

Opportunistische Wireless-Verschlüsselung

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Beschreibung](#)

[Schritte](#)

[Details zum Lab Repro](#)

[SCHULDENFLUSS](#)

[Original Beacon-Rahmen](#)

[Versteckte SSID-Beacons](#)

[Anfrage zur Überprüfung vom Client an OWE-Transition-SSID gesendet](#)

[Testantwort vom AP an Client gesendet](#)

[OFFENE Authentifizierung](#)

[Zuordnungsanforderung vom Client zum AP](#)

[Zuordnungsantwort vom AP zum Client gesendet](#)

[Schlüsselaustausch](#)

[L2-Authentifizierung erfolgreich](#)

[IP-Lernstatus](#)

[Client im RUN-Status](#)

[Clients, die für OWE-Verschlüsselung nicht unterstützt werden](#)

[Informationen zur schnellen Umrüstung](#)

[OWE wird von PSK/dot1x nicht unterstützt](#)

[Fehlerbehebung](#)

[RA Trace und EPC\(Embedded PAcKet Capture\)](#)

[LUFTKAPPE](#)

[Roaming](#)

Einleitung

Dieses Dokument beschreibt den OWE-Übergangsablauf und dessen Funktionsweise auf dem Catalyst 9800 Wireless LAN Controller (WLC).

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfigurieren des 9800 WLC, des Access Points (AP) für den Basisbetrieb
- Konfigurieren von WLAN- und Richtlinienprofilen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- C9800-80, Cisco IOS® XE 17.12.4 und getestet in Cisco IOS® XE 17.9.6
- AP-Modell: C9136I, sowohl im lokalen als auch im Flex-Connect-Modus geprüft

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Beschreibung

- OWE (Opportunistic Wireless Encryption) ist eine Erweiterung von IEEE 802.11, die eine Verschlüsselung für das Wireless-Medium bereitstellt. Der Zweck der OWE-basierten Authentifizierung besteht darin, offene, ungesicherte Wireless-Verbindungen zwischen den APs und Clients zu vermeiden.
- Das OWE verwendet die auf dem Diffie-Hellman-Algorithmus basierende Verschlüsselung, um die Wireless-Verschlüsselung einzurichten.
- Mit OWE führen der Client und der AP während des Zugriffsvorgangs einen Diffie-Hellman-Schlüsselaustausch durch und verwenden das resultierende paarweise Geheimnis mit dem 4-Wege-Handshake.
- Die Verwendung von OWE erhöht die Sicherheit von Wireless-Netzwerken in Bereitstellungen, in denen offene oder gemeinsam genutzte PSK-basierte Netzwerke bereitgestellt werden.

Schritte

1. Konfigurieren Sie ein OFFENES WLAN ohne Verschlüsselung/Sicherheit und aktivieren Sie Broadcast.
2. Konfigurieren Sie eine andere SSID mit OWE-Sicherheitseinstellungen, und ordnen Sie die OPEN WLAN-ID-Nummer in "sition-mode-wlan-id" zu. Deaktivieren Sie die Broadcast-SSID-Option in dieser OWE-Übergangs-SSID.
3. Ordnen Sie die OWE-Übergangs-WLAN-ID im Feld OPEN WLAN "sition-mode-wlan-id" zu.

Details zum Lab Repro

- Offener SSID-Name: OFFENER SCHULDNER

- SSID für OWE-Übergang: OWE-Übergang
- BSSID von OPEN-OWE: 40:ce:24:dd:2e:87
- BSSID des OWE-Übergangs: 40:ce:24:dd:2e:8f

SCHULDENFLUSS

1. Beacons können für OPEN SSID gesendet werden. Sie können sie anhand ihres SSID-Namens in AIR PCAP sehen.
2. In AIR PCAP wird auch die SSID mit aktivierter Sicherheitsfunktion und dem Namen "Wildcard" anstelle ihres eigenen SSID-Namens angezeigt.
3. Sobald die Clients den Beacon-Frame für die OPEN SSID empfangen haben, kann sie, wenn sie OWE hat oder unterstützt, eine Anfrage an die OWE-Übergangs-SSID senden (d. h., wenn die Sicherheit die SSID aktiviert hat, anstatt die OPEN SSID zu öffnen).
4. OWE-unterstützte Clients können die Antwort auf die Anfrage von der Übergangs-SSID erhalten.
5. Die OPEN-Authentifizierung kann zwischen Client und AP erfolgen.
6. Der Client kann eine Zuordnungsanforderung mit DH-Schlüsselaustauschdetails an den AP senden und den resultierenden paarweisen Schlüssel für einen 4-Wege-Handshake verwenden.
7. Der WAP kann eine Zuordnungsantwort senden.
8. Ein Vier-Wege-Handshake kann zwischen AP und Client-Gerät erfolgen.
9. Nach erfolgreicher Schlüsselverwaltung kann L2 PSK erfolgreich sein.
10. Der Client kann die IP von DHCP, ARP usw. erhalten.
11. Der Client kann in den Status "RUN" wechseln.
12. Wenn Client-Geräte OWE nicht unterstützen, kann es eine Anfrage an die OPEN SSID senden und direkt eine IP-Adresse erhalten, als sie in den RUN-Status wechseln kann.

