

Begrijp opportunistische draadloze encryptiestroom

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Beschrijving](#)

[Stappen](#)

[Details van Lab Repro](#)

[DEBET FLOW](#)

[Origineel beacon frame](#)

[Verborgen SSID-bakens](#)

[Probe-aanvraag verzonden van client naar OWE Transition SSID](#)

[Probe Response verzonden van AP naar client](#)

[VERIFICATIE OPENEN](#)

[Associatieaanvraag van client naar AP](#)

[Reactie van associatie verzonden van AP naar client](#)

[Key exchange](#)

[L2-verificatie geslaagd](#)

[IP-leerstatus](#)

[Cliënt in LOOPPAS staat](#)

[Clients die niet worden ondersteund voor OWE-codering](#)

[Informatie over snelle overgang](#)

[De OWE wordt niet ondersteund door PSK/dot1x](#)

[Probleemoplossing](#)

[RA Trace en EPC \(Embedded PAKet Capture\)](#)

[LUCHTDEKSEL](#)

[roaming](#)

Inleiding

Dit document beschrijft de OWE-overgangsstroom en hoe het werkt op de Catalyst 9800 draadloze LAN-controller (WLC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Hoe de 9800 WLC, het access point (AP) te configureren voor basisbediening
- Hoe WLAN- en beleidsprofielen te configureren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- C9800-80, Cisco IOS® XE 17.12.4 en ook getest in Cisco IOS® XE 17.9.6
- AP-model : C9136l, ingeschakeld in zowel de lokale als de flex-verbindingsmodus.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Beschrijving

- OWE (Opportunistic Wireless Encryption) is een uitbreiding van IEEE 802.11 die encryptie voor het draadloze medium verstrekt. Het doel van op OWE gebaseerde verificatie is om open onbeveiligde draadloze connectiviteit tussen de AP's en clients te voorkomen.
- De OWE gebruikt de op Diffie-Hellman algoritmen gebaseerde Cryptografie om de draadloze encryptie in te stellen.
- Met OWE voeren de client en AP tijdens de toegangsprocedure een Diffie-Hellman sleuteluitwisseling uit en gebruiken ze het resulterende paarsgewijze geheim met de 4-voudige handdruk.
- Het gebruik van OWE verbetert de draadloze netwerkbeveiliging voor implementaties waar op Open of gedeelde PSK gebaseerde netwerken worden geïmplementeerd.

Stappen

1. Configureer één OPEN WLAN zonder encryptie/beveiliging en schakel het uitzenden in.
2. Configureer een andere SSID met OWE-beveiligingsinstellingen en wijs het OPEN WLAN-id-nummer toe in de overgangsmodus-WLAN-id. Schakel de optie broadcast-SSID uit in deze OWE-overgangsSSID.
3. Wijs het OWE-overgangsWLAN-id-nummer toe in het veld OPEN WLAN "transition-mode-WLAN-id".

Details van Lab Repro

- Naam SID openen: OPENLIJK

- Naam OWE-transitie SSID: OWE-transitie
- BASIS VAN OPEN OWE: 40:ce:24:dd:2 e:87
- BSSID van OWE-Transition: 40:ce:24:dd:24e:81f

DEBET FLOW

1. De bakens kunnen voor OPEN SSID worden uitgezonden. U kunt het door zijn naam van SSID in AIR PCAP zien.
2. We kunnen ook de verborgen veiligheid toegelaten SSID met de naam "Wildcard" in plaats van zijn eigen SSID naam in AIR PCAP zien.
3. Zodra de cliënten het beacon frame voor OPEN SSID ontvangen, als het OWE heeft of steunt, dan kan het beginnen met het verzenden van sonde verzoek naar OWE transitie SSID (dat is dat veiligheid toegelaten SSID in plaats van OPEN SSID).
4. Door OWE ondersteunde clients kunnen een sonderrespons krijgen van transitie SSID.
5. Verificatie VOOR OPENEN kan plaatsvinden tussen client en AP.
6. De klant kan associatieverzoek verzenden naar de AP met DH-sleuteluitwisselingsdetails en het resulterende paarsgewijze geheim gebruiken voor 4-weg handdruk.
7. AP kan associatiereactie verzenden.
8. Vier-manier handdruk kan gebeuren tussen AP en cliënt apparaat.
9. Na succesvol sleutelbeheer kan L2 PSK succesvol zijn.
10. De client kan IP verkrijgen van DHCP, ARP etc.
11. De client kan naar RUN status gaan.
12. Als client-apparaten die geen OWE ondersteunen, dan kan het sonde-verzoek verzenden naar OPEN SSID zelf en kan het direct IP krijgen dan kan het gaan naar RUN-status.

