

Comprender el flujo de cifrado inalámbrico oportunista

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Descripción](#)

[Pasos](#)

[Detalles de Lab Repro](#)

[FLUJO DE DEUDA](#)

[Marco de baliza original](#)

[Indicadores SSID ocultos](#)

[Solicitud de sondeo enviada por el cliente al SSID de transición de OWE](#)

[Respuesta de sondeo enviada desde el AP al cliente](#)

[Autenticación abierta](#)

[Solicitud de asociación del cliente al AP](#)

[Respuesta de asociación enviada desde el AP al cliente](#)

[‘Intercambio de claves’](#)

[Autenticación L2 correcta](#)

[Estado de aprendizaje de IP](#)

[Cliente en estado EJECUCIÓN](#)

[Clientes que no son compatibles con el cifrado OWE](#)

[Información de transición rápida](#)

[OWE no es compatible con PSK/dot1x](#)

[Resolución de problemas](#)

[Rastreo RA y EPC \(captura de paquetes integrada\)](#)

[AIR PCAP](#)

[Itinerancia](#)

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".

No.	Time	Source	Destination	Protocol	Length	Info
47285	2025-01-21 09:53:18.259879	Cisco_dd:2e:87	Broadcast	802.11	376	Beacon frame, SN=1157, FN=0, Flags=.....C, BI=100, SSID="OPEN-OWE"
<pre> > Frame 47285: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Beacon frame, Flags:C < IEEE 802.11 Wireless Management > Fixed parameters (12 bytes) < Tagged parameters (300 bytes) < Tag: SSID parameter set: "OPEN-OWE" Tag Number: SSID parameter set (0) Tag length: 8 SSID: "OPEN-OWE" > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] > Tag: DS Parameter set: Current Channel: 48 > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap > Tag: Country Information: Country Code IN, Environment All > Tag: Power Constraint: 0 > Tag: QBSS Load Element 802.11e CCA Version > Tag: RM Enabled Capabilities (5 octets) > Tag: HT Capabilities (802.11n D1.10) > Tag: HT Information (802.11n D1.10) > Tag: Extended Capabilities (8 octets) > Tag: VHT Capabilities > Tag: VHT Operation > Tag: Tx Power Envelope > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element > Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5 > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11) > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44) < Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode Tag Number: Vendor Specific (221) Tag length: 25 OUI: 50:6f:9a (Wi-Fi Alliance) Vendor Specific OUI Type: 28 BSSID: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) SSID length: 14 SSID: OWE-Transition </pre>						

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".

No.	Time	Source	Destination	Protocol	Length	Info
22581	2025-01-21 09:52:23.230007	Cisco_dd:2e:8f	Broadcast	802.11	390	Beacon frame, SN=2483, FN=0, Flags=.....C, BI=100, SSID=Wildcard (Broadcast)
> Frame 22581: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Beacon frame, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (12 bytes) > Tagged parameters (314 bytes) > Tag: SSID parameter set: Wildcard SSID > Tag Number: SSID parameter set (0) > Tag length: 8 > SSID: <MISSING> > Tag: Supported Rates 6(0), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec] > Tag: DS Parameter set: Current Channel: 48 > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap > Tag: Country Information: Country Code IN, Environment All > Tag: Power Constraint: 0 > Tag: RSN Information > Tag: QBSS Load Element 802.11e CCA Version > Tag: PM Enabled Capabilities (5 octets) > Tag: HT Capabilities (802.11n D1.10) > Tag: HT Information (802.11n D1.10) > Tag: Extended Capabilities (8 octets) > Tag: VHT Capabilities > Tag: VHT Operation > Tag: Tx Power Envelope > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element > Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5 > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11) > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44) > Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode > Tag Number: Vendor Specific (221) > Tag length: 19 > OUI: 50:6f:9a (Wi-Fi Alliance) > Vendor Specific OUI Type: 28 > BSSID: Cisco_dd:2e:8f (40:ce:24:dd:2e:87) > SSID length: 8 > SSID: OPEN-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.

