تأكد من أساليب شبكة 802.11 المحلية اللاسلكية (WLAN) والتجوال السريع الآمن على Cuwn

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
الأمان من أعلى مستوى بمحول التجوال
WPA/WPA2-PSK
WPA/WPA2-EAP
CCKM مع التجوال السريع الآمن
CCKM مع FlexConnect
CCKM مع أيزم
CCKM مع بطاخ
تخزين المؤقت للمفاتيح/التخزين المؤقت للمفاتيح الذكاء المستخدم بالسريع الآمن للتجوال
تخزين المؤقت للمفاتيح الذكاء / PMKID للتخزين المؤقت للمفاتيح الذكاء مع FlexConnect
تخزين المؤقت للمفاتيح الذكاء / PMKID للتخزين المؤقت للمفاتيح الذكاء مع PROS
تخزين المؤقت للمفاتيح الذكاء / PMKID للتخزين المؤقت للمفاتيح الذكاء مع بطاخ
تخزين المؤقت للمفاتحات الانتهازي مع التخزين المؤقت للمفاتحات الانتهازي السريع للتجوال
تخزين المؤقت للمفاتحات الانتهازي مع التخزين المؤقت للمفاتحات الانتهازي مع FlexConnect
تخزين المؤقت للمفاتحات الانتهازي مع التخزين المؤقت للمفاتحات الانتهازي مع PROS
تخزين المؤقت للمفاتحات الانتهازي مع التخزين المؤقت للمفاتحات الانتهازي مع CONS
"تخزين المؤقت المستباق للمفاتيح" حل مصطلح لوحة ملاحظة
مقسم المصادقة المتكامل مع السريع الآمن للتجوال
مقسم المصادقة المتوافق مع PROS
مقسم المصادقة المتوافق مع بطاخ
802.11r مع السريع الآمن للتجوال
BSS الانتقالي عبر السريع الهواء
BSS الانتقالي عبر السريع DS
802.11r الارطاز مع FlexConnect تقنية
802.11r مع تأزيم
802.11r مع CONS
802.11r Adaptive
الخلاصة
معلومات ذات صلة

المقدمة

يصف هذا المستند أنواع التوجيه اللاسلكي والسرعة التأمين المتاحة لشبكات IEEE 802.11 المحلية اللاسلكية (WLANs) على الشبكة اللاسلكية الموحدة (CUWN).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- المعيار IEEE 802.11 WLAN Fundamentals
- أمان IEEE 802.11 WLAN
- أساسيات IEEE 802.1x/EAP

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى برنامج Cisco WLAN Controller Software، الإصدار 7.4.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

تستند المعلومات الواردة في هذا المستند إلى برنامج Cisco WLAN Controller Software، الإصدار 7.4، ولكن يمكن تطبيق المواضيع على مظم مخرجات تصحيح الأخطاء والسلوكيات الموضحة. تبقى الطرق الموضحة أيضا صالحة لأي إصدار برنامج مدعوم التي تمت مناقشتها. في شبكة المحلية اللاسلكية (WLAN) من Cisco يتم تكوين وحدة التحكم في زوم أسفل هذه النقطة (حتى الإصدار 8.3 عندما تحدث هذه المقالة).

يصف هذا المستند الأنواع المختلفة من طرق التوجيه اللاسلكي والتوجيه السريع الآمن المتاحة لشبكات IEEE 802.11 المحلية اللاسلكية (WLANs) المدعومة على شبكة Cisco اللاسلكية الموحدة (CUWN).

الغرض هو توفير الوثيقة جميع التفاصيل حول كيفية عمل كل طريقة وأيضا كيفية تكوينها. وفوائدها، وعيوب كل طريقة. يتم توفير أمثلة على تصحيح أخطاء وحدة تحكم الشبكة المحلية اللاسلكية (WLC)، ويتم إستخدام صور الحزم اللاسلكية لتحليل الأحداث التي تحدث لكل طريقة توجيه موصوفة وشرحها.

قبل تقديم وصف لمختلف طرق التوجيه السريعة التأمين المتاحة لشبكات WLAN، من المهم فهم كيفية عمل عملية اقتران WLAN، وكيفية حدوث حدث توجيه عادي عند عدم تكوين تأمين على معرف مجموعة الخدمة (SSID).

عندما يتصل عميل لاسلكي 802. 11 بنقطة وصول (AP)، قبل أن يبدأ في تمرير حركة مرور البيانات (إطارات البيانات اللاسلكية)، يجب أولا أن يجتاز عملية مصادقة النظام المفتوحة، يجب إكمال عملية الاقتران. بعد ذلك، تشبه عملية مصادقة النظام المفتوحة اتصال الكبل في نقطة الوصول التي يحددها العميل. وهذه نقطة مهمة للغاية، ولأن العميل اللاسلكي هو المبادئ من يحدد نقطة الوصول المفضلة، ويبني القرار على عوامل متعددة تختلف بين الموردين. ولهذا السبب يبدأ العميل هذه العملية بإرسال إطار

المصادقة إلى نقطة الوصول المحددة، كما هو موضح الحالة في هذا المستند. الآن يمكن لنقطة الوصول أن تطلب منك إنشاء اتصال.

بمجرد اكتمال عملية مصادقة النظام المفتوح بنجاح مع إستجابة من نقطة الوصول (AP) ("الكل متصل")، تنتهي عملية القتران بشكل أساسي من 802.11 ضوابط الطبقة 2 (L2) الذي يؤسس الارتباط بين العميل ونقطة الوصول. تقوم نقطة الوصول بتعيين معرف القتران للعميل في حالة نجاح الاتصال، وتقوم بتجهيزه من أجل تمرير حركة المرور وأ تنفيذ أسلوب تأمين عالي المستوى في حالة تكوينه على SSID. تتألف عملية مصادقة النظام المفتوح من إطاري للإدارة بالإضافة إلى عملية القتران. المصادقة وإطارات القتران هي **إطارات إدارة** لاسلكية، وليست إطارات بيانات، وهي أساسا الإطارات المستخدمة لعملية الاتصال بنقطة الوصول (AP).

فيما يلي صورة للإطارات اللاسلكية عبر الهواء لهذه العملية:

No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:68:d0	84:78:ac:f0:68:d0	802.11	2462	Authentication, SN=2443, FN=0, Flags=....
2	0.000784	Cisco_f0:68:d0	Aironet_b7:ab:5c	84:78:ac:f0:68:d0	802.11	2462	Authentication, SN=2771, FN=0, Flags=....
3	0.002428	Aironet_b7:ab:5c	Cisco_f0:68:d0	84:78:ac:f0:68:d0	802.11	2462	Association Request, SN=2444, FN=0, Flags
4	0.007122	Cisco_f0:68:d0	Aironet_b7:ab:5c	84:78:ac:f0:68:d0	802.11	2462	Association Response, SN=2772, FN=0, Flag
5	0.995428	0.0.0.0	255.255.255.255	84:78:ac:f0:68:d0	DHCP	2462	DHCP Discover - Transaction ID 0xba2bf0a4
6	2.996191	1.1.1.1	172.30.6.67	84:78:ac:f0:68:d0	DHCP	2462	DHCP Offer - Transaction ID 0xba2bf0a4
7	2.998532	0.0.0.0	255.255.255.255	84:78:ac:f0:68:d0	DHCP	2462	DHCP Request - Transaction ID 0xba2bf0a4
8	3.005016	1.1.1.1	172.30.6.67	84:78:ac:f0:68:d0	DHCP	2462	DHCP ACK - Transaction ID 0xba2bf0a4

ملاحظة: إذا كنت تريد معرفة المزيد عن تشذيب 802.11 اللاسلكي، وحول المرشحات/الألوان المستخدمة على Wireshark للصور التي تظهر في هذا المستند، فعليك زيارة منشور مجتمع دعم Cisco الذي يسمى تحليل صورة sniffer 802.11.

يبدأ العميل اللاسلكي إطار المصادقة، وترد نقطة الوصول بإطار مصادقة آخر. يرسل العميل بعد ذلك إطار طلب القتران، وتنتهي نقطة الوصول في رد باستخدام إطار "إستجابة القتران". كما هو موضح من حزم DHCP، بمجرد تمرير عمليات مصادقة النظام المفتوح 802.11 والقتران، يبدأ العميل في تمرير إطارات البيانات. في هذه الحالة، ال يوجد طريقة أمان مكونة على SSID، لذلك يبدأ العميل على الفور بإرسال إطارات البيانات (في هذه الحالة DHCP) التي ال يتم تشفيرها.

كما هو موضح الحالة في هذا المستند، في حالة تمكين الأمان على SSID، فهناك إطارات مصادقة وتشفير أعلى مستوى لطريقة الأمان المحددة، بعد إستجابة القتران مباشرة وقبل إرسال أي إطارات بيانات حركة مرور عميل، مثل DHCP وبروتوكول تحليل العنوان (ARP) وحزم التطبيقات التي يتم تشفيرها. يمكن إرسال إطارات البيانات فقط حتى تتم مصادقة العميل بالكامل، ويتم التفاوض على مفاتيح التشفير، استنادا إلى طريقة الأمان التي تم تكوينها.

بناء على الصورة السابقة، فيما يلي الرسائل التي تراها في مخرجات أمر **debug client** عندما يبدأ العميل اللاسلكي القتران بشبكة المحلية اللاسلكية **أخطاء** WLC (WLAN):

```
*apfMsConnTask_0: Jun 21 18:55:14.221: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID 84:78:ac:f0:68:d0
!--- This is the Association Request from the wireless client
     to the selected AP.

*apfMsConnTask_0: Jun 21 18:55:14.222: 00:40:96:b7:ab:5c
```

```
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d0
  (status 0) ApVapId 1 Slot 0
!--- This is the Association Response from the AP to the client.
```

ملاحظة: تصحيح أخطاء WLC المستخدم للمخرجات الموضحة في هذا المستند هو الأمر **debug client**، وتظهر الأمثلة بعض الرسائل ذات الصلة فقط، وليس الإخراج بالكامل. لمزيد من التفاصيل حول أمر تصحيح الأخطاء هذا، راجع المستند المسمى [فهم عميل تصحيح الأخطاء على وحدات التحكم في الشبكة المحلية اللاسلكية (WLCs)](#).

تظهر هذه الرسائل إطارات الاستجابة وطلب القارنة؛ التي تم تسجيل إطارات المصادقة الأولية في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لأن عملية المصافحة هذه تحدث بسرعة على مستوى نقطة الوصول على CUWN.

أية معلومات تظهر عندما يجول الزبون؟ يتبادل العميل دائما أربعة إطارات إدارية عند تأسيس اتصال بنقطة وصول، والذي يرجع إما إلى تأسيس العميل للاقتران أو إلى حدث تجوال. لم يتم إنشاء سوى اتصال واحد للعميل لنقطة وصول واحدة فقط في كل مرة. الفرق الوحيد في تبادل الإطارات بين اتصال جديد بالبنية الأساسية للشبكة المحلية اللاسلكية (WLAN) وحدث تجوال هو أن إطارات الاقتران الخاصة بحدث تجوال تسمى إطارات **إعادة** التعيين، والتي تشير إلى أن العميل يقوم بالتجوال من نقطة وصول أخرى دون محاولة إنشاء اقتران جديد بالشبكة المحلية اللاسلكية (WLAN). يمكن أن تحتوي هذه الإطارات على عناصر مختلفة يتم إستخدامها للتفاوض على حدث التجوال؛ يعتمد ذلك على الإعداد، ولكن هذه التفاصيل خارج نطاق هذا المستند.

فيما يلي مثال على تبادل الإطارات:

No.	Time	Source	Destination	BSSId	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:2a:90	84:78:ac:f0:2a:90	802.11	2437	Authentication, SN=2611, FN=0, Flags=.....
2	0.001608	Cisco_f0:2a:90	Aironet_b7:ab:5c	84:78:ac:f0:2a:90	802.11	2437	Authentication, SN=3010, FN=0, Flags=.....
3	0.003248	Aironet_b7:ab:5c	Cisco_f0:2a:90	84:78:ac:f0:2a:90	802.11	2437	Reassociation Request, SN=2612, FN=0, Flags
4	0.008122	Cisco_f0:2a:90	Aironet_b7:ab:5c	84:78:ac:f0:2a:90	802.11	2437	Reassociation Response, SN=3011, FN=0, Flag
5	4.291764	Aironet_b7:ab:5c	Broadcast	84:78:ac:f0:2a:90	ARP	2437	Who has 172.30.6.254? Tell 172.30.6.67
6	4.293918	Cisco_f5:4a:40	Aironet_b7:ab:5c	84:78:ac:f0:2a:90	ARP	2437	172.30.6.254 is at 00:1e:f7:f5:4a:40

تظهر هذه الرسائل في إخراج تصحيح الأخطاء:

```
*apfMsConnTask_2: Jun 21 19:02:19.709: 00:40:96:b7:ab:5c
  Reassociation received from mobile on BSSID 84:78:ac:f0:2a:90
!--- This is the Reassociation Request from the wireless client
     to the selected AP.

*apfMsConnTask_2: Jun 21 19:02:19.710: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:90
  (status 0) ApVapId 1 Slot 0
!--- This is the Reassociation Response from the AP to the client.
```

كما هو موضح، يقوم العميل بنجاح بتنفيذ حدث تجوال بعد إرسال طلب إعادة التعيين إلى نقطة الوصول الجديدة، ويستلم إستجابة إعادة التعيين من نقطة الوصول. بما أن العميل لديه عنوان IP بالفعل، فإن إطارات البيانات الأولى هي لحزم ARP.

إذا كنت تتوقع حدثا متنقلا، ولكن العميل يرسل طلب اقتران بدلا من طلب إعادة تعيين (والذي يمكنك تأكيده من بعض الصور وتصحيح الأخطاء المشابهة لتلك الموضحة مسبقا في هذا المستند)، فلن يكون العميل يجول بشكل فعلي. يبدأ العميل اقتران جديد بالشبكة المحلية اللاسلكية (WLAN) كما لو كان قد حدث قطع اتصال، ويحاول إعادة الاتصال من البداية. وقد يحدث ذلك لأسباب متعددة، مثل عندما يبتعد العميل عن نطاق التغطية ثم يجد نقطة وصول ذات جودة إشارة كافية لبدء الاقتران، ولكنها تشير عادة إلى مشكلة في العميل أو أنه يبدأ في حدث تجوال بسبب مشاكل في برامج التشغيل أو البرامج الثابتة أو البرامج.

ملاحظة: يمكنك التحقق من دورة العميل اللاسلكي لتحديد سبب المشكلة.

التجوال بمستوى أعلى من الأمان

في حالة تكوين SSID باستخدام مستوى تأمين أعلى من المستوى L2 بالإضافة إلى مصادقة نظام 802.11 الأساسية المفتوحة، يتطلب الأمر مزيدا من الإطارات للقارنة الأولي والتجوال. تم وصف طريقتي الأمان الأكثر شيوعا اللتين تم توحيدهما وتطبيقهما لشبكات 802.11 WLAN في هذه الوثيقة:

- **WPA/WPA2-PSK (مفاتيح مشتركة مسبقا)** - مصادقة العملاء باستخدام مفاتيح مشتركة مسبقا.
- **WPA/WPA2-EAP (بروتوكول المصادقة الموسع)** - مصادقة العملاء باستخدام طريقة 802. 1X/EAP للتحقق من بيانات الاعتماد الأكثر أمانا من خلال إستخدام خادم المصادقة، مثل الشهادات واسم المستخدم وكلمة المرور والرموز المميزة.

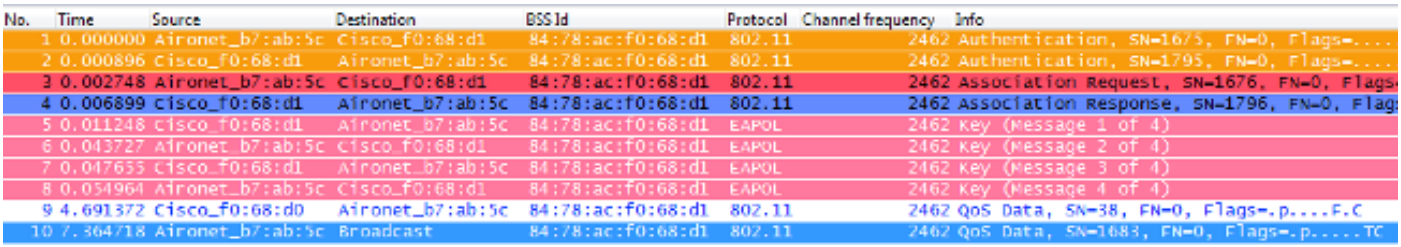
ومن المهم معرفة أنه على الرغم من أن هاتين الطريقتين (PSK و EAP) تثبتان/تحققان من صحة العملاء بطرق مختلفة، فإن كليهما يستخدم أساسا نفس قواعد WPA/WPA2 لعملية إدارة المفاتيح. سواء كان التأمين WPA/WPA2-PSK أو WPA/WPA2-EAP، فإن العملية الموضحة باسم WPA/WPA2 المصافحة رباعية الإتجاه تبدأ التفاوض الرئيسي بين العميل ونقطة الوصول (WLC/AP) كمادة أساسية أصلية بمجرد أن يتم التحقق من صحة العميل باستخدام طريقة مصادقة محددة مستخدمة.

فيما يلي ملخص للعملية:

1. يشتق MSK من مرحلة مصادقة EAP عند إستخدام تأمين 802.1X/EAP، أو من PSK عند إستخدام WPA/WPA2-PSK كطريقة تأمين.
2. من خلال MSK، يستخرج العميل و WLC/AP المفاتيح الرئيسي غير الحكيم (PMK)، وتووم WLC/AP بإنشاء مفاتيح رئيسي للمجموعة (GMK).
3. بمجرد أن يكون هذان المفتاحان الأساسيان جاهزين، يبدأ العميل و WLC/AP مصافحة WPA/WPA2 4-way (والتي يتم توضيحها في هذا القسم من المستند مع بعض صور الشاشة وتصحيح الأخطاء) مع المفاتيح الأساسية كبذور للتفاوض على مفاتيح التشفير الحقيقية.
4. ومفاتيح التشفير النهائية هذه تعرف باسم مفاتيح Pairwise المؤقت (PTK) ومفاتيح المجموعة المؤقت (GTK). يتم اشتقاق PTK من PMK ويتم إستخدامه لتشفير إطارات البث الأحادي مع العميل. يتم اشتقاق مفاتيح المجموعة المؤقت (GTK) من GMK، ويتم إستخدامه لتشفير البث/البث المتعدد على SSID/AP المحدد هذا.

WPA/WPA2-PSK

عند إجراء WPA-PSK أو WPA2-PSK عبر بروتوكول السمة المفاتيح المؤقتة (TKIP) أو معيار التشفير المتقدم (AES) للتشفير، يجب على العميل المرور بالعملية المعروفة باسم مصافحة WPA 4 في الإتجاه لكل من القارنة الأولي وأيضا عند التجوال. وكما سبق شرحه، فإن هذه هي أساسا عملية إدارة المفاتيح المستخدمة لاستخلاص مفاتيح التشفير من PSK، عند إجراء إستخدامه أيضا للتحقق من أن العميل لديه WPA/WPA2. وهو ذلك، تم تبني هذه العملية لحل النضمام إلى شبكة WLAN. مفاتيح مشترك مسبقا صالحة عند تنفيذ WPA أو WPA2 مع PSK:



No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:68:d1	84:78:ac:f0:68:d1	802.11	2462	Authentication, SN=1675, FN=0, Flags=....
2	0.000896	Cisco_f0:68:d1	Aironet_b7:ab:5c	84:78:ac:f0:68:d1	802.11	2462	Authentication, SN=1795, FN=0, Flags=....
3	0.002748	Aironet_b7:ab:5c	Cisco_f0:68:d1	84:78:ac:f0:68:d1	802.11	2462	Association Request, SN=1676, FN=0, Flags
4	0.006899	Cisco_f0:68:d1	Aironet_b7:ab:5c	84:78:ac:f0:68:d1	802.11	2462	Association Response, SN=1796, FN=0, Flag
5	0.011248	Cisco_f0:68:d1	Aironet_b7:ab:5c	84:78:ac:f0:68:d1	EAPOL	2462	Key (Message 1 of 4)
6	0.043727	Aironet_b7:ab:5c	Cisco_f0:68:d1	84:78:ac:f0:68:d1	EAPOL	2462	Key (Message 2 of 4)
7	0.047655	Cisco_f0:68:d1	Aironet_b7:ab:5c	84:78:ac:f0:68:d1	EAPOL	2462	Key (Message 3 of 4)
8	0.054964	Aironet_b7:ab:5c	Cisco_f0:68:d1	84:78:ac:f0:68:d1	EAPOL	2462	Key (Message 4 of 4)
9	4.691372	Cisco_f0:68:d0	Aironet_b7:ab:5c	84:78:ac:f0:68:d1	802.11	2462	QoS Data, SN=38, FN=0, Flags=.p....F.C
10	7.364718	Aironet_b7:ab:5c	Broadcast	84:78:ac:f0:68:d1	802.11	2462	QoS Data, SN=1683, FN=0, Flags=.p.....TC

كما هو موضح، بعد مصادقة النظام المفتوح وقبل المعيار 802.11 وعملية الاقتران، توجد أربعة إطارات EAPOL من مصافحة WPA رباعية الاتجاهات، والتي يتم استدلالها من قبل نقطة الوصول مع **الرسالة-1**، ويتنهي منها من قبل العميل باستخدام **الرسالة-4**. بعد مصافحة ناجحة، يبدأ العميل بتمرير إطارات البيانات (مثل DHCP)، والتي يتم تشفيرها في هذه الحالة بالمفاتيح المشتقة من مصافحة رباعية الإتجاه (ولهذا السبب لا يمكن رؤية المحتوى الفعلي لحركة مرور البيانات ونوعها من الصور اللاسلكية).

