SSID ABIERTO

Indicadores SSID ocultos

- Según la configuración WLAN, la "difusión" está inhabilitada para este SSID de "transición de OWE"; sin embargo, puede ver las balizas SSID ocultas en AIR PCAP que contienen el nombre SSID "comodín". Sin embargo, si verifica ese paquete, contiene detalles de transición de OWE.
- Obtenga el BSSID de SSID oculto mediante el uso de este paquete, como "40:ce:24:dd:2e:8f" y búsquelo en la captura de paquetes.
- En este paquete, muestra que, SSID "Falta" y contiene su SSID de transición como "OPEN-OWE" y su BSSID "40:ce:24:dd:2e:87".

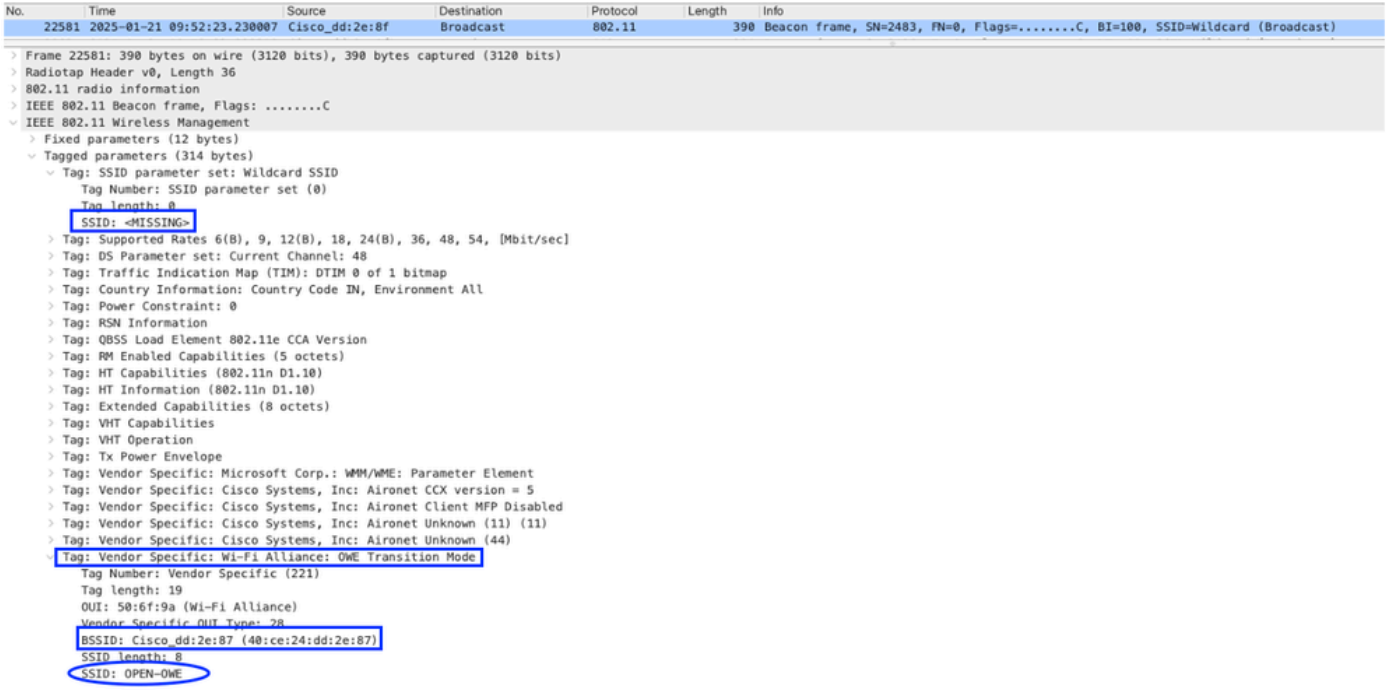

Imagen-2: SSID oculto - Transición de OWE

Solicitud de sondeo enviada por el cliente al SSID de transición de OWE

- Basándose en la trama de baliza "OPEN-OWE" SSID, el cliente llega a conocer los otros detalles SSID que necesita conectar, en este escenario, es "OWE-Transición". Si el cliente es capaz de soportar el cifrado OWE, puede enviar la solicitud de sondeo al SSID "OWE-Transition" y obtener una respuesta.
- Solicitud de sondeo enviada a OWE-Transition BSSID "40:ce:24:dd:2e:8f" y obtuvo una respuesta. Dentro de este paquete de respuesta de sondeo también, puede ver los detalles del SSID OPEN-OWE.

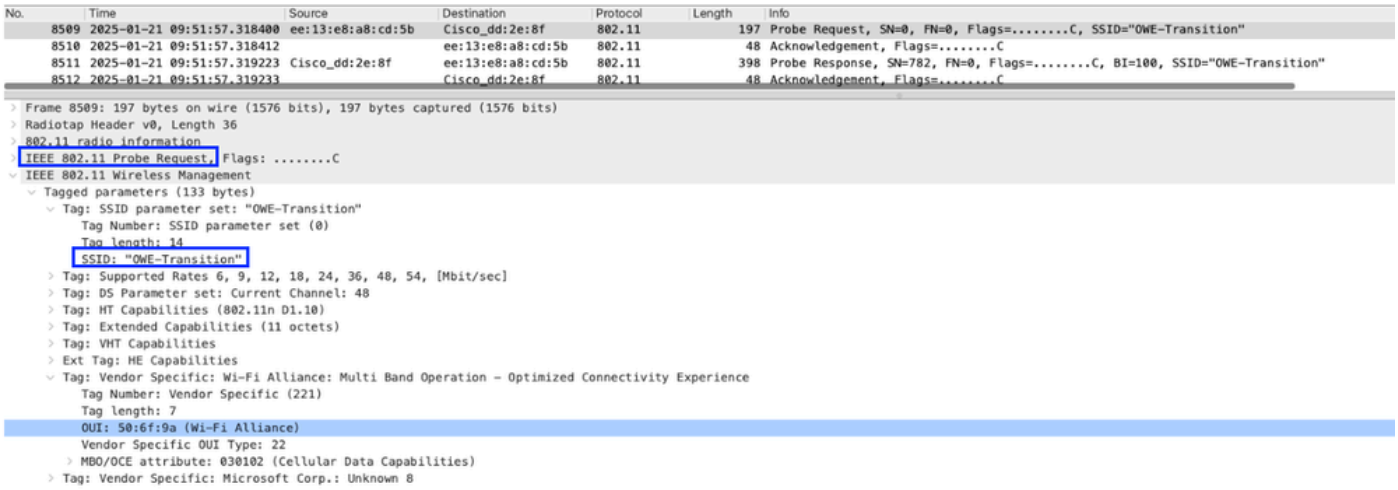

Imagen-3: Solicitud de sondeo

Respuesta de sondeo enviada desde el AP al cliente

- El cliente recibió una respuesta de sondeo para el SSID "OWE-Transition", pero tiene sus detalles SSID originales "OPEN-OWE" en WiFi Alliance.

