

Comprendere il flusso della crittografia wireless

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Descrizione](#)

[Passi](#)

[Dettagli di Lab Repro](#)

[FLUSSO DEL DEBITO](#)

[Cornice beacon originale](#)

[Beacon SSID nascosti](#)

[Richiesta di verifica inviata dal client all'SSID di transizione OWE](#)

[Risposta probe inviata dal punto di accesso al client](#)

[autenticazione OPEN](#)

[Richiesta di associazione dal client al punto di accesso](#)

[Risposta di associazione inviata dal punto di accesso al client](#)

[Scambio chiave](#)

[Autenticazione L2 riuscita](#)

[Stato di apprendimento IP](#)

[Client in stato RUN](#)

[Client non supportati per la crittografia OWE](#)

[Informazioni sulla transizione rapida](#)

[OWE non supportato con PSK/dot1x](#)

[Risoluzione dei problemi](#)

[RA Trace ed EPC \(Embedded Packet Capture\)](#)

[CAPPuccio](#)

[Roaming](#)

Introduzione

Questo documento descrive il flusso di transizione OWE e il suo funzionamento sul controller WLC (Wireless LAN Controller) Catalyst 9800.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Come configurare il WLC 9800, il punto di accesso (AP) per le operazioni di base
- Come configurare i profili WLAN e criteri.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- C9800-80, Cisco IOS® XE 17.12.4 e testato anche in Cisco IOS® XE 17.9.6
- Modello AP: C9136I, controllato sia in modalità locale che in modalità flex connect.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Descrizione

- OWE (Opportunistic Wireless Encryption) è un'estensione di IEEE 802.11 che fornisce la crittografia per il supporto wireless. Lo scopo dell'autenticazione basata su OWE è quello di evitare la connettività wireless aperta non protetta tra i punti di accesso e i client.
- Per impostare la crittografia wireless, OWE utilizza la crittografia basata sugli algoritmi Diffie-Hellman.
- Con OWE, il client e l'access point eseguono uno scambio di chiavi Diffie-Hellman durante la procedura di accesso e utilizzano il segreto pairwise risultante con l'handshake a 4 vie.
- L'utilizzo di OWE migliora la sicurezza delle reti wireless per le installazioni in cui vengono installate reti aperte o condivise basate su PSK.

Passi

1. Configurare una WLAN APERTA senza crittografia/sicurezza e abilitare la trasmissione.
2. Configurare un altro SSID con le impostazioni di sicurezza OWE ed eseguire il mapping del numero ID OPEN WLAN in modalità di transizione wlan-id. Disabilitare l'opzione SSID broadcast in questo SSID di transizione OWE.
3. Mappare il numero ID della WLAN di transizione OWE nel campo OPEN WLAN "transition-mode-wlan-id" (WLAN aperta, modalità di transizione: id-wlan).

Dettagli di Lab Repro

- Apri nome SSID: OPEN-OWE
- Nome SSID transizione OWE: OWE-Transition
- BSSID di OPEN-OWE: 40:ce:24:gg:2e:87

- BSSID della transizione verso il basso: 40:ce:24:gg:2e:8f

FLUSSO DEL DEBITO

1. I beacon possono essere trasmessi per OPEN SSID. È possibile visualizzarli tramite il relativo nome SSID in AIR PCAP.
2. In AIR PCAP è inoltre possibile visualizzare l'SSID protetto nascosto con il nome "Wildcard" anziché il nome SSID.
3. Dopo aver ricevuto il frame beacon per OPEN SSID, se dispone o supporta OWE, i client possono iniziare a inviare la richiesta di probe a OWE SSID di transizione (ovvero SSID abilitato per la sicurezza anziché OPEN SSID).
4. I client supportati da OWE possono ottenere la risposta del probe da SSID di transizione.
5. L'autenticazione OPEN può avvenire tra client e punto di accesso.
6. Il client può inviare la richiesta di associazione all'access point con i dettagli di scambio chiave DH e utilizzare il segreto pairwise risultante per l'handshake a 4 vie.
7. Il punto di accesso può inviare una risposta di associazione.
8. L'handshake a quattro vie può essere eseguito tra il punto di accesso e il dispositivo client.
9. Una volta completata la gestione delle chiavi, la chiave primaria di secondo livello può avere esito positivo.
10. Il client può ottenere IP da DHCP, ARP, ecc.
11. Il client può passare allo stato RUN.
12. Se i dispositivi client non supportano OWE, può inviare una richiesta di sonda a OPEN SSID e può ottenere direttamente l'indirizzo IP prima di passare allo stato RUN.

