

Opportunistic Wireless Encryptionのフローについて

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[説明](#)

[手順](#)

[ラボ再現の詳細](#)

[貸しフロー](#)

[オリジナルビーコンフレーム](#)

[隠しSSIDビーコン](#)

[クライアントからLEAD遷移SSIDにプローブ要求が送信されます。](#)

[APからクライアントに送信されるプローブ応答](#)

[オープン認証](#)

[クライアントからAPへのアソシエーション要求](#)

[APからクライアントに送信されるアソシエーション応答](#)

[キー交換](#)

[L2認証の成功](#)

[IPラーニングステート](#)

[RUN状態のクライアント](#)

[LEAD暗号化がサポートされていないクライアント](#)

[高速移行情報](#)

[LEANはPSK/dot1xではサポートされていません](#)

[トラブルシューティング](#)

[RAトレースおよびEPC \(組み込みパケットキャプチャ\)](#)

[エアーキャプ](#)

[ローミング](#)

はじめに

このドキュメントでは、LEAD移行のフローと、Catalyst 9800ワイヤレスLANコントローラ (WLC)での動作について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 9800 WLCの基本動作のアクセスポイント(AP)の設定方法
- WLANおよびポリシープロファイルの設定方法

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- C9800-80、Cisco IOS® XE 17.12.4、Cisco IOS® XE 17.9.6でもテスト済み
- APモデル：C9136I。ローカル接続モードとフレックス接続モードの両方でチェックされます。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

説明

- LEAN(Opportunistic Wireless Encryption)はIEEE 802.11の拡張で、ワイヤレスメディアに暗号化を提供します。LEADベースの認証の目的は、APとクライアントの間にセキュリティで保護されていないオープンなワイヤレス接続を回避することです。
- LEANでは、Diffie-Hellmanアルゴリズムベースの暗号化を使用して、ワイヤレス暗号化を設定します。
- LEANを使用すると、クライアントとAPはアクセス手順の間にDiffie-Hellman(DH)キー交換を実行し、その結果得られたペアワイズシークレットを4ウェイハンドシェイクで使します。
- LEADを使用すると、オープンまたは共有PSKベースのネットワークが導入されている環境のワイヤレスネットワークセキュリティが強化されます。

手順

1. 暗号化/セキュリティなしで1つのオープンWLANを設定し、ブロードキャストを有効にします。
2. LEADセキュリティを設定した別のSSIDを設定し、transition-mode-wlan-idでOPEN WLAN ID番号をマッピングします。このLEAD移行SSIDでブロードキャストSSIDオプションを無効にします。
3. OPEN WLANの「transition-mode-wlan-id」フィールドにLEAN移行WLAN ID番号をマッピングします。

ラボ再現の詳細

- Open SSID Name (オープンSSID名) :OPEN-LEAN
- LEAD遷移SSID名 : LEAD-Transition
- BSSID of OPEN-LEAN:40:ce:24:dd:2e:87
- BSSID of LEAD-Transition:40:ce:24:dd:2e:8f

貸しフロー

1. ビーコンはOPEN SSIDでブロードキャストできます。AIR PCAPでは、SSID名で確認できます。
2. また、AIR PCAPで、隠しセキュリティが有効なSSIDに、独自のSSID名ではなく「Wildcard」という名前が付いていることも確認できます。
3. クライアントがOPEN SSIDのビーコンフレームを受信すると、LEANを持つ、またはサポートしている場合、LEAN遷移SSID (OPEN SSIDの代わりにセキュリティが有効になっているSSID) にプローブ要求の送信を開始できます。
4. LEANをサポートするクライアントは、遷移SSIDからプローブ応答を取得できます。
5. オープン認証は、クライアントとAPの間で実行できます。
6. クライアントはDHキー交換の詳細を含むアソシエーション要求をAPに送信し、生成されたペアワイズシークレットを4ウェイハンドシェイクに使用できます。
7. APはアソシエーション応答を送信できます。
8. APとクライアントデバイスの間で4ウェイハンドシェイクが発生する可能性があります。
9. キー管理に成功すると、L2 PSKに成功する可能性があります。
10. クライアントはDHCP、ARPなどからIPを取得できる
11. クライアントはRUN状態になることができます。
12. LEANをサポートしていないクライアントデバイスは、OPEN SSID自体にプローブ要求を送信でき、RUN状態に移行するよりも直接IPを取得できます。