> **ملاحظة**: يتم إستخدام إطارات EAPOL لنقل جميع إطارات الإدارة الأساسية وإطارات المصادقة 802.1X/EAP عبر الهواء بين نقطة الوصول والعميل، ويتم إرسالها كإطارات بيانات لاسلكية.

تظهر هذه الرسائل في مخرجات تصحيح الأخطاء:

```
*apfMsConnTask_0: Jun 21 19:30:05.172: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID 84:78:ac:f0:68:d1
*apfMsConnTask_0: Jun 21 19:30:05.173: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d1
  (status 0) ApVapId 2 Slot 0
!--- The Association handshake is finished.

*dot1xMsgTask: Jun 21 19:30:05.178: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00
!--- Message-1 of the WPA/WPA2 4-Way handshake is sent
     from the WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.289: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.289: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2)
  from mobile 00:40:96:b7:ab:5c
!--- Message-2 of the WPA/WPA2 4-Way handshake is successfully
     received from the client.

*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.290: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- Message-3 of the WPA/WPA2 4-Way handshake is sent
     from the WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.309: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 19:30:05.310: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
!--- Message-4 (final message) of the WPA/WPA2 4-Way handshake
     is successfully received from the client, which confirms
     the installation of the derived keys. They can now be used in
```

```
order to encrypt data frames with current AP.
```

عند التجوال، يتعقب العميل بشكل أساسي نفس عملية تبادل الإطارات، حيث يلزم مصافحة WPA 4-way من أجل اشتقاق مفاتيح تشفير جديدة مع نقطة الوصول الجديدة. ويرجع ذلك إلى الأسباب الأمنية التي أرساها المعيار، وإلى أن نقطة الوصول الجديدة لا تعرف المفاتيح الأصلية. الفرق الوحيد هو أن هناك إطارات إعادة تشكيل بدلا من إطارات الاقتران، كما هو موضح في هذه الصورة:

No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:2a:91	84:78:ac:f0:2a:91	802.11	2437	Authentication, SN=2356, FN=0, Flags=.....
2	0.000846	Cisco_f0:2a:91	Aironet_b7:ab:5c	84:78:ac:f0:2a:91	802.11	2437	Authentication, SN=3694, FN=0, Flags=.....
3	0.004296	Aironet_b7:ab:5c	Cisco_f0:2a:91	84:78:ac:f0:2a:91	802.11	2437	Reassociation Request, SN=2357, FN=0, Flags
4	0.010867	Cisco_f0:2a:91	Aironet_b7:ab:5c	84:78:ac:f0:2a:91	802.11	2437	Reassociation Response, SN=3695, FN=0, Flag
5	0.013109	Cisco_f0:2a:91	Aironet_b7:ab:5c	84:78:ac:f0:2a:91	EAPOL	2437	Key (Message 1 of 4)
6	0.034339	Aironet_b7:ab:5c	Cisco_f0:2a:91	84:78:ac:f0:2a:91	EAPOL	2437	Key (Message 2 of 4)
7	0.041124	Cisco_f0:2a:91	Aironet_b7:ab:5c	84:78:ac:f0:2a:91	EAPOL	2437	Key (Message 3 of 4)
8	0.056241	Aironet_b7:ab:5c	Cisco_f0:2a:91	84:78:ac:f0:2a:91	EAPOL	2437	Key (Message 4 of 4)
9	0.695758	Aironet_b7:ab:5c	Broadcast	84:78:ac:f0:2a:91	802.11	2437	QoS Data, SN=2360, FN=0, Flags=.p..R..TC
10	0.698357	Cisco_f5:4a:40	Aironet_b7:ab:5c	84:78:ac:f0:2a:91	802.11	2437	QoS Data, SN=42, FN=0, Flags=.p....F.C

ستبدو الرسائل نفسها في مخرجات تصحيح الأخطاء، ولكن الحزمة الأولى من العميل هي إعادة تعيين بدلا من اقتران، كما هو موضح ومشروح مسبقا.

WPA/WPA2-EAP

عند إستخدام طريقة 802. 1X/EAP لمصادقة العملاء على SSID آمن، هناك المزيد من الإطارات المطلوبة قبل أن يبدأ العميل في تمرير حركة مرور البيانات. يتم إستخدام هذه الإطارات الإضافية لمصادقة بيانات اعتماد العميل، وتبعا لطريقة EAP، يمكن أن يكون هناك بين أربعة وعشرين إطارا. وتأتي هذه بعد الاقتران/إعادة الاندماج، ولكن قبل مصافحة WPA/WPA2 4-way، لأن مرحلة المصادقة تستمد MSK المستخدم كبداية لإنشاء مفاتيح التشفير النهائي في عملية إدارة المفاتيح (المصافحة بأربعة طرق).

تعرض هذه الصورة مثالا للإطارات المتبادلة عبر الهواء بين نقطة الوصول والعميل اللاسلكي في الاقتران الأولي عند تنفيذ WPA مع PEAPv0/EAP-MSCHAPv2:

No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	802.11	2462	Authentication, SN=2465, FN=0, Fla
2	0.000783	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	802.11	2462	Authentication, SN=275, FN=0, Flag
3	0.002579	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	802.11	2462	Association Request, SN=2466, FN=0
4	0.007765	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	802.11	2462	Association Response, SN=276, FN=0
5	0.012140	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Identity
6	0.052606	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAPOL	2462	Start
7	0.055257	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Identity
8	0.061197	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAP	2462	Response, Identity
9	0.081402	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
10	0.117423	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Client Hello
11	0.145293	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
12	0.167145	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAP	2462	Response, Protected EAP (EAP-PEAP)
13	0.183267	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
14	0.196221	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAP	2462	Response, Protected EAP (EAP-PEAP)
15	0.201527	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
16	0.210076	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Certificate, Client Key Exchange,
17	0.220032	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
18	0.222784	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAP	2462	Response, Protected EAP (EAP-PEAP)
19	0.227233	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
20	0.291267	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Application Data, Application Data
21	0.291862	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Application Data, Application Data
22	0.295816	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
23	0.297766	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Application Data, Application Data
24	0.304666	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
25	0.313817	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
26	0.315942	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Application Data, Application Data
27	0.321376	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Request, Protected EAP (EAP-PEAP)
28	0.323863	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	TLSv1	2462	Application Data, Application Data
29	0.328766	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAP	2462	Success
30	0.330360	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAPOL	2462	Key (Message 1 of 4)
31	0.334225	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAPOL	2462	Key (Message 2 of 4)
32	0.338645	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	EAPOL	2462	Key (Message 3 of 4)
33	0.341932	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	EAPOL	2462	Key (Message 4 of 4)
34	1.366605	Cisco_f0:68:d8	Aironet_b7:ab:5c	84:78:ac:f0:68:d8	802.11	2462	QoS Data, SN=448, FN=0, Flags=.p..
35	1.383200	Aironet_b7:ab:5c	Cisco_f0:68:d8	84:78:ac:f0:68:d8	802.11	2462	QoS Data, SN=2482, FN=0, Flags=.p.

في بعض الأحيان، يظهر هذا التبادل إطارات أكثر أو أقل، والتي تعتمد على عوامل متعددة، مثل طريقة EAP، أو إعادة الإرسال بسبب مشاكل، أو سلوك العميل (مثل طلبي الهوية في هذا

المثال، لأن العميل يرسل **بداية EAPOL** بعد أن ترسل نقطة الوصول أول طلب هوية)، أو إذا كان العميل قد تباطأ الشهادة مع الخادم بالفعل. كلما تم تكوين SSID لطريقة 802.1X/EAP، هناك المزيد من الإطارات (للمصادقة)، وبالتالي، فإنه يتطلب المزيد من الوقت قبل أن يبدأ العميل في إرسال إطارات البيانات.

هنا ملخص لرسائل تصحيح الأخطاء:

```
*apfMsConnTask_0: Jun 21 23:41:19.092: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID 84:78:ac:f0:68:d8
*apfMsConnTask_0: Jun 21 23:41:19.094: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d8
  (status 0) ApVapId 9 Slot 0
!--- The Association handshake is finished.

*dot1xMsgTask: Jun 21 23:41:19.098: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 1)
!--- The EAP Identity Request is sent to the client once it is
     associated in order to begin the higher-level authentication
     process. This informs the client that an identity to start
     this type of 802.1X/EAP authentication must be provided.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.226: 00:40:96:b7:ab:5c
  Received EAPOL START from mobile 00:40:96:b7:ab:5c
!--- The wireless client decides to start the EAP authentication
     process, and informs the AP with an EAPOL START data frame.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.227: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 2)
!--- WLC/AP sends another EAP Identity Request to the client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.235: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.235: 00:40:96:b7:ab:5c
  Received Identity Response (count=2) from mobile 00:40:96:b7:ab:5c
!--- The client responds with an EAP Identity Response on an EAPOL
     frame.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.301: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.301: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 3)
!--- Once the WLC/AP sends the client response to the Authentication
     Server on a RADIUS Access-Request packet, the server responds
     with a RADIUS Access-Challenge in order to officially start the
     EAP negotiation, handshake, and authentication with the client
     (sometimes with mutual authentication, dependent upon the EAP
     method). This response received by the WLC/AP is sent to the client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.344: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.344: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 3, EAP Type 25)
!--- The client responds with an EAP Response on an EAPOL frame, which
     is sent to the Authentication Server on a RADIUS Access-Request
     packet. The server responds with another RADIUS Access-Challenge.
     This process continues, dependent upon the EAP method (the exchange
     of certificates when used, the building of TLS tunnels, validation
```

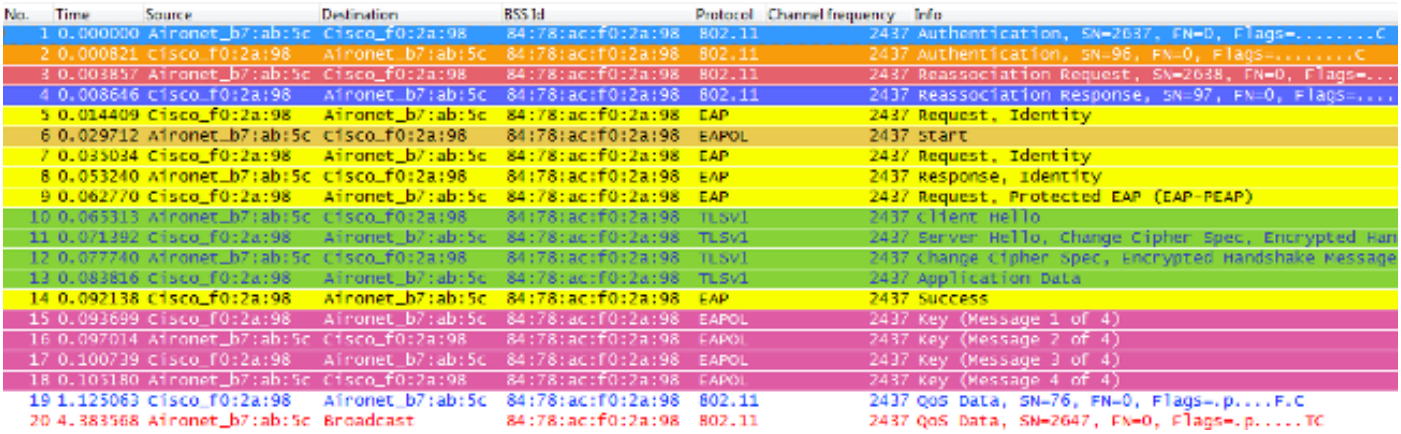
of client credentials, client validation of server identity when applicable). Hence, the next few messages are basically the same on the WLC/AP side, as this acts as a "proxy" between the client and the Authentication Server exchanges.

```
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.347: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.347: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 4)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.375: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.375: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 4, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.377: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.377: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 5)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.403: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.403: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 5, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.404: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.404: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 6)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.414: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.414: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 6, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.421: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.421: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 7)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.425: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.425: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 7, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.427: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c
```

```
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.427: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 8)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.434: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.434: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 8, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.436: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.436: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 9)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.440: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.440: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 9, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.442: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.442: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 10)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.449: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.449: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 10, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.452: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.452: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 11)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.457: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.457: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 11, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.459: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.459: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 13)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.469: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.469: 00:40:96:b7:ab:5c
```

```
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 13, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.472: 00:40:96:b7:ab:5c
  Processing Access-Accept for mobile 00:40:96:b7:ab:5c
!--- The authentication finishes and is successful for this client,
      so the RADIUS Server sends a RADIUS Access-Accept to the WLC/AP.
      This RADIUS Access-Accept comes with the special attributes
      that are assigned to this client (if any are configured on the
      Authentication Server for this client). This Access-Accept also
      comes with the MSK derived with the client in the EAP
      authentication process, so the WLC/AP installs it in order to
      initiate the WPA/WPA2 4-Way handshake with the wireless client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.473: 00:40:96:b7:ab:5c
  Sending EAP-Success to mobile 00:40:96:b7:ab:5c
  (EAP Id 13)
!--- The accept/pass of the authentication is sent to the client as
      an EAP-Success message.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.473: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00
!--- Message-1 of the WPA/WPA2 4-Way handshake is sent from the
      WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.481: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.481: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2)
  from mobile 00:40:96:b7:ab:5c
!--- Message-2 of the WPA/WPA-2 4-Way handshake is successfully
      received from the client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.481: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- Message-3 of the WPA/WPA2 4-Way handshake is sent from the
      WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.487: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 21 23:41:19.487: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
!--- Message-4 (final message) of the WPA/WPA2 4-Way handshake
      is successfully received from the client, which confirms the
      installation of the derived keys. They can now be used in
      order to encrypt data frames with the current AP.
```

لاوجا بولسلا قيبطت نود يداعلا كلسلاللا يملعلا يجري امدنع) ةداعإ بلط سيستخدم يملعلا نأ هو يحيولا قرفلا .روصلا يف حضوم وه امك ةقداصملا ةكرتشملا ةمئاقلا مداخ لبق نم ةقداصم ءارجإ وهو يملعلا رورملا سفن ىلع يملعلا بجي ،(نيمأتلا سيرع ام ،ىرخأ لوصو ةقطنم نم لاتجاوا لفعلاب ةقثوم ةديدجلا لوصولا ةطقنل ةرادلإا جاتحت ديدج حاتفم ءاشنإو ةلماكلا ةقداصملا ةيلمعلا لاسرإ ىلع يملعلا رورملا ةكرح ديزي:



No.	Time	Source	Destination	BSSId	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	802.11	2437	Authentication, SN=2637, FN=0, Flags=.....C
2	0.000821	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	802.11	2437	Authentication, SN=96, FN=0, Flags=.....C
3	0.003857	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	802.11	2437	Reassociation Request, SN=2638, FN=0, Flags=...
4	0.008646	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	802.11	2437	Reassociation Response, SN=97, FN=0, Flags=....
5	0.014409	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	EAP	2437	Request, Identity
6	0.029712	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	EAPOL	2437	Start
7	0.035084	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	EAP	2437	Request, Identity
8	0.053240	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	EAP	2437	Response, Identity
9	0.062770	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	EAP	2437	Request, Protected EAP (EAP-PEAP)
10	0.065313	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	TLSv1	2437	Client Hello
11	0.071292	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	TLSv1	2437	Server Hello, Change Cipher Spec, Encrypted Han
12	0.077740	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	TLSv1	2437	Change Cipher Spec, Encrypted Handshake Message
13	0.083816	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	TLSv1	2437	Application Data
14	0.092138	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	EAP	2437	Success
15	0.093699	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	EAPOL	2437	Key (Message 1 of 4)
16	0.097014	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	EAPOL	2437	Key (Message 2 of 4)
17	0.100739	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	EAPOL	2437	Key (Message 3 of 4)
18	0.105180	Aironet_b7:ab:5c	Cisco_f0:2a:98	84:78:ac:f0:2a:98	EAPOL	2437	Key (Message 4 of 4)
19	1.125063	Cisco_f0:2a:98	Aironet_b7:ab:5c	84:78:ac:f0:2a:98	802.11	2437	QoS Data, SN=76, FN=0, Flags=.p....F.C
20	4.383568	Aironet_b7:ab:5c	Broadcast	84:78:ac:f0:2a:98	802.11	2437	QoS Data, SN=2647, FN=0, Flags=.p.....TC

كما هو موضح، حتى في حالة وجود إطارات أقل من تلك الموجودة في المصادقة الأولية (والتي تتسبب فيها عوامل متعددة كما هو مذكور سابقا)، فإنه في حالة تجول العميل إلى نقطة وصول جديدة، فإنه يجب إتمام عمليات مصادقة EAP وإدارة مفاتيح WPA للاستمرار في تمرير إطارات البيانات (حتى في حالة إرسال حركة مرور البيانات بشكل نشط قبل التجوال). لذلك، إذا كان لدى العميل تطبيق نشط حساس للتأخيرات (مثل تطبيقات حركة مرور الصوت، أو التطبيقات الحساسة للمهلات)، فيمكن للمستخدم إدراك المشاكل عند التجوال، مثل الثغرات الصوتية أو قطع اتصال التطبيق. يعتمد هذا على المدة التي تستغرقها العملية لكي يستمر العميل في إرسال/إستقبال إطارات البيانات. يمكن أن يكون هذا التأخير أطول، معتمدا على: بيئة التردد اللاسلكي، ومقدار العملاء، ووقت الذهاب والعودة بين WLC و LAPs ومع خادم المصادقة، وأسباب أخرى.

فيما يلي ملخص لرسائل تصحيح الأخطاء الخاصة بهذا الحدث المتجول (وهي أساسا نفس الرسائل السابقة، لذا لا يتم وصف هذه الرسائل أكثر):

```
*apfMsConnTask_2: Jun 21 23:47:54.872: 00:40:96:b7:ab:5c
  Reassociation received from mobile on BSSID 84:78:ac:f0:2a:98

*apfMsConnTask_2: Jun 21 23:47:54.874: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:98
  (status 0) ApVapId 9 Slot 0

*dot1xMsgTask: Jun 21 23:47:54.879: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 1)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.895: 00:40:96:b7:ab:5c
  Received EAPOL START from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.895: 00:40:96:b7:ab:5c
  dot1x - moving mobile 00:40:96:b7:ab:5c into Connecting state

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.895: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 2)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.922: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.922: 00:40:96:b7:ab:5c
  Received Identity Response (count=2) from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.929: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.929: 00:40:96:b7:ab:5c
```

```
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 3)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.941: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.941: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 3, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.943: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.943: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 4)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.954: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.954: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 4, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.956: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.957: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 7)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.976: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.976: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 7, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.978: 00:40:96:b7:ab:5c
  Processing Access-Accept for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.978: 00:40:96:b7:ab:5c
  Sending EAP-Success to mobile 00:40:96:b7:ab:5c
  (EAP Id 7)

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.978: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.995: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.995: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2)
  from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 23:47:54.995: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_4: Jun 21 23:47:55.005: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
```

```
*Dot1x_NW_MsgTask_4: Jun 21 23:47:55.005: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
```

هذه هي الطريقة التي يعمل بها 802.1X/EAP و WPA/WPA2 إطار عمل الأمان. لمنع تأثير ذي تطبيق/الخدمة على التأخير من حدث تجوال منتظم، تقوم صناعة WiFi بتطوير وتنفيذ استخدام العديد من طرق التجوال السريعة التأمين من أجل تسريع عملية التجوال عند إجراء التأخير عند الاتصال بشبكة المحلية اللاسلكية (WLAN)/SSID. يواجه العملاء بعض التأمين على الشبكة المحلية اللاسلكية (WLAN). يعالج أمان نشر الخلل من نقاط التجوال بين الوصول أثناء التجوال حركة المرور في تمرير استمراره. EAP وعمليات المصادقة إلى ذلك يرجع .(WLAN) المستوى على الشبكة المحلية اللاسلكية إدارة المفاتيح المطلوبة من إعداد الأمان، كما هو موضح مسبقا.

من المهم أن تفهم أن التجوال السريع الآمن هو مجرد مصطلح تستخدمه الصناعة بالإشارة إلى تنفيذ طريقة/نظام يسرع عملية التجوال عندما يتم تكوين الأمان على الشبكة المحلية اللاسلكية (WLAN). يتم شرح مختلف طرق/مخططات التجوال السريعة التأمين المتاحة لشبكات WLAN، والمدعومة من قبل CUWN، في القسم التالي.