Original Beacon-Rahmen

- Hier, AIR PCAP zeigt, dass, die SSID "OPEN-OWE" Rundfunk (Beacon Frame). Diese enthält Einzelheiten zur SSID des Übergangs mit der Bezeichnung "OWE-Transition".

No.	Time	Source	Destination	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					

Versteckte SSID-Beacons

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

Anfrage zur Überprüfung vom Client an OWE-Transition-SSID gesendet

- Basierend auf dem Beacon-Frame "OPEN-OWE" SSID kennt der Client die anderen SSID-Details, die er verbinden muss, in diesem Szenario ist es "OWE-Transition". Wenn der Client die OWE-Verschlüsselung unterstützt, kann er die Anfrage an die OWE-Transition-SSID senden und eine Antwort erhalten.
- Anfrage an OWE-Transition BSSID "40:ce:24:dd:2e:8f" gesendet und Antwort erhalten. In diesem Paket für die Antwort auf die Anfrage sind auch die OPEN-OWE SSID-Details zu sehen.

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 D1.0)
    > Tag: Extended Capabilities (11 octets)
    > Tag: VHT Capabilities
    > Ext Tag: HE Capabilities
    > Tag: Vendor Specific: Wi-Fi Alliance: Multi Band Operation - Optimized Connectivity Experience
      Tag Number: Vendor Specific (221)
      Tag length: 7
      OUI: 50:6f:9a (Wi-Fi Alliance)
      Vendor Specific OUI Type: 22
      > MBO/OCE attribute: 030102 (Cellular Data Capabilities)
    > Tag: Vendor Specific: Microsoft Corp.: Unknown 8
  
```

Bild-3: Anfrage senden

Testantwort vom AP an Client gesendet

- Der Client erhielt eine Anfrage für die SSID "OWE-Transition", hat jedoch seine ursprünglichen SSID-Details "OPEN-OWE" in der 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: QSSS 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

Bild-4: Antwort des Tests

OFFENE Authentifizierung

- Nach Erhalt der Antwort auf die Anfrage kann zwischen dem Client und dem Access Point eine OPEN-Authentifizierung erfolgen, um die Wi-Fi-Details und -Funktionen der Clients vor der Zuordnung zu überprüfen.

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)						

Bild-5: OPEN-Authentifizierung nach erfolgreicher Prüfung

Zuordnungsanforderung vom Client zum AP

- Beachten Sie, dass der Client für die Verschlüsselung einen Diffie-Hellman-Parameterwert anhängen kann.

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						

Bild-6: Zuordnungsanforderung

- In der RA-Ablaufverfolgung können Sie die Client-Protokolle der Zuordnungsphase anzeigen.

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

Zuordnungsantwort vom AP zum Client gesendet

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

> Frame 8527: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Association Response, Flags: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

Bild-7: Assoziationsantwort

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

Schlüsselaustausch

Ein 4-Wege-Handshake kann zwischen dem AP und dem Client-Gerät erfolgen.

Schlüssel-1 vom AP gesendet

Schlüssel-2 vom Client gesendet

Schlüssel-3 vom AP gesendet

Schlüssel-4 vom Client gesendet

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	ee:13:e8:a8:cd:5b	Broadcast	802.11	48	Acknowledgement, Flags=.....C
8545	2025-01-21 09:51:57.366921	Cisco_dd:2e:8f	Broadcast	802.11	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	Broadcast	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

Bild-8: 4-Wege-Handshake

```

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-Authentifizierung erfolgreich

```

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-Lernstatus

```

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 im RUN-Status

```

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