Origineel beacon frame

- Hier laat AIR PCAP dat zien, de SSID "OPEN-OWE"-uitzending (Beacon Frame). Dat bevat transitie-SSID-details en het noemde "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
  
```

Verborgen SSID-bakens

- In de WLAN-configuratie is "broadcast" uitgeschakeld voor deze "OWE-Transition"-SSID, maar u kunt verborgen SID-bakens in AIR PCAP zien die de SSID-naam "Wildcard" bevatten. Als u dat pakket controleert, bevat het echter OWE-Overgangdetails.
- Krijg de BSSID van verborgen SSID door dit pakket, zoals "40:ce:24:dd:2e:8f" te gebruiken en zoek het in pakketopname.
- In dit pakket, toont het dat, SSID "ontbreekt" en het bevat zijn overgang SSID als "OPEN-OWE" en zijn 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: 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:87)
      SSID length: 8
      SSID: OPEN-OWE
  
```

Afbeelding 2 : Verborgen SSID - OWE Transition

Probe-aanvraag verzonden van client naar OWE Transition SSID

- Gebaseerd op het beacon frame "OPEN-OWE" SSID, komt de client de andere SSID details te kennen die het nodig heeft om te verbinden, in dit scenario, het is "OWE-Transition". Als client OWE-encryptie kan ondersteunen, dan kan het de sonderaanvraag naar "OWE-Transition" SSID sturen en een antwoord krijgen.
- Probe-aanvraag verzonden naar OWE-Transition BSSID "40:ce:24:dd:2e:8f" en kreeg een antwoord. Ook in dit reactiepakket voor sonde kunt u Open-OWE SSID-details zien.

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	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 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

```

Afbeelding 3: Probe-aanvraag

Probe Response verzonden van AP naar client

- De client heeft een probe-antwoord ontvangen voor de SSID "OWE-Transition", maar heeft zijn oorspronkelijke SSID-details "OPEN-OWE" in 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: QSS Load Element 802.11e CCA Version
    > Tag: PM Enabled Capabilities (5 octets)
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (8 octets)
    > Tag: VHT Capabilities
    > Tag: VHT Operation
    > Tag: Tx Power Envelope
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    > Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5
    > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled
    > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)
    > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44)
    > Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode
      Tag Number: Vendor Specific (221)
      Tag length: 19
      OUI: 50:6f:9a (Wi-Fi Alliance)
      Vendor Specific OUI Type: 28
      BSSID: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)
      SSID length: 8
      SSID: OPEN-OWE

```

Afbeelding 4 : Probe Response

VERIFICATIE OPENEN

- Na het verkrijgen van de sonde reactie, kan de Open authenticatie tussen Cliënt en AP gebeuren om de details/mogelijkheden van de cliënten wifi, vóór vereniging te controleren.

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)						

Afbeelding 5: OPEN verificatie na succesvolle test

Associatieaanvraag van client naar AP

- Merk op dat in dit pakket de client een Diffie-Hellman parameterwaarde voor codering kan toevoegen.

No.	Time	Source	Destination	Protocol	Length	Info
8522	2025-01-21 09:51:57.329457	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	802.11	337	Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Transition"
8523	2025-01-21 09:51:57.329466		ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
> Frame 8522: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Association Request, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (4 bytes) > Tagged parameters (269 bytes) Tag: SSID parameter set: "OWE-Transition" Tag Number: SSID parameter set (0) Tag length: 14 SSID: "OWE-Transition" > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] > Tag: Power Capability Min: -20, Max: 14 > Tag: Supported Channels > Tag: HT Capabilities (802.11n D1.10) > Tag: RSN Information > Tag: RM Enabled Capabilities (5 octets) > Tag: Supported Operating Classes > Tag: Extended Capabilities (11 octets) > Tag: VHT Capabilities > Tag: Vendor Specific: Samsung Electronics Co.,Ltd > Tag: Vendor Specific: Samsung Electronics Co.,Ltd > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element Ext Tag: OWE Diffie-Hellman Parameter Ext Tag length: 34 (Tag len: 35) Ext Tag Number: OWE Diffie-Hellman Parameter (32) Group: 256-bit random ECP group (19) Public Key: 7c2782ba4c77a98c7076d1fa2e3493347ec16d4c64345dccc8b9b68b212ff31						

Afbeelding 6 : Associatieaanvraag

- In RA spoor, kunt u beginnen de cliëntlogboeken van de fase van de Vereniging te zien,

```
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
```

Reactie van associatie verzonden van AP naar 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
```

Afbeelding 7: Reactie op associatie