Cornice beacon originale

- Qui, AIR PCAP lo mostra, la trasmissione SSID "OPEN-OWE" (Beacon Frame). che contiene i dettagli SSID della transizione e viene denominata "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

```

Beacon SSID nascosti

- In base alla configurazione WLAN, "broadcasting" è disabilitato per questo SSID "OWE-Transition". Tuttavia, è possibile visualizzare i beacon SSID nascosti in AIR PCAP che contengono il nome SSID "Wildcard". Tuttavia, se si controlla tale pacchetto, esso contiene i dettagli OWE-Transition.
- Ottenere il BSSID del SSID nascosto utilizzando questo pacchetto, ad esempio "40:ce:24:dd:2e:8f" ed eseguirne la ricerca nell'acquisizione del pacchetto.
- In questo pacchetto, viene mostrato che SSID "Missing" (Mancante) e che contiene il SSID di transizione "OPEN-OWE" e il 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(0), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec] > Tag: DS Parameter set: Current Channel: 48 > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap > Tag: Country Information: Country Code IN, Environment All > Tag: Power Constraint: 0 > Tag: RSN Information > Tag: 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						

Image-2 SSID nascosto - transizione OWE

Richiesta di verifica inviata dal client all'SSID di transizione OWE

- In base all'SSID "OPEN-OWE" del frame del beacon, il client viene a conoscenza degli altri dettagli SSID necessari per la connessione, in questo scenario è "OWE-Transition". Se il client è in grado di supportare la crittografia OWE, può inviare la richiesta di probe all'SSID "OWE-Transition" e ottenere una risposta.
- La richiesta di sonda è stata inviata a OWE-Transition BSSID "40:ce:24:dd:2e:8f" e ha ricevuto una risposta. Anche all'interno di questo pacchetto di risposta della sonda è possibile visualizzare i dettagli di OPEN-OWE SSID.

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

```

Image-3 Richiesta probe

Risposta probe inviata dal punto di accesso al client

- Il client ha ricevuto una risposta di richiesta per l'SSID "OWE-Transition", ma ha i suoi dettagli SSID originali "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: 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

```

Image-4 Risposta probe

autenticazione OPEN

- Dopo aver ricevuto la risposta della sonda, l'autenticazione OPEN può avvenire tra il client e l'access point per controllare i dettagli/le funzionalità wifi dei client, prima dell'associazione.

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)						

Image-5 Autenticazione OPEN dopo il completamento del probe

Richiesta di associazione dal client al punto di accesso

- In questo pacchetto, il client può allegare il valore del parametro Diffie-Hellman per la crittografia.

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						

Image-6 Richiesta associazione

- In RSA trace è possibile iniziare a visualizzare i log del client dalla fase di associazione,

```
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
```

Risposta di associazione inviata dal punto di accesso al client

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


