

يزاهتنالايكلساللاري فشتللقفدت مهف

تايوتحمل

[قمدقملا](#)

[قيساسالتابلطتملا](#)

[تابلطتملا](#)

[قمدختسملا تانوكملا](#)

[فصولا](#)

[تاوطخ](#)

[Lab Repro ليصافت](#)

[نن اذتست](#)

[يلصأالقرانملا راطا](#)

[قي فخم SSID طوطخ](#)

[OWE لي وحتب صاغلل SSID يللا لي مغللا نم قيقحت بلط لاسرامت](#)

[لي مغللا يللا AP نم فاشكت سالا قباحت سالا لاسرامت](#)

[ققداصملا حتف](#)

[AP يللا لي مغللا نم نارتقالا بلط](#)

[لي مغللا يللا AP نم نارتقالا قباحت سالا لاسرامت](#)

[حي تافملا لدايت](#)

[قحجان L2 ققداصم](#)

[IP ملعت قلاخ](#)

[لي غشتلا قلاخ يف لي مغللا](#)

[OWE ري فشتل ني موعدملا ريغ عالمغلا](#)

[عيرسللا لاقثتال تامولعم](#)

[OWE PSK/dot1x عم موعدم ريغ](#)

[اهجالصا واطخأال فاشكت سالا](#)

[\(نمضمللا ولدلا طاقثللا\) EPC و RA عبتت](#)

[يئاوه واطغ](#)

[لاوحت](#)

قمدقملا

ككبشلا يف مكحتلا قدحو ىلع هلمع ةي فيكو ني دللا لاقثنا قفدت دنتسملا اذه حضوي
Catalyst 9800 (WLC) ةيكلساللا ةيلحمل

قيساسال تابلطتملا

تابلطتملا

ةيلاللا عيضاوملاب ةفرعم كي دل نوكت نأ Cisco ي صوت

- 9800 زارط (WLC) ةيكل لسلال ةيكل حملا ةكبشل ي ف مكحتل رصنع نيوكت ةي فيك
ي ساسال ليغشتلل (AP) لوصول ةطقن
- WLAN و ةساسال فيرعت تافلم نيوكت ةي فيك

ةمدختسملاتانوكملا

٥٠: لایات الة ی دامال تان وکمل او چمار پل تارادصل ایلا دنت سمل اذه ی ف ة درا ول تامول عمل دنت ست

- Cisco IOS® XE 17.9.6 في اضيأ هرا بتخا متو Cisco IOS® XE 17.12.4، C9800-80
- عضوو يلحملا لاصتال عضو نم لك في هعادي مت ، C9136ا : لوصول ةطقن جذومن
نرمل لاصتال

•صاخ ةي لم عم ةئي ب ي ة دوجوم ةزهجال نم دنتسم ل اذه ي ة دراو ل تامول عم ل عاش ن م ت ناك اذ ا .(يضا رتفا) حوس مم ني وكت ب دنتسم ل اذه ي ة مدختسُم ل ةزهجال عي م ت اد ب رمأ ي ل لم تحت م ل ري ثأ تل ل كم ه ف نم دكأ ت ف ، لي غشت ل دي ق ك ت ك ب ش

فصولا

- ريفش ت رفو يذل IEEE 802.11 ل دادتما وه (يزاهاتنا يكلسال ريفش ت) OWE حتف بنجت وه OWE ىل ةدنتسمال ةقداصمالم نم ضرغالم نل. يكلسالال طسولل ءالمءالو لوصولو طاقن نيب نم آ ريغ يكلسال لاصتا.
- ريفش تال دادءال Diffie-Hellman تايمزراوخ ىل ةدنتسمال ريفش تال OWE مدختسي يكلسالال.
- ءانثأ Diffie-Hellman حيتافم لدابتب لوصولو ةطقنو ليمءال موقى، OWE لالء نم هاچتال ةيعابلرل ةحفاصمالم عم چتالال يومءال رسلال مادختساو لوصولو ءارچا.
- يتل رشنل تايلمءل ةيكلسالال ءكبشلل نامأ نيسحت ىل OWE مادختسا يءوئى.
- PSK ىل ةدنتسمال ءكرتشمالم وأ ةءوتفمالم تاكبشلل رشن اءىف مئى

