

Comprendre le flux de chiffrement sans fil opportuniste

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Description](#)

[Étapes](#)

[Détails de Lab Repro](#)

[DÉBIT DE LA DETTE](#)

[trame Beacon d'origine](#)

[Balises SSID masquées](#)

[Requête de sondage envoyée du client au SSID de transition OWE](#)

[Réponse d'enquête envoyée du point d'accès au client](#)

[Authentification ouverte](#)

[Demande d'association du client au point d'accès](#)

[Réponse d'association envoyée du point d'accès au client](#)

[Échange De Clés](#)

[Authentification L2 réussie](#)

[État d'apprentissage IP](#)

[Client en état d'exécution](#)

[Clients non pris en charge pour le cryptage OWE](#)

[information sur la transition rapide](#)

[OWE n'est pas pris en charge avec PSK/dot1x](#)

[Dépannage](#)

[RA Trace et EPC \(capture PAcKet intégrée\)](#)

[BOUCHON PNEUMATIQUE](#)

[Itinérance](#)

Introduction

Ce document décrit le flux de transition OWE et comment il fonctionne sur le contrôleur LAN sans fil (WLC) Catalyst 9800.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comment configurer le WLC 9800, le point d'accès (AP) pour le fonctionnement de base
- Comment configurer les profils WLAN et de stratégie.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- C9800-80, Cisco IOS® XE 17.12.4 et également testé sous Cisco IOS® XE 17.9.6
- Modèle AP : C9136I, coché en mode de connexion locale et en mode de connexion flexible.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Description

- OWE (Opportunistic Wireless Encryption) est une extension de la norme IEEE 802.11 qui assure le cryptage du support sans fil. L'objectif de l'authentification basée sur OWE est d'éviter une connectivité sans fil ouverte et non sécurisée entre les points d'accès et les clients.
- L'OWE utilise le cryptage basé sur les algorithmes Diffie-Hellman pour configurer le cryptage sans fil.
- Avec OWE, le client et le point d'accès effectuent un échange de clés Diffie-Hellman pendant la procédure d'accès et utilisent le secret par paire résultant avec la connexion en 4 étapes.
- L'utilisation d'OWE améliore la sécurité du réseau sans fil pour les déploiements où des réseaux basés sur une clé prépartagée ouverte ou partagée sont déployés.

Étapes

1. Configurez un WLAN OUVERT sans chiffrement/sécurité et activez la diffusion.
2. Configurez un autre SSID avec les paramètres de sécurité OWE et mappez le numéro d'ID WLAN OUVERT dans transition-mode-wlan-id. Désactivez l'option SSID de diffusion dans ce SSID de transition OWE.
3. Mappez le numéro d'ID WLAN de transition OWE dans le champ OPEN WLAN "transition-mode-wlan-id".

Détails de Lab Repro

- Nom SSID ouvert : DOUÉ DE TOUS

- Nom SSID de transition OWE : Transition OWE
- BSSID d'OPEN-OWE : 40:ce:24:dd:2e:87
- BSSID de OWE-Transition : 40:ce:24:dd:2e:8f

DÉBIT DE LA DETTE

1. Les balises peuvent être diffusées pour un SSID OUVERT. Vous pouvez le voir par son nom SSID dans AIR PCAP.
2. Nous pouvons également voir le SSID activé de sécurité cachée avec le nom "Wildcard" au lieu de son propre nom SSID dans AIR PCAP.
3. Une fois que les clients reçoivent la trame de balise pour le SSID OUVERT, s'il a ou prend en charge OWE, il peut commencer à envoyer une requête de sonde au SSID de transition OWE (qui est le SSID activé par la sécurité au lieu du SSID OUVERT).
4. Les clients pris en charge par OWE peuvent obtenir une réponse de sonde du SSID de transition.
5. L'authentification OPEN peut se produire entre le client et le point d'accès.
6. Le client peut envoyer une requête d'association au point d'accès avec des détails d'échange de clé DH et utiliser le secret par paire résultant pour la connexion en 4 étapes.
7. AP peut envoyer une réponse d'association.
8. Un échange en quatre étapes peut avoir lieu entre le point d'accès et le périphérique client.
9. Une fois la gestion des clés réussie, L2 PSK peut réussir.
10. Le client peut obtenir l'adresse IP auprès de DHCP, ARP, etc.
11. Le client peut passer à l'état EXÉCUTÉ.
12. Si les périphériques clients ne prennent pas en charge OWE, il peut alors envoyer une requête de sonde au SSID OUVERT lui-même et obtenir directement l'adresse IP avant de passer à l'état RUN.