```
> Frame 8527: 245 bytes on wire (1960 bits), 245 bytes captured (1960 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Association Response, Flags: .....C
  Type/Subtype: Association Response (0x0001)
  Frame Control Field: 0x1000
  .000 0000 0011 1100 = Duration: 60 microseconds
  Receiver address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b)
  Destination address: ee:13:e8:a8:cd:5b (ee:13:e8:a8:cd:5b)
  Transmitter address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)
  Source address: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)
  BSS Id: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)
  .... .. 0000 = Fragment number: 0
  0011 0001 0000 .... = Sequence number: 784
  Frame check sequence: 0x7fbed111 [unverified]
  [FCS Status: Unverified]
  [WLAN Flags: .....C]
> IEEE 802.11 Wireless Management
  Fixed parameters (6 bytes)
  Capabilities Information: 0x1111
  Status code: Successful (0x0000)
  ..00 0000 0000 0001 = Association ID: 0x0001
  Tagged parameters (175 bytes)
  Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
  Tag: RSN Information
  Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
  Tag: HT Capabilities (802.11n D1.10)
  Tag: HT Information (802.11n D1.10)
  Tag: Extended Capabilities (8 octets)
  Tag: VHT Capabilities
  Tag: VHT Operation
  Tag: RM Enabled Capabilities (5 octets)
  Tag: BSS Max Idle Period
```

Image-7 Risposta associazione

```
2025/01/21 15:21:57.391334260 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.392296819 {wncd_x_R0-0}{1}: [dot11] [21675]: (note): MAC: ee13.e8a8.cd5b Association
```

Scambio chiave

L'handshake a 4 vie può essere eseguito tra il punto di accesso e il dispositivo client.

Chiave 1 inviata dal punto di accesso

Chiave 2 inviata dal client

Chiave-3 inviata dal punto di accesso

Chiave 4 inviata dal client

No.	Time	Source	Destination	Protocol	Length	Info
8540	2025-01-21 09:51:57.360919	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	193	Key (Message 1 of 4)
8541	2025-01-21 09:51:57.360930	Cisco_dd:2e:8f	Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
8542	2025-01-21 09:51:57.363375	Cisco_dd:2e:8f	Broadcast	802.11	376	Beacon frame, SN=3335, FN=0, Flags=.....C, BI=100, SSID="OPEN-OWE"
8543	2025-01-21 09:51:57.365594	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	215	Key (Message 2 of 4)
8544	2025-01-21 09:51:57.365603	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
8545	2025-01-21 09:51:57.366921	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	267	Key (Message 3 of 4)
8546	2025-01-21 09:51:57.366929	Cisco_dd:2e:8f	Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
8547	2025-01-21 09:51:57.368482	Cisco_dd:2e: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: dd14000fac0421b558dab0a335c355e7f4daa4a633af

Image-8 Handshake a 4 vie

```

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

```

Autenticazione L2 riuscita

```

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

```

Stato di apprendimento IP

```
2025/01/21 15:21:57.434789679 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.436611026 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.437239513 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.437508189 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (info): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.534166453 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interface
2025/01/21 15:21:57.535325325 {wncd_x_R0-0}{1}: [client-iplearn] [21675]: (note): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.535874658 {wncd_x_R0-0}{1}: [sisf-packet] [21675]: (info): TX: DHCPv4 from interface
2025/01/21 15:21:57.536500021 {wncd_x_R0-0}{1}: [client-orch-sm] [21675]: (debug): MAC: ee13.e8a8.cd5b
```

Client in stato RUN

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

Client non supportati per la crittografia OWE

- Esaminando un frame del beacon, i client vengono a sapere se sono in grado di supportare o meno questo metodo di crittografia. Se non è supportata, può semplicemente inviare una richiesta di richiesta di verifica per aprire SSID "OPEN-OWE" e può eseguire una normale autenticazione aperta, ottenere l'indirizzo IP, quindi può passare allo stato RUN.

```
2025/01/16 15:36:06.178370757 {wncd_x_R0-2}{1}: [client-orch-sm] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:06.209288788 {wncd_x_R0-2}{1}: [dot11] [17332]: (note): MAC: d037.4587.8f35 Associati
2025/01/16 15:36:06.248651191 {wncd_x_R0-2}{1}: [client-auth] [17332]: (note): MAC: d037.4587.8f35 Ope
2025/01/16 15:36:06.248751507 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.281808554 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:06.303307756 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
2025/01/16 15:36:10.305041414 {wncd_x_R0-2}{1}: [client-iplearn] [17332]: (note): MAC: d037.4587.8f35
2025/01/16 15:36:10.305777492 {wncd_x_R0-2}{1}: [client-orch-state] [17332]: (note): MAC: d037.4587.8f3
```

Informazioni sulla transizione rapida

- È possibile configurare OWE solo nell'autenticazione OPEN o in Webauth (CWA/LWA/EWA).
- FT non è supportato nella transizione OWE.
- Se si attiva FT, viene visualizzato questo messaggio di errore:

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

Image-9 Messaggio di errore quando viene abilitato FT in OWE Transition SSID

OWE non supportato con PSK/dot1x

Non siamo in grado di abilitare OWE in queste combinazioni,

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

Se si tenta di attivare uno di questi metodi, è possibile che venga visualizzato il messaggio di

errore

Edit WLAN

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

Disabled

Over the DS

Reassociation Timeout *

20

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

OWE

802.1X-SHA256

FT + SAE

FT + 802.1X

Transition Mode WLAN ID

9

Cancel

Update & Apply to Device

Image-10 Ricevimento del messaggio di errore durante l'abilitazione di altri metodi di autenticazione in 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

Image 11 Messaggio di errore durante l'abilitazione di AKM

- Nella versione Cisco IOS® XE 17.9.6 IOS, è possibile visualizzare l'opzione "OWE" in AKM quando si seleziona "WPA2+WPA3". Tuttavia, è possibile visualizzare il messaggio di errore e non utilizzare OWE con questa combinazione.

⚠ 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

Image 12 Messaggio di errore quando si sceglie WPA2+WPA3

- Nella versione Cisco IOS® XE 17.12.4, se si sceglie "WPA2+WPA3", non è possibile

ottenere l'opzione "OWE" in AKM,

Edit WLAN

⌵

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

General

Security

Advanced

Add To Policy Tags

Layer2

Layer3

AAA

☐ WPA + WPA2

☒ WPA2 + WPA3

☐ WPA3

☐ Static WEP

☐ None

MAC Filtering

☐

Lobby Admin Access

☐

WPA Parameters

WPA Policy☐

GTK Randomize☐

WPA2 Policy☒

WPA3 Policy☒

Transition Disable☐

WPA2/WPA3 Encryption

AES(CCMP128)☒

GCMP128☐

CCMP256☐

GCMP256☐

Protected Management Frame

PMF

Required

Association Comeback Timer*

1

SA Query Time*

200

Fast Transition

Status

Enabled

Over the DS

☐

Reassociation Timeout *

20

Auth Key Mgmt

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

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

802.1X☐

PSK☐

CCKM ⚠☐

SAE☐

FT + SAE☐

FT + 802.1X☐

FT + PSK☐

802.1X-SHA256☐

PSK-SHA256☐

MPSK Configuration

Enable MPSK

☐

↶ Cancel

📄 Update & Apply to Device

Image 13 Messaggio di errore - Opzione OWE non disponibile in AKM

Risoluzione dei problemi

1. Verificare le configurazioni sia nelle WLAN, sia nell'OPEN SSID e nell'SSID di transizione OWE se l'ID della WLAN di transizione deve essere mappato.
2. L'opzione di trasmissione deve essere disabilitata in OWE Transition SSID. Deve essere abilitata solo in OPEN SSID.
3. Verificare i metodi di autenticazione/crittografia/FT supportati descritti in questo articolo.
4. Se le configurazioni sono adatte dall'estremità del WLC, raccogliere i log e gli output necessari per ridurre il problema,

RA Trace ed EPC (Embedded Packet Capture)

Login alla GUI WLC -> Risoluzione dei problemi -> Traccia radioattiva -> Aggiungi indirizzo MAC wifi client -> Casella di controllo di client selezionati -> Avvia

Login alla GUI WLC -> Risoluzione dei problemi -> Packet Capture -> Add new file name -> Scegliere l'interfaccia uplink e WMI VLAN/Interface -> Start (Avvia).

Dal computer client: Se possibile, è possibile installare l'applicazione wireshark e raccogliere l'acquisizione del pacchetto scegliendo l'interfaccia WiFi.

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

CAPPUCCIO

È possibile raccoglierlo utilizzando il laptop MAC o configurando uno dei punti di accesso in modalità sniffer, si prega di fare riferimento questi collegamenti,

Da laptop MAC:

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

Da 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>

Collegare un laptop (server wireshark) alla porta dello switch e deve contenere un'applicazione wireshark. Questo server wireshark deve essere raggiungibile dall'interfaccia WMI WLC. È necessario consentire l'uso del protocollo "5555 o 5000 o 5556" nel firewall se questo è posizionato tra il WLC e il server wireshark.

Controllare se c'è qualsiasi "gscaler" installato in quel PC dove wireshark installato, se è più di "spegnere" e provare, se si tratta di un firewall come windows defender o qualsiasi cosa presente in esso, disabilitare questi e provare a raccogliere PCAP.

Roaming

Quando il client esegue il roaming da un punto di accesso a un altro, deve eseguire la procedura seguente:

- Necessità di inviare una riassociazione/associazione - A seconda della richiesta del client.
- È necessario inviare i dettagli DH (Diffie-Hellman) nella richiesta di associazione.
- Il client può ottenere i dettagli DH nella risposta dell'associazione dall'access point, in base a questo PMK generato sia nel client che nell'access point.
- È possibile che l'handshake a 4 vie venga eseguito tra il punto di accesso e il client.
- In OWE non è possibile abilitare FT, quindi 802.11r non è possibile.
- Ogni volta, durante il roaming, il client deve eseguire l'handshake a 4 vie dopo lo scambio DH in associazione.
- Client e AP che utilizzano il proprio PMKID, è univoco per ogni AP e client.
- Se il client si connette allo stesso punto di accesso, può utilizzare lo stesso PMKID. In alcuni scenari, se il client è stato eliminato rispetto a AP può generare un nuovo PMKID, tuttavia il client utilizza lo stesso PMKID per l'handshake a 4 vie.

Esempio:

Se il client si connette allo stesso punto di accesso, è possibile visualizzare lo stesso PMKID sia in Association-Request che in Association-Response. Nella risposta Association non è possibile visualizzare i dettagli DH se viene utilizzato lo stesso PMKID.

```
8522 2025-01-21 09:51:57.329457 ee:13:e8:a8:cd:5b Cisco_dd:2e:8f 802.11 337 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af Association Request, SN=2, FN=0, Flags=.....C, SSID="OWE-Tr
44117 2025-01-21 09:53:12.047592 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(0), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec]
    > Tag: Power Capability Min: -20, Max: 14
    > Tag: Supported Channels
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: RSN Information
      > Tag Number: RSN Information (48)
      > Tag length: 42
      > RSN 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: PM Enabled Capabilities (5 octets)
    > Tag: Supported Operating Classes
    > Tag: Extended Capabilities (11 octets)
    > Tag: VHT Capabilities
    > Tag: Vendor Specific: Samsung Electronics Co.,Ltd
    > Tag: Vendor Specific: Samsung Electronics Co.,Ltd
    > Tag: Vendor Specific: Microsoft Corp.: WPA/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: 7c 27 82 ba 4c 77 a9 8c 70 76 d1 fa 2e 34 93 34 7e c1 6d 4c 64 34 5d cc f8 b9 bb 68 b2 12 ff 31
```

Image 14 Utilizzo dello stesso PMKID

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

Image 15 Risposta di associazione con lo stesso PMKID

Per il test, il client è stato eliminato manualmente dal WLC e associato di nuovo allo stesso AP. In questo momento, il client invia lo stesso PMKID, ma l'AP invia i dettagli DH nella risposta dell'associazione.

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

Image 16 Dopo l'eliminazione, il client ha inviato lo stesso PMKID con i dettagli DH

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
44121	2025-01-21 09:53:12.851872	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	266			Association Response, SN=1229, FN=0, Flags=.....C
> Frame 44121: 266 bytes on wire (2128 bits), 266 bytes captured (2128 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Association Response, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (6 bytes) > Tagged parameters (196 bytes) > Tag: Supported Rates 6(B), 9, 12(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: 0x00e8 > 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: RSS Max Idle Period > Ext Tag: OWE Diffie-Hellman Parameter > Ext Tag length: 34 (Tag len: 35) > Ext Tag Number: OWE Diffie-Hellman Parameter (32) > Group: 256-bit random ECP group (19) > Public Key: e4 44 ea 00 6f f3 69 35 33 93 59 3f 7d b7 2e ab d4 04 26 7e 62 da d9 2a 88 c9 4e f5 e2 69 a1 c5								

Image 17 AP utilizza i valori DH per generare il nuovo PMKID

In questo esempio: Sia AP che client utilizzano lo stesso PMKID durante l'handshake a 4 vie. Archiviare i messaggi "M1 e M2".

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

Immagine - 18: AP e client che utilizzano lo stesso PMKID

In questo esempio: Il client utilizza lo stesso PMKID ma il punto di accesso utilizza un PMKID diverso generato dopo l'eliminazione del client. Controllare i messaggi "M1 e M2".

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