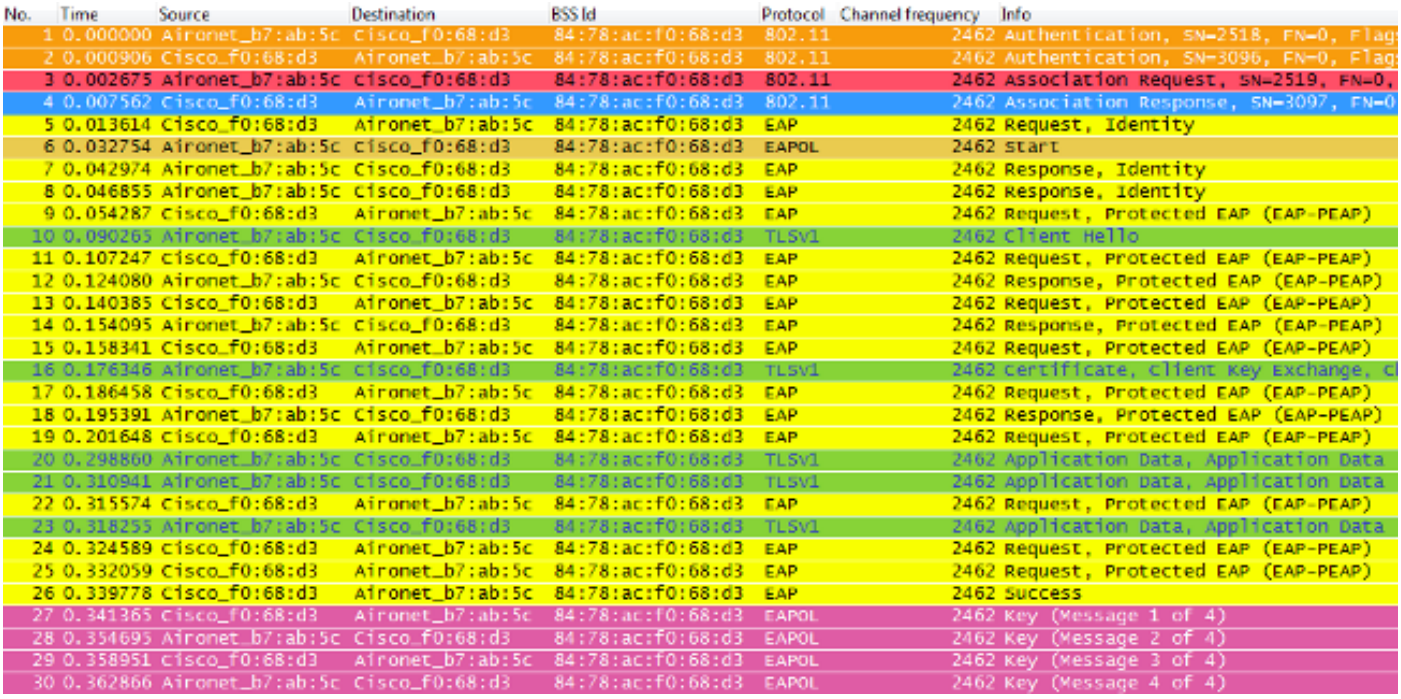
التجوال الآمن السريع مع CCKM

إدارة المفاتيح المركزية من Cisco (CCKM) هي أول طريقة تجوال سريعة الأمان يتم تطويرها وتنفيذها على شبكات WLAN الخاصة بالمؤسسات، والتي تم إنشاؤها بواسطة Cisco كحل يستخدم للحد من التأخيرات التي تم شرحها حتى الآن، عند إستخدام أمان 802.1X/EAP على شبكة WLAN. بما أن هذا برتوكول خاص من Cisco، فإنه مدعوم فقط من قبل أجهزة البنية الأساسية WLAN من Cisco والعملاء اللاسلكيين (من عدة موردين) المتوافقين مع Cisco Compatible Extension (CCX) ل CCKM.

يمكن تنفيذ CCKM باستخدام جميع طرق التشفير المختلفة المتاحة للشبكات المحلية اللاسلكية، لتضمين WEP و TKIP و AES. كما يتم دعم بمعظم طرق مصادقة 802.1X/EAP المستخدمة لشبكات WLAN، اعتمادا على إصدار CCX المدعوم من الأجهزة.

> **ملاحظة**: للحصول على نظرة عامة على محتوى الميزة المدعوم من الإصدارات المختلفة من مواصفات CCX (التي تتضمن أساليب EAP المدعومة)، قم بالرجوع إلى مستند إصدارات CCX ومتازيم، وتحقق من إصدار CCX الذي يدعم عملاؤك اللاسلكيون (إذا كانوا متوافقين مع CCX)، بحيث يمكنك تأكيد ما إذا كان يمكن تنفيذ طريقة الأمان التي ترغب في إستخدامها مع CCKM.

تقدم هذه الصورة اللاسلكية مثال عن الإطارات المتبادلة عند الاقتران المبدئي عند أداء 802.1X/EAP. هذا هو أساس طريقة PEAPv0/EAP-MSCHAPv2 و TKIP كتشفير، مع CCKM. هذه المرة، على الرغم من أن WPA/TKIP مع PEAPv0/EAP-MSCHAPv2 تم إجراؤه، فإن التبادل كما هو نفس التسلسل الهرمي للمفاتيح وطرق تذكرة التخزين المؤقت من أجل تنفيذ التجوال الآمن السريع عندما يتوجب على العميل التجوال:



No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	802.11	2462	Authentication, SN=2518, FN=0, Flag
2	0.000906	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	802.11	2462	Authentication, SN=3096, FN=0, Flag
3	0.002675	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	802.11	2462	Association Request, SN=2519, FN=0,
4	0.007562	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	802.11	2462	Association Response, SN=3097, FN=0
5	0.013614	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Identity
6	0.032754	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAPOL	2462	Start
7	0.042974	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAP	2462	Response, Identity
8	0.046855	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAP	2462	Response, Identity
9	0.054287	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
10	0.090265	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	TLSv1	2462	Client Hello
11	0.107247	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
12	0.124080	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAP	2462	Response, Protected EAP (EAP-PEAP)
13	0.140385	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
14	0.154095	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAP	2462	Response, Protected EAP (EAP-PEAP)
15	0.158341	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
16	0.176346	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	TLSv1	2462	Certificate, Client Key Exchange, C
17	0.186458	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
18	0.195391	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAP	2462	Response, Protected EAP (EAP-PEAP)
19	0.201648	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
20	0.298860	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	TLSv1	2462	Application Data, Application Data
21	0.310941	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	TLSv1	2462	Application Data, Application Data
22	0.315574	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
23	0.318255	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	TLSv1	2462	Application Data, Application Data
24	0.324589	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
25	0.332059	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Request, Protected EAP (EAP-PEAP)
26	0.339778	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAP	2462	Success
27	0.341365	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAPOL	2462	Key (Message 1 of 4)
28	0.354695	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAPOL	2462	Key (Message 2 of 4)
29	0.358951	Cisco_f0:68:d3	Aironet_b7:ab:5c	84:78:ac:f0:68:d3	EAPOL	2462	Key (Message 3 of 4)
30	0.362866	Aironet_b7:ab:5c	Cisco_f0:68:d3	84:78:ac:f0:68:d3	EAPOL	2462	Key (Message 4 of 4)

فيما يلي ملخص لرسائل تصحيح الأخطاء (مع إزالة بعض عمليات تبادل EAP لتقليل المخرجات):

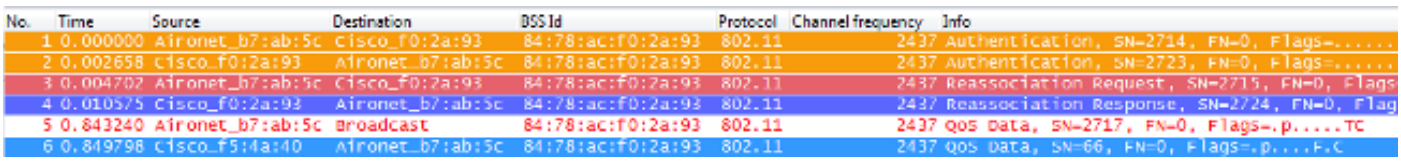
```
*apfMsConnTask_0: Jun 25 15:41:41.507: 00:40:96:b7:ab:5c
  Association received from mobile on BSSID 84:78:ac:f0:68:d3
!--- This is the Association Request from the client.

*apfMsConnTask_0: Jun 25 15:41:41.507: 00:40:96:b7:ab:5c
  Processing WPA IE type 221, length 22 for mobile
  00:40:96:b7:ab:5c
*apfMsConnTask_0: Jun 25 15:41:41.507: 00:40:96:b7:ab:5c
  CCKM: Mobile is using CCKM
!--- The WLC/AP finds an Information Element that claims CCKM
    support on the Association request that is sent from the client.

*apfMsConnTask_0: Jun 25 15:41:41.507: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8
!--- This is the key cache index for this client, which is set temporally.

*apfMsConnTask_0: Jun 25 15:41:41.508: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d3
  (status 0) ApVapId 4 Slot 0
!--- The Association Response is sent to the client.

*dot1xMsgTask: Jun 25 15:41:41.513: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 1)
!--- An EAP Identity Request is sent to the client once it is
     associated in order to begin the higher-level authentication
     process. This informs the client that an identity to start
     this type of 802.1X/EAP authentication must be provided.
     Further EAP messages are not described, as they are basically
     the same as the ones previously-explained.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.536: 00:40:96:b7:ab:5c
  Received EAPOL START from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.536: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
```

```
  (EAP Id 2)

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.546: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.546: 00:40:96:b7:ab:5c
  Received EAP Response packet with mismatching id
  (currentid=2, eapid=1) from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.550: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.550: 00:40:96:b7:ab:5c
  Received Identity Response (count=2) from mobile
  00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.555: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.555: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 3)

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.594: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.594: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 3, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.840: 00:40:96:b7:ab:5c
  Processing Access-Accept for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  Creating a PKC PMKID Cache entry for station 00:40:96:b7:ab:5c
  (RSN 0)<br/ >
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 0
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  CCKM: Create a global PMK cache entry
!--- WLC creates a global PMK cache entry for this client,
     which is for CCKM in this case.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  Sending EAP-Success to mobile 00:40:96:b7:ab:5c
  (EAP Id 13)
!--- The client is informed of the successful EAP authentication.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.841: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  INITPMK(message 1),replay counter 00.00.00.00.00.00.00.00
!--- Message-1 of the initial 4-Way handshake is sent from the
     WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2) from mobile
  00:40:96:b7:ab:5c
!--- Message-2 of the initial 4-Way handshake is received
     successfully from the client.
```

```
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: 00:40:96:b7:ab:5c
  CCKM: Sending cache add
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: CCKM: Sending CCKM PMK
  (Version_1) information to mobility group
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: CCKM: Sending CCKM PMK
  (Version_2) information to mobility group
!--- The CCKM PMK cache entry for this client is shared with
     the WLCs on the mobility group.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.858: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- Message-3 of the initial 4-Way handshake is sent from the
     WLC/AP to the client.

*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.866: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c
*Dot1x_NW_MsgTask_4: Jun 25 15:41:41.866: 00:40:96:b7:ab:5c Received
  EAPOL-key in PTKINITNEGOTIATING state (message 4) from mobile
  00:40:96:b7:ab:5c
!--- Message-4 (final message) of this initial 4-Way handshake
     is received successfully from the client, which confirms the
     installation of the derived keys. They can now be used in order
     to encrypt data frames with the current AP.
```

مع CCKM، يكون الربط الأولي إلى WLAN مماثل إلى WPA/WPA2 العادي، حيث MSK (المعروف أيضا باسم Network Session Key (NSK)) مشتق بشكل متبادل مع العميل وخادم RADIUS. يتم إرسال هذا المفتاح الأساسي من الخادم إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بعد مصادقة ناجحة، ويتم تخزينه مؤقتا كأساس لاشتقاق جميع المفاتيح التالية طوال فترة بقاء اقتران العميل بشبكة WLAN هذه. من هنا، يستخرج عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) والعميل معلومات البداية التي يتم إستخدامها للتواال الآمن السريع استنادا إلى CCKM، يمر هذا من خالل مصافحة رباعية الاتجاهات مماثلة لتلك التي في WPA/WPA2، من أجل إستخراج مفاتيح تشفير البث الأحادي (PTK) والبث المتعدد (GTK) باستخدام نقطة الوصول الأولى.

يالحظ الفرق الكبير عند التجوال. في هذه الحالة، يرسل عميل CCKM إطار طلب إعادة إستدعاء وحيد إلى ال AP/WLC (أن يتضمن MIC وقم عشوائي يتزايد بشكل تسلسلي)، ويوفر معلومات كافية (أن يتضمن ال ap {upper}mac address **-BSSID-**) in order to استخرج ال PTK جديد. مع طلب إعادة التعيين هذا، فإن WLC و AP الجديدة أيضا لديهم معلومات كافية من أجل إستحصال PTK الجديد، لذلك هم ببساطة يستجيبون مع إعادة إستدعاء إستجابة. يمكن للعميل الآن متابعة نقل البيانات، كما هو موضح في هذه الصورة:



No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:2a:93	84:78:ac:f0:2a:93	802.11	2437	Authentication, SN=2714, FN=0, Flags=.....
2	0.002658	Cisco_f0:2a:93	Aironet_b7:ab:5c	84:78:ac:f0:2a:93	802.11	2437	Authentication, SN=2723, FN=0, Flags=.....
3	0.004702	Aironet_b7:ab:5c	Cisco_f0:2a:93	84:78:ac:f0:2a:93	802.11	2437	Reassociation Request, SN=2715, FN=0, Flags
4	0.010575	Cisco_f0:2a:93	Aironet_b7:ab:5c	84:78:ac:f0:2a:93	802.11	2437	Reassociation Response, SN=2724, FN=0, Flag
5	0.843240	Aironet_b7:ab:5c	Broadcast	84:78:ac:f0:2a:93	802.11	2437	QoS Data, SN=2717, FN=0, Flags=.p.....TC
6	0.849798	Cisco_f5:4a:40	Aironet_b7:ab:5c	84:78:ac:f0:2a:93	802.11	2437	QoS Data, SN=66, FN=0, Flags=.p....F.C

فيما يلي ملخص للتصحيحات الخاصة بعنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لهذا الحدث المتجول:

```
*apfMsConnTask_2: Jun 25 15:43:33.749: 00:40:96:b7:ab:5c
  CCKM: Received REASSOC REQ IE
*apfMsConnTask_2: Jun 25 15:43:33.749: 00:40:96:b7:ab:5c
  Reassociation received from mobile on BSSID
  84:78:ac:f0:2a:93
*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
```

```
  Processing WPA IE type 221, length 22 for mobile
  00:40:96:b7:ab:5c
*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  CCKM: Mobile is using CCKM
!--- The Reassociation Request is received from the client,
      which provides the CCKM information needed in order to
      derive the new keys with a fast-secure roam.

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  Setting active key cache index 0 ---> 8

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  CCKM: Processing REASSOC REQ IE

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  CCKM: using HMAC MD5 to compute MIC
!--- WLC computes the MIC used for this CCKM fast-roaming
      exchange.

*apfMsConnTask_2: Jun 25 15:43:33.750: 00:40:96:b7:ab:5c
  CCKM: Received a valid REASSOC REQ IE

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  CCKM: Initializing PMK cache entry with a new PTK
!--- The new PTK is derived.

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 8

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 0

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Creating a PKC PMKID Cache entry for station
  00:40:96:b7:ab:5c (RSN 0) on BSSID 84:78:ac:f0:2a:93
!--- The new PMKID cache entry is created for this new
      AP-to-client association.

*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  CCKM: using HMAC MD5 to compute MIC
*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Including CCKM Response IE (length 62) in Assoc Resp to mobile
*apfMsConnTask_2: Jun 25 15:43:33.751: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:93
  (status 0) ApVapId 4 Slot 0
!--- The Reassociation Response is sent from the WLC/AP to
      the client, which includes the CCKM information required
      in order to confirm the new fast-roam and key derivation.

*dot1xMsgTask: Jun 25 15:43:33.757: 00:40:96:b7:ab:5c
  Skipping EAP-Success to mobile 00:40:96:b7:ab:5c
!--- EAP is skipped due to the fast roaming, and CCKM does not
      require further key handshakes. The client is now ready to
      pass encrypted data frames on the new AP.
```

كما هو موضح، يتم إجراء التجوال السريع والآمن بين نقاط الوصول التي تم تجنب إطارات مصادقة EAP وحتى المزيد من مصافحة أربعة اتجاهات، لأن مفاتيح التشفير الجديدة الزال مشتقة، ولكن التجوال إلى نقطة الوصول التالية يتم إكمال ذلك باستخدام إطارات إعادة تكوين CCKM. وتستند إلى المعلومات التي تم تخزينها مسبقا بواسطة العميل ووحدة التحكم في الشبكة اللاسلكية المحلية (WLC).

FlexConnect مع CCKM

- المصادقة المركزية مدعومة. ويتضمن ذلك تبديل البيانات المحلية والمركزية. يجب أن تكون نقاط الوصول عزاء من مجموعة FlexConnect نفسها.
- المصادقة المحلية المرنة مدعومة. في الوضع المتصل، يمكن توزيع ذاكرة التخزين المؤقت من نقطة الوصول إلى وحدة التحكم ثم إلى باقي نقاط الوصول في مجموعة FlexConnect.
- الوضع المستقل مدعوم. إذا كانت ذاكرة التخزين المؤقت موجودة بالفعل على نقطة الوصول (بسبب التوزيع السابق)، يجب أن تعمل التجوال السريع. لا تدعم المصادقة الجديدة في الوضع المستقل التجوال السريع الآمن.

مزايا مع CCKM

- CCKM هو أسرع طريقة تجوال سريعة الأمان يتم نشرها غالبا على شبكات WLAN الخاصة بالمؤسسات. التي تحتاج العملاء إلى تمرير مصافحة إدارة مفاتيح الاستخلاص مفاتيح جديدة عندما يحدث انتقال بين نقاط الوصول، والتي تطلب من مرة أخرى إجراء مصادقة 802.1X/EAP الكاملة باستخدام نقاط وصول جديدة خلال العمر الافتراضي للعميل على شبكة WLAN هذه.
- يدعم CCKM جميع طرق التشفير المتاحة في معيار 802.11 (WEP، TKIP، و AES)، بالإضافة إلى بعض أساليب Cisco الخاصة القديمة والتي لا تزال تستخدم على العملاء القدامى.

مخاريط مع CCKM

- CCKM هو أسلوب خاص من Cisco، والذي يحد من التنفيذ والدعم لبنية Cisco WLAN الأساسية وعملاء CCX اللاسلكي.
- لم يتم اعتماد CCX الإصدار 5 على نطاق واسع، لذلك فإن CCKM مع WPA2/AES غير مدعوم من قبل العديد من عملاء CCX اللاسلكيين (ويرجع ذلك أساسا إلى أن معظمهم جدا). التي لا تزال آمنة، والتي لا تزال تدعم CCKM بالفعل مع WPA/TKIP

التجوال السريع الآمن باستخدام ذاكرة التخزين المؤقت للمفاتيح/التخزين المؤقت للمفاتيح اللاصقة

يعتبر التخزين المؤقت لمعرف Key (PMKID) وأ **التخزين المؤقت للمفاتيح اللاصقة** (SKC) 802.11i، حيث 802.11 في تعديل الأمان لطريقة تجوال سريعة التأمين يقترحها معيار IEEE أول طريقة تجوال سريعة التأمين هذه كطريقة إختيارية لأجهزة WPA2 من أجل تحسين تقنية التجوال السريع التأمين هذه. تمت إضافة يكون الغرض الرئيسي هو توحيد مستوى عال من الأمان لشبكات WLAN. تنفيذ هذه التأمين عند التجوال.

وهذا مما يمكن أن يحدث في كل مرة تتم مصادقة العميل بالكامل على EAP، يستخدم العميل وخادم المصادقة MSK، والذي يتم إستخدامه لاستخلاص PMK. يستخدم هذا كذبذة لمصافحة WPA2 4-Way لاستخلاص مفاتيح تشفير البث الأحادي النهائي (PTK) الذي يتم إستخدامه (حتى يوجد العميل إلى نقطة وصول أخرى وأ تنتهي الجلسة)، ومن ثم، تمنع هذه الجلسة من أن يعيد إستخدام PMK الأصلي الذي تم تخزينه مؤقتا من قبل العميل و AP. يجب على العميل قطع إجراء تأكيد الاتصال رباعي الإتجاه WPA2 من أجل اشتقاق مفاتيح تشفير جديدة.

802.11 هذه الطريقة على نطاق واسع انظر لطريقة التجوال القياسية الآمنة التي تم نشر ها

الموصى بها وير جع ذلك بشكل أساسي إلى هذه الأسباب:

- هذه الطريقة إختيارية والا تدعمها جميع أجهزة WPA2، لأن الغرض من تعديل 802.11i ال يتعلق بالتجوال السريع والآمن، وقد عمل IEEE بالفعل على تعديل آخر لتوحيد التجوال السريع والآمن لشبكات WLAN (802.11r، والذي تمت تغطيته الحقا في هذا المستند).
- تفرض هذه الطريقة قيودا كبيرة على تنفيذها: لا يمكن للعملاء اللاسلكيين إجراء التجوال المؤمن بسرعة إلا عند التجوال مرة أخرى إلى نقطة وصول حيث سبق لهم التصديق/الاتصال.