No.	Time	Source	Destination	Protocol	Length	Info
8509	2025-01-21 09:51:57.318400	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	197	Probe Request, SN=0, FN=0, Flags=.....C, SSID="OWE-Transition"
8510	2025-01-21 09:51:57.318412	ee:13:e8:a8:cd:5b	ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
8511	2025-01-21 09:51:57.319223	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	398	Probe Response, SN=782, FN=0, Flags=.....C, BI=100, SSID="OWE-Transition"
8512	2025-01-21 09:51:57.319233	Cisco_dd:2e:8f	Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C


```
> Frame 8509: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits) on 0
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Probe Request, Flags: .....C
> IEEE 802.11 Wireless Management
  > Tagged parameters (133 bytes)
    > Tag: SSID parameter set: "OWE-Transition"
      Tag Number: SSID parameter set (0)
      Tag length: 14
      SSID: "OWE-Transition"
    > Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 48
    > Tag: HT Capabilities (802.11n D1.0)
    > Tag: Extended Capabilities (11 octets)
    > Tag: VHT Capabilities
    > Ext Tag: HE Capabilities
    > Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operation - Optimized Connectivity Experience
      Tag Number: Vendor Specific (221)
      Tag length: 7
      OUI: 50:6f:9a (Wi-Fi Alliance)
      Vendor Specific OUI Type: 22
      > MBO/OCE attribute: 030102 (Cellular Data Capabilities)
      > Tag: Vendor Specific: Microsoft Corp.: Unknown 8
```

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.

```

8509 2025-01-21 09:51:57.318400 ee:13:e8:a8:cd:5b Cisco_dd:2e:8f 802.11 197 Probe Request, SN=0, FN=0, Flags=.....C, SSID="OWE-Transition"
8510 2025-01-21 09:51:57.318412 ee:13:e8:a8:cd:5b 802.11 48 Acknowledgement, Flags=.....C
8511 2025-01-21 09:51:57.319223 Cisco_dd:2e:8f ee:13:e8:a8:cd:5b 802.11 398 Probe Response, SA=782, FN=0, Flags=.....C, BI=100, SSID="OWE-Transition"
8512 2025-01-21 09:51:57.319233 Cisco_dd:2e:8f 802.11 48 Acknowledgement, Flags=.....C

```

> Frame 8511: 398 bytes on wire (3184 bits), 398 bytes captured (3184 bits)

> Radiotap Header v0, Length 36

> 802.11 radio information

> IEEE 802.11 Probe Response Flags:C

> IEEE 802.11 Wireless Management

> Fixed parameters (12 bytes)

> Tagged parameters (322 bytes)

> Tag: SSID parameter set: "OWE-Transition"

> Tag Number: SSID parameter set (0)

> Tag length: 34

SSID: "OWE-Transition"

> Tag: Supported Rates 6(0), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]

> Tag: DS Parameter set: Current Channel: 48

> Tag: Country Information: Country Code IN, Environment All

> Tag: Power Constraint: 0

> Tag: RSN Information

> Tag: QoS Load Element 802.11e CCA Version

> Tag: RM Enabled Capabilities (5 octets)

> Tag: HT Capabilities (802.11n D1.10)

> Tag: HT Information (802.11n D1.10)

> Tag: Extended Capabilities (8 octets)

> Tag: VHT Capabilities

> Tag: VHT Operation

> Tag: Tx Power Envelope

> Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

> Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5

> Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled

> Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)

> Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44)

> Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode

> Tag Number: Vendor Specific (221)

> Tag length: 19

> OUI: 50:6f:9a (Wi-Fi Alliance)

> Vendor Specific OUI Type: 28

BSSID: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

SSID length: 8

SSID: OPEN-OWE

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.

No.	Time	Source	Destination	Protocol	Length	Info
8517	2025-01-21 09:51:57.327250	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	70	Authentication, SN=1, FN=0, Flags=.....C
8518	2025-01-21 09:51:57.327265		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C

> Frame 8517: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

> Radiotap Header v0, Length 36

> 802.11 radio information

> IEEE 802.11 Authentication, Flags:C

Type/Subtype: Authentication (0x000b)

> Frame Control Field: 0xb000

.000 0000 0011 1100 = Duration: 60 microseconds

> Receiver address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

> Destination address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

> Transmitter address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b)

> Source address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b)

> BSS Id: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

.... 0000 = Fragment number: 0

0000 0000 0001 = Sequence number: 1

Frame check sequence: 0x928f3869 [unverified]

[FCS Status: Unverified]

[WLAN Flags:C]

> IEEE 802.11 Wireless Management

> Fixed parameters (6 bytes)

Authentication Algorithm: Open System (0)

Authentication SEQ: 0x0001

Status code: Successful (0x0000)