تاو طخ

1. ثبت الـ SSID في الـ WLAN. ثبت الـ SSID في الـ WLAN. ثبت الـ SSID في الـ WLAN.
2. ثبت الـ SSID في الـ WLAN. ثبت الـ SSID في الـ WLAN. ثبت الـ SSID في الـ WLAN.
3. ثبت الـ SSID في الـ WLAN. ثبت الـ SSID في الـ WLAN. ثبت الـ SSID في الـ WLAN.

Lab Repro لی صافت

- نېدل ځان: SSID م س ا
- OWE ل ا ځان: OWE ل ځان م س ا
- BSSID م س ا: Open-Owe: 40:ce:24:dd:2e:87
- BSSID م س ا: Owe-Transfer: 40:ce:24:dd:2e:8f

نن ادت ست

1. هب صاخال SSID مسا لال خ نم اهتيؤر كنكمي .ةحوتفم ال SSID ل داشرالا ةزهجأ ثب نكمي .ءاوهال PCAP في
2. "لدب فرح" مسا مادختساب هنيكمت مت يذلي فيفخم ال SSID لىل عالطالا اننكمي امك . PCAP في هب صاخال SSID مسا نم الدب
3. SSID معدي وأ هيدل ناك اذا ،ةحوتفم ال SSID ل ةرانم الراطإ ءالمعل يقلت نأ درجم ب ، نكمم SSID وهو) يلاقنا SSID لىل راسفتسالا بلط لاسرا في ءدب ال هنيكمي (ةحوتفم SSID نم الدب نيميألل
4. SSID نم قيقت ءباجتسا لىل لوصحل OWE في نيميوعدم ال ءالمعلل نكمي .ةيلاقنا ال
5. AP و ليمل ال نيب ءحوتفم ال ءقداصلم لثدت نأ نكمي .
6. DH ءاتفم لدابت ليصافت عم لوصولو ءطقن لىل نارتقا بلط لاسرا ليملل نكمي .تاهاجتا ءعبرا في ءحفاصلم لكذ نع ءتانل لاصتا ال مدع رس مادختساو
7. نارتقا ال ءباجتسا لاسرا لوصولو ءطقنل نكمي .
8. ليمل زاهو لوصولو ءطقن نيب هاجتا ال ءيغابر ءحفاصلم ءارج نكمي .
9. اءان يناثل يوتسم ال نم PSK نوكني نأ نكمي ،ءان ب ءيئاتفم ال ءراذإ دع ب .
10. ،لكذ لىل امو ARP و DHCP نم IP لىل لوصحل ليملل نكمي .
11. RUN ءلا لىل لاقنا ال ليملل نكمي .
12. SSID ءتفل PROBE بلط لاسرا هنيكمي في ، OWE ءدمتعمل ريغ ليمل ال ءزهجأ تناك اذا . RUN ءلا لىل لاقنا ال هنيكمي امم ءرشابم IP لىل لوصحل هنيكمي وهسفن

يليصالا ءرانم الراطإ

- لىل يوتحي يذلي .(ءاعش راطإ) SSID "Open-Owe" ثب ،ءاوهال نم PCAP نيب ت ،انه "Owe-Transfer" يمسو ءيلاقنا ال SSID ليصافت

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) on interface 0 > 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: QSS 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						

ءحوتفم ال SSID ل ءرانم الراطإ : 1-ءروصل

ةيفخم SSID طوطخ

- "ثبلا" لي طعت متي ،(WLAN) ءيكلسال ال ءيلاءم ال ءكبشال نيوكتل اقفو

- يلائق تال ال SSID ىل ع يوتحتو "دوقفم" SSID، صاخال هذه رهطت، ةمزال هذه يفو "40:ce:24:dd:2e:87" ااب صاخال ال BSSID و "Open-Owe" ك ااب صاخال

OWE لاقتنا - في خم SSID : 2-ة واصل

- لصرحو OWE-Transition BSSID "40:ce:24:dd:2e:8f" ىلإ فاشكتس الابلط لاسرا مت
Probe ةباجتسإ ةمزح يف SSID لىصافت ىلع عالطال كنكمي امك. ةباجتسإ ىلع
هذه.