trame Beacon d'origine

- Ici, AIR PCAP montre que, la diffusion SSID "OPEN-OWE" (Beacon Frame). Qui contient des détails SSID de transition et il a appelé "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"

```

> 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
  
```

Image-1 : Trame de balise du SSID OUVERT

Balises SSID masquées

- Selon la configuration WLAN, la « diffusion » est désactivée pour ce SSID « OWE-Transition », cependant, vous pouvez voir les balises SSID masquées dans AIR PCAP qui contiennent le nom SSID « Wildcard ». Cependant, si vous vérifiez ce paquet, il contient des détails sur OWE-Transition.
- Obtenez le BSSID du SSID masqué en utilisant ce paquet, comme « 40:ce:24:dd:2e:8f » et recherchez-le dans la capture de paquets.
- Dans ce paquet, il montre que, SSID "Missing" et il contient son SSID de transition comme "OPEN-OWE" et son 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: 0
      SSID: <MISSING>
    > 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: RSN Information
    > 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: 19
      OUI: 50:6f:9a (Wi-Fi Alliance)
      Vendor Specific OUI Type: 28
      BSSID: Cisco_dd:2e:87 (40:ce:24:dd:2e:87)
      SSID length: 8
      SSID: OPEN-OWE
  
```

Requête de sondage envoyée du client au SSID de transition OWE

- Sur la base du SSID de la trame de balise « OPEN-OWE », le client apprend à connaître les autres détails du SSID dont il a besoin pour se connecter, dans ce scénario, il s'agit de « OWE-Transition ». Si le client est capable de prendre en charge le cryptage OWE, il peut alors envoyer la demande de sonde au SSID « OWE-Transition » et obtenir une réponse.
- Requête d'analyse envoyée au BSSID OWE-Transition « 40:ce:24:dd:2e:8f » et une réponse a été obtenue. À l'intérieur de ce paquet de réponse de sonde également, vous pouvez voir les détails du 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)
> 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 D1.10)
      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
  
```

Image-3 : Requête de sonde

Réponse d'enquête envoyée du point d'accès au client

- Le client a reçu une réponse de sonde pour le SSID « OWE-Transition », mais il a ses détails SSID d'origine « OPEN-OWE » dans 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, SN=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: 14
      SSID: "OWE-Transition"
        Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 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

```

Image-4 : Réponse De Sonde

Authentification ouverte

- Après avoir obtenu la réponse de sonde, l'authentification OPEN peut se produire entre le client et le point d'accès pour vérifier les détails/capacités du wifi du client, avant l'association.

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	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	ee:13:e8:a8:cd:5b	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	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)
  
```

Image-5 : Authentication OPEN après une analyse réussie

Demande d'association du client au point d'accès

- Dans ce paquet, notez que le client peut joindre une valeur de paramètre Diffie-Hellman pour le chiffrement.

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	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: 7c2782ba4c77a98c7076d1fa2e3493347ec16d4c64345dccc78b9bb68b212ff31
  
```

Image-6 : Demande D'Association

- Dans RA trace, vous pouvez commencer à voir les journaux du client depuis la phase d'association,

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

Réponse d'association envoyée du point d'accès au client

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	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: .....C
  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: .....C]
  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
  
```

Image-7 : Réponse d'association

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

Échange De Clés

Un échange en quatre étapes peut avoir lieu entre le point d'accès et le périphérique client.