オリジナルビーコンフレーム

- ここで、AIR PCAPは、SSIDが「OPEN-LEAN」ブロードキャスト (ビーコンフレーム) であることを示しています。移行SSIDの詳細を含み、「LEAR-Transition」と呼ばれます。

No.	Time	Source	Destination	Protocol	Length	Info
47285	2025-01-21 09:53:18.259879	Cisco_dd:2e:87	Broadcast	802.11	376	Beacon frame, SN=1157, FN=0, Flags=.....C, BI=100, SSID="OPEN-OWE"
<pre> > Frame 47285: 376 bytes on wire (3008 bits), 376 bytes captured (3008 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Beacon frame, Flags:C < IEEE 802.11 Wireless Management > Fixed parameters (12 bytes) < Tagged parameters (300 bytes) < Tag: SSID parameter set: "OPEN-OWE" Tag Number: SSID parameter set (0) Tag length: 8 SSID: "OPEN-OWE" > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] > Tag: DS Parameter set: Current Channel: 48 > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap > Tag: Country Information: Country Code IN, Environment All > Tag: Power Constraint: 0 > Tag: QBSS Load Element 802.11e CCA Version > Tag: RM Enabled Capabilities (5 octets) > Tag: HT Capabilities (802.11n D1.10) > Tag: HT Information (802.11n D1.10) > Tag: Extended Capabilities (8 octets) > Tag: VHT Capabilities > Tag: VHT Operation > Tag: Tx Power Envelope > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element > Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5 > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11) > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44) < Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode Tag Number: Vendor Specific (221) Tag length: 25 OUI: 50:6f:9a (Wi-Fi Alliance) Vendor Specific OUI Type: 28 BSSID: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f) SSID length: 14 SSID: OWE-Transition </pre>						

図1:OPEN SSIDのビーコンフレーム

隠しSSIDビーコン

- WLANの設定により、「ブロードキャスト」はこの「LEAR-Transition」SSIDに対して無効になっていますが、AIR PCAPにはSSID名「Wildcard」を含む非表示のSSIDビーコンが表示される場合があります。ただし、そのパケットを確認すると、LEAD-Transitionの詳細が含まれます。
- 「40:ce:24:dd:2e:8f」のように、このパケットを使用して隠しSSIDのBSSIDを取得し、パケットキャプチャで検索します。
- このパケットでは、SSID「Missing」が示され、このSSIDには「OPEN-LEAN」としての遷移SSIDと、そのBSSID「40:ce:24:dd:2e:87」が含まれています。

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)
<pre> > 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: 8 SSID: <MISSING> > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec] > Tag: DS Parameter set: Current Channel: 48 > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap > Tag: Country Information: Country Code IN, Environment All > Tag: Power Constraint: 0 > Tag: RSN Information > Tag: QBSS Load Element 802.11e CCA Version > Tag: PM Enabled Capabilities (5 octets) > Tag: HT Capabilities (802.11n D1.10) > Tag: HT Information (802.11n D1.10) > Tag: Extended Capabilities (8 octets) > Tag: VHT Capabilities > Tag: VHT Operation > Tag: Tx Power Envelope > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element > Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5 > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11) > Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44) > Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode Tag Number: Vendor Specific (221) Tag length: 19 OUI: 50:6f:9a (Wi-Fi Alliance) Vendor Specific OUI Type: 28 BSSID: Cisco_dd:2e:8f (48:ce:24:dd:2e:8f) SSID length: 8 SSID: OPEN-OWE </pre>						

図-2：非表示のSSID – 使用期限の移行

クライアントからLEAD遷移SSIDにプローブ要求が送信されます。

- ビーコンフレーム「OPEN-LEAN」SSIDに基づいて、クライアントは接続する必要がある他のSSIDの詳細を認識します。このシナリオでは、「LEAN-Transition」です。クライアントがLEAD暗号化をサポートできる場合、プローブ要求を「LEAD-Transition」SSIDに送信して応答を取得できます。
- プローブ要求がLEAN-Transition BSSID「40:ce:24:dd:2e:8f」に送信され、応答を受け取りました。このプローブ応答パケット内でも、OPEN-LEAD SSIDの詳細を確認できます。

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) on 0
> 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
```

図-3：プローブ要求

APからクライアントに送信されるプローブ応答

- クライアントはSSID「LEAN-Transition」のプローブ応答を受信しましたが、WiFi Allianceには元のSSIDの詳細「OPEN-LEAN」があります。

```

8509 2025-01-21 09:51:57.318400 ee:13:e8:a8:cd:5b Cisco_dd:2e:8f 802.11 197 Probe Request, SN=0, FN=0, Flags=.....C, SSID="OWE-Transition"
8510 2025-01-21 09:51:57.318412 ee:13:e8:a8:cd:5b 802.11 48 Acknowledgement, Flags=.....C
8511 2025-01-21 09:51:57.319223 Cisco_dd:2e:8f ee:13:e8:a8:cd:5b 802.11 398 Probe Response, SN=782, FN=0, Flags=.....C, BI=100, SSID="OWE-Transition"
8512 2025-01-21 09:51:57.319233 Cisco_dd:2e:8f 802.11 48 Acknowledgement, Flags=.....C

```

> Frame 8511: 398 bytes on wire (3184 bits), 398 bytes captured (3184 bits)

> Radiotap Header v0, Length 36

> 802.11 radio information

> IEEE 802.11 Probe Response Flags:C

> IEEE 802.11 Wireless Management

> Fixed parameters (12 bytes)

> Tagged parameters (322 bytes)

> Tag: SSID parameter set: "OWE-Transition"

> Tag Number: SSID parameter set (0)

> Tag length: 14

SSID: "OWE-Transition"

> Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]

> Tag: DS Parameter set: Current Channel: 48

> Tag: Country Information: Country Code IN, Environment All

> Tag: Power Constraint: 0

> Tag: RSN Information

> Tag: QoS Load Element 802.11e CCA Version

> Tag: RM Enabled Capabilities (5 octets)

> Tag: HT Capabilities (802.11n D1.10)

> Tag: HT Information (802.11n D1.10)

> Tag: Extended Capabilities (8 octets)

> Tag: VHT Capabilities

> Tag: VHT Operation

> Tag: Tx Power Envelope

> Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

> Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5

> Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled

> Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)

> Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44)

> Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode

> Tag Number: Vendor Specific (221)

> Tag length: 19

> OUI: 50:6f:9a (Wi-Fi Alliance)

> Vendor Specific OUI Type: 28

BSSID: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)

SSID length: 8

SSID: OPEN-OWE

図-4：プローブ応答

オープン認証

- ・プローブ応答を取得した後、クライアントとAPの間でオープン認証を実行し、関連付けの前にクライアントのWiFiの詳細と機能を確認できます。

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)						

図-5：プローブ成功後のオープン認証

クライアントからAPへのアソシエーション要求

- このパケットでは、クライアントが暗号化のためにDiffie-Hellmanパラメータ値を付加できることに注意してください。

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						

図6：関連付け要求

- RAトレースでは、アソシエーションフェーズからクライアントログの確認を開始できます
 -

```
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
```

APからクライアントに送信されるアソシエーション応答

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:
- 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:
- > 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: RRM Enabled Capabilities (5 octets)
 - > Tag: BSS Max Idle Period

図7：アソシエーション応答

```
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
```

キー交換

APとクライアントデバイスの中で4ウェイハンドシェイクが発生する可能性があります。

APによるキー1送信

クライアントによるキー2送信

APによるキー3の送信

クライアントによるキー4送信

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	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C

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

イメージ8:4ウェイハンドシェイク

```

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認証の成功

```

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ラーニングステート

```
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
```

RUN状態のクライアント

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

LEAD暗号化がサポートされていないクライアント

- ビーコンフレーム自体を確認することで、クライアントはこの暗号化方式をサポートできるかどうかを知ることができます。サポートされていない場合は、オープンSSID「OPEN-LEAN」にプローブ要求を送信するだけで、通常のオープン認証を実行し、IPアドレスを取得し、RUN状態に移行できます。