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

```

قيقحت ال بلط : 3-ةروصل

للمعمل إلى AP نم فاشكت السال ةباجتسإ لاسرا مت

- ليصافت كلمي هنا إلى SSID "Owe-Transfer" ل ءاصقت السال ةباجتسإ للمعمل يقلت
WiFi Alliance. في "Open-OWE" ةي لصل ال SSID

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

```

> Frame 8511: 398 bytes on wire (3184 bits), 398 bytes captured (3184 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
> IEEE 802.11 Probe Response, Flags: .....C
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
  Tagged parameters (322 bytes)
    Tag: SSID parameter set: "OWE-Transition"
      Tag Number: SSID parameter set (0)
      Tag length: 14
      SSID: "OWE-Transition"
    Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 48
    Tag: Country Information: Country Code IN, Environment All
    Tag: Power Constraint: 0
    Tag: RSN Information
    Tag: QSS Load Element 802.11e CCA Version
    Tag: PM Enabled Capabilities (5 octets)
    Tag: HT Capabilities (802.11n D1.10)
    Tag: HT Information (802.11n D1.10)
    Tag: Extended Capabilities (8 octets)
    Tag: VHT Capabilities
    Tag: VHT Operation
    Tag: Tx Power Envelope
    Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    Tag: Vendor Specific: Cisco Systems, Inc: Aironet CCX version = 5
    Tag: Vendor Specific: Cisco Systems, Inc: Aironet Client MFP Disabled
    Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (11) (11)
    Tag: Vendor Specific: Cisco Systems, Inc: Aironet Unknown (44)
    Tag: Vendor Specific: Wi-Fi Alliance: OWE Transition Mode
      Tag Number: Vendor Specific (221)
      Tag length: 19
      OUI: 50:6f:9a (Wi-Fi Alliance)
      Vendor Specific OUI Type: 28
      BSSID: Cisco_dd:2e:8f (40:ce:24:dd:2e:8f)
      SSID length: 8
      SSID: OPEN-OWE

```

رابسمل اب ةباجتسإ : 4-ةروصل

ةق ءاصملا حتف

- للمعمل نيب ءحوت فملا ءق ءاصملا ءدحت نأ نكمي ،رابسمل ءباجتسإ يلع لوصحل ءعب
نارثقالا لبق ءالمعمل WiFi ءايناكم/ليصافت نم ققحتلل AP و

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)						

حاجاتنا لاصق تسال دعب قق داصم الحتف : ةروصل

AP لي عمال نم نارتقالا بلط

- ريفش ل Diffie-Hellman عم لم عم قق اف را لي عمال نكمي هنا طحال، عمز الحتف هذه ي

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.: WMN/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: 7c2782ba4c77a98c7076d1fa2e3493347ec16d4c64345dccc78b9bb68b212ff31						

نارتقالا بلط : ةروصل

- نارتقالا ةلحرم نم ليمعلا تالچس ةيؤر ءدب كنكمي RA، عبتت ي ف

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

ليمعلا ىل AP نم نارتقالا ةباجتسا لاسرا مت

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

نارتقالا لالځ نم ةباجتسا لال : 7-ةروصولا

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

حياتافملا لدابت

ليمعلا زاهجو لوصولو ةطقن نيب هاجتالا ةيعابر ةحفاصم ءارج كنكمي

لوصولو ةطقن ةطساوب 1-حاتفملا لاسرا

ليمعلا ةطساوب KEY-2 لاسرا

لوصولو ةطقن ةطساوب 3-حاتفملا لاسرا

ليمعلا ةطساوب KEY-4 لاسرا

No.	Time	Source	Destination	Protocol	Length	Info
8540	2025-01-21 09:51:57.360919	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	193	Key (Message 1 of 4)
8541	2025-01-21 09:51:57.360930	Cisco_dd:2e:8f	Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
8542	2025-01-21 09:51:57.363375	Cisco_dd:2e:8f	Broadcast	802.11	376	Beacon frame, SN=3335, FN=0, Flags=.....C, BI=100, SSID="OPEN-OWE"
8543	2025-01-21 09:51:57.365594	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	215	Key (Message 2 of 4)
8544	2025-01-21 09:51:57.365603	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	802.11	48	Acknowledgement, Flags=.....C
8545	2025-01-21 09:51:57.366921	Cisco_dd:2e:8f	ee:13:e8:a8:cd:5b	EAPOL	267	Key (Message 3 of 4)
8546	2025-01-21 09:51:57.366929	Cisco_dd:2e:8f	Cisco_dd:2e:8f	802.11	48	Acknowledgement, Flags=.....C
8547	2025-01-21 09:51:57.368482	Cisco_dd:2e:86	Broadcast	802.11	376	Beacon frame, SN=3336, FN=0, Flags=.....C, BI=100, SSID="newssid"
8548	2025-01-21 09:51:57.373313	ee:13:e8:a8:cd:5b	Cisco_dd:2e:8f	EAPOL	171	Key (Message 4 of 4)
8549	2025-01-21 09:51:57.373334	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

تاہاجاتالای عی عا بر ؤ ح ف اص م : 8- ؤ ر و ص ل ا