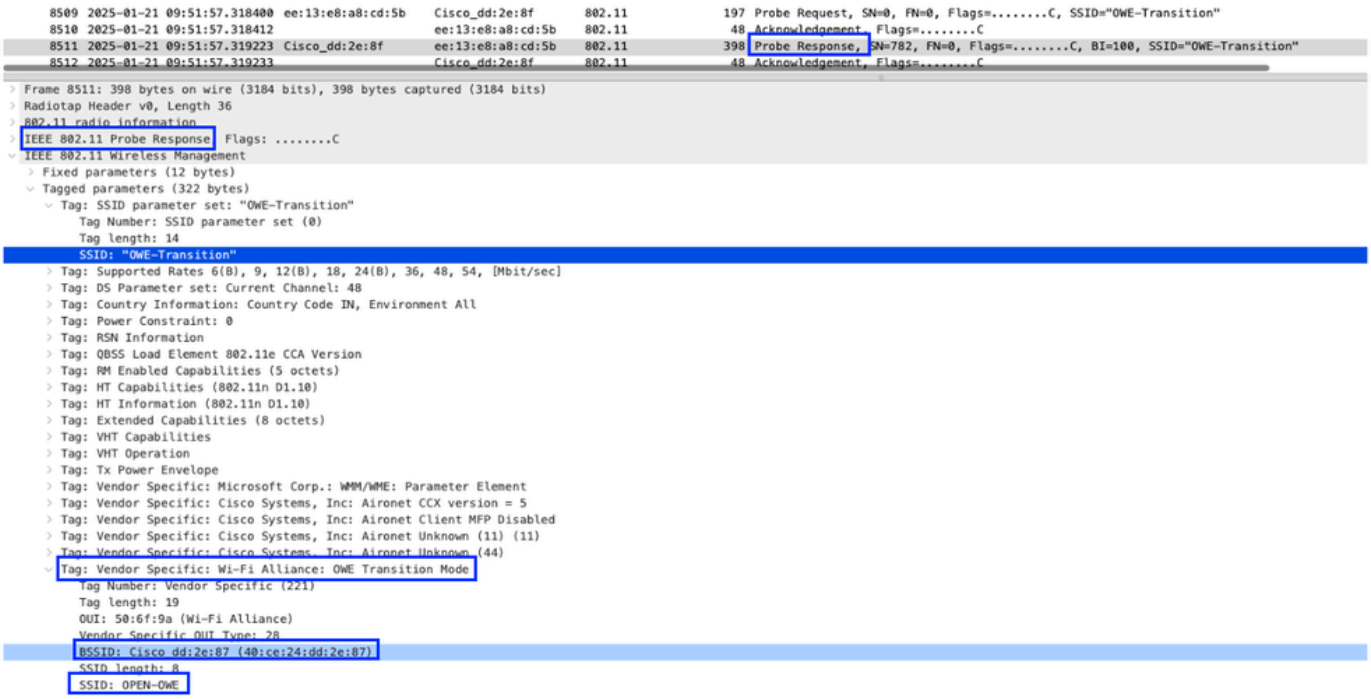

Imagen-4: Respuesta de sondeo

Autenticación abierta

- Después de obtener la respuesta de sondeo, la autenticación OPEN puede ocurrir entre el cliente y el AP para verificar los detalles/capacidades wifi de los clientes, antes de la asociación.

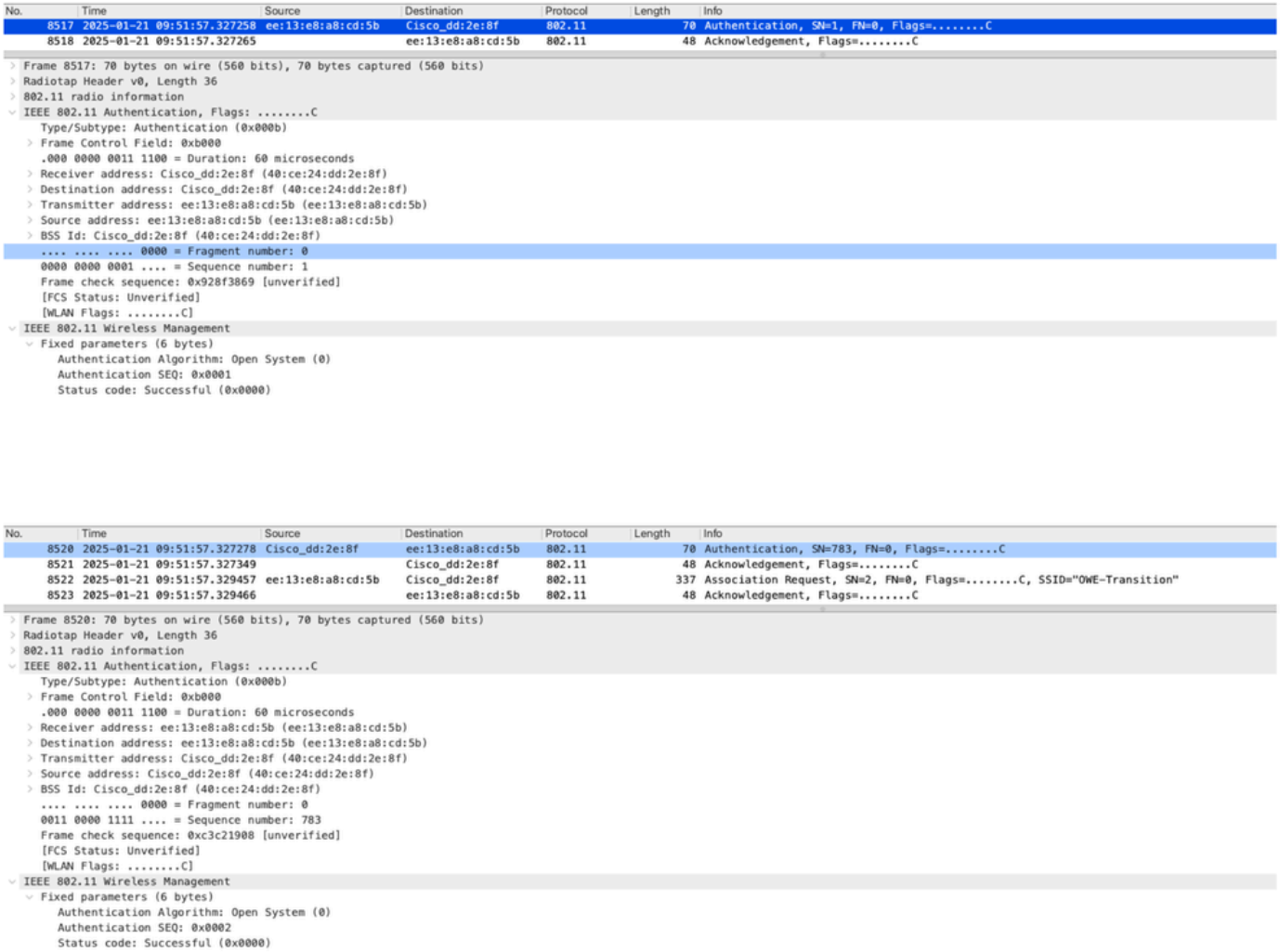

Imagen-5: Autenticación ABIERTA después de una sonda satisfactoria

Solicitud de asociación del cliente al AP

- En este paquete, observe que el cliente puede adjuntar el valor del parámetro Diffie-Hellman para el cifrado.