باستخدام هذه الطريقة، يكون القتران الأولي بأي نقطة وصول بمثابة مصادقة عادية لأول مرة للشبكة المحلية اللاسلكية (WLAN)، حيث يجب أن تحدث المصادقة 802. 1X/EAP بالكامل مقابل خادم المصادقة والمصافحة رباعية الإتجاه لإنشاء المفاتيح قبل أن يتمكن العميل من إرسال إطارات البيانات، كما هو موضح في صورة الشاشة هذه:

No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	802.11	2462	Authentication, SN=2, FN=0, Flags=.....
2	0.000814	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	802.11	2462	Authentication, SN=4052, FN=0, Flags=...
3	0.002747	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	802.11	2462	Association Request, SN=3, FN=0, Flags=.
4	0.007357	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	802.11	2462	Association Response, SN=4053, FN=0, Fla
5	0.011957	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Identity
6	0.022896	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Identity
7	0.044470	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
8	0.069885	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Client Hello
9	0.093349	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
10	0.095916	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Protected EAP (EAP-PEAP)
11	0.112358	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
12	0.116114	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Protected EAP (EAP-PEAP)
13	0.120221	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
14	0.129519	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Certificate, Client Key Exchange, Change
15	0.139156	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
16	0.162262	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Protected EAP (EAP-PEAP)
17	0.166459	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
18	0.171454	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data
19	0.175710	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
20	0.178181	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data
21	0.182858	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
22	0.187006	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data
23	0.192835	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
24	0.197049	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data
25	0.202860	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
26	0.205372	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data
27	0.210763	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAP	2462	Success
28	0.212505	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 1 of 4)
29	0.215434	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 2 of 4)
30	0.219023	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 3 of 4)
31	0.221930	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 4 of 4)
32	0.224559	Apple_15:39:32	Cisco_f5:4a:40	84:78:ac:f0:68:d2	802.11	2462	QoS Data, SN=0, FN=0, Flags=.p.....TC

تكشف الأخطاء عن تبادل إطار مصادقة EAP نفسه كما هو الطرق عند المصادقة الأولية للشبكة المحلية اللاسلكية (WLAN)، مع إضافة بعض المخرجات في ما يتعلق بتقنيات التخزين المؤقت الأساسية المستخدمة هنا. تم خفض مخرجات تصحيح الأخطاء هذه لعرض المعلومات الجديدة بشكل أساسي، وليس تبادل إطارات EAP بالكامل، لأنه تم تبادل نفس المعلومات بشكل أساسي في كل مرة لمصادقة العميل مقابل خادم المصادقة. وهذا موضح حتى الآن، وتطابق مع إطارات مصادقة EAP الموضحة في صور الحزمة، حتى تتم إزالة معظم رسائل EAP من مخرجات تصحيح الأخطاء للتبسيط:

```
*apfMsConnTask_0: Jun 22 00:23:15.097: ec:85:2f:15:39:32
  Association received from mobile on BSSID 84:78:ac:f0:68:d2
!--- This is the Association Request from the client.

*apfMsConnTask_0: Jun 22 00:23:15.098: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 20 for mobile ec:85:2f:15:39:32
!--- The WLC/AP finds an Information Element that claims PMKID
     Caching support on the Association request that is sent
     from the client.

*apfMsConnTask_0: Jun 22 00:23:15.098: ec:85:2f:15:39:32
```

```
  Received RSN IE with 0 PMKIDs from mobile ec:85:2f:15:39:32
!--- Since this is an initial association, the Association
     Request comes without any PMKID.

*apfMsConnTask_0: Jun 22 00:23:15.098: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 8

*apfMsConnTask_0: Jun 22 00:23:15.099: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d2
  (status 0) ApVapId 3 Slot 0
!--- The Association Response is sent to the client.

*dot1xMsgTask: Jun 22 00:23:15.103: ec:85:2f:15:39:32
  Sending EAP-Request/Identity to mobile ec:85:2f:15:39:32
  (EAP Id 1)

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.118: ec:85:2f:15:39:32
  Received EAPOL EAPPKT from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.118: ec:85:2f:15:39:32
  Received Identity Response (count=1) from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.126: ec:85:2f:15:39:32
  Processing Access-Challenge for mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.126: ec:85:2f:15:39:32
  Sending EAP Request from AAA to mobile ec:85:2f:15:39:32
  (EAP Id 2)

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.146: ec:85:2f:15:39:32
  Received EAPOL EAPPKT from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.146: ec:85:2f:15:39:32
  Received EAP Response from mobile ec:85:2f:15:39:32
  (EAP Id 2, EAP Type 25)

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Processing Access-Accept for mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Creating a PKC PMKID Cache entry for station ec:85:2f:15:39:32
  (RSN 2)
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 8
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 0
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Adding BSSID 84:78:ac:f0:68:d2 to PMKID cache at index 0
  for station ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274:
  New PMKID: (16)
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274:
  [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
!--- WLC creates a PMK cache entry for this client, which is
     used for SKC in this case, so the PMKID is computed with
     the AP MAC address (BSSID 84:78:ac:f0:68:d2).

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.274: ec:85:2f:15:39:32
  Sending EAP-Success to mobile ec:85:2f:15:39:32
  (EAP Id 12)

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.275:
  Including PMKID in M1  (16)
!--- The hashed PMKID is included on the Message-1 of the
```

```
     WPA/WPA2 4-Way handshake.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.275:
  [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
!--- This is the hashed PMKID.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.275: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00
!--- Message-1 of the WPA/WPA2 4-Way handshake is sent from
     the WLC/AP to the client.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.284: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.284: ec:85:2f:15:39:32
  Received EAPOL-key in PTK_START state (message 2) from mobile
  ec:85:2f:15:39:32
!--- Message-2 of the WPA/WPA-2 4-Way handshake is successfully
     received from the client.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.284: ec:85:2f:15:39:32
  PMK: Sending cache add

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.285: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32
  state PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- Message-3 of the WPA/WPA2 4-Way handshake is sent from
     the WLC/AP to the client.

*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.291: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 22 00:23:15.291: ec:85:2f:15:39:32
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile ec:85:2f:15:39:32
!--- Message-4 (final message) of this initial WPA/WPA2 4-Way
     handshake is successfully received from the client, which
     confirms the installation of the derived keys. They can
     now be used in order to encrypt data frames with the current AP.
```

باستخدام هذه الطريقة، تقوم نقاط الوصول وذاكرة التخزين المؤقت للعميل اللاسلكي بنسخ PMKs الخاصة بالاقترانات الآمنة التي تم إنشاؤها بالفعل. وبالتالي، إذا تجول العميل اللاسلكي إلى نقطة وصول جديدة لم تقترن بها قط، فيجب على العميل إجراء مصادقة EAP كاملة مرة أخرى، كما هو موضح في هذه الصورة حيث يجول العميل إلى نقطة وصول جديدة:

No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	802.11	2437	Authentication, SN=462, FN=0, Flags=.
2	0.000819	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	802.11	2437	Authentication, SN=3633, FN=0, Flags=
3	0.002754	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	802.11	2437	Reassociation Request, SN=463, FN=0,
4	0.007638	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	802.11	2437	Reassociation Response, SN=3634, FN=0
5	0.013519	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	EAP	2437	Request, Identity
6	0.043063	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	EAP	2437	Request, Protected EAP (EAP-PEAP)
7	0.054400	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	TLSv1	2437	Client Hello
8	0.060031	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	TLSv1	2437	Server Hello, Change Cipher Spec, Enc
9	0.093278	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	TLSv1	2437	Change Cipher Spec, Encrypted Handsha
10	0.099981	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	TLSv1	2437	Application Data
11	0.105545	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	TLSv1	2437	Application Data
12	0.110891	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	EAP	2437	Success
13	0.112656	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	EAPOL	2437	Key (Message 1 of 4)
14	0.115722	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	EAPOL	2437	Key (Message 2 of 4)
15	0.119364	Cisco_f0:2a:92	Apple_15:39:32	84:78:ac:f0:2a:92	EAPOL	2437	Key (Message 3 of 4)
16	0.123520	Apple_15:39:32	Cisco_f0:2a:92	84:78:ac:f0:2a:92	EAPOL	2437	Key (Message 4 of 4)
17	2.374472	Apple_15:39:32	IPv6mcast_00:00:0	84:78:ac:f0:2a:92	802.11	2437	QoS Data, SN=6, FN=0, Flags=.p.....TC

ومع ذلك، إذا عاد العميل اللاسلكي إلى نقطة وصول حدثت فيها اقتران/مصادقة سابقة، يرسل العميل إطار طلب إعادة تعيين يسرد العديد من PMKIDs، والذي يقوم بإعلام نقطة

الوصول بمجموعات PMK المخزنة مؤقتا من جميع نقاط الوصول التي قام العميل بالمصادقة عليها مسبقا. لذلك، فبما أن العميل يجول مرة أخرى إلى نقطة وصول تحتوي أيضا على PMK مخزن مؤقتا لهذا العميل، فلا يحتاج العميل إلى إعادة المصادقة من خلال EAP لاستخراج PMK جديد. يمر العميل ببساطة بمصافحة WPA2 4-way من أجل اشتقاق مفاتيح التشفير المؤقتة الجديدة:

No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	802.11	2462	Authentication, SN=1506, FN=0, Flags=.....
2	0.002104	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	802.11	2462	Reassociation Request, SN=1134, FN=0, Flags
3	0.007239	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	802.11	2462	Reassociation Response, SN=1507, FN=0, Flag
4	0.014511	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 1 of 4)
5	0.019507	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 2 of 4)
6	0.023478	Cisco_f0:68:d2	Apple_15:39:32	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 3 of 4)
7	0.026743	Apple_15:39:32	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 4 of 4)

ملاحظة: لا تعرض هذه الصورة إطار مصادقة النظام المفتوح الأول وفقا لمعيار 802.11 من العميل، ولكن إذا لا يرجع إلى الطريقة التي تم تنفيذها، حيث إن إذا الإطار مطلوب دائما. السبب وه أن إذا الإطار المحدد لا يتم تصويره بواسطة المحول أو برنامج صورة الحزمة اللاسلكية المستخدم لشم الإطارات عبر الهواء لهذا المثال، ولكنه يترك هكذا على المثال ألغراض تعليمية. مدرك أن هناك احتمال أن إذا يمكن أن يحدث عندما تقوم بأداء صور حزم عبر الهواء، بعض الإطارات يمكن أن تفقد من قبل الصورة، لكن في الواقع يتم تبادلها بين العميل و AP. وإلا فإن التجوال لا يبدأ على هذا المثال.

فيما يلي ملخص للتصحيحات الخاصة بعنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لطريقة التجوال سريعة الأمان هذه:

```
*apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32
  Reassociation received from mobile on BSSID
  84:78:ac:f0:68:d2
!--- This is the Reassociation Request from the client.

*apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 38 for mobile
  ec:85:2f:15:39:32
!--- The WLC/AP finds an Information Element that claims PMKID
     Caching support on the Association request that is sent
     from the client.

*apfMsConnTask_0: Jun 22 00:26:40.787: ec:85:2f:15:39:32
  Received RSN IE with 1 PMKIDs from mobile
  ec:85:2f:15:39:32
!--- The Reassociation Request from the client comes with
     one PMKID.

*apfMsConnTask_0: Jun 22 00:26:40.787:
  Received PMKID:  (16)
*apfMsConnTask_0: Jun 22 00:26:40.788:
  [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
!--- This is the PMKID that is received.

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Searching for PMKID in MSCB PMKID cache for mobile
  ec:85:2f:15:39:32
!--- WLC searches for a matching PMKID on the database.

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
```

```
  Found an cache entry for BSSID 84:78:ac:f0:68:d2 in
  PMKID cache at index 0 of station ec:85:2f:15:39:32

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Found a valid PMKID in the MSCB PMKID cache for mobile
  ec:85:2f:15:39:32
!--- The WLC validates the PMKID provided by the client,
      and confirms that it has a valid PMK cache for this
      client-and-AP pair.

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Setting active key cache index 1 ---> 0

*apfMsConnTask_0: Jun 22 00:26:40.788: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID
  84:78:ac:f0:68:d2(status 0) ApVapId 3 Slot 0
!--- The Reassociation Response is sent to the client, which
      validates the fast-roam with SKC.

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32
  Initiating RSN with existing PMK to mobile
  ec:85:2f:15:39:32
!--- WLC initiates a Robust Secure Network association with
      this client-and-AP pair based on the cached PMK found.
Hence, EAP is avoided as per the next message.

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32
  Skipping EAP-Success to mobile ec:85:2f:15:39:32

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32
  Found an cache entry for BSSID 84:78:ac:f0:68:d2 in
  PMKID cache at index 0 of station ec:85:2f:15:39:32

*dot1xMsgTask: Jun 22 00:26:40.795: Including PMKID in M1(16)
!--- The hashed PMKID is included on the Message-1 of the
      WPA/WPA2 4-Way handshake.

*dot1xMsgTask: Jun 22 00:26:40.795:
  [0000] c9 4d 0d 97 03 aa a9 0f 1b c8 33 73 01 f1 18 f5
!--- The PMKID is hashed. The next messages are the same
      WPA/WPA2 4-Way handshake messages described thus far
      that are used in order to finish the encryption keys
      generation/installation.

*dot1xMsgTask: Jun 22 00:26:40.795: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.811: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32
  Received EAPOL-key in PTK_START state (message 2) from mobile
  ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32
  PMK: Sending cache add

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.812: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.820: ec:85:2f:15:39:32
```

```
  Received EAPOL-Key from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 22 00:26:40.820: ec:85:2f:15:39:32
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile ec:85:2f:15:39:32
```

FlexConnect مع ذاكرة التخزين المؤقت ل PMKID / ذاكرة التخزين المؤقت للمفاتيح اللاصقة

- عند إستخدام هذه الطريقة على إعداد FlexConnect، قد تعمل ودي دقي السلوك مما الثال لما يحدث عندما تقوم باستخدام المصادقة المركزية مرة أخرى إلى عنصر التحكم في شرحه سابقا إذا تم (WLC) (باستخدام التوحيد المركزي أو المحلي)، وعلى ذلك، الشبكة المحلية اللاسلكية FlexConnect. ال يتم دعم طريقة SKC هذه على
- هذا أسلوب فقط معتمد رسميا على CUWN مع أسلوب APs محلي، ليس على FlexConnect أو أسلوب آخر.

PROS مع ذاكرة التخزين المؤقت ل PMKID / ذاكرة التخزين المؤقت للمفاتيح اللاصقة

يمكن تنفيذ هذه الطريقة محليا بواسطة نقاط الوصول (AP) المستقلة، دون الحاجة إلى جهاز مركزي لإدارة المفاتيح المخزنة مؤقتا.

مخالط مع ذاكرة التخزين المؤقت ل PMKID / ذاكرة التخزين المؤقت للمفاتيح اللاصقة

- وكما تمت الإشارة إليه مسبقا في هذا المستند، فإن التحدي الرئيسي لهذه الطريقة هو أنه يمكن للعميل إجراء التجوال المؤمن بسرعة فقط عند التجوال مرة أخرى إلى نقطة وصول حيث كانت ترتبط/تصادق من قبل. في حالة التجوال إلى نقطة وصول جديدة، يجب على العميل إكمال مصادقة EAP الكاملة مرة أخرى.
- يجب أن يتذكر العميل اللاسلكي و APs كل PMKs المشتقة من كل مصادقة جديدة، لذلك فهذه الميزة تقتصر عادة على مقدار معين من PMKs التي يتم تخزينها مؤقتا. ونظرا لأن هذا الحد غير محدد بوضوح بواسطة المعيار، فيمكن للموردين تحديد حدود مختلفة على عمليات تنفيذ SKC الخاصة بهم. على سبيل المثال، يمكن لوحدات التحكم في الشبكة المحلية اللاسلكية (WLAN) من Cisco تخزين وحدات التحكم (PMK) من عميل المصادقة إلى ثمانية نقاط وصول (APs). إن التجول بين أكثر من ثمانية APs لكل جلسة، أزالت الأقدم APs من التخزين المؤقت قائمة in order to تخزين الإدخالات حديثا.
- هذه الطريقة إختيارية وال تزال غير معتمدة من قبل العديد من أجهزة WPA2، وبالتالي، فإن هذه الطريقة غير معتمدة وال يتم نشرها على نطاق واسع.
- ال يتم دعم SKC عند إجراء التجوال بين وحدات التحكم البينية، والذي يحدث عند النقل بين نقاط الوصول التي تتم إدارتها بواسطة وحدات تحكم الشبكة المحلية اللاسلكية (WLC) مختلفة، حتى إذا كانت على نفس مجموعة التنقل.

التجوال السريع الآمن مع التخزين المؤقت للمفاتيح الانتهازي

إن التخزين المؤقت الانتهازي للمفاتيح (OKC)، والمعروف أيضا باسم التخزين المؤقت

الاستباقي للمفاتيح (PKC) (يتم شرح هذا المصطلح بمزيد من التفصيل في ملاحظة تعد تالية)، وهي في الأساس تحسين لطريقة التخزين المؤقت WPA2 PMKID الموضحة سابقا، وهذا هو السبب وراء تسميتها أيضا التخزين المؤقت الاستباقي/الانتمازي PMKID. وبالتالي، من المهم ملاحظة أن هذه الطريقة ليست طريقة تجوال سريعة التأمين معرفة بمعيار 802.11 والعديد من أجهزة كثيرة، ولكنها تعمل مع WPA2-EAP تمامًا مثل التخزين المؤقت لـ PMKID.

يسمح هذا الأسلوب للعميل اللاسلكي والبنية الأساسية للشبكة المحلية اللاسلكية (WLAN) بتخزين PMK واحد فقط لاول العمر الافتراضي لاقتران العميل مع شبكة WLAN هذه (المستمد من MSK بعد مصادقة 802.1X/EAP الأولية مع خادم المصادقة)، حتى عند التجوال بين نقاط الوصول المتعددة، حيث أنها تشترك جميعها في PMK الأصلية التي تم إستخدامها كبذرة على جميع رسائل WPA2 الرباعية الإتجاه. وهو ما يزال هذا مطلوبا، كما هو الحال في SKC، من أجل إنشاء مفاتيح تشفير جديدة في كل مرة يعيد فيها العميل الاتصال بنقاط الوصول. لكي تتمكن نقاط الوصول من مشاركة PMK الأصلي هذا من جلسة عمل العميل، يجب أن تكون جميعها تحت نوع ما من التحكم الإداري، مع جهاز مركزي يقوم بتخزين PMK الأصلي وتوزيعه لجميع نقاط الوصول. وهذا مماثل لـ CUWN، حيث تقوم WLC بأداء هذه المهمة لجميع نقاط الوصول في الوضع Lightweight (LAPs) تحت التحكم فيها، وتستخدم مجموعات التنقل لمعالجة PMK هذه بين نقاط الوصول في الوضع Lightweight (WLCs) المتعددة، وبالتالي، يعد هذا قيدا على بيئات AP المستقلة.

باستخدام هذه الطريقة، تمامًا كما هو الحال في التخزين المؤقت PMKID (SKC)، يكون الاقتران الأولي لأي نقطة وصول مصادقة منتظمة لأول مرة للشبكة المحلية اللاسلكية (WLAN)، حيث يجب عليك إكمال مصادقة 802.1X/EAP بالكامل مقابل خادم المصادقة والمصافحة رباعية الإتجاه لإنشاء المفاتيح قبل أن تتمكن من إرسال إطارات البيانات. هنا صورة شاشة توضح هذا:

No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	802.11	2462	Authentication, SN=2421, FN=0, Flags=...
2	0.001369	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	802.11	2462	Authentication, SN=3299, FN=0, Flags=...
3	0.003199	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	802.11	2462	Association Request, SN=2422, FN=0, Flag
4	0.008447	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	802.11	2462	Association Response, SN=3300, FN=0, Flag
5	0.107400	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Identity
6	0.121755	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
7	0.162562	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Client Hello
8	0.178720	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
9	0.192059	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Protected EAP (EAP-PEAP)
10	0.207860	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
11	0.227297	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Protected EAP (EAP-PEAP)
12	0.231517	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
13	0.242089	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Certificate, Client Key Exchange, Change
14	0.251854	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
15	0.254304	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAP	2462	Response, Protected EAP (EAP-PEAP)
16	0.258723	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
17	0.265390	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data, Application Data
18	0.269769	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
19	0.272225	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data, Application Data
20	0.276927	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
21	0.280525	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data, Application Data
22	0.287232	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
23	0.290451	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data, Application Data
24	0.302861	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Request, Protected EAP (EAP-PEAP)
25	0.313281	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	TLSv1	2462	Application Data, Application Data
26	0.337874	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAP	2462	Success
27	0.339642	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 1 of 4)
28	0.353971	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 2 of 4)
29	0.358041	Cisco_f0:68:d2	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 3 of 4)
30	0.378569	Aironet_b7:ab:5c	Cisco_f0:68:d2	84:78:ac:f0:68:d2	EAPOL	2462	Key (Message 4 of 4)
31	0.462588	Aironet_b7:ab:5c	Broadcast	84:78:ac:f0:68:d2	802.11	2462	QoS Data, SN=2437, FN=0, Flags=.p.....TC
32	0.473985	Cisco_f0:68:d0	Aironet_b7:ab:5c	84:78:ac:f0:68:d2	802.11	2462	QoS Data, SN=81, FN=0, Flags=.p....F.C

تظهر مخرجات تصحيح الأخطاء أساسا نفس تبادل إطار مصادقة EAP مثل بقية الطرق المدعومة في هذا المستند عند المصادقة الأولية للشبكة المحلية اللاسلكية (WLAN) (كما هو موضح في الصور)، بالإضافة إلى بعض المخرجات التي تتعلق بتقنيات التخزين المؤقت الأساسية المستخدمة من قبل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) هنا. يتم خفض إخراج تصحيح الأخطاء هذا أيضا لعرض المعلومات ذات الصلة فقط:

```
*apfMsConnTask_0: Jun 21 21:46:06.515: 00:40:96:b7:ab:5c
```