```

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

```

ؤ ح ج ا ن L2 ؤ ق د اص م

```

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 م ل ع ت ؤ ل ا ح

```
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
```

ليغشت الةلاح في لي ماعلا

```
2025/01/21 15:21:57.537017277 {wncd_x_R0-0}{1}: [client-orch-state] [21675]: (note): MAC: ee13.e8a8.cd5
```

OWE ريف شتل ني موع دم لاري غءالم ع ل

- ممد یلع نیرداق اوناک اذا ام یلع عالمعل فرعتی، هسفن قرانملا راطا عچارم لالخنو قیقحت بلط لاسرا طقف اهل نكمی، اهممد مدع لایفو. ال ما هذه ریفشتل ققیرط یلع لوصحل اویداع عحتوفم عقداصمب ما یقل اهنكمیو "OPEN-OWE" SSID حتفل RUN. لایق لایفنت مثنو، IP ناونع

```
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 Oper
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
```

عيرس للاق تال تامول عم

- WebAuth (CWA/LWA/EWA) في وأ ءحوتفملا ءقءاصملا في طقف OWE نيوكء اننكمي.
- OWE لاقءنا في موعءم ريغ FT.
- ،هءه أطءللا ءلاسر رلعل لصءءس ،FT نيكمءب ءمق اءا

⚠ 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

OWE لي وحتل SSID في FT نيكمت دنع أطخ ةلاس ر : 9-ةروصل

OWE PSK/dot1x عم موعدم ريغ

تأبكرتال هذه في OWE نيكمت ىل ع نيرداق ريغ نحن

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

أطخال ةلاس ر ىل ع لوصخال كنكمي ،بيلالال هذه نم ي نيكمت تلواح اذا

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

SSID OWE في ىرخأ ةقداصم قرط نيكمت ءانثأ أطخ ةلاس رىلع لوصح ال: 10-ةروصل

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

☐

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

AKM نيكمت ءانثأ أطخ ةلاسر :11-ةروصل

- ام دنع AKM نمض "OWE" راخي رت نأ كنكمي، Cisco IOS® XE 17.9.6 IOS رادصلإي ف يلع رداق ريغ تنأف، أطخلا ةلاسر يلع لوصحلا كنكمي لاجيأ يلع "WPA2+WPA3" ددحت ةومحلا هذه عم OWE مادختسا.