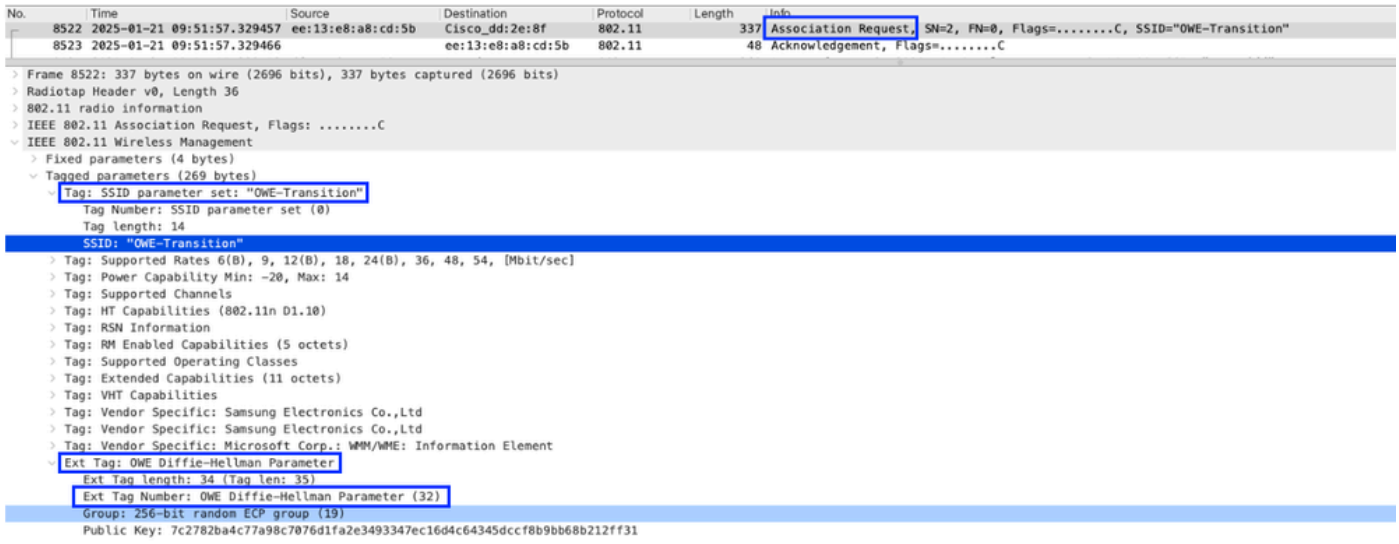

Imagen-6: Solicitud de asociación

- En el seguimiento de RA, puede empezar a ver los registros del cliente desde la fase de asociación,

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

Respuesta de asociación enviada desde el AP al cliente

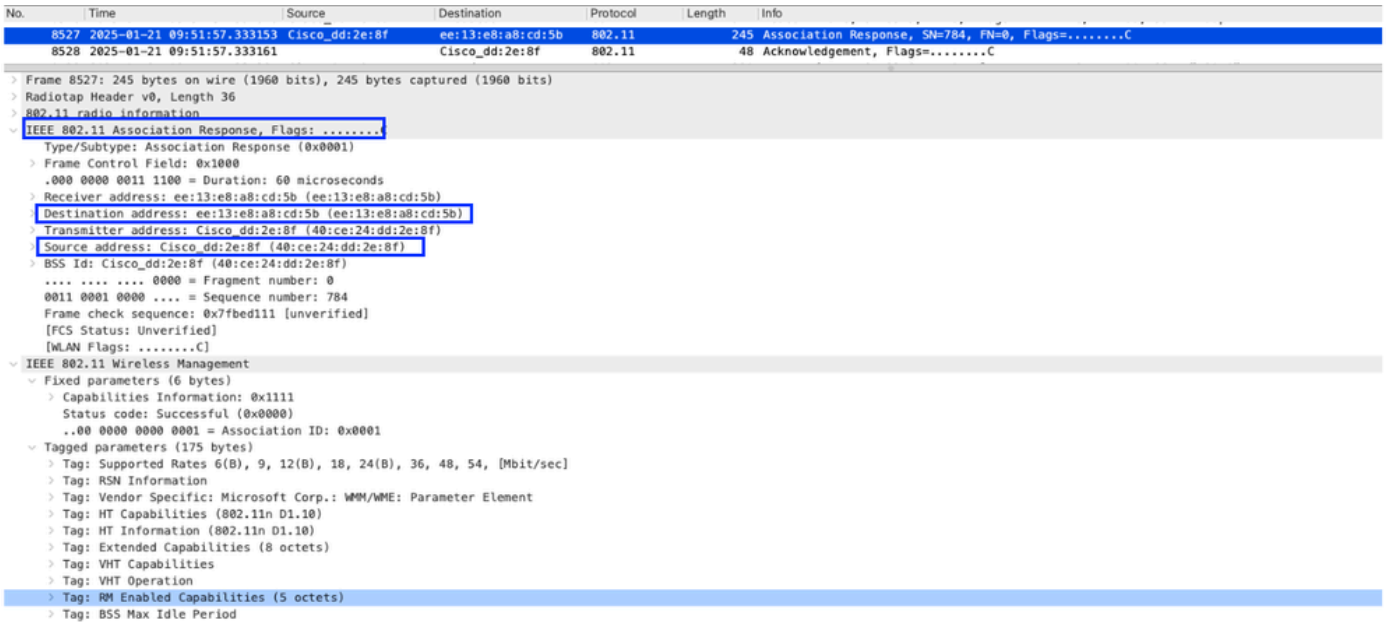

Imagen-7: Respuesta de asociación

```
2025/01/21 15:21:57.391334260 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.392296819 {wncd_x_R0-0}{1}: [dot11] [21675]: (note): MAC: ee13.e8a8.cd5b  Associati
```

‘Intercambio de claves’

La entrada en contacto de 4 vías puede ocurrir entre el AP y el dispositivo del cliente.

Key-1 send by AP

Clave 2 enviada por el cliente

Clave 3 enviada por AP

Clave 4 enviada por el cliente

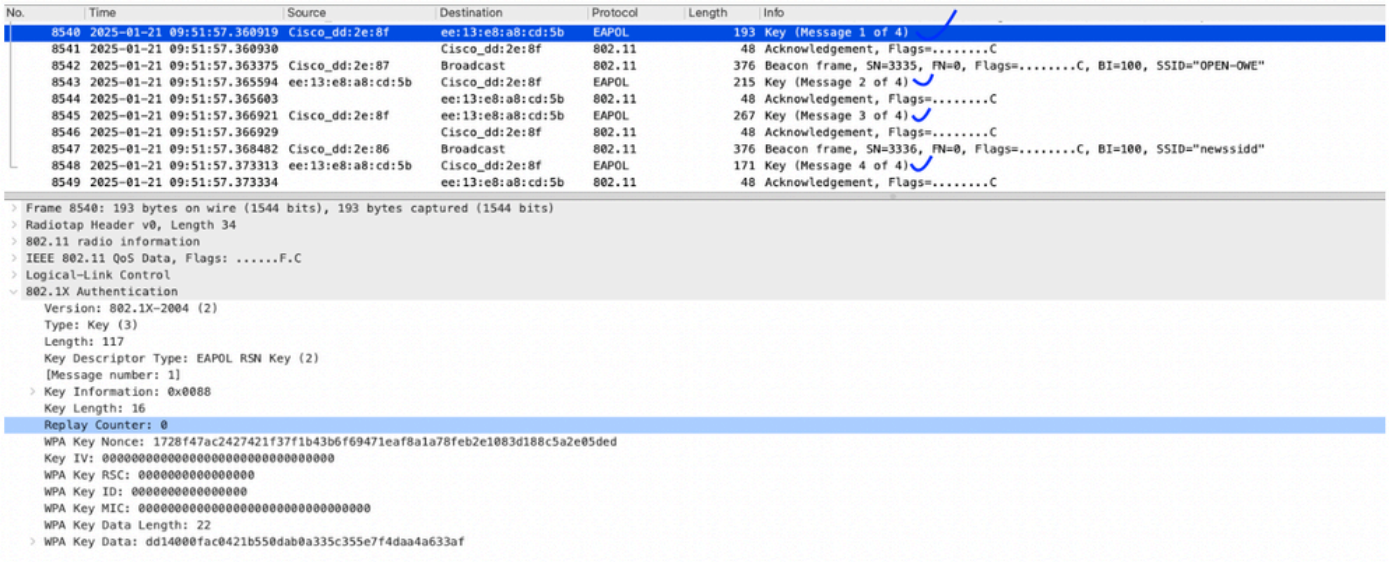

Imagen-8: Apretón De Manos De 4 Vías

```
2025/01/21 15:21:57.392538716 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.392557538 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.392640494 {wncd_x_R0-0}{1}: [client-auth] [21675]: (note): MAC: ee13.e8a8.cd5b  L2
2025/01/21 15:21:57.394830551 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli
2025/01/21 15:21:57.395171903 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli
2025/01/21 15:21:57.420590731 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli

2025/01/21 15:21:57.420706435 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.420775720 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.426548998 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.426725965 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.426727805 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.434078994 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b

2025/01/21 15:21:57.434099154 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (note): MAC: ee13.e8a8.cd5b
```