Key-1 envoyé par AP

Clé 2 envoyée par le client

Key-3 envoyé par AP

Envoi de la clé 4 par le client

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	Cisco_dd:2e:8f	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	Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
8547	2025-01-21 09:51:57.368482	Cisco_dd:2e:86	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	Cisco_dd:2e:8f	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: 0000000000000000

WPA Key ID: 0000000000000000

WPA Key MIC: 00000000000000000000000000000000

WPA Key Data Length: 22

> WPA Key Data: dd14000fac0421b550dab0a335c355e7f4daa4a633af

Image-8 : Connexion en quatre étapes

```

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

```

Authentification L2 réussie

```

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

```

État d'apprentissage 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
```

Client en état d'exécution

```
2025/01/21 15:21:57.537017277 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
```

Clients non pris en charge pour le cryptage OWE

- En examinant une trame de balise elle-même, les clients savent s'ils sont en mesure de prendre en charge cette méthode de chiffrement ou non. S'il n'est pas pris en charge, alors il peut simplement envoyer une demande d'enquête pour ouvrir le SSID « OPEN-OWE » et peut faire une authentification ouverte normale, obtenir une adresse IP, puis il peut passer à l'état 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: d037.4587.8f35
2025/01/16 15:36:06.281808554 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:06.303307756 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f35
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: d037.4587.8f35
```

information sur la transition rapide

- Nous sommes en mesure de configurer OWE uniquement dans l'authentification OPEN ou dans Webauth (CWA/LWA/EWA).
- FT n'est pas pris en charge dans la transition OWE.
- Si vous activez FT, vous obtenez ce message d'erreur,

⚠ 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 Enabled ▾

Over the DS

Reassociation Timeout * 20

WPA2/WPA3 Encryption

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

Auth Key Mgmt

Fast Transition needs to be disabled

SAE	<input type="checkbox"/>	FT + SAE	<input type="checkbox"/>
OWE	<input checked="" type="checkbox"/>	FT + 802.1X	<input type="checkbox"/>
802.1X-SHA256	<input type="checkbox"/>		

Transition Mode WLAN ID 9

Protected Management Frame

PMF Required ▾

Association Comeback Timer* 1

SA Query Time* 200

Image-9 : Message d'erreur lorsque nous activons FT dans OWE Transition SSID

OWE n'est pas pris en charge avec PSK/dot1x

Nous ne sommes pas en mesure d'activer OWE dans ces combinaisons,

1. 802.1x ou FT+802.1x
2. PSK ou FT+PSK ou PSK-SHA256
3. SAE ou FT+SAE
4. 802.1x-SHA256 ou FT+802.1x-SHA256

Si vous essayez d'activer l'une de ces méthodes, vous pouvez obtenir le message d'erreur,

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

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

Protected Management Frame

PMF ▼
Association Comeback Timer*
SA Query Time*

Cancel

Update & Apply to Device

Image-10 : Message d'erreur obtenu lors de l'activation d'autres méthodes d'authentification dans OWE SSID

⚠ 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
 Association Comeback Timer*
 SA Query Time*

Fast Transition

Status
 Over the DS
 Reassociation Timeout *

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

Cancel

Update & Apply to Device

Image-11 : Message d'erreur lors de l'activation AKM

- Dans la version IOS de Cisco IOS® XE 17.9.6, vous pouvez voir l'option "OWE" sous AKM quand vous sélectionnez "WPA2+WPA3" cependant vous pouvez obtenir le message d'erreur, vous ne pouvez pas utiliser OWE avec cette combinaison.