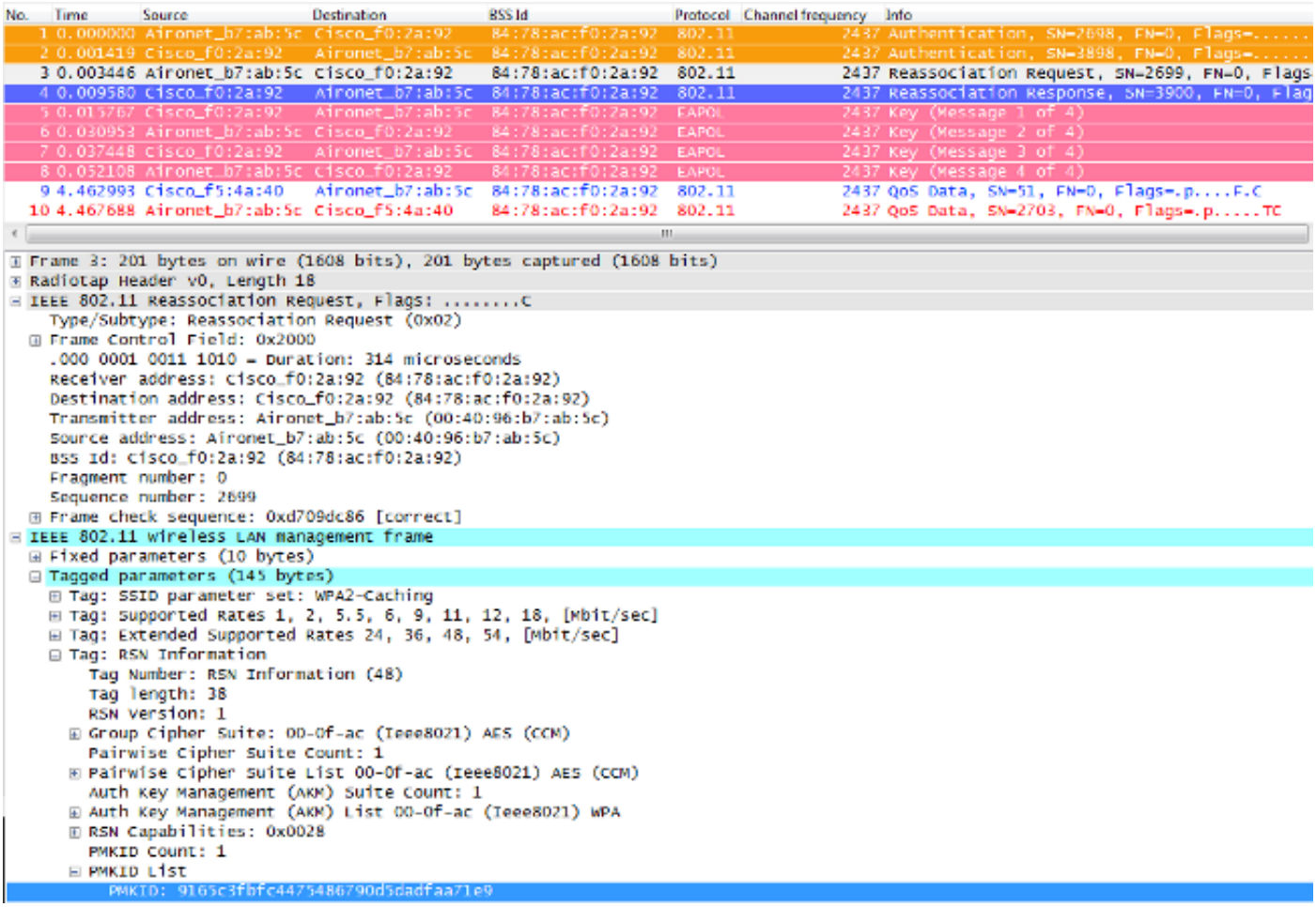
```
  Association received from mobile on BSSID
  84:78:ac:f0:68:d2
!--- This is the Association Request from the client.

*apfMsConnTask_0: Jun 21 21:46:06.516: 00:40:96:b7:ab:5c
  Processing RSN IE type 48, length 20 for mobile
  00:40:96:b7:ab:5c
!--- The WLC/AP finds an Information Element that claims
     PMKID Caching support on the Association request that
     is sent from the client.

*apfMsConnTask_0: Jun 21 21:46:06.516: 00:40:96:b7:ab:5c
  Received RSN IE with 0 PMKIDs from mobile
  00:40:96:b7:ab:5c
!--- Since this is an initial association, the Association
     Request comes without any PMKID.

*apfMsConnTask_0: Jun 21 21:46:06.516: 00:40:96:b7:ab:5c
  Setting active key cache index 0 ---> 8

*apfMsConnTask_0: Jun 21 21:46:06.516: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID
  84:78:ac:f0:68:d2 (status 0) ApVapId 3 Slot
!--- The Association Response is sent to the client.

*dot1xMsgTask: Jun 21 21:46:06.522: 00:40:96:b7:ab:5
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 1)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.614: 00:40:96:b7:ab:5c
  Received EAPOL START from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.614: 00:40:96:b7:ab:5c
  Sending EAP-Request/Identity to mobile 00:40:96:b7:ab:5c
  (EAP Id 2)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.623: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.623: 00:40:96:b7:ab:5c
  Received Identity Response (count=2) from mobile
  00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.630: 00:40:96:b7:ab:5c
  Processing Access-Challenge for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.630: 00:40:96:b7:ab:5c
  Sending EAP Request from AAA to mobile 00:40:96:b7:ab:5c
  (EAP Id 3)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.673: 00:40:96:b7:ab:5c
  Received EAPOL EAPPKT from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.673: 00:40:96:b7:ab:5c
  Received EAP Response from mobile 00:40:96:b7:ab:5c
  (EAP Id 3, EAP Type 25)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.843: 00:40:96:b7:ab:5c
  Processing Access-Accept for mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Creating a PKC PMKID Cache entry for station
  00:40:96:b7:ab:5c (RSN 2)
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
```

```
  Setting active key cache index 8 ---> 8
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Setting active key cache index 8 ---> 0
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Adding BSSID 84:78:ac:f0:68:d2 to PMKID cache at index 0
  for station 00:40:96:b7:ab:5
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: New PMKID: (16)
*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844:
  [0000] 4e a1 7f 5a 75 48 9c f9 96 e3 a8 71 25 6f 11 d0
!--- WLC creates a PMK cache entry for this client, which is
     used for OKC in this case, so the PMKID is computed
     with the AP MAC address (BSSID 84:78:ac:f0:68:d2).

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  PMK sent to mobility group
!--- The PMK cache entry for this client is shared with the
     WLCs on the mobility group.

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Sending EAP-Success to mobile 00:40:96:b7:ab:5c (EAP Id 13)

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Found an cache entry for BSSID 84:78:ac:f0:68:d2 in PMKID
  cache at index 0 of station 00:40:96:b7:ab:5

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: Including PMKID
  in M1  (16)
!--- The hashed PMKID is included on the Message-1 of the
     WPA/WPA2 4-Way handshake.

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844:
  [0000] 4e a1 7f 5a 75 48 9c f9 96 e3 a8 71 25 6f 11 d0
!--- This is the hashed PMKID. The next messages are the same
     WPA/WPA2 4-Way handshake messages described thus far that
     are used in order to finish the encryption keys
     generation/installation.

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.844: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.865: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.865: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2)
  from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.865: 00:40:96:b7:ab:5c
  PMK: Sending cache add

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.865: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.889: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:46:06.890: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
```

باستخدام هذه الطريقة، يقوم العميل اللاسلكي ووحدة التحكم في الشبكة المحلية

اللاسلكية (WLC) (لجميع نقاط الوصول المدارة) بذاكرة التخزين المؤقت لبطاقة PMK الأصلية الوحيدة للاقتران الآمن الذي تم إنشاؤه في البداية. أساسا، في كل مرة يتصل فيها العميل اللاسلكي بنقطة وصول معينة، تتم تجزئة PMKID بناء على: عنوان MAC العميل وعنوان MAC لنقطة الوصول (BSSID من WLAN)، والحزمة PMK المشتقة من نقطة الوصول هذه. لذلك، بما أن OKC يقوم بتخزين نفس PMK الأصلي لجميع نقاط الوصول والعميل المحدد، عندما يرتبط هذا العميل (re)ب نقطة وصول أخرى، فإن القيمة الوحيدة التي تتغير من أجل تجزئة PMKID الجديد هي عنوان AP MAC الجديد.

عندما يقوم العميل بدء التجوال إلى نقطة وصول جديدة ويرسل إطار طلب إعادة الإنشاء، فإنه يضيف PMKID على عنصر معلومات WPA2 RSN إذا كان يريد إعلام نقطة الوصول باستخدام PMK المخزنة مؤقتا للتجوال الآمن بسرعة. إنه يعرف بالفعل عنوان MAC الخاص ب BSSID (AP) الأين يجول، ثم يقوم العميل ببساطة بتقييد PMKID الجديد المستخدم في طلب إعادة التعيين هذا. عندما تتلقى نقطة الوصول هذا الطلب من العميل، فإنها تقسم أيضا PMKID بالقيم التي تمتلكها بالفعل (PMK المخزنة مؤقتا وعنوان MAC للعميل وعنوان MAC الخاص ب)، وتستجيب مع إستجابة إعادة الإدماج الناجحة التي تؤكد تطابق PMKIDs. يمكن إستخدام PMK المخزنة مؤقتا كبذرة لبدء مصافحة WPA2 4-Way لاستخلاص مفاتيح التشفير الجديدة (وتخطي EAP):



في هذه الصورة، يتم تحديد إطار طلب إعادة التشغيل من العميل وتوسيعه بحيث يمكنك رؤية المزيد من تفاصيل الإطار. معلومات عنوان MAC وكذلك عنصر معلومات شبكة الأمان القوية (RSN، وفقا ل 802.11i - WPA2)، حيث يتم عرض معلومات حول إعدادات WPA2 المستخدمة لهذه الاقتران (يتم التركيز على PMKID الذي تم الحصول عليه من الصيغة المحسوبة).

فيما يلي ملخص بتصحيح أخطاء عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لطريقة التجوال سريعة الأمان هذه مع OKC:

```
*apfMsConnTask_2: Jun 21 21:48:50.562: 00:40:96:b7:ab:5c
  Reassociation received from mobile on BSSID
  84:78:ac:f0:2a:92
!--- This is the Reassociation Request from the client.

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Processing RSN IE type 48, length 38 for mobile
  00:40:96:b7:ab:5c
!--- The WLC/AP finds and Information Element that claims
     PMKID Caching support on the Association request that
     is sent from the client.

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Received RSN IE with 1 PMKIDs from mobile
  00:40:96:b7:ab:5c
!--- The Reassociation Request from the client comes with
     one PMKID.

*apfMsConnTask_2: Jun 21 21:48:50.563:
  Received PMKID:  (16)

*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Searching for PMKID in MSCB PMKID cache for mobile
  00:40:96:b7:ab:5c
*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  No valid PMKID found in the MSCB PMKID cache for mobile
  00:40:96:b7:ab:5
!--- As the client has never authenticated with this new AP,
     the WLC cannot find a valid PMKID to match the one provided
     by the client. However, since the client performs OKC
     and not SKC (as per the following messages), the WLC computes
     a new PMKID based on the information gathered (the cached PMK,
     the client MAC address, and the new AP MAC address).

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Trying to compute a PMKID from MSCB PMK cache for mobile
  00:40:96:b7:ab:5c

*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: Find PMK in cache: BSSID =  (6)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 84 78 ac f0 2a 90
*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: Find PMK in cache: realAA =  (6)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 84 78 ac f0 2a 92
*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: Find PMK in cache: PMKID =  (16)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9
*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: AA (6)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 84 78 ac f0 2a 92
*apfMsConnTask_2: Jun 21 21:48:50.563:
  CCKM: SPA (6)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 00 40 96 b7 ab 5c
*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Adding BSSID 84:78:ac:f0:2a:92 to PMKID cache at
  index 0 for station 00:40:96:b7:ab:5c
```

```
*apfMsConnTask_2: Jun 21 21:48:50.563:
  New PMKID: (16)
*apfMsConnTask_2: Jun 21 21:48:50.563:
  [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9
*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Computed a valid PMKID from MSCB PMK cache for mobile
  00:40:96:b7:ab:5c
!--- The new PMKID is computed and validated to match the
      one provided by the client, which is also computed with
      the same information. Hence, the fast-secure roam is
      possible.

*apfMsConnTask_2: Jun 21 21:48:50.563: 00:40:96:b7:ab:5c
  Setting active key cache index 0 ---> 0

*apfMsConnTask_2: Jun 21 21:48:50.564: 00:40:96:b7:ab:5c
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:92
  (status 0) ApVapId 3 Slot
!--- The Reassociation response is sent to the client, which
      validates the fast-roam with OKC.

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c
  Initiating RSN with existing PMK to mobile
  00:40:96:b7:ab:5c
!--- WLC initiates a Robust Secure Network association with
      this client-and AP pair with the cached PMK found.
Hence, EAP is avoided, as per the the next message.

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c
  Skipping EAP-Success to mobile 00:40:96:b7:ab:5c

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c
  Found an cache entry for BSSID 84:78:ac:f0:2a:92 in
  PMKID cache at index 0 of station 00:40:96:b7:ab:5c

*dot1xMsgTask: Jun 21 21:48:50.570:
  Including PMKID in M1  (16)
!--- The hashed PMKID is included on the Message-1 of the
      WPA/WPA2 4-Way handshake.

*dot1xMsgTask: Jun 21 21:48:50.570:
  [0000] 91 65 c3 fb fc 44 75 48 67 90 d5 da df aa 71 e9
!--- The PMKID is hashed. The next messages are the same
      WPA/WPA2 4-Way handshake messages described thus far,
      which are used in order to finish the encryption keys
      generation/installation.

*dot1xMsgTask: Jun 21 21:48:50.570: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  INITPMK (message 1), replay counter 00.00.00.00.00.00.00.00

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTK_START state (message 2) from mobile
  00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.589: 00:40:96:b7:ab:5c
  PMK: Sending cache add

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.590: 00:40:96:b7:ab:5c
  Sending EAPOL-Key Message to mobile 00:40:96:b7:ab:5c state
  PTKINITNEGOTIATING (message 3), replay counter
```

```
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.610: 00:40:96:b7:ab:5c
  Received EAPOL-Key from mobile 00:40:96:b7:ab:5c

*Dot1x_NW_MsgTask_4: Jun 21 21:48:50.610: 00:40:96:b7:ab:5c
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile 00:40:96:b7:ab:5c
```

كما هو موضح في بداية عملية تصحيح الأخطاء، يجب حساب PMKID بعد تلقي طلب إعادة التعيين من العميل. يلزم هذا للتحقق من صحة PMKID وتأكيد استخدام PMK المخزن مؤقتا. ال WPA2 4-Way Key هو آلية التشفير والمصادقة المستخدمة مع الوصول السريع للتنقل. CCKM، بل OKC، هو أيضا مسمى مستخدم من قبل WLC لتلك المخرجات، مثل CCKM. كما هو موضح سابقا، يجب تصحيح الأخطاء الخاصة بـ CCKM للتأكد من أن العميل يقوم بالتبديل بين نقاط الوصول (APs) في مجموعة FlexConnect نفسها، فإن التجوال السريع الآمن يتم بواسطة وحدة التحكم. وإلا فإن التجوال السريع الآمن يتم بواسطة نقطة الوصول، ولكن هذا ليس إعداد مستحسن أو مدعوم.

ملاحظة: يمكن أن يعمل هذا الإعداد إذا لم تكن نقاط الوصول (APs) في مجموعة FlexConnect نفسها، ولكن هذا ليس إعداد مستحسن أو مدعوم.

- المصادقة المحلية المرنة مدعومة. في الوضع المتصل، يمكن توزيع ذاكرة التخزين المؤقت من نقطة الوصول إلى وحدة التحكم ثم إلى باقي نقاط الوصول في مجموعة FlexConnect.
- الوضع المستقل مدعوم. إذا كانت ذاكرة التخزين المؤقت موجودة بالفعل على نقطة الوصول (انظر للتوزيع السابق)، يجب أن تعمل التجوال السريع الآمن. لا تدعم المصادقة الجديدة في الوضع المستقل التجوال السريع الآمن.

التخزين المؤقت للمفاتيح الانتهازي مع FlexConnect

- المصادقة المركزية مدعومة. وتتضمن ذلك تبديل البيانات المحلية والمركزية. إذا كانت نقطة الوصول جزءا من مجموعة FlexConnect نفسها، فإن التجوال سريع الأمان يتم بواسطة وحدة التحكم. وإلا فإن التجوال سريع الأمان يتم بواسطة نقطة الوصول (APs) في مجموعة FlexConnect نفسها، ولكن هذا ليس إعداد مستحسن أو مدعوم.
- المصادقة المحلية المرنة مدعومة. في الوضع المتصل، يمكن توزيع ذاكرة التخزين المؤقت من نقطة الوصول إلى وحدة التحكم ثم إلى باقي نقاط الوصول في مجموعة FlexConnect.
- الوضع المستقل مدعوم. إذا كانت ذاكرة التخزين المؤقت موجودة بالفعل على نقطة الوصول (انظر للتوزيع السابق)، يجب أن تعمل التجوال السريع الآمن. لا تدعم المصادقة الجديدة في الوضع المستقل التجوال السريع الآمن.

التخزين المؤقت للمفاتيح الانتهازي مع PROS ذاكرة

- الحاجة العميل اللاسلكي والبنية الأساسية للشبكة المحلية اللاسلكية (WLAN) إلى تذكر العديد من PMKIDs، بل بمساطة تخزين PMK الأصلي الواحد من ذاكرة المصادقة الأولية إلى الشبكة المحلية اللاسلكية (WLAN). بعد ذلك يجب إعادة تجزئة PMKID المناسب (المستخدم في طلب إعادة التعيين) المطلوب مع كل اقتران آمن للتحقق من صحة التجوال السريع الآمن.
- هناك يقوم العميل اللاسلكي بالتجوال السريع والآمن إلى نقطة وصول جديدة على نفس شبكة WLAN/SSID، حتى وإن لم تكن قد أبدأت نقطة الوصول تلك (وليس الحالة في SKC). طالما يقوم العميل بتنفيذ المصادقة الأولية لـ 802.1X/EAP باستخدام نقطة وصول واحدة تتم إدارتها بواسطة النشر المركزي الذي يعالج ذاكرة التخزين المؤقت لـ PMK لجميع نقاط الوصول حيث يتجول العميل، فلن تكون هناك أي مصادقة كاملة أخرى مطلوبة لبقية فترة بقاء العميل على شبكة WLAN هذه.

التخزين المؤقت للمفاتيح الانتهازي مع CONS

- يتم نشر هذه الطريقة فقط على بيئة مركزية حيث تكون جميع نقاط الوصول تحت شبكة المحلية اللاسلكية (WLAN) التحكم الإداري (مثل وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN) نوع ما من جلسة عمل مشتركة من ذاكرة PMK الأصلية الواحدة والمؤقتة عن التخزين المؤقت. لذلك، هذا يقيد على بيئات AP المستقلة.
- والتقنيات التي تم تطبيقها في هذه الطريقة غير مقترحة أو موصوفة في معيار

802.11، ذلك، هو عزاز إلى آخر. تختلف الدعم بشكل كبير من جهاز إلى آخر، لذلك هي لا تزال هذه الطريقة التي تم اعتمادها بشكل أكبر في انتظار الإصدار 802.11r.

ملاحظة حول مصطلح "التخزين المؤقت الاستباقي للمفاتيح"

يعرف التخزين المؤقت الاستباقي للمفاتيح (أو PKC) باسم OKC (ذاكرة التخزين المؤقت للمفاتيح الانتهازي)، ويتم إستخدام المصطلحين بالتبادل عند الإشارة إلى نفس الطريقة للمفاتيح المؤقتة التي تم تقديمها في عام 2001. ومع ذلك، لم يكن هذا سوى مصطلح استخدمه المجال الجوي لوصف أساس 802.11i الذي تم إستخدامه بعد ذلك مباشرة لتوحيد طريقة تخزين المفاتيح المؤقت (والتي أصبحت تعرف رسميا بإسم "المصادقة المسبقة" (وهو أسلوب آخر من أساليب التجوال السريع المأمون والمضحة أدناه). PKC ليس Preauthentication أو OKC (التخزين المؤقت للمفاتيح الانتهازي)، ولكن إلى OKC، ولكن إلى ما قبل المصادقة. هو الأساس الذي يتم عن PKC أو تقريبا عن، فإن المرجع عند تسمية

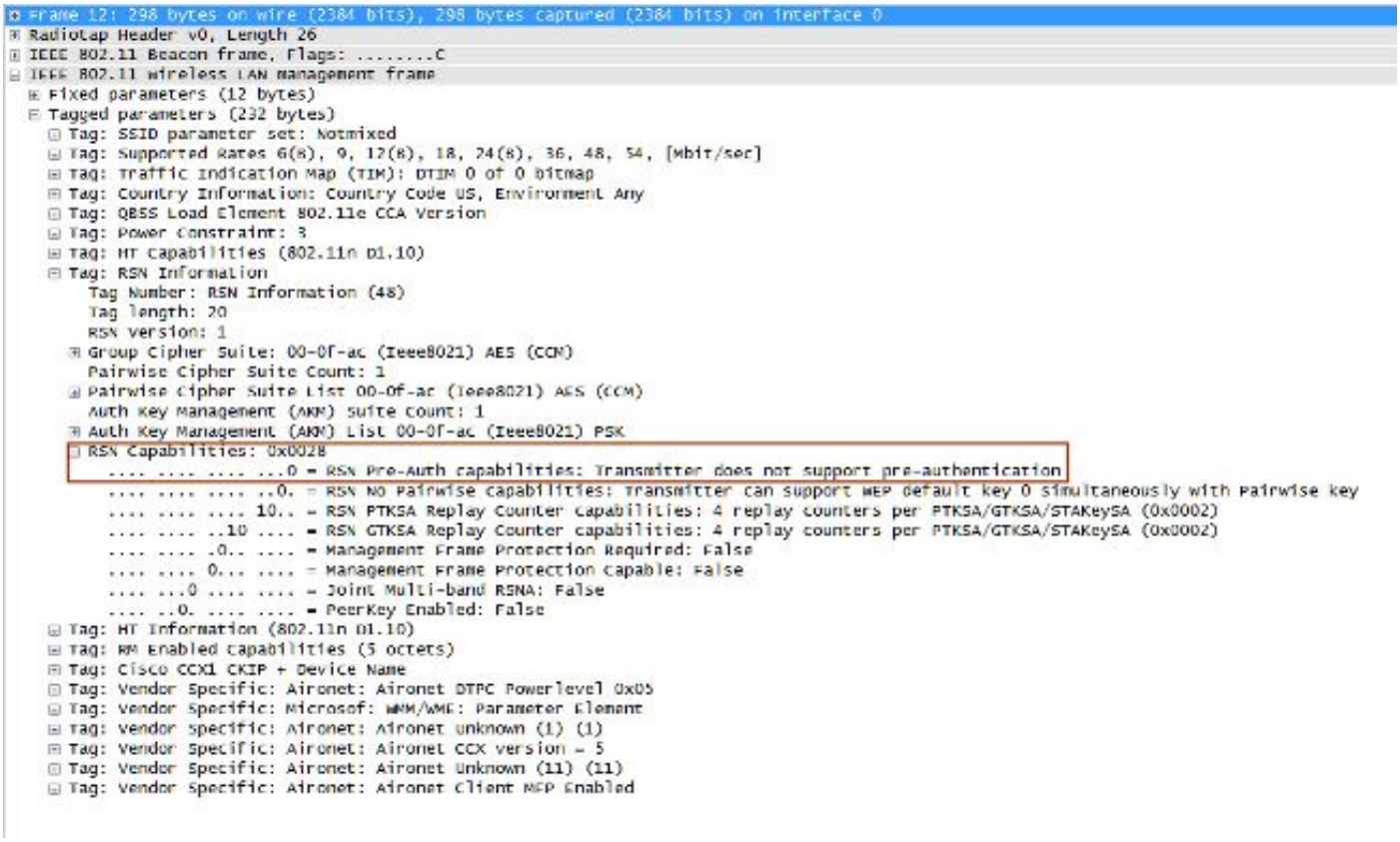
التجوال الآمن السريع مع إمكانية المصادقة المسبقة

802.11i، ذلك تم إقتراح هذه الطريقة من قبل مجموعة IEEE 802.11 العاملة لتعديل الأمان 802.11 لتتمكن من التجوال الآمن السريع التي تعمل أيضا مع WPA2، ولكنها الطريقة الوحيدة للتجوال الآمن السريع التي تدعمها Cisco. ولهذا السبب، لا يشرح الإيجاز هنا وبدون البنية الأساسية لشبكة WLAN من Cisco. ولهذا السبب، لا يشرح الإيجاز هنا وبدون تفاصيل.

قبل عملية المصادقة باستخدام المصادقة باستخدام نقاط الوصول الحالية. عندما يحدث ذلك، يرسل العميل إطارات مصادقة EAP إلى نقطة الوصول الحالية حيث تكون متصلة، ولكنها موجهة إلى نقطة الوصول الأخرى حيث يريد العميل إجراء المصادقة المسبقة (نقاط الوصول المجاورة التي يمكن ترشيحها للتجوال). ترسل نقطة الوصول الحالية هذه الإطارات إلى نقاط الوصول (AP) الهدف عبر نظام التوزيع. تقوم نقطة الوصول الجديدة بإجراء مصادقة EAP مع الخادم RADIUS لذا العميل، لذلك يتم إكمال مصافحة المصادقة المسبقة كما لو كانت نقطة الوصول الجديدة هذه هي نقطة الوصول الجديدة بالكامل، وتعمل.

قبل أن تتمكن المجموعة (APs) من نقل مفتاح PMK إلى نقاط الوصول (APs) المجاورة في إجراء المصادقة واشتقاق PMK، تتم مصادقة العميل بالفعل بالتجوال إليها، لذلك عندما يحين الوقت للتجوال، يقوم العميل بالفعل بالتجوال بين نقاط الوصول المجاورة وبوجود PMK مخزنة مؤقتا بالفعل لهذا الاقتران الآمن الجديد، لا يحتاج العميل إلى إجراء المصافحة الرباعية الإتجاه والتجربة، لذلك يمكن للعميل بدء عملية السريع بعد أن يرسل العميل طلب إعادة الدمج الأولي الخاص به.

هذه الميزة من ميزات AP تظهر حقل RSN IE الذي يعلن عن دعم للمصادقة المسبقة (هذا واحد من نقاط الوصول Cisco، حيث يتم التأكد من أن المصادقة المسبقة غير مدعومة):



PROS مع ما قبل المصادقة

هناك PMK واحد لكل اقتران آمن ل AP-to-client، والذي يمكن اعتباره ميزة أمان في حالة أختراق نقطة وصول وسرقة المفاتيح (ال يمكن إستخدامها مع نقاط وصول أخرى). ومع ذلك، يتم التعامل مع ميزة الأمان هذه بواسطة البنية الأساسية للشبكة المحلية اللاسلكية (WLAN) بطرق مختلفة على طرق أخرى.

مخالط مع ما قبل المصادقة

- بسبب وجود PMK واحد لكل نقطة وصول، يكون للعملاء حد على مقدار نقاط الوصول التي يمكنهم مصادقتها مسبقا.
- في كل مرة يقوم فيها العميل بإجراء مصادقة مسبقة مع نقطة وصول جديدة، يكون هناك تبادل مصادقة EAP كامل، مما يعني المزيد من التحميل على الشبكة وعلى خادم المصادقة.
- الي سانديان معظم الزبائن اللاسلكيين هذه الطريقة، لأنها لم تكن أبدا معتمدة بشكل عال (كانت OKC معتمدة بشكل أكبر).

التجوال السريع الآمن مع 802.11r

تقنية التجوال السريع-الآمن القائمة على التعديل 802.11r (المسمى رسميا **الانتقال السريع ل BSS** حسب معيار 802.11، والمعروفة باسم **FT**) هي الطريقة الأولى التي تم التصديق عليها رسميا (في 2008) من قبل IEEE لمعيار 802.11 باعتباره الحل لإجراء عمليات انتقال سريعة بين نقاط الوصول (مجموعات الخدمات الأساسية أو وحدات BSS)، والذي يحدد بشكل واضح التسلسل الهرمي للمفاتيح الذي يتم إستخدامه عند معالجة مفاتيح التخزين المؤقت على شبكة محلية لاسلكية (WLAN). ومع ذلك، كان اعتماده بطيئا، ويعزى ذلك أساسا إلى الحلول الأخرى المتاحة بالفعل عندما كانت هناك حاجة فعلية إلى عمليات انتقال سريعة، مثل عمليات تنفيذ شبكات VoWLAN عند إستخدامها مع إحدى الطرق الموضحة سابقا في هذا المستند. الي يوجد سوى عدد قليل من الأجهزة التي تدعم حاليا بعض

خيارات ft (بحلول عام 2013).

هذا الأسلوب أكثر تعقيدا للشرح من الطرق الأخرى، حيث يقدم مفاهيم جديدة وطبقات فرعية (مخططة) تتحكم في مجموعة من PMKs التي يتم تخزينها مؤقتا على أجهزة نقطة الوصول (مخططة)، ويوفر المزيد من الخيارات للتجوال الآمن بسرعة. لذلك، يتم توفير ملخص موجز عن هذه الطريقة والطريقة التي يتم بها تنفيذها مع كل خيار متاح.

يختلف معيار 802.11r عن معيار SKC ومعيار OKC، ويرجع ذلك في المقام الأول إلى الأسباب التالية:

- تحدث رسائل المصافحة (PMKID، ANonce، و SNonce exchange، على سبيل المثال) في إطارات مصادقة 802.11 أو في إطارات إعادة التعيين. على عكس المصافحة المنفصلة التي تتم تجنب مرحلة المصافحة، يتم تخزين PMKID المؤقت لـ PMKID، وهو أساليب ذاكرة التخزين المؤقت الاختيارية. تبدأ مصافحة إعادة(إعادة) الارتباط لرسائل المصافحة الرباعية الإتجاه، والتي يتم نقلها بعد تداول الرسائل مع نقطة الوصول الجديدة قبل أن يقوم العميل بالتجوال/إعادة التثبيت مع المفاتيح نقطة الوصول الجديدة هذه.
- يوفر طريقتين للمصافحة سريعة التجوال: عبر الهواء ونظام التوزيع (DS).
- يحتوي 802.11r على المزيد من طبقات هيكل المفاتيح.
- بما أن هذا البروتوكول يتجنب المصافحة رباعية الإتجاه لإدارة المفاتيح عندما يجول العميل (ويولد مفاتيح تشفير جديدة -PTK و GTK- دون حاجة إلى هذه المصافحة)، يمكن استخدام مع PSK، وليس فقط عندما يتم إختبارات WPA2 أيضا تطبيقها على أساس المصادقة. يسرع هذا من التجوال أكثر لهذه التجهيزات حيث لا يوجد EAP أو 802.1X/EAP المصافحة الرباعية.

باستخدام هذه الطريقة، يقوم العميل اللاسلكي بإجراء مصادقة أولية واحدة فقط مقابل نقطة البنية الأساسية للشبكة المحلية اللاسلكية (WLAN) عند تأسيس اتصال بنقطة الوصول الأولى، ويقوم بتنفيذ التجوال السريع الآمن أثناء التجوال بين نقاط الوصول من نفس مجال تنقل FT.

هذا هو أحد المفاهيم الجديدة، والتي تشير أساسا إلى نقاط الوصول التي تستخدم نفس مفاتيح FT. SSID (المعروفة باسم مجموعة الخدمة الموسعة أو ESS) والتي تتعامل مع نفس مجال تنقل FT. هذا مماثل للأساليب الأخرى التي تم شرحها حتى الآن. عادة ما تستند الطريقة التي تتعامل بها نقاط الوصول مع مفاتيح مجال تنقل FT إلى إعداد مركزي، مثل مجموعة WLC أو مجموعات التنقل، ومع ذلك، يمكن تنفيذ هذه الطريقة أيضا على بيئات AP المستقلة.

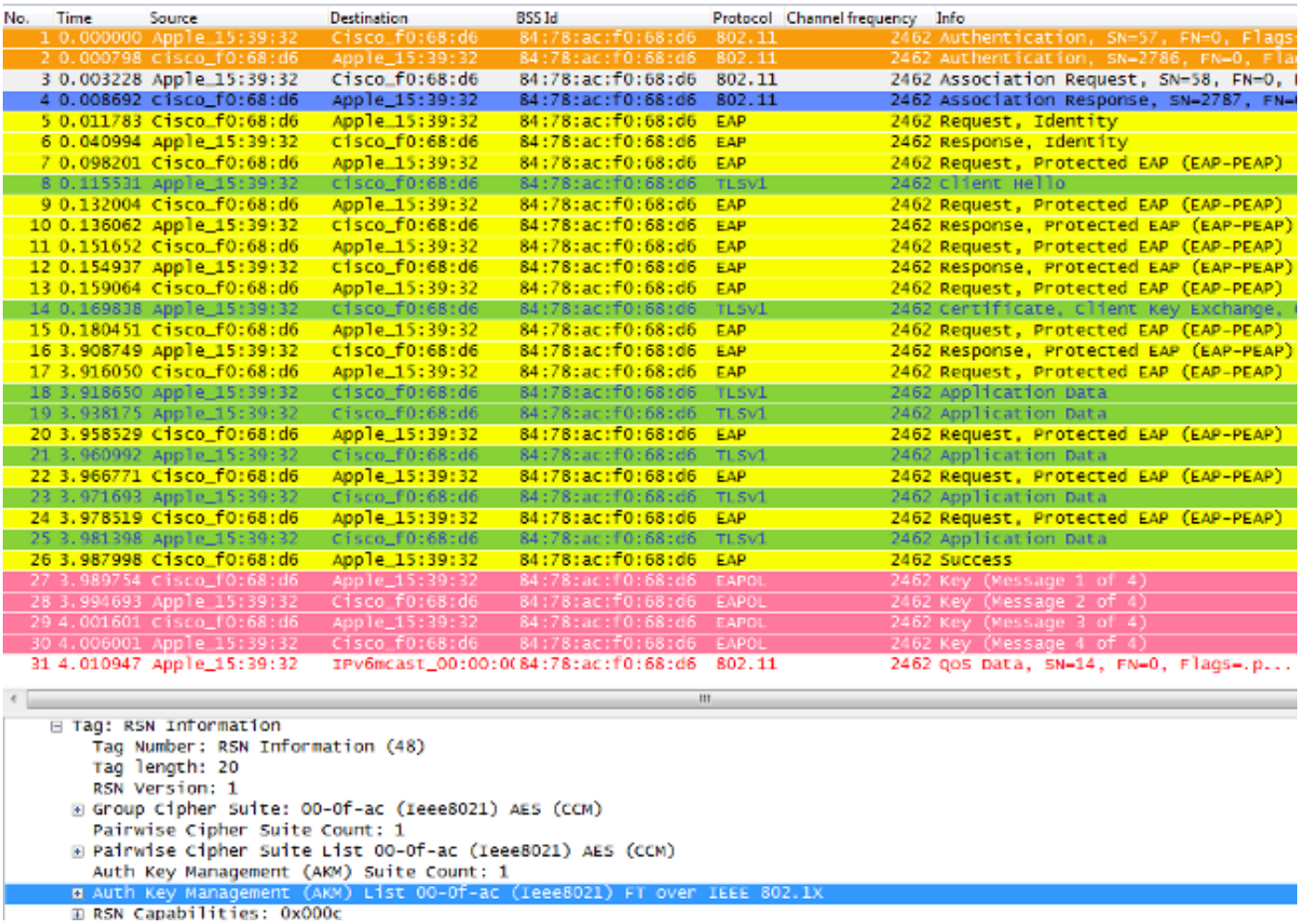
فيما يلي ملخص للتسلسل الهرمي للمفاتيح:

- ال MSK المشتقة على طالب العميل وخادم المصادقة من مرحلة مصادقة 802.1X/EAP الأولية (يتم توجيهها من خادم المصادقة إلى المصدق (WLC) بمجرد نجاح المصادقة). عندما يتم إستخدام MSK هذا، مثل الطرق الأخرى، كبذرة للتدرج الهرمي لمفاتيح FT. إذا كان هذا MSK يكون في الأساس PSK، فإن مصادقة EAP الدنيا من أسلوب WPA2-PSK تستخدم.
- يتم اشتقاق مفتاح R0 الرئيسي غير الكيمي (PMK-R0) من MSK، والذي هو مفتاح المستوى الأول من التسلسل الهرمي لمفاتيح FT. أصحاب المفاتيح لهذا PMK-R0 هم WLC والعميل.
- يتم اشتقاق مفتاح المستوى الثاني، يسمى مفتاح R1 الرئيسي Pairwise (PMK-R1)، من PMK-R0، وحملة المفاتيح هم العميل ونقاط الوصول التي تديرها WLC التي تحمل PMK-R0.
- مفتاح المستوى الثالث والأخير للتدرج الهرمي لمفاتيح FT هو PTK، والذي هو المفتاح المماثل للأساليب النهائي المستخدم لتشفير إطارات بيانات البث الأحادي 802.11 (WPA2/AES أو WPA/TKIP الأخرى التي تستخدم). يتم اشتقاق PTK هذا على FT من PMK-R1، وحاملو المفاتيح هم العميل ونقاط الوصول التي تديرها WLC.

ملاحظة: يمكن للبنية الأساسية للشبكة المحلية اللاسلكية (WLAN) نقل المفاتيح ومعالجتها بطريقة مختلفة، وذلك بناء على مورد الشبكة المحلية اللاسلكية (WLAN) وشرائح التنفيذ (مثل نقاط الوصول (AP) المستقلة أو FlexConnect أو Mesh). بل إنه يستطيع حتى تغيير أدوار حاملي المفاتيح، ولكن نظرا لأن ذلك خارج نطاق هذا المستند، فإن الأمثلة المستندة إلى ملخص التدرج الهرمي الرئيسي الذي تم تقديمه سابقا هي التركيز التالي. إن الاختلافات في الواقع ليست بتلك الأهمية لفهم العملية، ما لم تكن بحاجة بالفعل إلى التحليل التفصيلي لأجزاء البنية الأساسية (ورموزها) من أجل اكتشاف مشكلة في البرنامج.

انتقال BSS السريع عبر الهواء

باستخدام هذه الطريقة، يكون أول اقتران بأي نقطة وصول مصادقة منتظمة من المرة الأولى للشبكة المحلية اللاسلكية (WLAN)، حيث يجب أن تحدث مصادقة 802. 1X/EAP بالكامل مقابل خادم المصادقة ومصافحة 4 طرق لإنشاء المفاتيح قبل إرسال إطارات البيانات، كما هو موضح في صورة الشاشة هذه:



والاختلافات الرئيسية هي:

- يختلف تفاوض إدارة مفتاح المصادقة إختلافا طفيفا عن تفاوض WPA/WPA2 العادي، لذلك يتم إستخدام بعض المعلومات الإضافية لإجراء هذا التفاوض عند حدوث اقتران ببنية أساسية لشبكة WLAN تدعم ft. كما هو موضح في الصورة، يتم تحديد إطار طلب الاقتران من العميل ويتم تمييز حقل AKM الخاص بعنصر معلومات RNS لإظهار أن هذا العميل يريد تنفيذ FT أكثر من 802.1X/EAP.
- كما يظهر عنصر معلومات مجال التنقل (جزء من FT)، حيث يشير حقل **قدرة FT والسياسة** إلى ما إذا كان الانتقال السريع ل BSS مكتمل عبر الهواء أو عبر DS عند التجوال السريع

(يشير ذلك إلى ما وهو عبر الهواء في هذه الصورة).

- كما تتم إضافة عنصر معلومات آخر (نقل BSS السريع أو FT IE، والموضحة في هذه الحالة في FT.
  المستند) مع المعلومات المطلوبة لتنفيذ تسلسل مصادقة FT عند تجوال FT.
- على الرغم من أن التسلسل الهرمي للمفاتيح باختلاف المفاتيح، لذلك يختلف جيل المفاتيح في الواقع إلا أنه في مشابهة للمصافحة WPA/WPA2 4-Way، وتبدو مصافحة FT 4-way تختلف قليلاً في المحتوى.

تظهر الأخطاء بشكل أساسي نفس تباديل إطار مصادقة EAP كما يقطر عند المصادقة الأولية للشبكة المحلية اللاسلكية (من الصور، لكن تتم إضافة بعض ظاهر وهو كما)، ولكن تتم إضافة بعض المخرجات التي تتعلق بتقنيات التخزين المؤقت للمفاتيح المستخدمة من قبل وحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، وبالتالي، يتم قطع إخراج تصحيح الأخطاء هذا لعرض المعلومات ذات الصلة فقط:

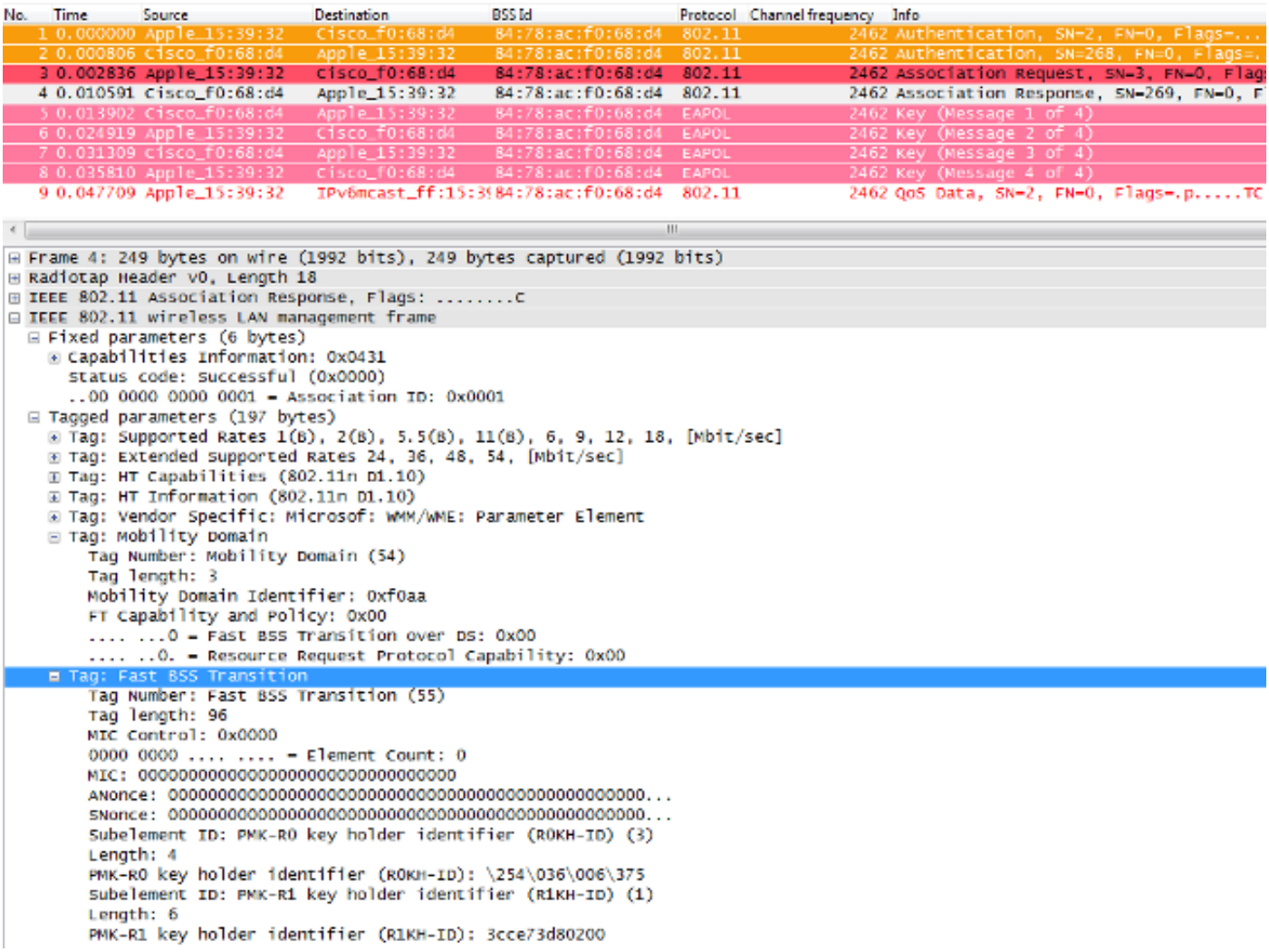
```
*apfMsConnTask_0: Jun 27 19:25:23.426: ec:85:2f:15:39:32
  Association received from mobile on BSSID
  84:78:ac:f0:68:d6
!--- This is the Association request from the client.

*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Marking this mobile as TGr capable.
!--- WLC recognizes that the client is 802.11r-capable.

*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 20 for mobile
  ec:85:2f:15:39:32
!--- The WLC/AP finds an Information Element that claims FT
     support on the Association request that is sent from the client.

*apfMsConnTask_0: Jun 27 19:25:23.427:
  Sending assoc-resp station:ec:85:2f:15:39:32
  AP:84:78:ac:f0:68:d0-00 thread:144be808
*apfMsConnTask_0: Jun 27 19:25:23.427:
  Adding MDIE, ID is:0xaaf0
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Including FT Mobility Domain IE (length 5) in Initial
  assoc Resp to mobile
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Sending R0KH-ID as:-84.30.6.-3
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Sending R1KH-ID as 3c:ce:73:d8:02:00
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Including FT IE (length 98) in Initial Assoc Resp to mobile
*apfMsConnTask_0: Jun 27 19:25:23.427: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d6
  (status 0) ApVapId 7 Slot 0
!--- The Association Response is sent to the client once the
     FT information is computed (as per the previous messages),
     so this is included in the response.

*dot1xMsgTask: Jun 27 19:25:23.432: ec:85:2f:15:39:32
  Sending EAP-Request/Identity to mobile ec:85:2f:15:39:32
  (EAP Id 1)
!--- EAP begins, and follows the same exchange explained so far.

*apfMsConnTask_0: Jun 27 19:25:23.436: ec:85:2f:15:39:32
  Got action frame from this client.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.449: ec:85:2f:15:39:32
  Received EAPOL EAPPKT from mobile ec:85:2f:15:39:32
```

```
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.449: ec:85:2f:15:39:32
  Received Identity Response (count=1) from mobile
  ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.456: ec:85:2f:15:39:32
  Processing Access-Challenge for mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.456: ec:85:2f:15:39:32
  Sending EAP Request from AAA to mobile ec:85:2f:15:39:32
  (EAP Id 2)

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.479: ec:85:2f:15:39:32
  Received EAPOL EAPPKT from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.479: ec:85:2f:15:39:32
  Received EAP Response from mobile ec:85:2f:15:39:32
  (EAP Id 2, EAP Type 25)

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.627: ec:85:2f:15:39:32
  Processing Access-Accept for mobile ec:85:2f:15:39:32
!--- The client is validated/authenticated by the RADIUS Server.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.627: ec:85:2f:15:39:32
  Creating a PKC PMKID Cache entry for station
  ec:85:2f:15:39:32 (RSN 2)
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.627: ec:85:2f:15:39:32
  Resetting MSCB PMK Cache Entry 0 for station
  ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.627: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 8
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.628: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 0
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.628: ec:85:2f:15:39:32
  Adding BSSID 84:78:ac:f0:68:d6 to PMKID cache at index 0
  for station ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.628: New PMKID: (16)
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.628:
  [0000] 52 b8 8f cf 50 a7 90 98 2b ba d6 20 79 e4 cd f9
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.629: ec:85:2f:15:39:32
  Created PMK Cache Entry for TGr AKM:802.1x ec:85:2f:15:39:32
!--- WLC creates a PMK cache entry for this client, which is
      used for FT with 802.1X in this case, so the PMKID is
      computed with the AP MAC address (BSSID 84:78:ac:f0:68:d6).

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.629:
  ec:85:2f:15:39:32   R0KH-ID:172.30.6.253
  R1KH-ID:3c:ce:73:d8:02:00  MSK Len:48 pmkValidTime:1807
!--- The R0KH-ID and R1KH-ID are defined, as well as the PMK
      cache validity period.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: ec:85:2f:15:39:32
  PMK sent to mobility group
!--- The FT PMK cache entry for this client is shared with the
      WLCs on the mobility group.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: ec:85:2f:15:39:32
  Sending EAP-Success to mobile ec:85:2f:15:39:32 (EAP Id 12)

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: ec:85:2f:15:39:32
  Found an cache entry for BSSID 84:78:ac:f0:68:d6 in PMKID
  cache at index 0 of station ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: Including PMKID in
  M1  (16)
```

```
!--- The hashed PMKID is included on the Message-1 of the
     initial FT 4-Way handshake.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630:
  [0000] 52 b8 8f cf 50 a7 90 98 2b ba d6 20 79 e4 cd f9

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.630: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  INITPMK (message 1), replay counter 00.00.00.00.00.00.00.0
!--- Message-1 of the FT 4-Way handshake is sent from the
     WLC/AP to the client.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Received EAPOL-key in PTK_START state (message 2) from
  mobile ec:85:2f:15:39:32
!--- Message-2 of the FT 4-Way handshake is received
     successfully from the client.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Calculating PMKR0Name
!--- The PMKR0Name is calculated.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  DOT11R: Sending cache add

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: Adding MDIE,
  ID is:0xaaf0
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Adding TIE for reassociation deadtime:20000 milliseconds
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.639: ec:85:2f:15:39:32
  Adding TIE for R0Key-Data valid time :1807
*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.640: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01
!--- After the MDIE, TIE for reassociation deadtime, and TIE
     for R0Key-Data valid time are calculated, the Message-3
     of this FT 4-Way handshake is sent from the WLC/AP to the
     client with this information.

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.651: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:25:23.651: ec:85:2f:15:39:32
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile ec:85:2f:15:39:32
!--- Message-4 (final message) of this initial FT 4-Way handshake
     is received successfully from the client, which confirms the
     installation of the derived keys. They can now be used in order
     to encrypt data frames with the current AP.
```

ملاحظة: لتصحيح أخطاء هذه الطريقة والوصول إلى مخرجات 802.11r/ft الإضافية، وهو **تمكين تصحيح الأخطاء لعميل** مع إضافي تصحيح أخطاء إضافي تم تمكين، انه الموضح **أحداث debug ft**.

فيما يلي الصور وتصحيح أخطاء اقتران أولي بشبكة WLAN عند تنفيذ FT باستخدام WPA2-PSK (بدلا من طريقة 802.1X/EAP)، حيث تم تحديد إطار إستجابة الاقتران من نقطة الوصول لعرض عنصر معلومات انتقال BSS السريع (مبرزة). كما تم عرض بعض المعلومات الأساسية اللازمة لإجراء مصافحة FT 4-Way:



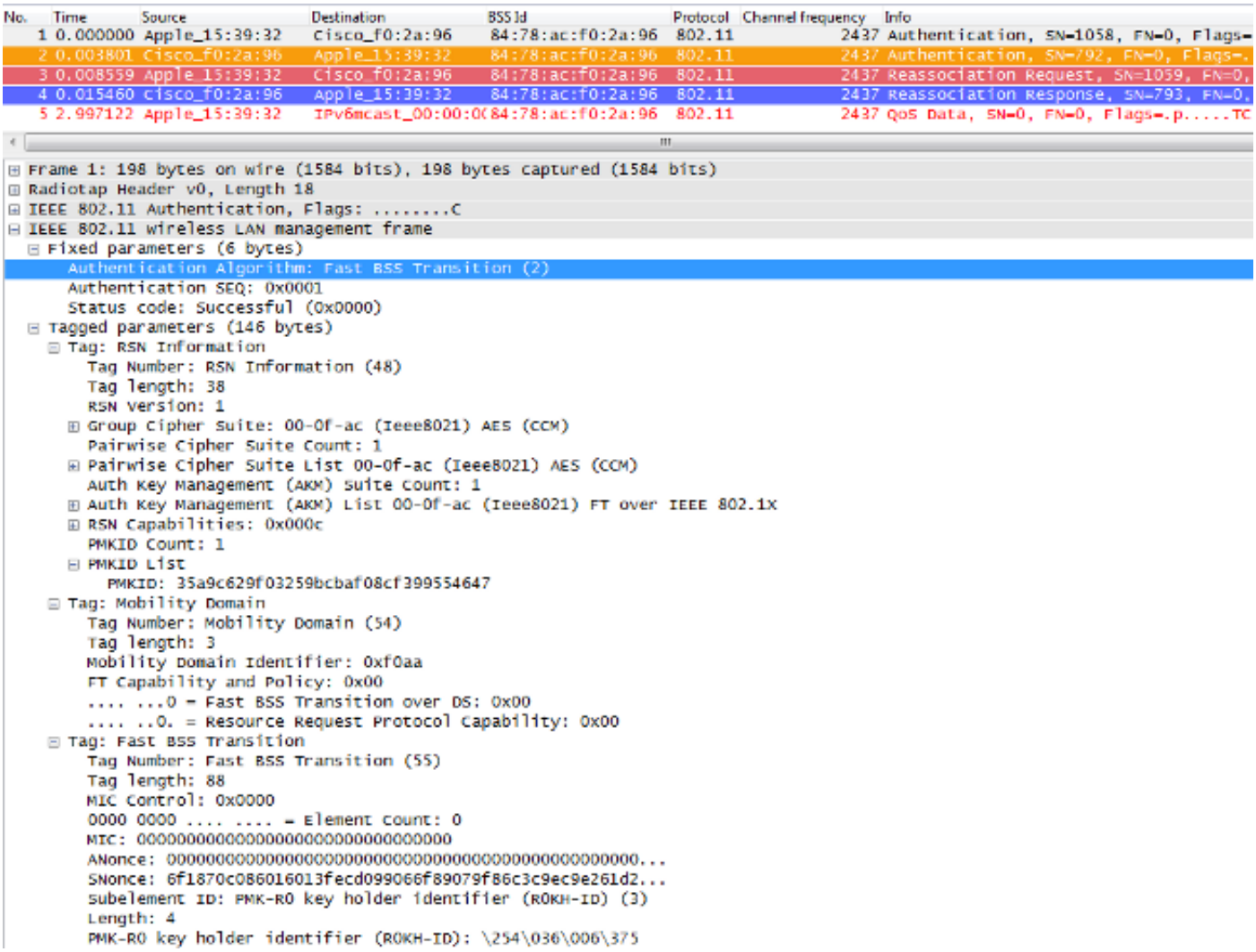

```
*apfMsConnTask_0: Jun 27 19:29:09.136: ec:85:2f:15:39:32
  Association received from mobile on BSSID
  84:78:ac:f0:68:d4

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Marking this mobile as TGr capable.

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 20 for mobile
  ec:85:2f:15:39:32

*apfMsConnTask_0: Jun 27 19:29:09.137: Sending assoc-resp
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:68:d0-00
  thread:144be808

*apfMsConnTask_0: Jun 27 19:29:09.137: Adding MDIE,
  ID is:0xaaf0

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Including FT Mobility Domain IE (length 5) in Initial
  assoc Resp to mobile

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
```

```
  Sending R0KH-ID as:-84.30.6.-3

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Sending R1KH-ID as 3c:ce:73:d8:02:00

*apfMsConnTask_0: Jun 27 19:29:09.137: ec:85:2f:15:39:32
  Including FT IE (length 98) in Initial Assoc Resp to mobile

*apfMsConnTask_0: Jun 27 19:29:09.138: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID 84:78:ac:f0:68:d4
  (status 0) ApVapId 5 Slot 0

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Creating a PKC PMKID Cache entry for station
  ec:85:2f:15:39:32 (RSN 2)

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Resetting MSCB PMK Cache Entry 0 for station
  ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 8

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Setting active key cache index 8 ---> 0

*dot1xMsgTask: Jun 27 19:29:09.141: ec:85:2f:15:39:32
  Adding BSSID 84:78:ac:f0:68:d4 to PMKID cache at
  index 0 for station ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.142: New PMKID: (16)

*dot1xMsgTask: Jun 27 19:29:09.142:
  [0000] 17 4b 17 5c ed 5f c7 1d 66 39 e9 5d 3a 63 69 e7

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  Creating global PMK cache for this TGr client

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  Created PMK Cache Entry for TGr AKM:PSK
  ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  R0KH-ID:172.30.6.253   R1KH-ID:3c:ce:73:d8:02:00
  MSK Len:48 pmkValidTime:1813

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  Initiating RSN PSK to mobile ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.142: ec:85:2f:15:39:32
  Found an cache entry for BSSID 84:78:ac:f0:68:d4 in
  PMKID cache at index 0 of station ec:85:2f:15:39:32

*dot1xMsgTask: Jun 27 19:29:09.142: Including PMKID
  in M1  (16)

*dot1xMsgTask: Jun 27 19:29:09.142:
  [0000] 17 4b 17 5c ed 5f c7 1d 66 39 e9 5d 3a 63 69 e7

*dot1xMsgTask: Jun 27 19:29:09.143: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32
  state INITPMK (message 1), replay counter
  00.00.00.00.00.00.00.00
```

```
*apfMsConnTask_0: Jun 27 19:29:09.144: ec:85:2f:15:39:32
  Got action frame from this client.

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.152: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: ec:85:2f:15:39:32
  Received EAPOL-key in PTK_START state (message 2) from
  mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: ec:85:2f:15:39:32
  Calculating PMKR0Name

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: Adding MDIE,
  ID is:0xaaf0

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: ec:85:2f:15:39:32
  Adding TIE for reassociation deadtime:20000 milliseconds

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.153: ec:85:2f:15:39:32
  Adding TIE for R0Key-Data valid time :1813

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.154: ec:85:2f:15:39:32
  Sending EAPOL-Key Message to mobile ec:85:2f:15:39:32 state
  PTKINITNEGOTIATING (message 3), replay counter
  00.00.00.00.00.00.00.01

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.163: ec:85:2f:15:39:32
  Received EAPOL-Key from mobile ec:85:2f:15:39:32

*Dot1x_NW_MsgTask_2: Jun 27 19:29:09.163: ec:85:2f:15:39:32
  Received EAPOL-key in PTKINITNEGOTIATING state (message 4)
  from mobile ec:85:2f:15:39:32
```

باستخدام 802.11r، يكون الارتباط الأولي بالشبكة المحلية اللاسلكية (WLAN) هو الأساس المستخدم للاتصال المفاتيح الأساسية المستخدمة في هذه الأسلوب، تمامًا كما هو الحال في طرق التوجال الأخرى سريعة الأمان. وأهم الفروق هي عندما يبدأ العميل في التواصل، والتي تتجنب ft 802.1X/EAP عند طقف إستخدام ذلك، ولكنه ينفذ في الواقع طريقة مصادقة وإعادة تعيين النظام" ل 802.11 تاراخإ نيب عمجت ةيلاعف رثكأ لاجأ نم (لوصولا قاطن نيب لاجتوال دنع ءانثأ مدختسإ متي يتلاو) "حوتفملا تاباثلا عم FT واتخالصا مفاتيح تشفير ديناميكية جديدة بدلا من المصافحة الرباعية الإتجاه.

تظهر الصورة التالية الإطارات المتبادلة عند إجراء انتقال BSS سريع عبر الهواء مع أمان 802.1X/EAP. يتم تحديد إطار مصادقة النظام المفتوح من العميل إلى نقطة الوصول لترى عناصر معلومات ورموز FT لطلب عدة تفاوض مفاتيح FT. يتم إستخدام هذه الإجراء لتمييز PTK الجديدة من نقطة الوصول الجديدة (استنادا إلى PMK-R1). يتم تمكين مصادقة النظام إجراء مع العميل الذي يظهر خوارزمية المصادقة الظاهرة أن هذه الحقل لـ BSS: مفتوحة بسيطة، بل عملية انتقال سريعة

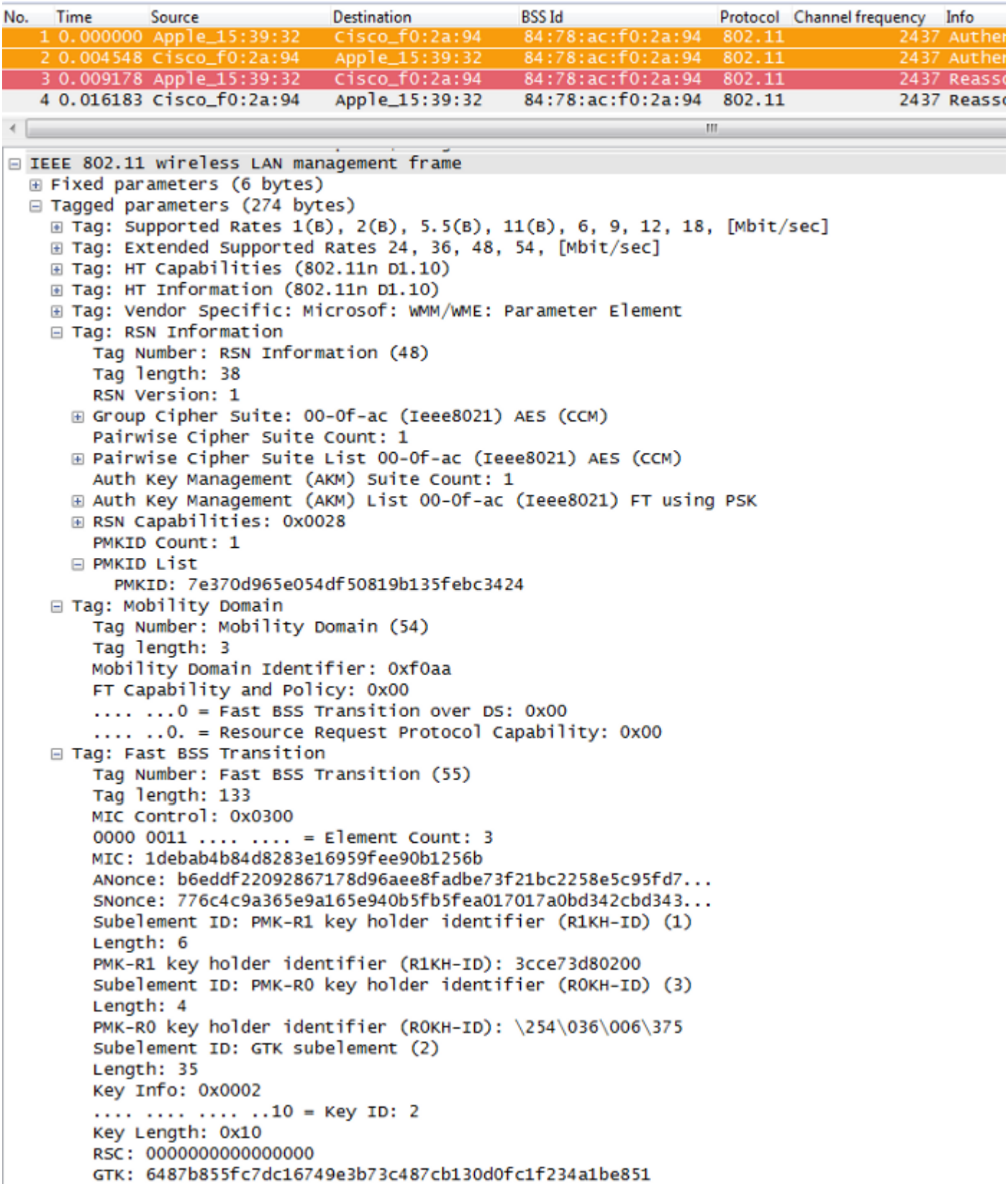


فيما يلي مخرجات تصحيح الأخطاء من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) عند حدوث حدث تجوال FT هذا مع 802.1X/EAP:

```
*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  Doing preauth for this client over the Air
!--- WLC begins FT fast-secure roaming over-the-Air with
      this client and performs a type of preauthentication,
      because the client asks for this with FT on the Authentication
      frame that is sent to the new AP over-the-Air
      (before the Reassociation Request).

*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  Doing local roaming for destination address
  84:78:ac:f0:2a:96
!--- WLC performs the local roaming event with the new AP to
      which the client roams.

*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  Got 1 AKMs in RSNIE
*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  RSNIE AKM matches with PMK cache entry :0x3
!--- WLC receives one PMK from this client (known as AKM here),
      which matches the PMK cache entry hold for this client.

*apfMsConnTask_2: Jun 27 19:25:48.751: ec:85:2f:15:39:32
  Created a new preauth entry for AP:84:78:ac:f0:2a:96
*apfMsConnTask_2: Jun 27 19:25:48.751: Adding MDIE,
  ID is:0xaaf0
```

```
!--- WLC creates a new preauth entry for this AP-and-Client pair,
     and adds the MDIE information.

*apfMsConnTask_2: Jun 27 19:25:48.763: Processing assoc-req
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a:90-00
  thread:144bef38
*apfMsConnTask_2: Jun 27 19:25:48.763: ec:85:2f:15:39:32
  Reassociation received from mobile on BSSID
  84:78:ac:f0:2a:96
!--- Once the client receives the Authentication frame reply from the
     WLC/AP, the Reassociation request is sent, which is received at
     the new AP to which the client roams.

*apfMsConnTask_2: Jun 27 19:25:48.764: ec:85:2f:15:39:32
  Marking this mobile as TGr capable.

*apfMsConnTask_2: Jun 27 19:25:48.764: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 38 for mobile
  ec:85:2f:15:39:32

*apfMsConnTask_2: Jun 27 19:25:48.765: ec:85:2f:15:39:32
  Roaming succeed for this client.
!--- WLC confirms that the FT fast-secure roaming is successful
     for this client.

*apfMsConnTask_2: Jun 27 19:25:48.765: Sending assoc-resp
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a:90-00
  thread:144bef38
*apfMsConnTask_2: Jun 27 19:25:48.766: Adding MDIE,
  ID is:0xaaf0
*apfMsConnTask_2: Jun 27 19:25:48.766: ec:85:2f:15:39:32
  Including FT Mobility Domain IE (length 5) in
  reassociation assoc Resp to mobile
*apfMsConnTask_2: Jun 27 19:25:48.766: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID 84:78:ac:f0:2a:96
  (status 0) ApVapId 7 Slot 0
!--- The Reassociation response is sent to the client, which
     includes the FT Mobility Domain IE.

*dot1xMsgTask: Jun 27 19:25:48.769: ec:85:2f:15:39:32
  Finishing FT roaming for mobile ec:85:2f:15:39:32
!--- FT roaming finishes and EAP is skipped (as well as any
     other key management handshake), so the client is ready
     to pass encrypted data frames with the current AP.

*dot1xMsgTask: Jun 27 19:25:48.769: ec:85:2f:15:39:32
  Skipping EAP-Success to mobile ec:85:2f:15:39:32
```