Autenticación L2 correcta

```
2025/01/21 15:21:57.434111288 {wncd_x_R0-0}{1}: [client-keymgmt] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.434250308 {wncd_x_R0-0}{1}: [client-auth] [21675]: (note): MAC: ee13.e8a8.cd5b  L2
2025/01/21 15:21:57.434286035 {wncd_x_R0-0}{1}: [client-auth] [21675]: (info): MAC: ee13.e8a8.cd5b  Cli
2025/01/21 15:21:57.434308953 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

Estado de aprendizaje de IP

```
2025/01/21 15:21:57.434789679 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.436611026 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.437239513 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
2025/01/21 15:21:57.437508189 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.534166453 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interfac
2025/01/21 15:21:57.535325325 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.535874658 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interfac
2025/01/21 15:21:57.536500021 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

Cliente en estado EJECUCIÓN

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

Clientes que no son compatibles con el cifrado OWE

- Al revisar la trama de una baliza, los clientes llegan a saber si son capaces de soportar este método de encripción o no. Si no es compatible, entonces puede enviar una solicitud de sondeo para abrir SSID "OPEN-OWE" y puede hacer una autenticación abierta normal, obtener la dirección IP y luego puede pasar al estado RUN.

```
2025/01/16 15:36:06.178370757 {wncd_x_R0-2}{1}: [client-orch-sm] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:06.209288788 {wncd_x_R0-2}{1}: [dot11] [17332]: (note): MAC: d037.4587.8f35  Associati
2025/01/16 15:36:06.248651191 {wncd_x_R0-2}{1}: [client-auth] [17332]: (note): MAC: d037.4587.8f35  Ope
2025/01/16 15:36:06.248751507 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.281808554 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.303307756 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:10.305041414 {wncd_x_R0-2}{1}: [client-iplearn] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:10.305777492 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
```

Información de transición rápida

- Solo podemos configurar OWE en autenticación ABIERTA o en Webauth (CWA/LWA/EWA).
- FT no es compatible con la transición de OWE.
- Si activa FT, aparece este mensaje de error:

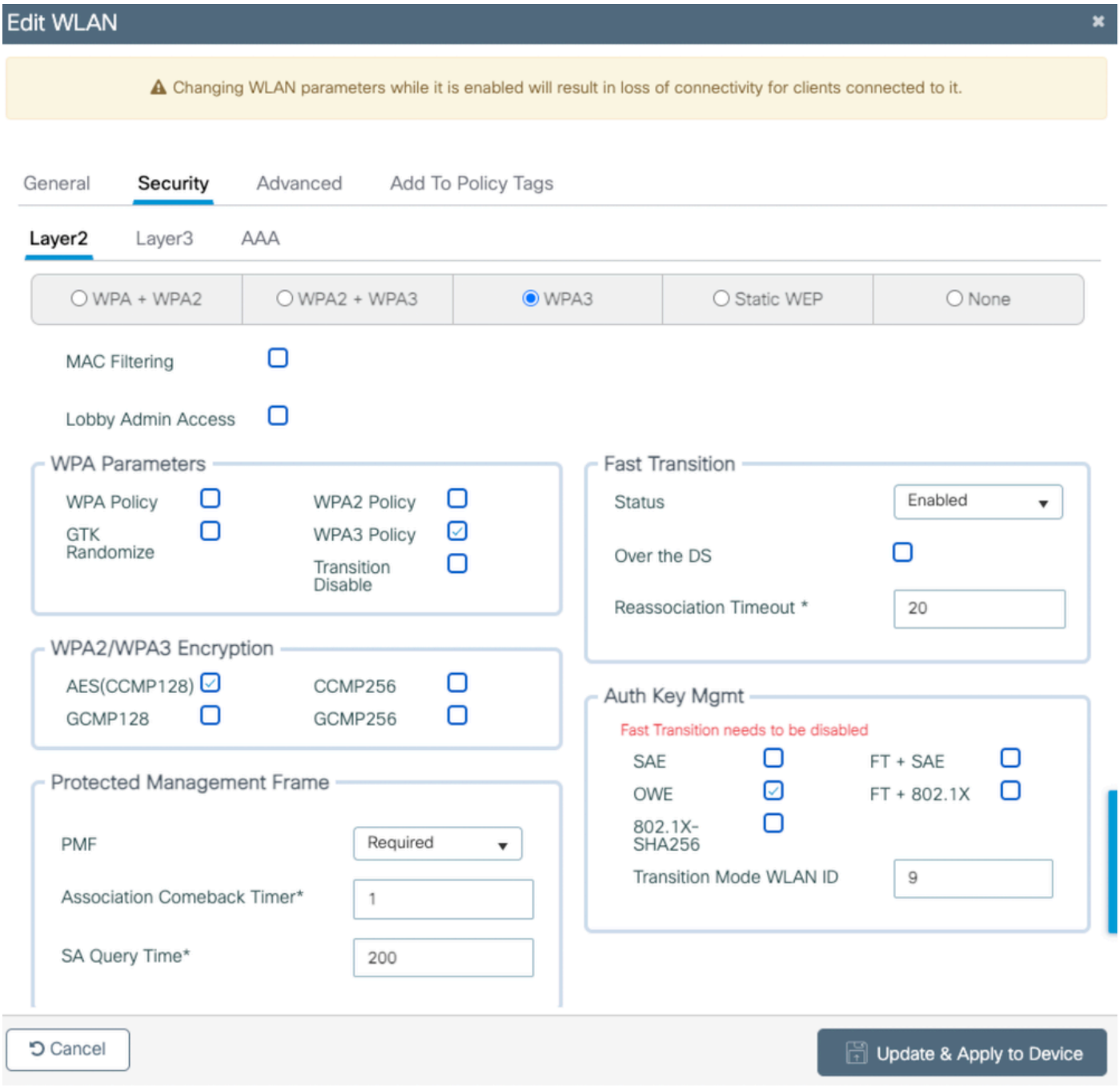

Imagen-9: Mensaje de error cuando habilitamos FT en OWE Transition SSID

OWE no es compatible con PSK/dot1x

No podemos habilitar OWE en estas combinaciones.

1. 802.1x o FT+802.1x

2. PSK o FT+PSK o PSK-SHA256

3. SAE o FT+SAE

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

Si intenta habilitar cualquiera de estos métodos, puede obtener el mensaje de error,