⚠ 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

<input type="radio"/> WPA + WPA2	<input checked="" type="radio"/> WPA2 + WPA3	<input type="radio"/> WPA3	<input type="radio"/> Static WEP	<input type="radio"/> None
----------------------------------	--	----------------------------	----------------------------------	----------------------------

MAC Filtering

Lobby Admin Access

WPA Parameters

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

Fast Transition

Status Disabled ▾

Over the DS

Reassociation Timeout *

WPA2/WPA3 Encryption

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

Protected Management Frame

PMF Required ▾

Association Comeback Timer*

SA Query Time*

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	<input type="checkbox"/>	PSK	<input type="checkbox"/>
CCKM ⚠	<input type="checkbox"/>	SAE	<input type="checkbox"/>
FT + SAE	<input type="checkbox"/>	OWE	<input checked="" type="checkbox"/>
FT + 802.1x	<input type="checkbox"/>	FT + PSK	<input type="checkbox"/>
802.1x-SHA256	<input type="checkbox"/>	PSK-SHA256	<input type="checkbox"/>

Transition Mode WLAN ID

MPSK Configuration

Enable MPSK

↶ Cancel

📄 Update & Apply to Device

Image-12 : Message d'erreur lorsque nous choisissons WPA2+WPA3

- Dans la version 17.12.4 de Cisco IOS® XE, lorsque vous choisissez "WPA2+WPA3", vous

ne pouvez pas obtenir l'option "OWE" dans 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	<input type="checkbox"/>	WPA2 Policy	<input checked="" type="checkbox"/>
GTK Randomize	<input type="checkbox"/>	WPA3 Policy	<input checked="" type="checkbox"/>
		Transition Disable	<input type="checkbox"/>

WPA2/WPA3 Encryption

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

Protected Management Frame

PMF

Association Comeback Timer*

SA Query Time*

Fast Transition

Status

Over the DS

Reassociation Timeout *

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	<input type="checkbox"/>	PSK	<input type="checkbox"/>
CCKM ⚠	<input type="checkbox"/>	SAE	<input type="checkbox"/>
FT + SAE	<input type="checkbox"/>	FT + 802.1X	<input type="checkbox"/>
FT + PSK	<input type="checkbox"/>	802.1X-SHA256	<input type="checkbox"/>
PSK-SHA256	<input type="checkbox"/>		

MPSK Configuration

Enable MPSK

Image-13 : Message d'erreur - Option OWE non obtenue dans AKM

Dépannage

1. Vérifiez les configurations dans les deux WLAN, dans OPEN SSID et dans OWE transition SSID doivent avoir transition WLAN ID mappé.
2. L'option de diffusion doit être désactivée dans le SSID de transition OWE, elle doit être activée uniquement dans le SSID OUVERT.
3. Vérifiez les méthodes d'authentification/cryptage/FT prises en charge décrites dans cet article.
4. Si les configurations sont correctes de l'extrémité WLC, que s'il vous plaît recueillir les journaux et les sorties nécessaires pour réduire le problème,

RA Trace et EPC (capture PAcKet intégrée)

Connexion à l'interface utilisateur graphique WLC -> Dépannage -> Suivi radioactif -> Ajouter l'adresse MAC wifi du client -> Cochez cette case pour les clients -> Démarrer

Connectez-vous à l'interface graphique WLC -> Dépannage -> Capture de paquets -> Ajouter un nouveau nom de fichier -> Choisissez l'interface de liaison ascendante et WMI VLAN/Interface -> Démarrer.

À partir de la machine client : Si possible, vous pouvez installer l'application Wireshark et collecter la capture de paquets en choisissant l'interface 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>

BOUCHON PNEUMATIQUE

Vous pouvez le collecter en utilisant un ordinateur portable MAC ou en configurant l'un des points d'accès en mode renifleur, veuillez consulter ces liens,

Depuis un ordinateur portable MAC :

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

À partir de 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>

Connectez un ordinateur portable (serveur Wireshark) au port du commutateur et il doit avoir l'application Wireshark installée dedans, ce serveur Wireshark doit avoir l'accessibilité à l'interface WMI WLC. Nécessité d'autoriser le protocole « 5555 ou 5000 ou 5556 » dans le pare-feu s'il se présente entre votre WLC et le serveur Wireshark.