```
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
```

Key exchange

Er kan een 4-voudige handdruk optreden tussen het toegangspunt en het clientapparaat.

Sleutel-1 verzenden via AP

Key-2 verzenden per client

Key-3 verzenden via AP

Key-4 verzenden per 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	Broadcast	802.11	48	Acknowledgement, Flags=.....C
8542	2025-01-21 09:51:57.363375	Cisco_dd:2e:8f	Broadcast	802.11	376	Beacon frame, SN=3335, FN=0, Flags=.....C, BI=100, SSID="OPEN-OWE"
8543	2025-01-21 09:51:57.365594	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	215	Key (Message 2 of 4)
8544	2025-01-21 09:51:57.365603	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
8545	2025-01-21 09:51:57.366921	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	267	Key (Message 3 of 4)
8546	2025-01-21 09:51:57.366929	Cisco_dd:2e:8f	Broadcast	802.11	48	Acknowledgement, Flags=.....C
8547	2025-01-21 09:51:57.368482	Cisco_dd:2e:8f	Broadcast	802.11	376	Beacon frame, SN=3336, FN=0, Flags=.....C, BI=100, SSID="newssid"
8548	2025-01-21 09:51:57.373313	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	171	Key (Message 4 of 4)
8549	2025-01-21 09:51:57.373334	ee:13:e8:a8:cd:5b	ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C

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

Afbeelding 8: 4-voudige handdruk

```

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
  
```

L2-verificatie geslaagd

```

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
  
```

IP-leerstatus

```
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 in LOOPPAS staat

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

Clients die niet worden ondersteund voor OWE-codering

- Door een beacon frame zelf te bekijken, komen de clients te weten of ze deze encryptie methode kunnen ondersteunen of niet. Als het niet wordt ondersteund, dan kan het gewoon een sonde aanvraag sturen om SSID "OPEN-OWE" te openen en kan een normale open verificatie doen, IP-adres krijgen, dan kan het gaan de RUN staat.

```
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
```

Informatie over snelle overgang

- We zijn in staat om OWE alleen in OPEN authenticatie of in Webauth (CWA/LWA/EWA) te configureren.
- FT wordt niet ondersteund bij de OWE-overgang.
- Als je FT inschakelt, krijg je deze foutmelding:

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

Afbeelding 9 : Foutmelding wanneer we FT in OWE Transition SSID inschakelen

De OWE wordt niet ondersteund door PSK/dot1x

We zijn niet in staat om OWE in deze combinaties toe te laten,

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

Als u een van deze methoden probeert in te schakelen, krijgt u de foutmelding:

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

Afbeelding 10: Foutmelding ontvangen terwijl andere verificatiemethoden in OWE SSID zijn ingeschakeld

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

Afbeelding 11: Foutmelding bij het inschakelen van AKM

- In Cisco IOS® XE 17.9.6 IOS-versie kunt u de optie "OWE" onder AKM zien wanneer u "WPA2+WPA3" selecteert, maar u kunt de foutmelding krijgen; u kunt OWE met deze combinatie niet gebruiken.

⚠ 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

Afbeelding 12: Foutmelding bij kiezen voor WPA2+WPA3

- In Cisco IOS® XE 17.12.4 versie kunt u, wanneer u "WPA2+WPA3" kiest, de optie "OWE"

niet in de AKM ophalen,

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

Afbeelding 13: Foutmelding - geen OWE-optie in AKM

Probleemoplossing

1. Controleer de configuraties in zowel de WLAN's, in OPEN SSID als in OWE-overgang SSID moet een WLAN-id van de overgang in kaart zijn gebracht.
2. De omroepoptie moet in OWE transitie SSID worden onbruikbaar gemaakt, moet het slechts in OPEN SSID worden toegelaten.
3. Controleer de ondersteunde verificatie-/encryptie-/FT-methoden die in dit artikel worden beschreven.
4. Als de configuraties van WLC eind zijn, dan verzamel gelieve de vereiste logboeken en de output om de kwestie te versmallen,

RA Trace en EPC (Embedded PAcKet Capture)

Aanmelden bij WLC GUI -> Problemen oplossen -> Radioactive Trace -> Add client wifi MAC-adres -> Klik op dat client checkbox -> Start

Aanmelden bij WLC GUI -> Problemen oplossen -> Packet Capture -> Nieuwe bestandsnaam toevoegen -> De uplink-interface en WMI VLAN/interface kiezen -> Start.

Vanaf clientmachine: Indien mogelijk kunt u een wireshark-toepassing installeren en de pakketopname verzamelen door de WiFi-interface te kiezen.

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

LUCHTDEKSEL

U kunt het verzamelen door MAC laptop of het configureren van een van de AP in om te snuffelen modus, verwijzen naar deze links,

Van MAC-laptop:

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

Van 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>

Verbind één laptop (wireshark server) met de switch poort en het moet hebben wireshark applicatie geïnstalleerd in het, deze wireshark server moet bereikbaarheid hebben om WLC WMI interface. Moet toestaan het protocol "5555 of 5000 of 5556" in firewall als het aanwezig is tussen uw WLC en wireshark server.