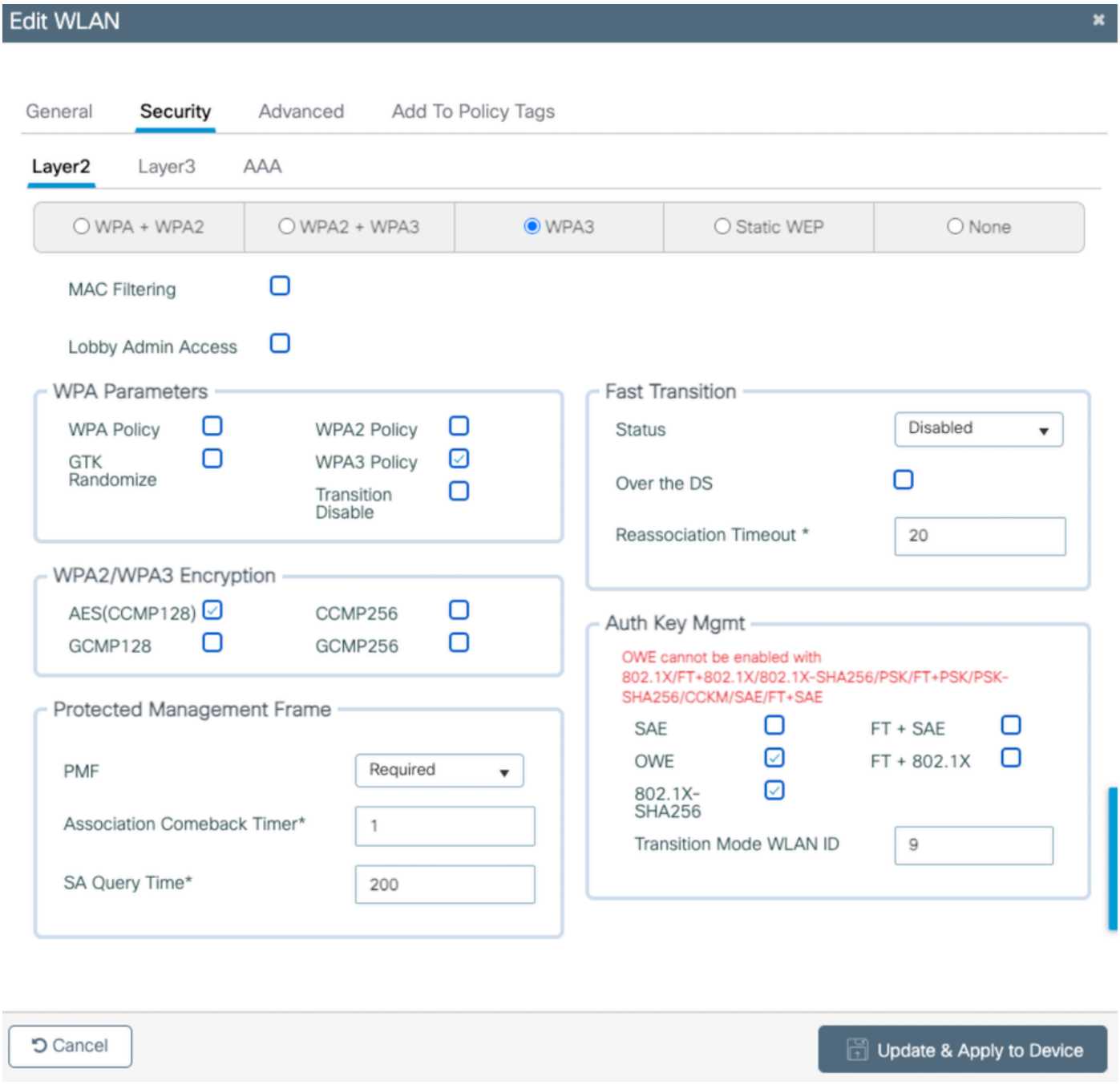

Imagen-10: Mensaje de error al obtener al habilitar otros métodos de autenticación en OWE SSID

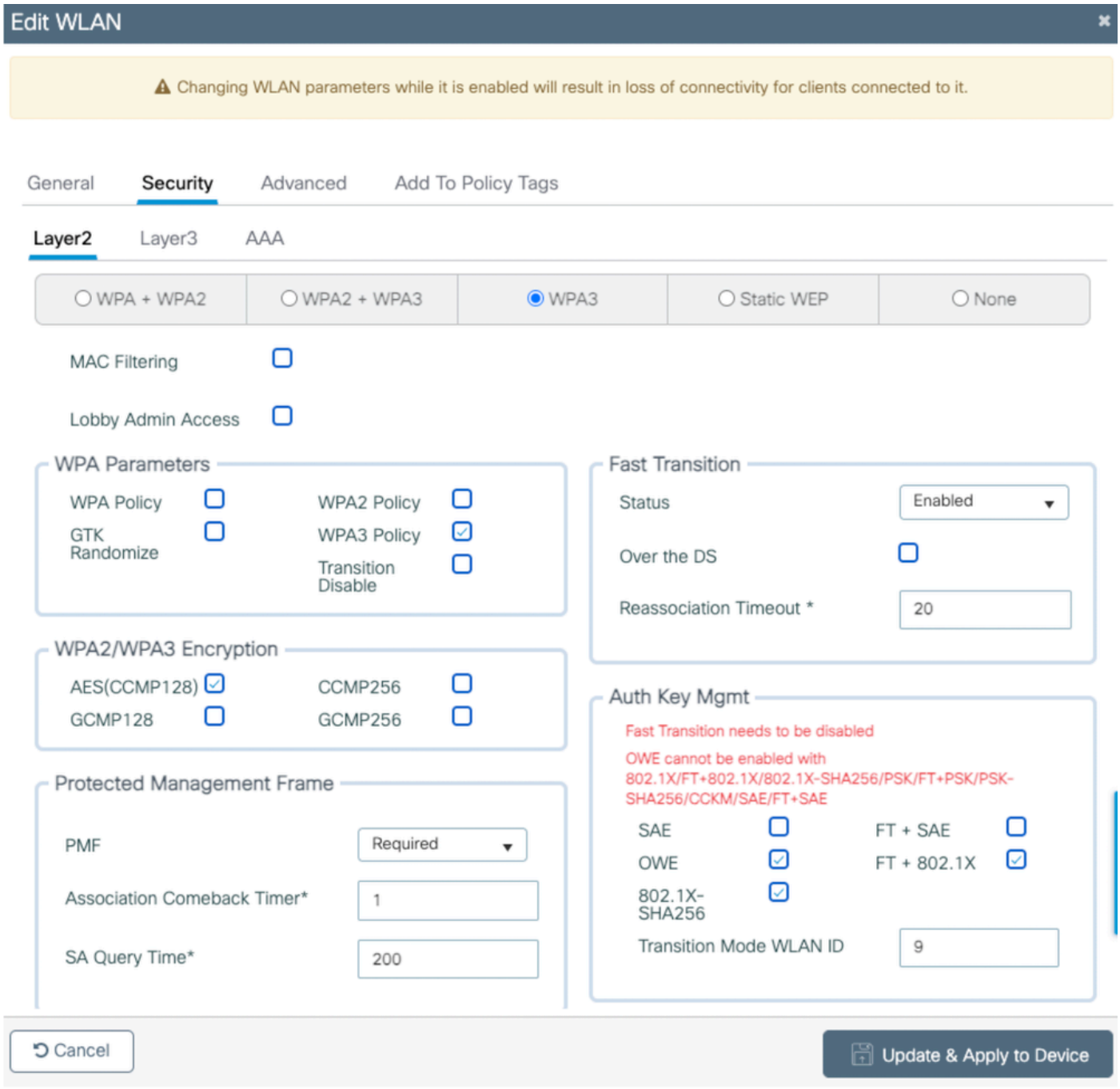

Imagen-11: Mensaje de error al habilitar AKM

- En Cisco IOS® XE versión 17.9.6 IOS, puede ver la opción "OWE" en AKM cuando selecciona "WPA2+WPA3"; sin embargo, puede ver el mensaje de error: no puede utilizar OWE con esta combinación.