Vérifiez s'il y a un « gscaler » installé dans ce PC où wireshark installé, si c'est que s'il est s'il vous

plaît "éteignez" et essayez, si c'est un pare-feu comme Windows Defender ou tout ce qui y est présent, s'il vous plaît désactiver ceux-ci et essayer de recueillir PCAP.

Itinérance

Lorsque le client se déplace d'un point d'accès à un autre, il doit effectuer ces étapes,

- Nécessité d'envoyer une nouvelle association/association : dépend de la demande du client.
- Besoin d'envoyer les détails DH (Diffie-Helman) dans la demande d'association.
- Le client peut obtenir des détails DH dans la réponse d'association du point d'accès, en fonction de ce PMK est généré à la fois dans le client et le point d'accès.
- Un échange en quatre étapes peut avoir lieu entre le point d'accès et le client.
- Dans OWE, vous ne pouvez pas activer la fonction FT, donc la norme 802.11r n'est pas possible.
- À chaque fois, lorsque le client se déplace, il doit établir une connexion en quatre étapes après un échange DH en association.
- Client et point d'accès utilisant leur propre PMKID, il est unique pour chaque point d'accès et client.
- Si le client se connecte au même AP, il peut utiliser le même PMKID. Dans certains scénarios, si le client a été supprimé, AP peut générer un nouveau PMKID, mais le client utilise le même PMKID pour la connexion en 4 étapes.

Exemple :

Si le client se connecte au même AP, alors vous pouvez voir le même PMKID dans Association-Request et Association-Response. Dans la réponse Association, vous ne pouvez pas voir les détails DH s'il utilise le même 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-Tr
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-Tr

> 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, D(0)/sec)
    > Tag: Power Capability Min: -20, Max: 14
    > Tag: Supported Channels
    > Tag: HT Capabilities (802.11n D1.0)
    > Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 42
      RSN 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) 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: 00:0fac (Ieee 802.11) GIP (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.: WPA/WPE: 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
```

Image-14 : Utilisation du même 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: 0x00e8
      > 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.: WPM/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
  
```

Image-15 : Réponse d'association avec le même PMKID

Pour le test, a supprimé ce client manuellement du WLC et il a été associé à nouveau au même AP, à ce moment, le client envoie un même PMKID mais AP envoie des détails DH dans la réponse d'association.

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.: WPM/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
  
```

Image-16 : Après la suppression, le client a envoyé le même PMKID avec les détails 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(B), 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: 00:0f: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: 00000000
      > PMKID Count: 0
      > PMKID List
      > Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
    > Tag: Vendor Specific: Microsoft Corp.: WMM/PMME: Parameter Element
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (8 octets)
    > Tag: WHT Capabilities
    > Tag: WHT Operation
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: BSS Max Idle Period
  > Ext Tag: 0xE Diffie-Hellman Parameter
    > Ext Tag length: 34 (Tag len: 35)
    > Ext Tag Number: 0xE 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

```

Image-17 : Le point d'accès utilise des valeurs DH pour générer son nouveau PMKID

Dans cet exemple : Le point d'accès et le client utilisent le même PMKID lors de la connexion en 4 étapes. Consultez les messages « M1 et 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 00 00 00 00 00 00 00 00
  > WPA Key ID: 00 00 00 00 00 00 00 00 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: 00:0f:ac (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

```

Image- 18 : AP et client utilisant le même PMKID

Dans cet exemple : Le client utilisant le même PMKID mais AP utilisant un PMKID différent qu'il a généré après la suppression du client, cochez les messages "M1 et 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 fe 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

> 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

Image-19 : AP et client utilisant un PMKID différent

À partir de la trace RA interne :

Dans cet exemple : Le client a envoyé des paramètres DH dans la demande d'association et le point d'accès a traité la 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

```

Après cela, le même client se connectant au même AP, à ce moment-là, AP n'a pas généré de nouveau 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

```

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.