Controleer of er een "gscaler" geïnstalleerd is in die PC waar wireshark geïnstalleerd is, als het is dan alstublieft "uitzetten" en probeer, als het een firewall zoals windows verdediger of iets

aanwezig in het is, schakel die uit en probeer PCAP te verzamelen.

roaming

Wanneer de client van het ene toegangspunt naar het andere zwerft, moet deze stap worden uitgevoerd.

- Noodzaak om re-associatie/associatie te versturen - hangt af van het verzoek van de klant.
- Noodzaak om DH (Diffie-Helman) details te sturen in associatieaanvraag.
- De client kan DH-gegevens verkrijgen in associatiereactie van AP, op basis van deze PMK wordt gegenereerd in zowel client als AP.
- 4-way handshake kan gebeuren tussen AP en client.
- In OWE kunt u FT niet inschakelen, zodat 802.11r niet mogelijk is.
- Elke keer, wanneer de client zwerft, moet het 4-way handshake doen na DH-uitwisseling in associatie.
- Client en AP gebruiken hun eigen PMKID, het is uniek voor elke AP en clients.
- Als client verbinding maakt met dezelfde AP, dan kan dezelfde PMKID gebruikt worden. In sommige scenario, als de client verwijderd dan AP kan een nieuwe PMKID genereren, maar de client gebruikt dezelfde PMKID voor 4-way handshake.

Voorbeeld:

Als client verbinding maakt met dezelfde AP, dan kunt u dezelfde PMKID zien in zowel Association-request als Association-Response. In reactie van de Vereniging, kunt u geen DH details zien als het dezelfde PMKID gebruikt.

```
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 09:53:12.047592 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(B), 9, 12(B), 10, 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.: MM/ME: 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 64 34 5d cc f8 b9 bb 68 b2 12 ff 31
```

Afbeelding 14: Dezelfde PMKID gebruiken

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.: 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								

Afbeelding 15: Associatie-respons met dezelfde PMKID

Voor het testen, verwijderde deze client handmatig uit WLC en het werd opnieuw gekoppeld aan dezelfde AP, op dit moment, de client stuurt een dezelfde PMKID maar AP stuurt DH details in associatiereactie.

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
44117	2025-01-21 09:51:12.847592	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								

Afbeelding 16: Na het verwijderen, client verzonden dezelfde PMKID met DH details

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: 00:0fac (Ieee 802.11) AES (COM) > Pairwise Cipher Suite Count: 1 > Pairwise Cipher Suite List 00:0fac (Ieee 802.11) AES (COM) > Auth Key Management (AKM) Suite Count: 1 > Auth Key Management (AKM) List 00:0fac (Ieee 802.11) Opportunistic Wireless Encryption > RSN Capabilities: 00000000 > PMKID Count: 0 > PMKID List > Group Management Cipher Suite: 00:0fac (Ieee 802.11) BIP (128) > Tag: Vendor Specific: Microsoft Corp.: WMM/WMF: Parameter Element > Tag: HT Capabilities (802.11n D1.10) > Tag: HT Information (802.11n D1.10) > Tag: Extended Capabilities (8 octets) > Tag: VHT Capabilities > Tag: VHT Operation > Tag: RM Enabled Capabilities (5 octets) > Tag: BSS Max Idle Period > Ext Tag: OWE Diffie-Hellman Parameter > Ext Tag length: 34 (Tag len: 35) > Ext Tag Number: OWE Diffie-Hellman Parameter (32) > Group: 256-bit random ECP group (19) > Public Key: e4 44 ea 00 6f f3 69 35 33 93 59 3f 7d b7 2e ab d4 04 26 7e 62 da d9 2a 88 c9 4e f5 e2 69 a1 c5								

Afbeelding 17: AP gebruikt DH-waarden om zijn nieuwe PMKID te genereren

In dit voorbeeld: Zowel AP als client gebruikt dezelfde PMKID tijdens het 4-way handshake, controleer "M1 en in M2" berichten.

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: 00:0fac (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								

Afbeelding 18: AP en client met dezelfde PMKID

In dit voorbeeld: Cliënt die de zelfde PMKID maar AP gebruiken die verschillende PMKID gebruiken die het produceerde nadat de cliënt werd geschrap, controleer "M1 en M2"berichten.

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

```

Afbeelding 19: AP en client met verschillende PMKID

Interne RA-sporen:

In dit voorbeeld: De client zond DH-parameters in associatieverzoek en AP verwerkt dan de PMK gegenereerd.

```

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

```

Hierna heeft dezelfde client die verbinding maakt met dezelfde AP, op dit moment, AP geen nieuwe PMKID gegenereerd,

```

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

```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.