⚠ 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

WPA2+WPA3 راتخن امدنع أطخ ةلاس ر: 12-ةروصل

- لوصول كنكمي ال "WPA2+WPA3" راتخت امدنع، Cisco IOS® XE 17.12.4 رادصلإا يف

AKM، ف "OWE" رايجل ىلع

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

AKM ف OWE رايجل ىلع لوصحل مدع - أطخ ةلاس ر : 13-ةروصل

اهحال صإو عاطخأل فاشكتسا

1. يفو ءحوتفم ال SSID يفو WLAN تاكبش نم لك يف ءدوجوم ال تانيوكتل نم ققحت .
يلاق تنا ال WLAN فرعم نييغت بجي SSID OWE TRANSITION .
2. SSID يف طقف هنيكمت بجيو ، OWE لقنل SSID يف ثبل رايل ليطعت بجي .
ءحوتفم ال .
3. ءلاقم ال هذو يف ءحضوم ال ءموءدم ال ft/ريفشتل/ءقءاصم ال بيلاسأ نم ققحت .
4. ءبولطم ال تاراءصإل او تالءس ال ءمء ءءري ف ، WLC ءي هان نم ءءء تانيوكتل تناك اءا .
ءلءشم ال قاطن قئيضتل ،

(نمضم ال ولدل طاقتل) EPC و RA عبتت

-> اءحال صإو عاطخأل فاشكتسا -> WLC ءي مومسرل مءءتسم ال ءءاو ءل لوءدل لءءست
ءء -> "ءالمءل" رايءخال ءناخ قوف رقنا -> لءمءل WiFi ناوئع ءفاضا -> ءشم عبتت

تامومسرل مءءتسم ءءءاوب ءصاال (GUI) ءي مومسرل مءءتسم ال ءءاو ءل لوءدل لءءست
ءءءاو رءءأ -> ءءء فلم مسا ءفاضا -> مزال طاقتل -> اءحال صإو عاطخأل فاشكتسا -> (WLC)
ءء -> ءءءاوب ال WMI VLAN و ءلصول

رايءءاب ءمزال طاقتل ءمءءو Wireshark قئيبطت تي بءء كنكمي ، كنمأ نإ : لءمءل زاوء نم
WiFi ءءو .

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

ئي او ءاطء

ءءرل ، sniffer ءضو يف لوصول طاقن ءءا نيوكت وأ Mac بساا مءءتساب هءمء كنكمي
، تاطا بءرال هذو ءل ءوءرل ،

لومءم ال Mac رءوي بم كنم :

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

Sniffer لوصول ءطقن نم :

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

ءل ءوئءي نأ بجيو لومءم ال ءفنم ب (wireshark مءاا) ءءاو لومءم رءوي بم كنم لءصوب مق
ءل لوصول ءي ناكم ءل ءءو Wireshark مءاا ءوئءي نأ بجيو ، ءي تءءم Wireshark قئيبطت
ناك اءا ءي مءال راءء يف "5556 وأ 5000 وأ 5555" لوكوءوربلاب ءامسل بجي . WLC ءءءو
Wireshark مءاا و WLC مءاا ني بءءوم .

ناك اءا ، Wireshark تي بءء مءءءي رءوي بم كنم ال ءءو يف تءءم "gscaler" ءي ءوءو نم ققءتل
ءي وأ Windows Defender لءم ءي مءال راءء ءي كانه ناك اءا ، ءل وءم "لءءشء فاقءي" ءءرل رءء

PCAP. عي مجت ةل و احم و هذه لي طعت ءا ج رلا ، هي ف دوجوم عي ش

لاوجت

، تاو طخلال هذهب ماي قلا لىل ا ج ا تحي ه ن ا ف ، رخ ا لىل ل و ص و ة ط ق ن ن م لىم ع ل ل و ج تى ا م د ن ع