```
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
```

高速移行情報

- LEANは、オープン認証(OAM)またはWebauth(CWA/LWA/EWA)でのみ設定できます。
- FTは借入移行ではサポートされていません。
- FTを有効にすると、

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

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

図-9:LEAD遷移SSIDでFTを有効にした場合のエラーメッセージ

LEANはPSK/dot1xではサポートされていません

これらの組み合わせではBORNを有効にできません

1. 802.1xまたはFT+802.1x
2. PSK、FT+PSKまたはPSK-SHA256
3. SAEまたはFT+SAE
4. 802.1x-SHA256またはFT+802.1x-SHA256

これらの方法のいずれかを有効にしようとすると、エラーメッセージ

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

図10:LEAN SSIDで他の認証方式を有効にしているときにエラーメッセージが表示される

⚠ 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

Enabled ▼

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

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

イメージ11:AKMを有効にしているときのエラーメッセージ

- Cisco IOS® XE 17.9.6 IOSバージョンでは、「WPA2+WPA3」を選択するとAKMの下に「LEAR」オプションが表示されますが、エラーメッセージが表示されることから、この組み合わせで「LEAD」を使用することはできません。

⚠ 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

イメージ12:WPA2+WPA3を選択したときのエラーメッセージ

- Cisco IOS® XE 17.12.4バージョンで「WPA2+WPA3」を選択すると、AKMで「LEAN」オ

プシヨンを取得できません。

Edit WLAN

⌵

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

GeneralSecurityAdvancedAdd To Policy Tags

Layer2Layer3AAA

☐ 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☐

CCKM ⚠☐

FT + SAE☐

FT + PSK☐

PSK-SHA256☐

PSK☐

SAE☐

FT + 802.1X☐

802.1X-SHA256☐

MPSK Configuration

Enable MPSK☐

↶ Cancel

📄 Update & Apply to Device

画像-13 : エラーメッセージ - AKMでLEANオプションが表示されない

トラブルシューティング

1. 両方のWLANの設定を確認します。OPEN SSIDとLEAD transition SSIDでは、移行WLAN IDがマッピングされている必要があります。
2. ブロードキャストリングオプションはLEAD移行SSIDで無効にする必要があります。OPEN SSIDでのみ有効にする必要があります。
3. この記事で説明されているサポートされている認証/暗号化/FT方式を確認します。
4. WLC側から設定に問題がない場合は、問題を絞り込むために必要なログと出力を収集してください。

RAトレースおよびEPC (組み込みパケットキャプチャ)

WLC GUIにログイン -> Troubleshooting -> Radioactive Trace -> Add client wifi MAC address -> Click that clients checkbox -> Start

WLC GUIへのログイン ->トラブルシューティング ->パケットキャプチャ ->新しいファイル名の追加 ->アップリンクインターフェイスおよびWMI VLAN/インターフェイスの選択 ->開始

クライアントマシンから：可能であれば、Wiresharkアプリケーションをインストールし、WiFiインターフェイスを選択してパケットキャプチャを収集できます。

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

エアーキャップ

MACラップトップを使用するか、APのいずれかをスニファモードに設定することで、この情報を収集できます。次のリンクを参照してください。

MACラップトップから：

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

スニファAPから：

<https://www.cisco.com/c/en/us/support/docs/wireless/catalyst-9800-series-wireless-controllers/217057-configure-access-point-in-sniffer-mode-o.html>

スイッチポートに1台のラップトップ (Wiresharkサーバ) を接続します。このラップトップにはWiresharkアプリケーションがインストールされている必要があります、このWiresharkサーバはWLC WMIインターフェイスに到達する必要があります。WLCとWiresharkサーバの間にプロトコル「5555、5000、または5556」が存在する場合は、ファイアウォールでプロトコル「5555、5000、または5556」を許可する必要があります。

WiresharkがインストールされているそのPCに「gscaler」がインストールされていることを確認します。それが「オフ」をオフにして試してください。Windows Defenderなどのファイアウォー

ルまたはその中に存在するものであれば、それらを無効にしてPCAPを収集してください。

ローミング

クライアントがあるAPから別のAPにローミングする場合は、次の手順を実行する必要があります。

- ・ 再関連付け/関連付けを送信する必要がある：クライアントの要求によって異なります。
- ・ 関連付け要求でDH (Diffie-Helman)詳細を送信する必要があります。
- ・ クライアントは、このPMKがクライアントとAPの両方で生成されることに基づいて、APからのアソシエーション応答でDHの詳細を取得できます。
- ・ APとクライアントの間で4ウェイハンドシェイクが発生する可能性があります。
- ・ LEANではFTを有効にできないため、802.11rは使用できません。
- ・ クライアントがローミングするたびに、DH交換後に4ウェイハンドシェイクを関連付けて実行する必要があります。
- ・ クライアントとAPは独自のPMKIDを使用し、APとクライアントごとに一意です。
- ・ クライアントが同じAPに接続する場合、同じPMKIDを使用できます。場合によっては、クライアントが削除されると、APは新しいPMKIDを生成できますが、クライアントは4ウェイハンドシェイクに同じPMKIDを使用します。

例：

クライアントが同じAPに接続する場合、Association-RequestとAssociation-Responseの両方で同じPMKIDを確認できます。アソシエーション応答では、同じPMKIDを使用する場合はDHの詳細を表示できません。