No.	Time	Source	Destination	Protocol	Length	Info
8520	2025-01-21 09:51:57.327278	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	70	Authentication, SN=783, FN=0, Flags=.....C
8521	2025-01-21 09:51:57.327349		Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
8522	2025-01-21 09:51:57.329457	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	337	Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Transition"
8523	2025-01-21 09:51:57.329466		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C

> Frame 8520: 70 bytes on wire (560 bits), 70 bytes captured (560 bits)

> Radiotap Header v0, Length 36

> 802.11 radio information

> IEEE 802.11 Authentication, Flags:C

Type/Subtype: Authentication (0x000b)

> Frame Control Field: 0xb000

.000 0000 0011 1100 = Duration: 60 microseconds

> Receiver address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b)

> Destination address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b)

> Transmitter address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

> Source address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

> BSS Id: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

.... 0000 = Fragment number: 0

0011 0000 1111 = Sequence number: 783

Frame check sequence: 0xc3c21908 [unverified]

[FCS Status: Unverified]

[WLAN Flags:C]

> IEEE 802.11 Wireless Management

> Fixed parameters (6 bytes)

Authentication Algorithm: Open System (0)

Authentication SEQ: 0x0002

Status code: Successful (0x0000)

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.

No.	Time	Source	Destination	Protocol	Length	Info
8522	2025-01-21 09:51:57.329457	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	337	Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Transition"
8523	2025-01-21 09:51:57.329466		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C

> Frame 8522: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits)

> Radiotap Header v0, Length 36

> 802.11 radio information

> IEEE 802.11 Association Request, Flags:C

> IEEE 802.11 Wireless Management

> Fixed parameters (4 bytes)

> Tagged parameters (269 bytes)

Tag: SSID parameter set: "OWE-Transition"

Tag Number: SSID parameter set (0)

Tag length: 14

SSID: "OWE-Transition"

> Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

> Tag: Power Capability Min: -20, Max: 14

> Tag: Supported Channels

> Tag: HT Capabilities (802.11n D1.10)

> Tag: RSN Information

> Tag: RM Enabled Capabilities (5 octets)

> Tag: Supported Operating Classes

> Tag: Extended Capabilities (11 octets)

> Tag: VHT Capabilities

> Tag: Vendor Specific: Samsung Electronics Co.,Ltd

> Tag: Vendor Specific: Samsung Electronics Co.,Ltd

> Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element

Ext Tag: OWE Diffie-Hellman Parameter

Ext Tag length: 34 (Tag len: 35)

Ext Tag Number: OWE Diffie-Hellman Parameter (32)

Group: 256-bit random ECP group (19)

Public Key: 7c2782ba4c77a98c7076d1fa2e3493347ec16d4c64345dccc8b9b68b212ff31

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
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

No.	Time	Source	Destination	Protocol	Length	Info
8527	2025-01-21 09:51:57.333153	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	245	Association Response, SN=784, FN=0, Flags=.....C
8528	2025-01-21 09:51:57.333161	Cisco_dd:2e:8f		802.11	48	Acknowledgement, Flags=.....C

> Frame 8527: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits)

- > Radiotap Header v0, Length 36
- > 802.11 radio information
 - IEEE 802.11 Association Response, Flags:
 - Type/Subtype: Association Response (0x0001)
 - Frame Control Field: 0x1000
 - .000 0000 0011 1100 = Duration: 60 microseconds
 - Receiver address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b)
 - Destination address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b)
 - Transmitter address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)
 - Source address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)
 - BSS Id: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)
 - 0000 = Fragment number: 0
 - 0011 0001 0000 = Sequence number: 784
 - Frame check sequence: 0x7fbed111 [unverified]
 - [FCS Status: Unverified]
 - [WLAN Flags:
- > IEEE 802.11 Wireless Management
 - > Fixed parameters (6 bytes)
 - > Capabilities Information: 0x1111
 - Status code: Successful (0x0000)
 - ..00 0000 0000 0001 = Association ID: 0x0001
 - > Tagged parameters (175 bytes)
 - > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
 - > Tag: RSN Information
 - > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
 - > Tag: HT Capabilities (802.11n D1.10)
 - > Tag: HT Information (802.11n D1.10)
 - > Tag: Extended Capabilities (8 octets)
 - > Tag: VHT Capabilities
 - > Tag: VHT Operation
 - > Tag: RM Enabled Capabilities (5 octets)
 - > Tag: BSS Max Idle Period

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.cd5b
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

No.	Time	Source	Destination	Protocol	Length	Info
8540	2025-01-21 09:51:57.360919	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	193	Key (Message 1 of 4)
8541	2025-01-21 09:51:57.360930	Cisco_dd:2e:8f	Broadcast	802.11	48	Acknowledgement, Flags=.....C
8542	2025-01-21 09:51:57.363375	Cisco_dd:2e:8f	Broadcast	802.11	376	Beacon frame, SN=3335, FN=0, Flags=.....C, BI=100, SSID="OPEN-OWE"
8543	2025-01-21 09:51:57.365594	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	215	Key (Message 2 of 4)
8544	2025-01-21 09:51:57.365603	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
8545	2025-01-21 09:51:57.366921	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	267	Key (Message 3 of 4)
8546	2025-01-21 09:51:57.366929	Cisco_dd:2e:8f	Broadcast	802.11	48	Acknowledgement, Flags=.....C
8547	2025-01-21 09:51:57.368482	Cisco_dd:2e:8f	Broadcast	802.11	376	Beacon frame, SN=3336, FN=0, Flags=.....C, BI=100, SSID="newssid"
8548	2025-01-21 09:51:57.373313	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	171	Key (Message 4 of 4)
8549	2025-01-21 09:51:57.373334	ee:13:e8:a8:cd:5b	ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C

> Frame 8540: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits)
 > Radiotap Header v0, Length 34
 > 802.11 radio information
 > IEEE 802.11 QoS Data, Flags:F.C
 > Logical-Link Control
 > 802.1X Authentication
 Version: 802.1X-2004 (2)
 Type: Key (3)
 Length: 117
 Key Descriptor Type: EAPOL RSN Key (2)
 [Message number: 1]
 > Key Information: 0x0088
 Key Length: 16
 Replay Counter: 0
 WPA Key Nonce: 1728f47ac2427421f37f1b43b6f69471eaf8a1a78feb2e1083d188c5a2e05ded
 Key IV: 00000000000000000000000000000000
 WPA Key RSC: 00000000000000000000000000000000
 WPA Key ID: 00000000000000000000000000000000
 WPA Key MIC: 00000000000000000000000000000000
 WPA Key Data Length: 22
 > WPA Key Data: dd14000fac0421b550dab0a335c355e7f4daa4a633af

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.cd5b
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.cd5b
2025/01/21 15:21:57.437239513 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
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 interface
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 interface
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.cd5b

```

Cientes 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 encriptación 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:

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
Enabled

Over the DS
☐

Reassociation Timeout *
20

WPA2/WPA3 Encryption

AES(CCMP128)
☒
CCMP256
☐

GCMP128
☐
GCMP256
☐

Protected Management Frame

PMF
Required

Association Comeback Timer*
1

SA Query Time*
200

Auth Key Mgmt

Fast Transition needs to be disabled

SAE
☐
FT + SAE
☐

OWE
☒
FT + 802.1X
☐

802.1X-SHA256
☐

Transition Mode WLAN ID
9

Cancel
Update & Apply to Device

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,

General **Security** Advanced Add To Policy Tags**Layer2** Layer3 AAA☐ WPA + WPA2☐ WPA2 + WPA3☒ WPA3☐ Static WEP☐ NoneMAC Filtering ☐Lobby Admin Access ☐

WPA Parameters

WPA Policy ☐GTK Randomize ☐WPA2 Policy ☐WPA3 Policy ☒Transition Disable ☐

WPA2/WPA3 Encryption

AES(CCMP128) ☒GCMP128 ☐CCMP256 ☐GCMP256 ☐

Protected Management Frame

PMF Association Comeback Timer* SA Query Time*

Fast Transition

Status Over the DS ☐Reassociation Timeout *

Auth Key Mgmt

OWE cannot be enabled with
802.1X/FT+802.1X/802.1X-SHA256/PSK/FT+PSK/PSK-
SHA256/CCKM/SAE/FT+SAE

SAE ☐FT + SAE ☐OWE ☒FT + 802.1X ☐802.1X-SHA256 ☒Transition Mode WLAN ID

Cancel

Update & Apply to Device

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

Edit WLAN

⚠ Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

☐ WPA + WPA2

☐ WPA2 + WPA3

☒ WPA3

☐ Static WEP

☐ None

MAC Filtering

☐

Lobby Admin Access

☐

WPA Parameters

WPA Policy

☐

WPA2 Policy

☐

GTK Randomize

☐

WPA3 Policy

☒

Transition Disable

☐

WPA2/WPA3 Encryption

AES(CCMP128)

☒

CCMP256

☐

GCMP128

☐

GCMP256

☐

Protected Management Frame

PMF

Required

Association Comeback Timer*

1

SA Query Time*

200

Fast Transition

Status

Enabled

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt

Fast Transition needs to be disabled

OWE cannot be enabled with
802.1X/FT+802.1X/802.1X-SHA256/PSK/FT+PSK/PSK-SHA256/CCKM/SAE/FT+SAE

SAE

☐

FT + SAE

☐

OWE

☒

FT + 802.1X

☒

802.1X-SHA256

☒

Transition Mode WLAN ID

9

Cancel



Update & Apply to Device

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.

⚠ 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

Disabled ▼

Over the DS

☐

Reassociation Timeout *

20

WPA2/WPA3 Encryption

AES(CCMP128) ☒

CCMP256 ☐

GCMP128 ☐

GCMP256 ☐

Protected Management Frame

PMF

Required ▼

Association Comeback Timer*

1

SA Query Time*

200

Auth Key Mgmt

WPA2 security valid combinations: 1. SuiteB cipher, 2. 802.1X-SHA256/FT-802.1X/802.1X AKM and AES cipher, 3. PSK-SHA256/FT-PSK/PSK AKM and AES cipher, 4. CCKM AKM and AES Cipher

OWE is supported with WPA3 (WPA/WPA2 must be disabled)

802.1x

☐

PSK

☐

CCKM ⚠

☐

SAE

☐

FT + SAE

☐

OWE

☒

FT + 802.1x

☐

FT + PSK

☐

802.1x-SHA256

☐

PSK-SHA256

☐

Transition Mode WLAN ID

7

MPSK Configuration

Enable MPSK

☐

↶ Cancel

📄 Update & Apply to Device

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,

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☐

GTK Randomize☐

WPA2 Policy☒

WPA3 Policy☒

Transition Disable☐

WPA2/WPA3 Encryption

AES(CCMP128)☒

GCMP128☐

CCMP256☐

GCMP256☐

Protected Management Frame

PMF

Required

Association Comeback Timer*

1

SA Query Time*

200

Fast Transition

Status

Enabled

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt

WPA2 security valid combinations: 1. SuiteB cipher, 2. 802.1X-SHA256/FT-802.1X/802.1X AKM and AES cipher, 3. PSK-SHA256/FT-PSK/PSK AKM and AES cipher, 4. CCKM AKM and AES Cipher

WPA3 security valid combinations: 1. SuiteB cipher, 2. 802.1X-SHA256/FT-802.1X AKM and AES cipher, 3. SAE/FT-SAE/OWE AKM and AES cipher.

802.1X☐

CCKM ⚠☐

FT + SAE☐

FT + PSK☐

PSK-SHA256☐

PSK☐

SAE☐

FT + 802.1X☐

802.1X-SHA256☐

MPSK Configuration

Enable MPSK

☐

↶ Cancel

📄 Update & Apply to Device

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.

8522	2025-01-21 09:51:57.329457	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	337	21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af	Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Tri
44117	2025-01-21 09:53:12.847592	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	337	21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af	Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Tri

Frame 8522: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits)

> Radiotap Header v0, Length 36

> 802.11 radio information