```

Clients, die für OWE-Verschlüsselung nicht unterstützt werden

- Durch die Überprüfung eines Beacon-Frames an sich werden die Clients darauf aufmerksam, ob sie diese Verschlüsselungsmethode unterstützen können oder nicht. Wenn es nicht unterstützt wird, kann es einfach eine Anfrage senden, um SSID zu öffnen "OPEN-OWE" und eine normale offene Authentifizierung durchführen, IP-Adresse abrufen, dann kann es den RUN-Status gehen.

```

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

```

Informationen zur schnellen Umrüstung

- Wir können OWE nur in der OPEN Authentifizierung oder in Webauth (CWA/LWA/EWA) konfigurieren.
- FT wird bei der OWE-Umstellung nicht unterstützt.
- Wenn Sie FT aktivieren, erhalten Sie diese Fehlermeldung,

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

Bild-9: Fehlermeldung bei Aktivierung von FT in OWE Transition-SSID

OWE wird von PSK/dot1x nicht unterstützt

Wir können OWE in diesen Kombinationen nicht aktivieren.

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

Wenn Sie eine dieser Methoden aktivieren, können Sie die Fehlermeldung

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

Bild-10: Fehlermeldung beim Abrufen der anderen Authentifizierungsmethoden in der OWE-SSID

Edit WLAN

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

General **Security** Advanced Add To Policy Tags

Layer2 Layer3 AAA

☐ WPA + WPA2

☐ WPA2 + WPA3

☒ WPA3

☐ Static WEP

☐ None

MAC Filtering

☐

Lobby Admin Access

☐

WPA Parameters

WPA Policy

☐

WPA2 Policy

☐

GTK Randomize

☐

WPA3 Policy

☒

Transition Disable

☐

WPA2/WPA3 Encryption

AES(CCMP128)

☒

CCMP256

☐

GCMP128

☐

GCMP256

☐

Protected Management Frame

PMF

Required

Association Comeback Timer*

1

SA Query Time*

200

Fast Transition

Status

Enabled

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt

Fast Transition needs to be disabled

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

SAE

☐

FT + SAE

☐

OWE

☒

FT + 802.1X

☒

802.1X-SHA256

☒

Transition Mode WLAN ID

9

Cancel

Update & Apply to Device

Bild-11: Fehlermeldung beim Aktivieren von AKM

- In der Cisco IOS® XE 17.9.6 IOS-Version können Sie die Option "OWE" unter AKM sehen, wenn Sie "WPA2+WPA3" auswählen. Sie können jedoch die Fehlermeldung erhalten, dass Sie OWE mit dieser Kombination nicht verwenden können.

⚠ 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

Bild-12: Fehlermeldung bei Auswahl von WPA2+WPA3

- Wenn Sie in der Version Cisco IOS® XE 17.12.4 "WPA2+WPA3" auswählen, wird die Option

"OWE" in AKM nicht angezeigt.

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

Bild-13: Fehlermeldung - OWE-Option wird in AKM nicht abgerufen

Fehlerbehebung

1. Überprüfen Sie, ob die Konfigurationen in beiden WLANs, in OPEN SSID und in OWE Transition SSID müssen Transition WLAN ID zugeordnet.
2. Die Broadcasting-Option muss in der OWE-Übergangs-SSID deaktiviert sein, sie darf nur in der OPEN-SSID aktiviert sein.
3. Überprüfen Sie die in diesem Artikel beschriebenen unterstützten Authentifizierungs-/Verschlüsselungs-/FT-Methoden.
4. Wenn die Konfigurationen von WLC-Ende an in Ordnung sind, erfassen Sie die erforderlichen Protokolle und Ausgaben, um das Problem einzugrenzen.

RA Trace und EPC (Embedded PAcKet Capture)

Login to WLC GUI -> Troubleshooting -> Radioactive Trace -> Add client wifi MAC address -> Click that clients checkbox -> Start

Anmelden bei der WLC-GUI -> Fehlerbehebung -> Paketerfassung -> Neuen Dateinamen hinzufügen -> Wählen Sie die Uplink-Schnittstelle und WMI VLAN/Interface -> Start aus.

Vom Client-Computer: Wenn möglich, können Sie Wireshark-Anwendung installieren und die Paketerfassung sammeln, indem Sie WiFi-Schnittstelle auswählen.

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

LUFTKAPPE

Sie können es erfassen, indem Sie den MAC-Laptop verwenden oder einen der APs für den Sniffer-Modus konfigurieren. Weitere Informationen finden Sie unter diesen Links,

Von MAC-Laptop:

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

Von 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>

Schließen Sie einen Laptop (Wireshark-Server) an den Switch-Port an, und es muss eine Wireshark-Anwendung installiert sein. Dieser Wireshark-Server muss über eine WLC WMI-Schnittstelle verfügen. Das Protokoll "5555 oder 5000 oder 5556" muss in der Firewall zugelassen werden, wenn es sich zwischen Ihrem WLC und dem Wireshark-Server befindet.