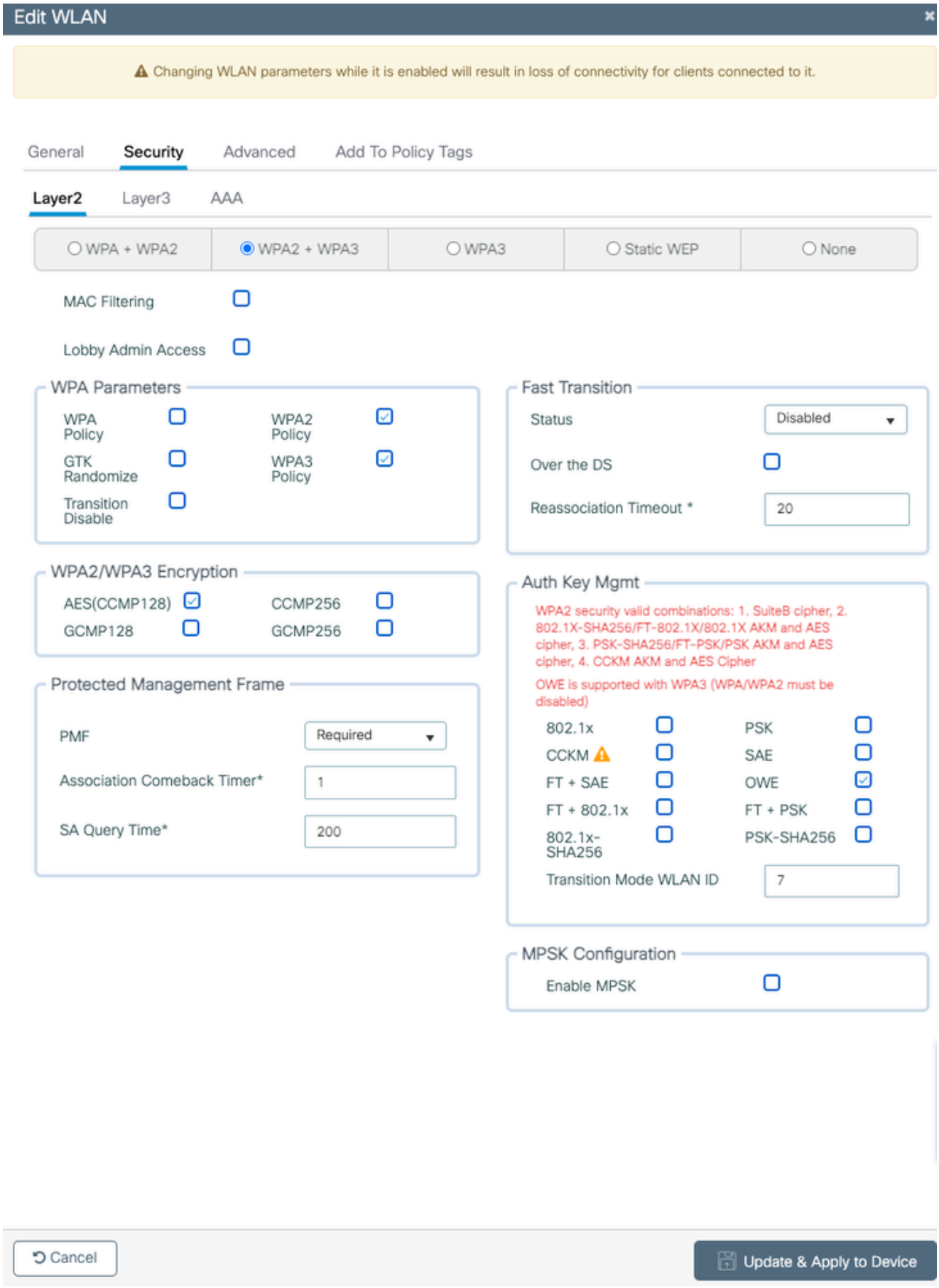

Imagen-12: Mensaje de error al elegir WPA2+WPA3

- En la versión 17.12.4 del IOS® XE de Cisco, cuando elige "WPA2+WPA3", no puede

obtener la opción "OWE" en AKM,

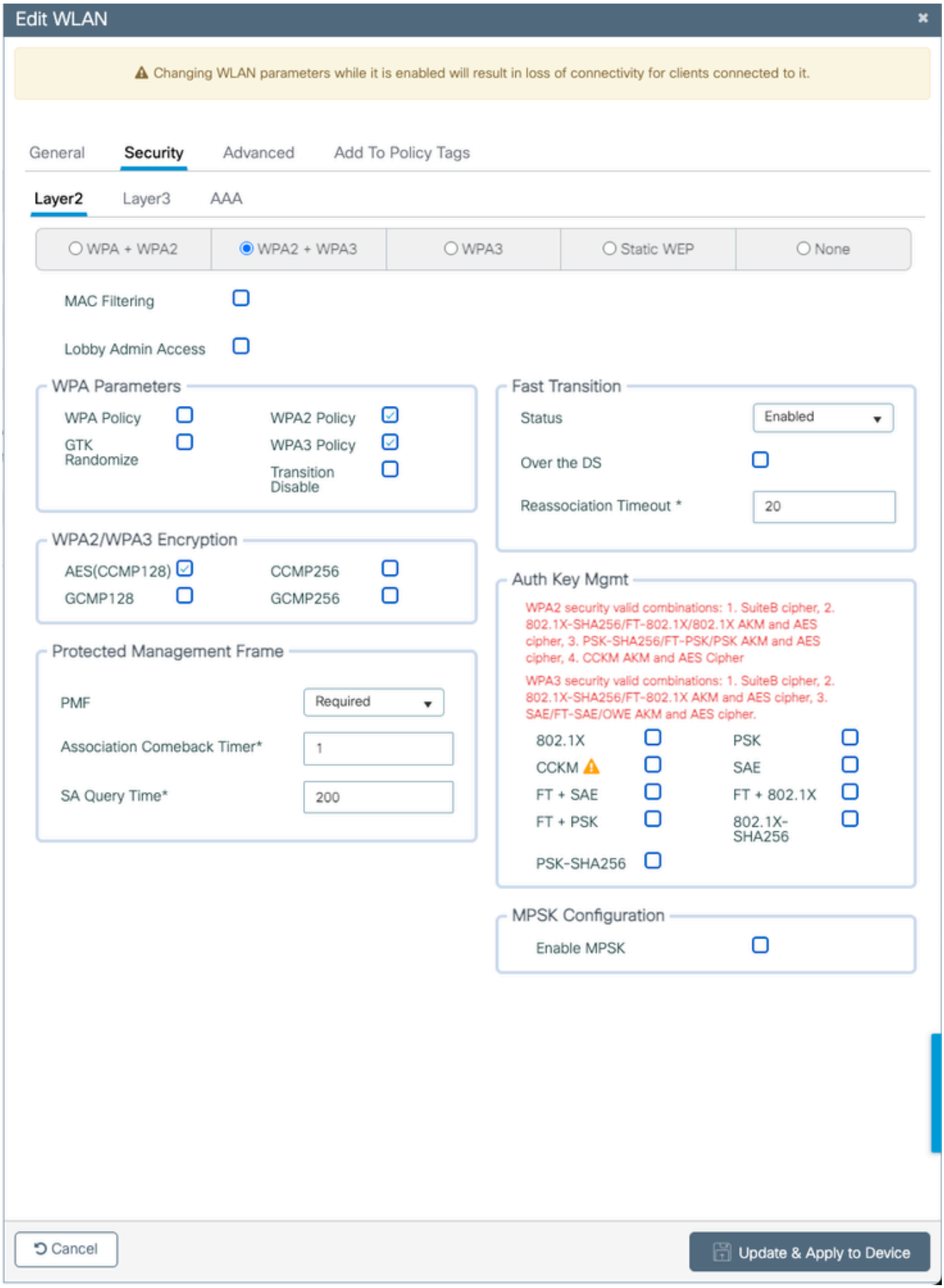

Imagen-13: Mensaje de error - No se obtiene la opción OWE en AKM

Resolución de problemas

1. Verifique las configuraciones en ambas WLAN, en OPEN SSID y en OWE transición SSID debe tener la transición WLAN ID asignada.
2. La opción de difusión debe estar desactivada en el SSID de transición de OWE, debe estar activada sólo en el SSID ABIERTO.
3. Compruebe los métodos de autenticación/cifrado/FT compatibles descritos en este artículo.
4. Si las configuraciones están bien desde el extremo del WLC, que recopile los registros y las salidas requeridos para reducir el problema,

Rastreo RA y EPC (captura de paquetes integrada)

Inicie sesión en la GUI del WLC -> Troubleshooting -> Radioactive Trace -> Add client wifi MAC address -> Haga clic en la casilla de verificación de los clientes -> Start

Inicie sesión en WLC GUI -> Troubleshooting -> Packet Capture -> Add new file name -> Choose the uplink interface and WMI VLAN/Interface -> Start.

Desde el equipo cliente: Si es posible, puede instalar la aplicación wireshark y recopilar la captura de paquetes eligiendo la interfaz WiFi.

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

AIR PCAP

Puede recopilarlo usando el ordenador portátil MAC o configurando uno de los AP en el modo sniffer, consulte estos enlaces,

Desde un ordenador portátil MAC:

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

Desde Sniffer AP:

https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217057-configure-access-point-in-sniffer-mode-o.html

Conecte un ordenador portátil (servidor wireshark) al puerto del switch y debe tener instalada la aplicación wireshark; este servidor wireshark debe tener acceso a la interfaz WMI del WLC. Necesita permitir el protocolo "5555 o 5000 o 5556" en el firewall si se presenta entre su WLC y el servidor wireshark.

Compruebe si hay algún "gscaler" instalado en ese PC donde wireshark instalado, si es que por favor "apague" e intente, si es cualquier firewall como windows defender o cualquier cosa presente en él, por favor inhabilite esos y tratar de recoger PCAP.

Itinerancia

Cuando el cliente se traslada de un AP a otro, necesita realizar estos pasos,

- Necesidad de enviar reasociación/asociación: depende de la solicitud del cliente.
- Es necesario enviar los detalles DH (Diffie-Helman) en la solicitud de asociación.
- El cliente puede obtener detalles DH en la respuesta de asociación del AP, según este PMK se genera en el cliente y el AP.
- El intercambio de señales de 4 vías puede ocurrir entre el AP y el cliente.
- En OWE, no puede habilitar FT, por lo que 802.11r no es posible.
- Cada vez, cuando el cliente se desplaza, necesita dar un apretón de manos de 4 vías después del intercambio DH en asociación.
- Cliente y AP usando su propio PMKID, es único para cada AP y clientes.
- Si el cliente se conecta al mismo AP, entonces puede utilizar el mismo PMKID. En algún escenario, si el cliente fue eliminado que el AP puede generar un nuevo PMKID, sin embargo el cliente utiliza el mismo PMKID para la entrada en contacto de 4 vías.

Ejemplo:

Si el cliente se conecta con el mismo AP, entonces puede ver el mismo PMKID tanto en la Solicitud de Asociación como en la Respuesta de Asociación. En la respuesta de asociación, no puede ver los detalles de DH si utiliza el mismo PMKID.

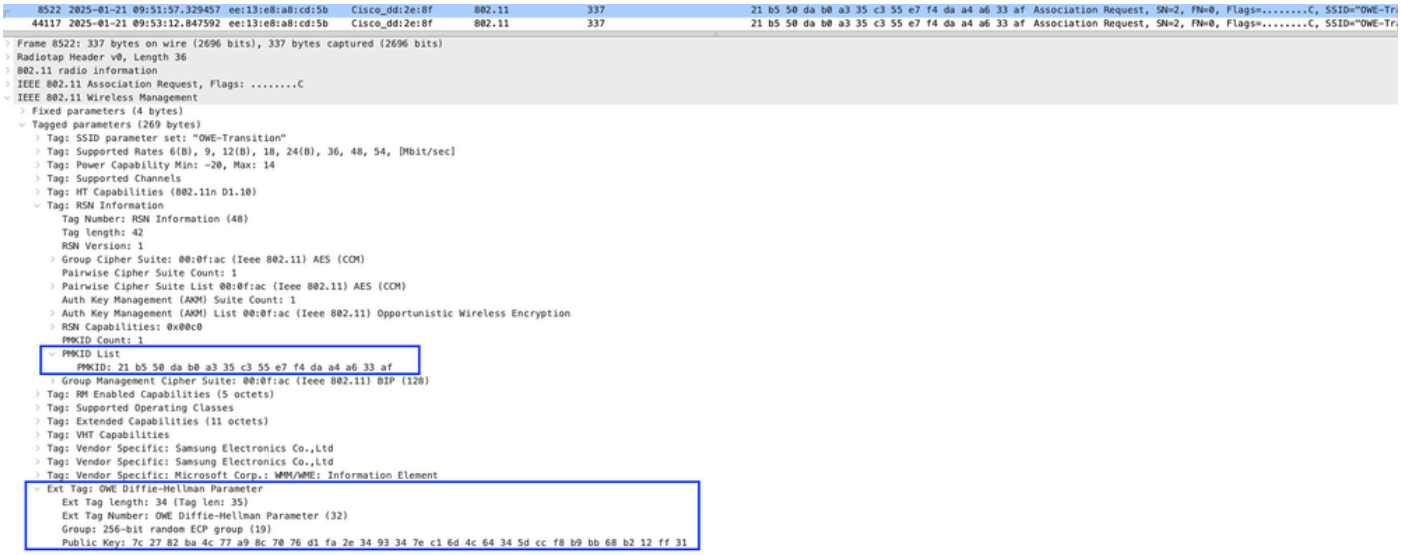

Imagen-14: Uso del mismo PMKID

Imagen-15: Respuesta de asociación con el mismo PMKID

Para la prueba, eliminó este cliente manualmente del WLC y se asoció otra vez al mismo AP, en este momento, el cliente envía un PMKID mismo sin embargo AP envía los detalles DH en la respuesta de la asociación.

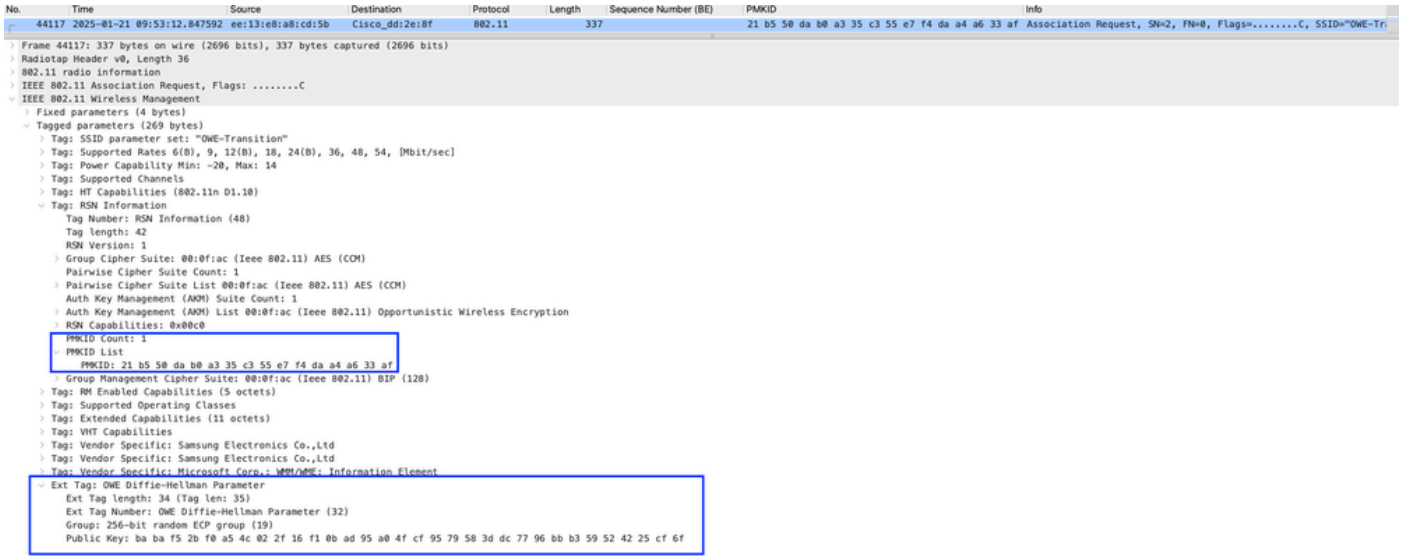

Imagen-16: Después de la eliminación, el cliente envió el mismo PMKID con los detalles DH

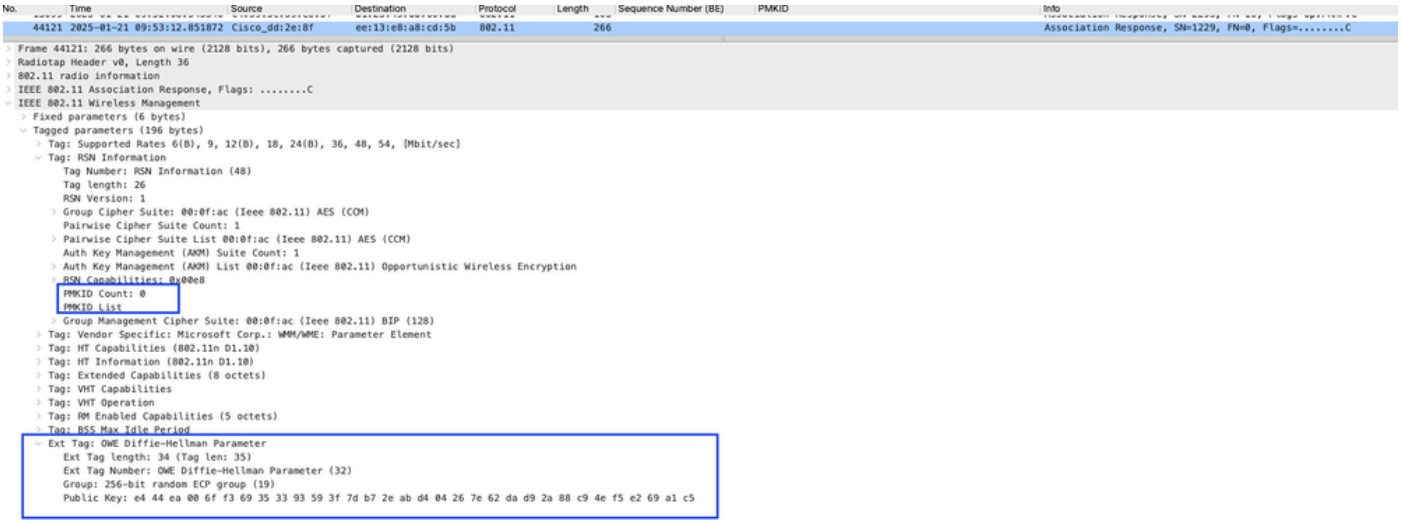

Imagen-17: El AP utiliza los valores DH para generar su nuevo PMKID

En este ejemplo: Tanto el AP como el cliente utilizan el mismo PMKID mientras hacen el intercambio de señales de 4 vías, verifique los mensajes "M1 y M2".

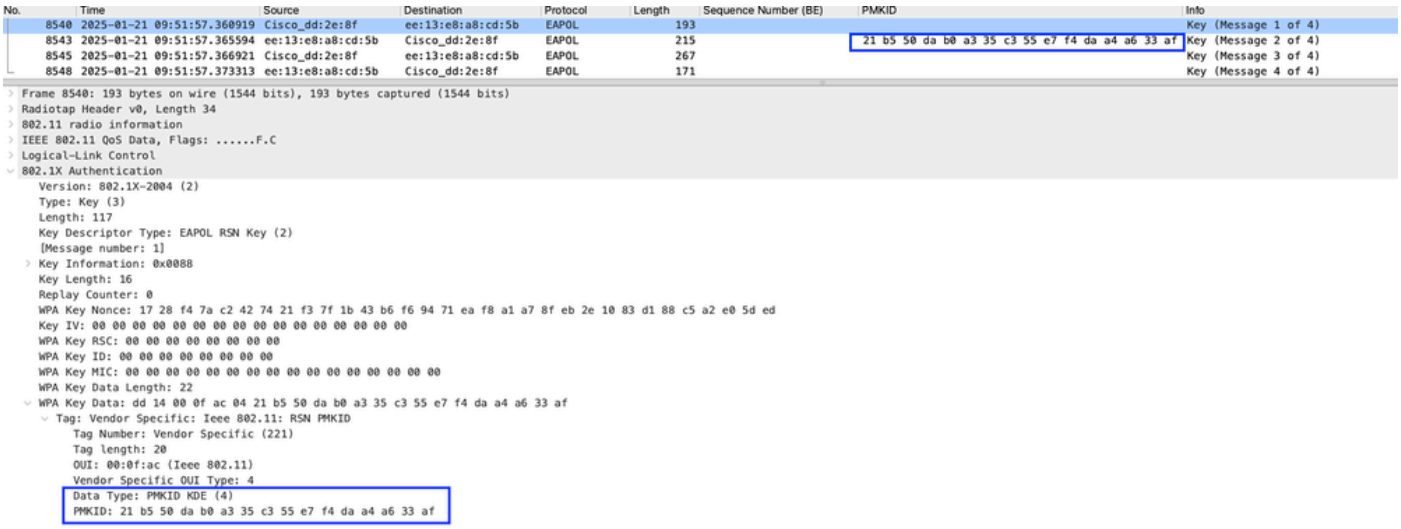

Imagen- 18: AP y cliente que utilizan el mismo PMKID

En este ejemplo: El cliente que utiliza el mismo PMKID pero AP que utiliza PMKID diferente que generó después de que el cliente fue eliminado, verifique los mensajes "M1 y M2".

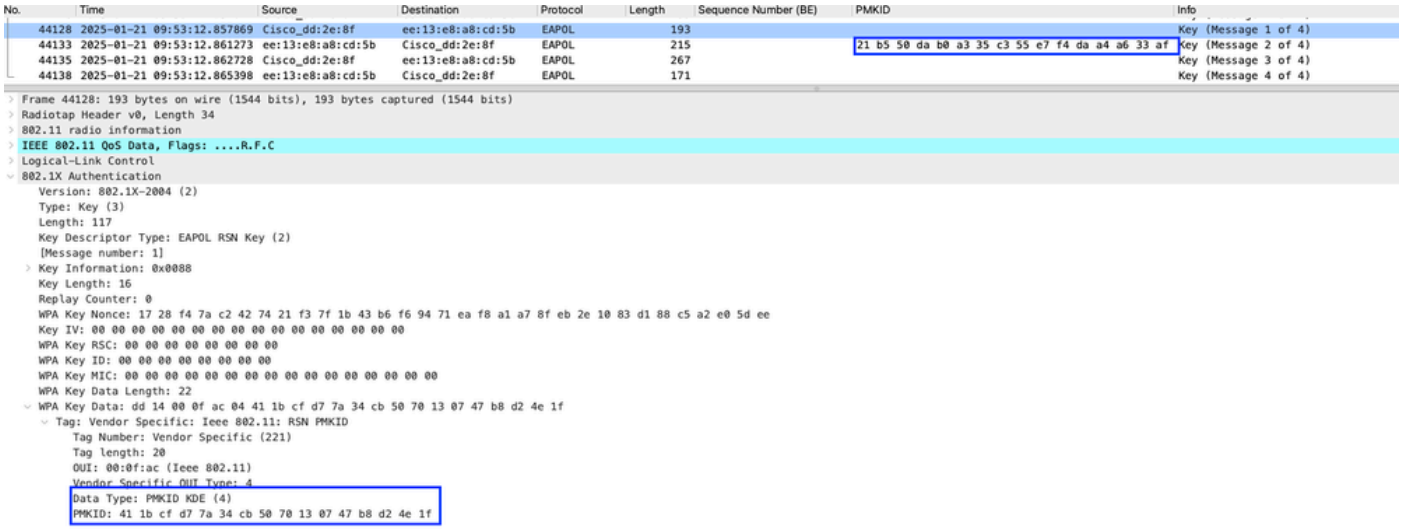

Imagen-19: AP y cliente que utilizan PMKID diferente

Desde el seguimiento de RA interno:

En este ejemplo: El cliente envió parámetros DH en la solicitud de asociación y el AP procesado que generó el PMK.

```
2025/01/21 15:18:50.157081690 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157082294 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157523328 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157531792 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532236 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532538 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157841380 {wncd_x_R0-0}{1}: [dot11-frame] [21675]: (debug): MAC: ee13.e8a8.cd5b  OW
```

Después de esto, el mismo cliente que se conectaba al mismo AP, en este momento, AP no generaba un nuevo PMKID,

```
2025/01/21 15:21:57.391898613 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391903915 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906073 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906329 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

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).