> IEEE 802.11 Association Request, Flags:C

> IEEE 802.11 Wireless Management

> Fixed parameters (4 bytes)

> Tagged parameters (269 bytes)

> Tag: SSID parameter set: "OWE-Transition"

> Tag: Supported Rates 6(0), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]

> Tag: Power Capability Min: -20, Max: 14

> Tag: Supported Channels

> Tag: HT Capabilities (802.11n D1.10)

> Tag: RSN Information

> Tag Number: RSN Information (48)

> Tag length: 42

> RSN Versions: 1

> Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)

> Pairwise Cipher Suite Count: 1

> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)

> Auth Key Management (AKM) Suite Count: 1

> Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption

> RSN Capabilities: 0x00c0

> PMKID Count: 1

> PMKID List

> PMKID: 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af

> Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) GIP (128)

> Tag: PM Enabled Capabilities (5 octets)

> Tag: Supported Operating Classes

> Tag: Extended Capabilities (11 octets)

> Tag: VHT Capabilities

> Tag: Vendor Specific: Samsung Electronics Co.,Ltd

> Tag: Vendor Specific: Samsung Electronics Co.,Ltd

> Tag: Vendor Specific: Microsoft Corp.: WMM/OWE: Information Element

> Ext Tag: OWE Diffie-Hellman Parameter

> Ext Tag length: 34 (Tag len: 35)

> Ext Tag Number: OWE Diffie-Hellman Parameter (32)

> Group: 256-bit random ECP group (19)

> Public Key: 7c 27 82 ba 4c 77 a9 8c 70 76 d1 fa 2e 34 93 34 7e c1 6d 4c 64 34 5d cc f8 b9 bb 68 b2 12 ff 31

Imagen-14: Uso del mismo PMKID

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
8527	2025-01-21 09:51:57.333153	Cisco_ddi2e:8f	ee:13:e8:a8:cd:5b	802.11	245		21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af	Association Response, SN=784, FN=0, Flags=.....C
> Frame 8527: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Association Response, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (6 bytes) > Tagged parameters (175 bytes) > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] > Tag: RSN Information Tag Number: RSN Information (48) Tag length: 42 RSN Version: 1 > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM) Pairwise Cipher Suite Count: 1 > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM) Auth Key Management (AKM) Suite Count: 1 > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption RSN Capabilities: 0x00e0 PMKID Count: 1 PMKID List PMKID: 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128) > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element > Tag: HT Capabilities (802.11n D1.10) > Tag: HT Information (802.11n D1.10) > Tag: Extended Capabilities (8 octets) > Tag: VHT Capabilities > Tag: VHT Operation > Tag: RM Enabled Capabilities (5 octets) > Tag: BSS Max Idle Period								

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.

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
44117	2025-01-21 09:53:12.847592	ee:13:e8:a8:cd:5b	Cisco_ddi2e:8f	802.11	337		21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af	Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Tr
> Frame 44117: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Association Request, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (4 bytes) > Tagged parameters (269 bytes) > Tag: SSID parameter set: "OWE-Transition" > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] > Tag: Power Capability Min: -20, Max: 14 > Tag: Supported Channels > Tag: HT Capabilities (802.11n D1.10) > Tag: RSN Information Tag Number: RSN Information (48) Tag length: 42 RSN Version: 1 > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM) Pairwise Cipher Suite Count: 1 > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM) Auth Key Management (AKM) Suite Count: 1 > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption RSN Capabilities: 0x00c0 PMKID Count: 1 PMKID List PMKID: 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128) > Tag: RM Enabled Capabilities (5 octets) > Tag: Supported Operating Classes > Tag: Extended Capabilities (11 octets) > Tag: VHT Capabilities > Tag: Vendor Specific: Samsung Electronics Co.,Ltd > Tag: Vendor Specific: Samsung Electronics Co.,Ltd > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element > Ext Tag: OWE Diffie-Hellman Parameter Ext Tag length: 34 (Tag len: 35) Ext Tag Number: OWE Diffie-Hellman Parameter (32) Group: 256-bit random ECP group (19) Public Key: ba ba f5 2b f0 a5 4c 02 2f 16 f1 0b ad 95 a0 4f cf 95 79 58 3d dc 77 96 bb b3 59 52 42 25 cf 6f								

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

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
44121	2025-01-21 09:53:12.851872	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	266			Association Response, SN=1229, FN=0, Flags=.....C
> Frame 44121: 266 bytes on wire (2128 bits), 266 bytes captured (2128 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Association Response, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (6 bytes) > Tagged parameters (196 bytes) > Tag: Supported Rates 6(0), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec] > Tag: RSN Information > Tag Number: RSN Information (48) > Tag length: 26 > RSN Version: 1 > Group Cipher Suite: 00:0fac (Ieee 802.11) AES (COM) > Pairwise Cipher Suite Count: 1 > Pairwise Cipher Suite List 00:0fac (Ieee 802.11) AES (COM) > Auth Key Management (AKM) Suite Count: 1 > Auth Key Management (AKM) List 00:0fac (Ieee 802.11) Opportunistic Wireless Encryption > RSN Capabilities: 00008 > PMKID Count: 0 > PMKID List > Group Management Cipher Suite: 00:0fac (Ieee 802.11) BIP (128) > Tag: Vendor Specific: Microsoft Corp.: WMM/WMF: Parameter Element > Tag: HT Capabilities (802.11n D1.10) > Tag: HT Information (802.11n D1.10) > Tag: Extended Capabilities (8 octets) > Tag: VHT Capabilities > Tag: VHT Operation > Tag: RM Enabled Capabilities (5 octets) > Tag: BSS Max Idle Period > Ext Tag: OWE Diffie-Hellman Parameter > Ext Tag length: 34 (Tag len: 35) > Ext Tag Number: OWE Diffie-Hellman Parameter (32) > Group: 256-bit random ECP group (19) > Public Key: e4 44 ea 00 6f f3 69 35 33 93 59 3f 7d b7 2e ab d4 04 26 7e 62 da d9 2a 88 c9 4e f5 e2 69 a1 c5								

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".

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
8540	2025-01-21 09:51:57.360919	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	193			Key (Message 1 of 4)
8543	2025-01-21 09:51:57.365594	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	215		21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af	Key (Message 2 of 4)
8545	2025-01-21 09:51:57.366921	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	267			Key (Message 3 of 4)
8548	2025-01-21 09:51:57.373313	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	171			Key (Message 4 of 4)
> Frame 8540: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) > Radiotap Header v0, Length 34 > 802.11 radio information > IEEE 802.11 QoS Data, Flags:F.C > Logical-Link Control > 802.1X Authentication > Version: 802.1X-2004 (2) > Type: Key (3) > Length: 117 > Key Descriptor Type: EAPOL RSN Key (2) > [Message number: 1] > Key Information: 0x0088 > Key Length: 16 > Replay Counter: 0 > WPA Key Nonce: 17 28 f4 7a c2 42 74 21 f3 7f 1b 43 b6 f6 94 71 ea f8 a1 a7 8f eb 2e 10 83 d1 88 c5 a2 e0 5d ed > Key IV: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 > WPA Key RSC: 00 00 00 00 00 00 00 00 > WPA Key ID: 00 00 00 00 00 00 00 00 > WPA Key MIC: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 > WPA Key Data Length: 22 > WPA Key Data: dd 14 00 0f ac 04 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af > Tag: Vendor Specific: Ieee 802.11: RSN PMKID > Tag Number: Vendor Specific (221) > Tag length: 20 > OUI: 00:0fac (Ieee 802.11) > Vendor Specific OUI Type: 4 > Data Type: PMKID KDE (4) > PMKID: 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af								

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".

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
44128	2025-01-21 09:53:12.857869	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	193			Key (Message 1 of 4)
44133	2025-01-21 09:53:12.861273	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	215		21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af	Key (Message 2 of 4)
44135	2025-01-21 09:53:12.862728	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	267			Key (Message 3 of 4)
44138	2025-01-21 09:53:12.865398	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	171			Key (Message 4 of 4)

> Frame 44128: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits)

> Radiotap Header v0, Length 34

> 802.11 radio information

> IEEE 802.11 QoS Data, Flags:R.F.C

> Logical-Link Control

> 802.1X Authentication

Version: 802.1X-2004 (2)

Type: Key (3)

Length: 117

Key Descriptor Type: EAPOL RSN Key (2)

[Message number: 1]

> Key Information: 0x0088

Key Length: 16

Replay Counter: 0

WPA Key Nonce: 17 28 f4 7a c2 42 74 21 f3 7f 1b 43 b6 f6 94 71 ea f8 a1 a7 8f eb 2e 10 83 d1 88 c5 a2 e0 5d ee

Key IV: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

WPA Key RSC: 00 00 00 00 00 00 00 00

WPA Key ID: 00 00 00 00 00 00 00 00

WPA Key MIC: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

WPA Key Data Length: 22

WPA Key Data: dd 14 00 0f ac 04 41 1b cf d7 7a 34 cb 50 70 13 07 47 b8 d2 4e 1f

> WPA Key Data: dd 14 00 0f ac 04 41 1b cf d7 7a 34 cb 50 70 13 07 47 b8 d2 4e 1f

> Tag: Vendor Specific: IEEE 802.11: RSN PMKID

Tag Number: Vendor Specific (221)

Tag length: 20

OUI: 00:0f:ac (IEEE 802.11)

Vendor Specific OUI Type: 4

Data Type: PMKID KDE (4)

PMKID: 41 1b cf d7 7a 34 cb 50 70 13 07 47 b8 d2 4e 1f

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).