```
8522 2025-01-21 09:51:57.329457 ee13: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 ee13: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)
    Groups: 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
```

イメージ14：同じPMKIDの使用

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								

画像-15：同じPMKIDを使用したアソシエーション応答

テストのために、このクライアントをWLCから手動で削除し、同じAPに再度関連付けました。この時点で、クライアントは同じPMKIDを送信しますが、APは関連付け応答でDHの詳細を送信します。

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								

画像-16：削除後、クライアントは同じPMKIDをDH詳細とともに送信

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
44121	2025-01-21 09:53:12.851872	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	266			Association Response, SN=1229, FN=0, Flags=.....C
> Frame 44121: 266 bytes on wire (2128 bits), 266 bytes captured (2128 bits) > Radiotap Header v0, Length 36 > 802.11 radio information > IEEE 802.11 Association Response, Flags:C > IEEE 802.11 Wireless Management > Fixed parameters (6 bytes) > Tagged parameters (196 bytes) > Tag: Supported Rates 6(B), 9, 12(0), 18, 24(0), 36, 48, 54, [Mbit/sec] > Tag: RSN Information > Tag Number: RSN Information (48) > Tag length: 26 > RSN Version: 1 > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM) > Pairwise Cipher Suite Count: 1 > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM) > Auth Key Management (AKM) Suite Count: 1 > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption > RSN Capabilities: 0x00e8 > PMKID Count: 0 > PMKID List > Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128) > Tag: Vendor Specific: Microsoft Corp.: WMM/WMF: Parameter Element > Tag: HT Capabilities (802.11n D1.10) > Tag: HT Information (802.11n D1.10) > Tag: Extended Capabilities (8 octets) > Tag: VHT Capabilities > Tag: VHT Operation > Tag: RM Enabled Capabilities (5 octets) > Tag: BSS Max Idle Period > Ext Tag: OWE Diffie-Hellman Parameter > Ext Tag length: 34 (Tag len: 35) > Ext Tag Number: OWE Diffie-Hellman Parameter (32) > Group: 256-bit random ECP group (19) > Public Key: e4 44 ea 00 6f f3 69 35 33 93 59 3f 7d b7 2e ab d4 04 26 7e 62 da d9 2a 88 c9 4e f5 e2 69 a1 c5								

画像-17:APはDH値を使用して新しいPMKIDを生成します

この例では、APとクライアントの両方が4ウェイハンドシェイクの実行中に同じPMKIDを使用し、「M1およびM2」メッセージを確認します。

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: 00:0f:ac (Ieee 802.11) > Vendor Specific OUI Type: 4 > Data Type: PMKID KDE (4) > PMKID: 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af								

図18：同じPMKIDを使用するAPとクライアント

この例では、クライアントが同じPMKIDを使用しているが、クライアントの削除後に生成された異なるPMKIDをAPが使用している場合、「M1およびM2」メッセージを確認します。

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

```

図19：異なるPMKIDを使用するAPとクライアント

内部RAトレースから：

次の例では、クライアントが関連付け要求でDHパラメータを送信し、APがPMKを生成したものよりも処理しています。

```

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

```

その後、同じクライアントが同じAPに接続していますが、この時点では、APは新しいPMKIDを生成しませんでした。

```

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

```

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。