- لىم ع ل ل ب ل ط لىل ع د م ت ع ي - ن ا ر ت ق ا / ن ا ر ت ق ا ة د ا ع ل ل ا س ر ا لىل ا ج ا ح ل
- ن ا ر ت ق ا ل ا ب ل ط لىل ف DH (Diffie-helman) لى ص ا ف ت ل ا س ر ا م ز لى
- لىل ع ا ن ب ، AP ن م ن ا ر ت ق ا ل ا ة ب ا ج ت س ا لىل ف DH لى ص ا ف ت لىل ع ل و ص ح ل لىم ع ل ل ن ك م ي AP و لىم ع ل ل ن م ل ك لىل ف ه و ا ش ن ا م تى ، ا ذ ه PMK
- لىم ع ل ل و ل و ص و ل ا ة ط ق ن ن ب ه ا ج ت ا ل ا ة لى ع ا ب ر لىل ف ا ل ا ب ء ح ف ا ص م ث د ح ت ن ا ن ك م ي
- ن ك م م س لىل 802.11r ك ل ذ ل ، ft ن ك م ي ن ا ز ج ع ي ت ن ا ، OWE لىل ف
- د ع ب ت ا ه ا ج ت ا ل ا ة لى ع ا ب ر ء ح ف ا ص م ا ر ج ا لىل ا ج ا تحي ه ن ا ف ، لىم ع ل ل ل و ج ي ا م د ن ع ، ة ر م ل ك لىل ف و ة ك ر ت ش م ة س س و م لىل ف DH ل د ا ب ت
- ة ط ق ن ل ك ل ة لى ر ف ن و ك ت ، ا ه ب ة ص ا خ ل PMKID م د خ ت س ت لىل ل و ص و ل ا ة ط ق ن و لىم ع ل ل ء ا ل م ع و ل و ص و
- ض ع ب لىل ف PMKID س ف ن م د خ ت س لىل ف ن ا ن ك م ي لىل ف ، ل و ص و ل ا ة ط ق ن س ف ن ب لىم ع ل ل ل ص ت ا ا ذ ا PMKID ء ا ش ن ا لىل ع ل و ص و ل ا ة ط ق ن ة ر د ق ن م ر ث ك لىل ف م د خ ت ا ذ ا ، ت ا ه و ل ر ا ن لىل ف ق ر ط ة ع ب ر ا ب ء ح ف ا ص م ل ل PMKID س ف ن م د خ ت س لىل ف ن ا ن م م ر ل لىل ع ، لىل ف

ل ا ل م :

ن م ل ك لىل ف ه س ف ن PMKID ة د ه ا ش م ل ك ن ك م لىل ف ، ل و ص و ل ا ة ط ق ن س ف ن ب لىم ع ل ل ل ص ت ا ا ذ ا ة لى و ر ل ك ن ك م لىل ف ، "ن ا ر ت ق ا ل ا" ة ب ا ج ت س ا لىل ف Association-Request و Association-Response. PMKID س ف ن م د خ ت س ت ن ا ك ا ذ ا DH لىل ف ص ا ف ت

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-Transition"
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-Transition"
Frame 8522: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits) on interface 0							
Ethernet II, Src: Intel(R) Dual Band Wireless-AC (88:ee:13:e8:a8:cd:5b), Dst: Intel(R) Dual Band Wireless-AC (88:ee:13:e8:a8:cd:5b)							
Radiotap Header v0, Length 36							
802.11 radio information							
IEEE 802.11 Association Request, Flags:							
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 D1.0)							
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							

PMKID س ف ن م ا د خ ت س : 14- ة ر و ص ل ا

No.	Time	Source	Destination	Protocol	Length	Sequence Number (BE)	PMKID	Info
8527	2025-01-21 09:51:57.333153	Cisco_dd12e: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								

هسفن PMKID عم ةي عمجل ةباجتسإ: 15-ةروصولا

ةيكل لسلاللا ةي ل حمل م ةك بشلل ي ف م كحتل رصنع نم اي ودي لي عمل اذه فذب مق ، رابتخالل سفن لي عمل لسري ، تقولا اذه ي ف ، لوصول ةطقن سفن ب ىرأ ةرم هنارتقا متو (WLC) نارتقالا ةباجتسإ ي ف DH لي صافات لوصول ةطقن لسرت كلذ عم و PMKID.