Markieren Sie, ob es irgendeinen "gscaler" in diesem PC installiert, wo wireshark installiert, wenn es als bitte "ausschalten" und versuchen, wenn es eine Firewall wie Windows Defender oder

etwas in ihm vorhanden ist, deaktivieren Sie diese und versuchen, PCAP zu sammeln.

Roaming

Wenn ein Client von einem Access Point zu einem anderen wechselt, muss er folgende Schritte ausführen:

- Erneute Zuordnung/Zuordnung erforderlich - Abhängig von der Kundenanforderung.
- Die DH-Daten (Diffie-Helman) müssen in der Zuordnungsanfrage gesendet werden.
- Der Client kann DH-Details in der Zuordnungsantwort vom Access Point abrufen, basierend auf diesen PMK-Informationen, die sowohl im Client als auch im Access Point generiert werden.
- Ein 4-Wege-Handshake kann zwischen AP und Client erfolgen.
- In OWE können Sie FT nicht aktivieren. 802.11r ist daher nicht möglich.
- Jedes Mal, wenn der Client Roaming, es muss 4-Wege-Handshake nach DH Austausch in Verbindung.
- Client und AP verwenden eine eigene PMKID, die für jeden AP und jeden Client eindeutig ist.
- Wenn der Client eine Verbindung mit demselben Access Point herstellt, kann dieselbe PMKID verwendet werden. Wenn der Client gelöscht wurde, als der Access Point eine neue PMKID generieren kann, verwendet der Client in einigen Szenarien dieselbe PMKID für den 4-Wege-Handshake.

Beispiel:

Wenn der Client eine Verbindung mit demselben Access Point herstellt, wird dieselbe PMKID sowohl in der Zuordnungsanforderung als auch in der Zuordnungsantwort angezeigt. In der Zuordnungsantwort werden keine DH-Details angezeigt, wenn dieselbe PMKID verwendet wird.

```
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(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 4c 64 34 5d cc f8 b9 bb 68 b2 12 ff 31
```

Bild-14: Verwendung derselben 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.: 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								

Bild-15: Assoziationsantwort mit derselben PMKID

Zum Testen wurde dieser Client manuell vom WLC gelöscht und erneut mit demselben AP verknüpft. Zu diesem Zeitpunkt sendet der Client dieselbe PMKID, jedoch sendet der AP DH-Details als Antwort auf die Zuordnung.

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

Bild-16: Nach dem Löschen hat der Client dieselbe PMKID mit DH-Details gesendet.

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(B), 18, 24(B), 36, 48, 54, [Mbit/sec] > Tag: RSN Information > Tag Number: RSN Information (48) > Tag length: 26 > RSN Version: 1 > Group Cipher Suite: 00:0fac (Ieee 802.11) AES (COM) > Pairwise Cipher Suite Count: 1 > Pairwise Cipher Suite List 00:0fac (Ieee 802.11) AES (COM) > Auth Key Management (AKM) Suite Count: 1 > Auth Key Management (AKM) List 00:0fac (Ieee 802.11) Opportunistic Wireless Encryption > RSN Capabilities: 00008 > PMKID Count: 0 > PMKID List > Group Management Cipher Suite: 00:0fac (Ieee 802.11) BIP (128) > Tag: Vendor Specific: Microsoft Corp.: WMM/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: 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								

Bild-17: AP verwendet DH-Werte, um die neue PMKID zu generieren

In diesem Beispiel: AP und Client verwenden beim 4-Wege-Handshake dieselbe PMKID und checken M1- und M2-Nachrichten ein.

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

Bild 18: AP und Client mit derselben PMKID

In diesem Beispiel: Client, der dieselbe PMKID verwendet, aber AP, der eine andere PMKID verwendet, die er generiert hat, nachdem der Client gelöscht wurde, überprüfen Sie die Meldungen "M1 und 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

```

Bild-19: AP und Client mit unterschiedlicher PMKID

Aus interner RA-Verfolgung:

In diesem Beispiel: Der Client sendete DH-Parameter in der Zuordnungsanforderung, und der Access Point wurde verarbeitet als auf dem PMK generiert.

```

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

```

Anschließend hat derselbe Client, der sich mit demselben Access Point verbindet, zu diesem Zeitpunkt keine neue PMKID generiert.

```

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

```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.