```

> Frame 44128: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits)
> Radiotap Header v0, Length 34
> 802.11 radio information
> IEEE 802.11 QoS Data, Flags: ....R.F.C
> Logical-Link Control
> 802.1X Authentication
  > Version: 802.1X-2004 (2)
  > Type: Key (3)
  > Length: 117
  > Key Descriptor Type: EAPOL RSN Key (2)
  > [Message number: 1]
  > Key Information: 0x0088
  > Key Length: 16
  > Replay Counter: 0
  > WPA Key Nonce: 17 28 f4 7a c2 42 74 21 f3 7f 1b 43 b6 f6 94 71 ea f8 a1 a7 8f eb 2e 10 83 d1 88 c5 a2 e0 5d ee
  > Key IV: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  > WPA Key RSC: 00 00 00 00 00 00 00 00
  > WPA Key ID: 00 00 00 00 00 00 00 00
  > WPA Key MIC: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  > WPA Key Data Length: 22
  > WPA Key Data: dd 14 00 0f ac 04 41 1b cf d7 7a 34 cb 50 70 13 07 47 b8 d2 4e 1f
    > Tag: Vendor Specific: IEEE 802.11: RSN PMKID
      > Tag Number: Vendor Specific (221)
      > Tag length: 20
      > OUI: 00:0f:ac (IEEE 802.11)
      > Vendor Specific OUI Type: 4
      > Data Type: PMKID KDE (4)
      > PMKID: 41 1b cf d7 7a 34 cb 50 70 13 07 47 b8 d2 4e 1f

```

Image 19 AP e client che utilizzano un PMKID diverso

Da traccia RA interna:

In questo esempio: Il client ha inviato i parametri DH nella richiesta di associazione e l'access point è stato elaborato prima della generazione della chiave PMK.

```

2025/01/21 15:18:50.157081690 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157082294 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157523328 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157531792 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532236 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157532538 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:18:50.157841380 {wncd_x_R0-0}{1}: [dot11-frame] [21675]: (debug): MAC: ee13.e8a8.cd5b  OW

```

In seguito, lo stesso client che si connette allo stesso punto di accesso, in questo momento, non ha generato un nuovo PMKID,

```

2025/01/21 15:21:57.391898613 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391903915 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906073 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b
2025/01/21 15:21:57.391906329 {wncd_x_R0-0}{1}: [dot11-validate] [21675]: (debug): MAC: ee13.e8a8.cd5b

```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).