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_dd12e: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								

DH لي صافات عم PMKID سفن لي عمل لسرأ ، فنجل ادب: 16-ةروصولا

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 (CCM) > Pairwise Cipher Suite Count: 1 > Pairwise Cipher Suite List 00:0fac (Ieee 802.11) AES (CCM) > Auth Key Management (AKM) Suite Count: 1 > Auth Key Management (AKM) List 00:0fac (Ieee 802.11) Opportunistic Wireless Encryption > RSN Capabilities: 00000000 > PMKID Count: 0 > PMKID List > Group Management Cipher Suite: 00:0fac (Ieee 802.11) BIP (128) > Tag: Vendor Specific: Microsoft Corp.: WMM/WM: Parameter Element > Tag: HT Capabilities (802.11n D1.10) > Tag: HT Information (802.11n D1.10) > Tag: Extended Capabilities (8 octets) > Tag: VHT Capabilities > Tag: VHT Operation > Tag: RM Enabled Capabilities (5 octets) > Tag: 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 73 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								

أب صاخال دي دجال PMKID عاشن إال DH مقي لوصولو ةطقن مدختست :17-ةروصولا

عارج إا نأ PMKID س فن AP لي م عمل او لوصولو ةطقن نم لك مدختسي :لأا ثمل اذه يف "M1 و M2" لئاسر نم ققحت ،هأجت إال ةيعابر ةحفاصم

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: 0x0000 > Key Length: 16 > Replay Counter: 0 > WPA Key Nonce: 17 28 f4 7a c2 42 74 21 f3 7f 1b 43 b6 f6 94 71 ea f8 a1 a7 8f eb 2e 10 83 d1 88 c5 a2 e0 5d ed > Key IV: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 > WPA Key RSC: 00 00 00 00 00 00 00 00 > WPA Key ID: 00 00 00 00 00 00 00 00 > WPA Key MIC: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 > WPA Key Data Length: 22 > WPA Key Data: dd 14 00 0f ac 04 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af > Tag: Vendor Specific: Ieee 802.11: RSN PMKID > Tag Number: Vendor Specific (221) > Tag length: 20 > OUI: 00:0fac (Ieee 802.11) > Vendor Specific OUI Type: 4 > Data Type: PMKID KDE (4) > PMKID: 21 b5 50 da b0 a3 35 c3 55 e7 f4 da a4 a6 33 af								

PMKID س فن نامدختسي نألال لي م عمل او AP :18-ةروصولا

م ةفل تخم PMKID مادختساب AP نكلو PMKID س فن مدختسي يذل لي م عمل :لأا ثمل اذه يف "M1 و M2" لئاسر نم ققحت ،لي م عمل فذح دعب اهؤاشن

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

ف ل تخم PMKID م اد خ ت سا ب ل ي م ع ل ا و AP : 19-ة ر و ص ل

RA: ع ب ت ت ل خ ا د ن م

PMK. ل ه و ا ش ن ا م ت ا م م AP ج ل ا ع و ن ا ر ت ق ا ل ا ب ل ط ي ف DH ت ا م ل ع م ل ي م ع ل ل س ر ا : ل ا ث م ل ا ذ ه ي ف

```

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

```

ة ط ق ن ، ت ق و ل ا ذ ه ي ف ، ل و ص و ل ا ة ط ق ن س ف ن ب ل ص ت ي ي ذ ل ا ه س ف ن ل ي م ع ل ا م ق ي م ل ، ا ذ ه د ع ب
دي د ج PMKID اء ا ش ن ا ب (AP) ل و ص و ل ا

```

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

```

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م ج ر ت
م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م ج ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م م ج ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م ج ر ت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا م ج ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems
(ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا