

Entender O Fluxo De Criptografia Sem Fio Oportunista

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Descrição](#)

[Etapas](#)

[Detalhes do Lab Repro](#)

[FLUXO DE DÉBITO](#)

[Quadro original de beacon](#)

[Beacons de SSID ocultos](#)

[Solicitação de Investigação enviada do cliente para o SSID de Transição OWE](#)

[Resposta de sondagem enviada do AP para o cliente](#)

[autenticação OPEN](#)

[Solicitação de Associação do cliente para o AP](#)

[Resposta de associação enviada do AP para o cliente](#)

[Intercâmbio de chave](#)

[Autenticação L2 Bem-sucedida](#)

[Estado de aprendizagem IP](#)

[Cliente no estado EXECUTAR](#)

[Clientes sem suporte para criptografia OWE](#)

[Informações sobre a transição rápida](#)

[OWE não é suportado com PSK/dot1x](#)

[Troubleshooting](#)

[RA Trace e EPC \(Captura de PArket Incorporada\)](#)

[AIR PCAP](#)

[Roaming](#)

Introdução

Este documento descreve o fluxo de transição OWE e como ele funciona no Catalyst 9800 Wireless LAN Controller (WLC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como configurar a WLC 9800, o ponto de acesso (AP) para operação básica
- Como configurar perfis de WLAN e de política.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- C9800-80, Cisco IOS® XE 17.12.4 e também testado no Cisco IOS® XE 17.9.6
- Modelo de AP: C9136I, verificado nos modos de conexão local e flexível.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Descrição

- OWE (Opportunistic Wireless Encryption) é uma extensão do IEEE 802.11 que fornece criptografia para o meio sem fio. A finalidade da autenticação baseada em OWE é evitar a conectividade sem fio aberta e não segura entre o AP e os clientes.
- O OWE usa a criptografia baseada em algoritmos Diffie-Hellman para configurar a criptografia sem fio.
- Com o OWE, o cliente e o AP executam uma troca de chave Diffie-Hellman durante o procedimento de acesso e usam o segredo resultante em pares com o handshake de 4 vias.
- O uso do OWE melhora a segurança da rede sem fio para implantações em que redes abertas ou compartilhadas baseadas em PSK são implantadas.

Etapas

1. Configure uma WLAN ABERTA sem qualquer criptografia/segurança e habilite a transmissão.
2. Configure outro SSID com configurações de segurança OWE e mapeie o número de ID de WLAN OPEN no modo de transição-wlan-id. Desabilite a opção de SSID de transmissão neste SSID de transição OWE.
3. Mapeie o número de ID da WLAN de transição OWE no campo OPEN WLAN "transition-mode-wlan-id".

Detalhes do Lab Repro

- Nome do SSID aberto: OPEN-OWE

- Nome do SSID de transição OWE: Transição OWE
- BSSID de OPEN-OWE: 40:ce:24:dd:2e:87
- BSSID de OWE-Transition: 40:ce:24:dd:2e:8f

FLUXO DE DÉBITO

1. Os beacons podem ser transmitidos para o SSID ABERTO. Você pode vê-lo por seu nome SSID no AIR PCAP.
2. Também podemos ver o SSID habilitado para segurança oculta com o nome "Curinga" em vez de seu próprio nome SSID no AIR PCAP.
3. Quando os clientes receberem o quadro beacon para o SSID ABERTO, se ele tiver ou suportar o OWE, ele poderá começar a enviar a solicitação de sondagem para o SSID de transição do OWE (que é o SSID com segurança ativada em vez do SSID ABERTO).
4. Os clientes compatíveis com OWE podem obter resposta de sondagem do SSID de transição.
5. A autenticação OPEN pode ocorrer entre o cliente e o AP.
6. O cliente pode enviar uma solicitação de associação ao AP com detalhes de troca de chave DH e usar o segredo resultante em pares para o handshake de 4 vias.
7. O AP pode enviar a resposta da associação.
8. O handshake de quatro vias pode acontecer entre o AP e o dispositivo do cliente.
9. Após o gerenciamento bem-sucedido de chaves, a L2 PSK pode ser bem-sucedida.
10. O cliente pode obter o IP de DHCP, ARP, etc.
11. O cliente pode ir para o estado EXECUTAR.
12. Se os dispositivos cliente não estiverem suportando OWE, ele poderá enviar a solicitação de sondagem para o próprio SSID OPEN e poderá obter diretamente o IP do que poderá ir para o estado RUN.

Quadro original de beacon

- Aqui, AIR PCAP mostra isso, o SSID "OPEN-OWE" broadcast (Quadro de Beacon). Que contém detalhes do SSID de transição e é chamado de "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>						

Imagem-1: Quadro de beacon do SSID ABERTO

Beacons de SSID ocultos

- De acordo com a configuração da WLAN, a "transmissão" está desabilitada para esse SSID de "transição OWE". No entanto, você pode ver beacons de SSID ocultos no AIR PCAP que contêm o nome de SSID "Curinga". No entanto, se você verificar esse pacote, ele conterá detalhes de OWE-Transition.
- Obtenha o BSSID do SSID oculto usando este pacote, como "40:ce:24:dd:2e:8f" e pesquise-o na captura de pacotes.
- Nesse pacote, ele mostra que o SSID está "ausente" e contém seu SSID de transição como "OPEN-OWE" e seu 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: 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:87 (40:ce:24:dd:2e:87)
      SSID length: 8
      SSID: OPEN-OWE

```

Solicitação de Investigação enviada do cliente para o SSID de Transição OWE

- Com base no quadro de beacon SSID "OPEN-OWE", o cliente passa a conhecer os outros detalhes do SSID que precisa conectar; nesse cenário, é "OWE-Transition". Se o cliente for capaz de suportar a criptografia OWE, ele poderá enviar a solicitação de sondagem para o SSID "OWE-Transition" e obter uma resposta.
- Solicitação de sondagem enviada para OWE-Transition BSSID "40:ce:24:dd:2e:8f" e obteve uma resposta. Dentro desse pacote de resposta de sondagem também, você pode ver detalhes do 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
  
```

Imagem 3: Solicitação de Sondagem

Resposta de sondagem enviada do AP para o cliente

- O cliente recebeu uma resposta de sondagem para o SSID "OWE-Transition", no entanto, ele tem seus detalhes de SSID originais "OPEN-OWE" na 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, 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: 34
    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

```

Imagem-4: Resposta da Sondagem

autenticação OPEN

- Depois de obter a resposta da sonda, a autenticação OPEN pode acontecer entre o cliente e o AP para verificar os detalhes/capacidades wifi dos clientes, antes da associação.

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)						

Imagem 5: ABRIR autenticação após investigação bem-sucedida

Solicitação de Associação do cliente para o AP

- Neste pacote, observe que o cliente pode estar anexando o valor do parâmetro Diffie-Hellman para criptografia.

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.: WM/WMIE: 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						

Imagem-6: Solicitação de Associação

- No rastreamento de RA, você pode começar a ver os logs de cliente da fase de Associação,

```
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
```

Resposta de associação enviada do AP para o 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	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
```

Imagem-7: Resposta da associação

```
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 Association
```

Intercâmbio de chave

O handshake de 4 vias pode acontecer entre o AP e o dispositivo do cliente.

Key-1 enviado por AP

Key-2 enviada pelo cliente

Key-3 enviada pelo AP

Key-4 enviado pelo 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	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	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

Imagem-8: Handshake em quatro vias

```

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

```

Autenticação L2 Bem-sucedida

```

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 aprendizagem 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 no estado EXECUTAR

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

Clientes sem suporte para criptografia OWE

- Ao revisar um quadro beacon em si, os clientes ficam sabendo se eles são capazes de suportar esse método de criptografia ou não. Se não for suportado, ele pode simplesmente enviar uma solicitação de sondagem para abrir o SSID "OPEN-OWE" e pode fazer uma autenticação aberta normal, obter o endereço IP e, em seguida, passar para o 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
```

Informações sobre a transição rápida

- Podemos configurar o OWE apenas na autenticação OPEN ou em Webauth (CWA/LWA/EWA).
- O FT não é suportado na transição OWE.
- Se você habilitar o FT, receberá esta mensagem de erro,

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
☐

Fast Transition

Status
Enabled

Over the DS
☐

Reassociation Timeout *
20

WPA2/WPA3 Encryption

AES(CCMP128)
☒

GCMP128
☐

CCMP256
☐

GCMP256
☐

Protected Management Frame

PMF
Required

Association Comeback Timer*
1

SA Query Time*
200

Auth Key Mgmt

Fast Transition needs to be disabled

SAE
☐

OWE
☒

802.1X-SHA256
☐

FT + SAE
☐

FT + 802.1X
☐

Transition Mode WLAN ID
9

Cancel
Update & Apply to Device

Imagem-9: Mensagem de erro quando habilitamos FT no SSID de transição OWE

OWE não é suportado com PSK/dot1x

Não podemos habilitar o OWE nessas combinações,

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

Se você tentar ativar qualquer um desses métodos, receberá a mensagem de erro,

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

Imagem-10: Mensagem de erro ao obter ao habilitar outros métodos de autenticação no SSID OWE

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

Imagem-11: Mensagem de erro ao habilitar o AKM

- Na versão IOS do Cisco IOS® XE 17.9.6, você pode ver a opção "OWE" no AKM quando seleciona "WPA2+WPA3". No entanto, você pode obter a mensagem de erro, você não pode usar OWE com essa combinação.

⚠ 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

Imagem-12: Mensagem de erro ao escolher WPA2+WPA3

- No Cisco IOS® XE versão 17.12.4, quando você escolhe "WPA2+WPA3", você não pode

obter a opção "OWE" no 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

☐

PSK

☐

CCKM ⚠

☐

SAE

☐

FT + SAE

☐

FT + 802.1X

☐

FT + PSK

☐

802.1X-SHA256

☐

PSK-SHA256

☐

MPSK Configuration

Enable MPSK

☐

↶ Cancel

📄 Update & Apply to Device

Imagem-13: Mensagem de erro - Não obtendo a opção OWE no AKM

Troubleshooting

1. Verifique as configurações nas duas WLANs, no SSID ABERTO e no SSID de transição OWE, para que o ID da WLAN de transição seja mapeado.
2. A opção de difusão deve ser desabilitada no SSID de transição OWE; ela deve ser habilitada somente no SSID OPEN.
3. Verifique os métodos de autenticação/criptografia/FT suportados descritos neste artigo.
4. Se as configurações estiverem corretas na extremidade da WLC, colete os logs e as saídas necessários para restringir o problema.

RA Trace e EPC (Captura de PAKet Incorporada)

Login to WLC GUI -> Troubleshooting -> Radioative Trace -> Add client wifi MAC address -> Clique na caixa de seleção desse cliente -> Start

Faça login na GUI da WLC -> Solução de problemas -> Captura de pacotes -> Adicione um novo nome de arquivo -> Escolha a interface de uplink e a VLAN/Interface da WMI -> Iniciar.

Da Máquina Cliente: Se possível, você pode instalar o aplicativo wireshark e coletar a captura de pacotes escolhendo a 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>

AIR PCAP

Você pode coletá-lo usando o laptop MAC ou configurando um dos AP no modo farejador, consulte estes links,

Do laptop MAC:

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

Do AP farejador:

<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 um laptop (servidor wireshark) à porta do switch e ele deve ter um aplicativo wireshark instalado. Esse servidor wireshark deve ter acessibilidade para a interface WMI da WLC. É necessário permitir o protocolo "5555, 5000 ou 5556" no firewall se ele estiver entre o WLC e o servidor do Wireshark.

Verifique se há algum "gscaler" instalado no PC em que o Wireshark está instalado, se for o que, por favor, "desligue" e tente, se houver qualquer firewall como o Windows Defender ou qualquer coisa presente nele, desabilite-os e tente coletar o PCAP.

Roaming

Quando o cliente faz roaming de um AP para outro, ele precisa executar estas etapas,

- Necessidade de enviar reassociação/associação - Depende da solicitação do cliente.
- É necessário enviar detalhes DH (Diffie-Helman) na solicitação de associação.
- O cliente pode obter detalhes de DH na resposta de associação do AP, com base nas obtenções de PMK geradas no cliente e no AP.
- O handshake de 4 vias pode acontecer entre o AP e o cliente.
- No OWE, você não consegue habilitar a FT, portanto, o 802.11r não é possível.
- Cada vez, quando o cliente faz roaming, ele precisa fazer um handshake de 4 vias após a troca de DH em associação.
- Cliente e AP que usam seu próprio PMKID, é exclusivo para cada AP e clientes.
- Se o cliente se conectar ao mesmo AP, ele poderá usar o mesmo PMKID. Em algum cenário, se o cliente foi excluído do que o AP pode gerar um novo PMKID, no entanto, o cliente usa o mesmo PMKID para handshake de 4 vias.

Exemplo:

Se o cliente se conectar ao mesmo AP, você poderá ver o mesmo PMKID tanto na solicitação de associação quanto na resposta de associação. Na resposta de Associação, você não poderá ver detalhes de DH se ele usar o mesmo 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, (Mbit/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 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							

Imagem-14: Usando o mesmo 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								

Imagem-15: Resposta de Associação com o mesmo PMKID

Para testes, excluiu manualmente esse cliente da WLC e ele foi associado novamente ao mesmo AP, nesse momento, o cliente envia um mesmo PMKID, mas o AP envia detalhes de DH na resposta de associação.

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								

Imagem-16: Após a exclusão, o cliente enviou a mesma PMKID com detalhes de 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 (CM) > Pairwise Cipher Suite Count: 1 > Pairwise Cipher Suite List 00:0fac (Ieee 802.11) AES (CM) > Auth Key Management (AKM) Suite Count: 1 > Auth Key Management (AKM) List 00:0fac (Ieee 802.11) Opportunistic Wireless Encryption > RSN Capabilities: 00000000 > PMKID Count: 0 > PMKID List > Group Management Cipher Suite: 00:0fac (Ieee 802.11) BIP (128) > Tag: Vendor Specific: Microsoft Corp.: WMM/WM: 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: RSS 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								

Imagem-17: O AP usa valores DH para gerar seu novo PMKID

Neste exemplo: Tanto o AP como o cliente usam o mesmo PMKID ao fazer handshake de 4 vias, verifique as mensagens "M1 e em 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	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	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	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	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: 0x0000 > 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								

Imagem- 18: AP e cliente usando o mesmo PMKID

Neste exemplo: O cliente que usa o mesmo PMKID, mas o AP que usa um PMKID diferente que ele gerou depois que o cliente foi excluído, verifique as mensagens "M1 e 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

> 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

Imagem-19: AP e cliente usando PMKID diferente

Do rastreamento RA interno:

Neste exemplo: O cliente enviou parâmetros DH na solicitação de associação e o AP processou mais do que gerou a 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

```

Depois disso, o mesmo cliente se conectando ao mesmo AP, neste momento, o AP não gerou o novo 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

```

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.