فيما يلي صورة تعرض انتقال سريع لـ BSS عبر الهواء مع أمان WPA2-PSK، حيث يتم تحديد إطار إستجابة إعادة التكوين النهائي من نقطة الوصول إلى العميل لإظهار مزيد من التفاصيل حول تبادل FT هذا:



No.	Time	Source	Destination	BSS Id	Protocol	Channel frequency	Info
1	0.000000	Apple_15:39:32	Cisco_f0:2a:94	84:78:ac:f0:2a:94	802.11	2437	Auther
2	0.004548	Cisco_f0:2a:94	Apple_15:39:32	84:78:ac:f0:2a:94	802.11	2437	Auther
3	0.009178	Apple_15:39:32	Cisco_f0:2a:94	84:78:ac:f0:2a:94	802.11	2437	Reasso
4	0.016183	Cisco_f0:2a:94	Apple_15:39:32	84:78:ac:f0:2a:94	802.11	2437	Reasso

```
IEEE 802.11 wireless LAN management frame
  Fixed parameters (6 bytes)
  Tagged parameters (274 bytes)
    Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    Tag: HT Capabilities (802.11n D1.10)
    Tag: HT Information (802.11n D1.10)
    Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
    Tag: RSN Information
        Tag Number: RSN Information (48)
        Tag length: 38
        RSN Version: 1
      Group Cipher Suite: 00-0f-ac (Ieee8021) AES (CCM)
        Pairwise Cipher Suite Count: 1
      Pairwise Cipher Suite List 00-0f-ac (Ieee8021) AES (CCM)
        Auth Key Management (AKM) Suite Count: 1
      Auth Key Management (AKM) List 00-0f-ac (Ieee8021) FT using PSK
      RSN Capabilities: 0x0028
        PMKID Count: 1
      PMKID List
          PMKID: 7e370d965e054df50819b135febc3424
    Tag: Mobility Domain
        Tag Number: Mobility Domain (54)
        Tag length: 3
        Mobility Domain Identifier: 0xf0aa
        FT Capability and Policy: 0x00
        .... ...0 = Fast BSS Transition over DS: 0x00
        .... ..0. = Resource Request Protocol Capability: 0x00
    Tag: Fast BSS Transition
        Tag Number: Fast BSS Transition (55)
        Tag length: 133
        MIC Control: 0x0300
        0000 0011 .... .... = Element Count: 3
        MIC: 1debab4b84d8283e16959fee90b1256b
        ANonce: b6eddf22092867178d96aee8fadbe73f21bc2258e5c95fd7...
        SNonce: 776c4c9a365e9a165e940b5fb5fea017017a0bd342cbd343...
        Subelement ID: PMK-R1 key holder identifier (R1KH-ID) (1)
        Length: 6
        PMK-R1 key holder identifier (R1KH-ID): 3cce73d80200
        Subelement ID: PMK-R0 key holder identifier (R0KH-ID) (3)
        Length: 4
        PMK-R0 key holder identifier (R0KH-ID): \254\036\006\375
        Subelement ID: GTK subelement (2)
        Length: 35
        Key Info: 0x0002
        .... .... .... ..10 = Key ID: 2
        Key Length: 0x10
        RSC: 0000000000000000
        GTK: 6487b855fc7dc16749e3b73c487cb130d0fc1f234a1be851
```

فيما يلي مخرجات تصحيح الأخطاء عند حدوث حدث تجوال FT هذا مع PSK، والتي تكون مماثلة لتلك التي يتم فيها إستخدام 802.1X/EAP:

```
*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  Doing preauth for this client over the Air

*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  Doing local roaming for destination address
```

```
  84:78:ac:f0:2a:94

*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  Got 1 AKMs in RSNIE

*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  RSNIE AKM matches with PMK cache entry :0x4

*apfMsConnTask_2: Jun 27 19:29:29.854: ec:85:2f:15:39:32
  Created a new preauth entry for AP:84:78:ac:f0:2a:94

*apfMsConnTask_2: Jun 27 19:29:29.854: Adding MDIE,
  ID is:0xaaf0

*apfMsConnTask_2: Jun 27 19:29:29.867: Processing assoc-req
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a:90-00
  thread:144bef38

*apfMsConnTask_2: Jun 27 19:29:29.867: ec:85:2f:15:39:32
  Reassociation received from mobile on BSSID
  84:78:ac:f0:2a:94

*apfMsConnTask_2: Jun 27 19:29:29.868: ec:85:2f:15:39:32
  Marking this mobile as TGr capable.

*apfMsConnTask_2: Jun 27 19:29:29.868: ec:85:2f:15:39:32
  Processing RSN IE type 48, length 38 for mobile
  ec:85:2f:15:39:32

*apfMsConnTask_2: Jun 27 19:29:29.869: ec:85:2f:15:39:32
  Roaming succeed for this client.

*apfMsConnTask_2: Jun 27 19:29:29.869: Sending assoc-resp
  station:ec:85:2f:15:39:32 AP:84:78:ac:f0:2a:90-00
  thread:144bef38

*apfMsConnTask_2: Jun 27 19:29:29.869: Adding MDIE,
  ID is:0xaaf0

*apfMsConnTask_2: Jun 27 19:29:29.869: ec:85:2f:15:39:32
  Including FT Mobility Domain IE (length 5) in
  reassociation assoc Resp to mobile

*apfMsConnTask_2: Jun 27 19:29:29.870: ec:85:2f:15:39:32
  Sending Assoc Response to station on BSSID
  84:78:ac:f0:2a:94 (status 0) ApVapId 5 Slot 0

*dot1xMsgTask: Jun 27 19:29:29.874: ec:85:2f:15:39:32
  Finishing FT roaming for mobile ec:85:2f:15:39:32
```

طاب ترا ط على عاني ع السري BSS لق نو ض افو ت الذي درج م، ة روص الذي في ح ضو م وه ام ك
ت ي تي ع أر ة ت ال ت ار ا ط إ م دا خ ت س إ م ت ي ،(WLAN) ة ي ك ل س ا ل ل ة ي ح ل م ا ل ة ك ب ش ا ب ي ل أ و ا
ل ل ج ت و ا ب ط ل ا و ا م د خ ت س إ) ل ي م ع ل ن م ح و ت ف م ل ا م ا ظ ن ا م ة ق ا د ص ا و م ي م ع ة ق ا د ص ا م ظ ا
ن ي ي ع ت ل ا ة د ا ع إ ل ة ب ا ج ت س ا ل ا و ي ع ي ي ع ت ل ا ة د ا ع إ ل ب ل ط و ل و ص و ل ا ة ط ق ن ن م ة ح و ت ف م ل ا
ي ك م ص ا ف ح ة FT ع ب ر أ ع ط ر ق ن م ج أ ل ا ش ت ا ق ا PTK ل ا ج د ي د) ي ا ح أ ل ا ب ل ا ر ي ف ش ت ح ا ت ف م)
.(ر ي ف ش ت ح ا ت ف م/د د ع ت م ل ا ر ي ف ش ت ح ا ت ف م) GTK و

ي ك و ن، ت ا ر ا ط إ ل ا ه ذ ه ل د ا ب ت س ا ب ا ذ ه ا ي ق و م ي
و FT ى و ت ح م و ض ا ف ت و ه ذ ه ى ل ع ت ا ح ف م ل ا ه ذ ه ى ل ع ض ا ف و ت س ت ن ك ا ذ ا م س ف ن و ه ت ا ر ا ط إ ل ا
ي ذ ل ا و، ي س ي ئ ر ل ا ف ل ا خ ت ل ا و ه AKM ل ق ح ، ف إ ن ة ، ر و ص ل ا ي ف ح ض و م و ه ا م ك .ن ي ي أ ت ة ق ي ر ط PSK
ة ظ ح ا ل م ل ا م ه م ل ا ن م ، ذ ل ك .802.1X أ و PSK م ا د ت س ا ب ا ذ ي ف ن ت ب ي ق و م ي ل ي م ع ل ا ن ا ك ا ذ ا م د ك ؤ ي
ن أ ه ذ ه ا ل إ ا ر ا ط ا ت ا ل أ ر ب ع ة ا ل ت ح ت و ي ع ا د ة ع ل ى ا ذ ه ا ل ن و ع م ن م ع ل و م ا ت ا ل أ م ا ن ل ل ت ا ف و ض ا ل أ س ا س ي ،

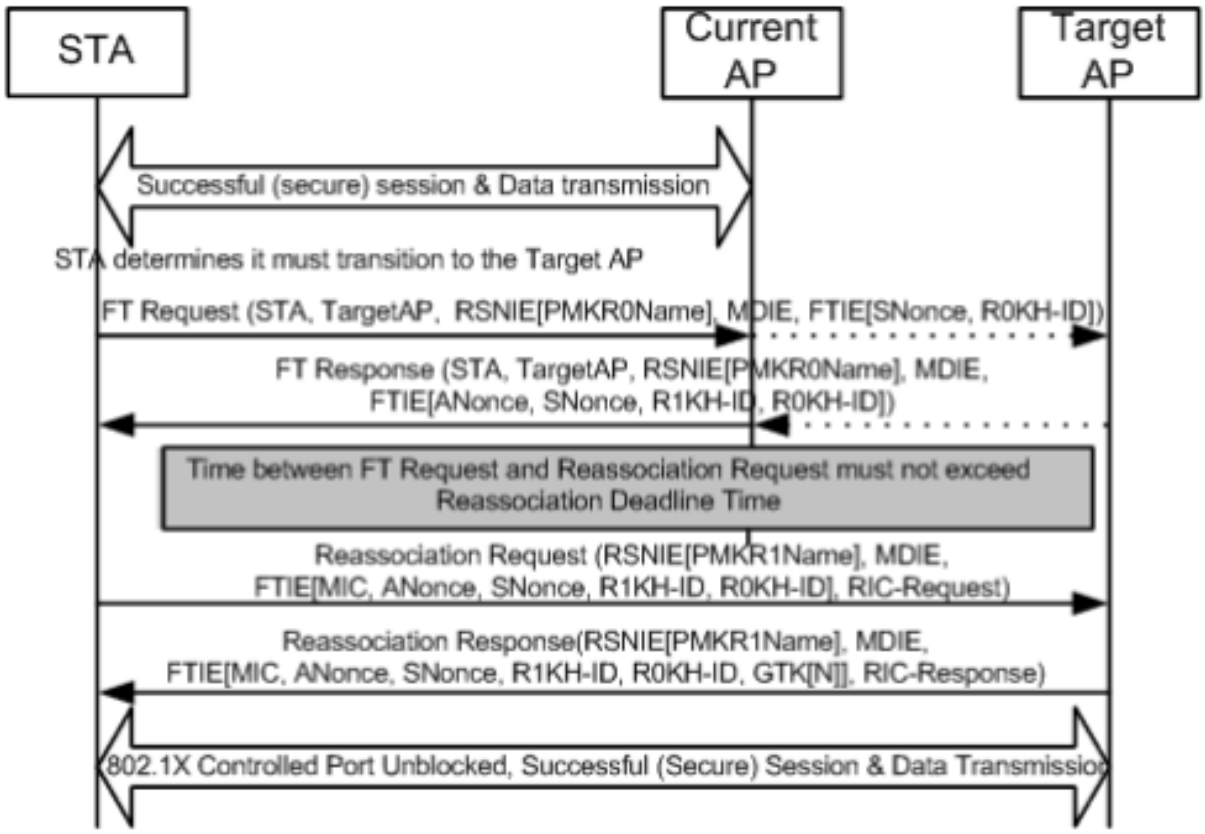
ولكن فقط عندما يقوم العميل بالتجوال إذا تم تنفيذ 802.11r والتفاوض بشأنها بين العميل والبنية الأساسية للشبكة المحلية اللاسلكية (WLAN) عند القارن الأولي.

انتقال BSS السريع عبر DS

802.11r يسمح بتنفيذ آخر للتحويل السريع BSS، حيث يبدأ العميل التجوال على الفك السلكي مع نقطة الوصول الجديدة التي يتجول العميل من أجلها عبر DS (نظام التوزيع)، وليس عبر الهواء. في هذه الحالة، يتم إستخدام إطارات إجراء FT لبدء التفاوض الرئيسي بدلا من إطارات مصادقة النظام المفتوحة.

في الأساس، عندما يقرر العميل أنه يمكنه التجوال إلى نقطة وصول أفضل، يرسل العميل إطار طلب إجراء FT إلى نقطة الوصول الأصلية حيث تكون متصلة حاليا قبل التجوال. يشير العميل إلى BSSID (عنوان MAC) لنقطة الوصول الهدف حيث يريد التجوال. تقوم نقطة الوصول الأصلية بإعادة توجيه إطار طلب إجراء FT هذا إلى نقطة الوصول الهدف عبر نظام التوزيع (عادة ما تكون البنية الأساسية السلكية)، وتستجيب نقطة الوصول الهدف إلى العميل من خلال إطار إستجابة إجراء FT (أيضا عبر DS، حتى يمكنها في النهاية إرسالها عبر الهواء إلى العميل). بمجرد نجاح تبادل إطار إجراء FT هذا، ينهي العميل تجوال FT؛ يرسل العميل، (عبر الهواء هذه المرة) طلب إعادة النشر إلى نقطة الوصول الهدف لتأكيد التجوال واشتقاق المفاتيح إستجابة إعادة تعيين من نقطة الوصول الجديدة النهائية.

باختصار، هناك أربعة إطارات للتفاوض على انتقال BSS سريع واستخلاص مفاتيح تشفير جديدة، ولكن هناك إطارات مصادقة النظام المفتوح إطارات إستبدال يتم تبادلها مع نقطة الوصول الهدف عبر نظام التوزيع مع طلب/إستجابة إجراء FT، والتي يتم تبادلها عبر نقطة الوصول الحالية. هذا الأسلوب صحيح أيضا لكل من طرق الأمان 802.1X/EAP و PSK، كما هذا، مع ذلك؛ Cisco من شبكة LAN اللاسلكية من مجموعة من وحدات التحكم في مجموعة من نقاط الوصول WiFi صناعة اللاسلكيين في معظم العملاء الذين يدعمون عبر DS غير انتقال الإطارات وتصحيح الأخطاء هي نفسها أساسا (وبما أن مخرجات تبادل الإطارات يتم توفير الف)، وبما أن هذه الصورة لعرض انتقال السريع المستند. بدلا من ذلك، يتم إستخدام هذه المثلة في الأ BSS عبر-DS:



تقنية FlexConnect مع الطراز 802.11r

- المصادقة المركزية مدعومة. ويتضمن ذلك تبديل البيانات المحلية والمركزية. يجب أن تكون نقاط الوصول جزءا من مجموعة FlexConnect نفسها.
- المصادقة المحلية غير مدعومة.
- الوضع المستقل غير مدعوم.

ميزات مع 802.11r

- هذه الطريقة هي الأولى التي تستخدم ترابط هرمي رئيسي تم تعريفه بشكل واضح بواسطة IEEE على مقياس 802.11 كتعديل (802.11r)، لذلك فإن تنفيذ تقنيات ft هذه يكون أكثر توافقا بين الموردين ودون تأويلات مختلفة.
- 802.11R تقنيات متعددة مفيدة تعتمد على إحتياجاتك (عبر الهواء وعبر نظام ds وأمان 802.1x/EAP وأمان PSK).
- يقوم العميل اللاسلكي بتنفيذ التجوال السريع الآمن إلى نقطة وصول جديدة على الشبكة المحلية اللاسلكية (WLAN)/SSID نفسها، حتى ولو لم تكن مقترنة بنقطة الوصول تلك مطلقا، دون الحاجة إلى حفظ العديد من بروتوكولات PMKID.
- هذه هي أول طريقة تجوال سريعة التأمين تتيح التجوال بسرعة أكبر حتى مع تأمين PSK، وتتجنب المصافحة الرباعية الإتجاه المطلوبة عند التجوال بين نقاط الوصول باستخدام WPA/WPA2 PSK. الغرض الأساسي من طرق التجوال السريعة التأمين هو تجنب مصافحة 802.1X/EAP عند تطبيق طريقة الأمان هذه، ومع ذلك، لأمان PSK يتم تسريع حدث التجوال أكثر مع 802.11r عند تجنب المصافحة الرباعية الإتجاه.

CONS مع 802.11r

- هناك عدد قليل من أجهزة العميل اللاسلكية التي تدعم بالفعل عمليات الانتقال السريعة لـ BSS، وفي معظم الحالات، لا تدعم جميع التقنيات المتوفرة على معيار 802.11r.
- نظرًا لحقيقة أن عمليات التنفيذ هذه صغيرة جدًا، لا توجد نتائج إختبار كافية من بيئات الإنتاج الحقيقي وأ نتائج تصحيح أخطاء كافية لمعالجة التنبيهات المحتملة التي يمكن أن تظهر.
- عندما تقوم بتكوين شبكة WLAN/SSID التي تستخدم أي من طرق FT، يمكن فقط للعملاء اللاسلكي الذين يدعمون معيار 802.11r الاتصال بشبكة WLAN/SSID هذه. إعدادات FT ليست إختيارية للعملاء، لذا إذا كان العملاء اللاسلكيين الذين لا يؤيدون معيار 802.11r الاتصال بشبكة محلية سلكية (WLAN)/SSID منفصلة حيث لم يتم تكوين FT على الإطلاق.

Adaptive 802.11r

- يتعذر على بعض العملاء القدامى الاقتران بشبكة WLAN/SSID التي تم تمكين عملاء على نفس مستوى الأمان (والذين يأملون أن يكونوا قادرين على الاتصال بـ "الوضع المختلط" في 802.11r). يحدث ذلك عندما يكون برنامج تشغيل مستخدم العميل المسؤول عن تحليل عناصر معلومات شبكة الأمان القوية (RSN IE) قديمًا أو لا يدعم 802.11r، ومن ثم، تحتاج إلى إرسال طلبات الاقتران إلى شبكات WLAN التي تعلن عن دعم 802.11r. انظر هذا التحديد، لا يمكن للعملاء إرسال مجموعات AKM الإضافية في IE. وبدلاً من ذلك، يقوم العملاء بإرسال طلبات الاقتران إلى شبكات WLAN التي تعلن عن دعم 802.11r. وشبكة WLAN/SSID واحدة لعملاء 802.11r وشبكة WLAN/SSID منفصلة للعملاء الذين لا تدعم شبكة 802.11r.
- ومن أجل التغلب على هذه المشكلة، قدمت البنية الأساسية لشبكة LAN اللاسلكية في مستوى الشبكة Adaptive 802.11r. عند تعيين وضع FT على Adaptive في شبكة 802.11r على شبكة المحلية اللاسلكية (WLAN)، تعلن WLAN عن معرف مجال التنقل MDIE على دعم Apple iOS10 وما بعده. تحدد بعض أجهزة عميل WLAN التي تم تمكين 802.11i بالفعل إنشاء اقتران 80211i/WPA2 وتقوم بمصافحة خاصة من أجل شبكة محلية سلكية 802.11r. بمجرد أن يكمل العميل اقتران 802.11r الناجح، يمكنه القيام بالتجوال عبر الإنترنت كما هو الحال في شبكة WLAN العادية التي تم تمكين 802.11r بها. الآن يمكن لجميع أجهزة Apple iOS10 (والإصدارات الأحدث) المحددة. يمكن العثور على مزيد من الوثائق حول هذه الميزة الجديدة المقدمة لأجهزة iOS10 وما بعدها في [أفضل ممارسات Cisco Wireless LAN على شبكة Cisco IOS لأجهزة المؤسسات](#).

الخلاصة

- تذكر دائمًا أن العميل هو الذي يقرر التجوال إلى نقطة وصول معينة، ولا يمكن أن يقرر العميل هذا. نقاط الوصول/وحدات التحكم في الشبكة المحلية اللاسلكية (WLC) هي عناصر التحكم في الشبكة المحلية اللاسلكية (WLC) التي يجب أن تعتبر أنه يجب عليه بدء التجوال. يتم بدء التجوال من قبل العميل اللاسلكي بمجرد أن يعتبر أنه يجب عليه التجوال.
- تدعم عناصر التحكم في الشبكة المحلية اللاسلكية (WLC) الجمع بين معظم أو جميع شبكة WLAN/SSID. ومع ذلك، كن على طرق FSR (التجوال السريع الآمن) مع إعدادات مختلفة جدًا (على سبيل المثال، حيث يتم تعطيل أحد الأساليب على العميل بينما يتم تمكين الأسلوب الآخر على العميل) يمكن أن يتسبب في حدوث مشكلات عند محاولة العميل التجوال بين وحدات التحكم في عبر الأجهزة المحمولة المختلفة (على سبيل المثال، من أجل الدعم أو حتى فهم ما تحاول وحدة التحكم في

الشبكة المحلية اللاسلكية (WLC) الإعلان عن مدموع. وبدلا من تحقيق قابلية التشغيل البيني في معرف SSID واحد فقط، يكون هناك عادة عدد من المشاكل أكبر من ذلك. يجب إكمال الاختبار العميق مع جميع المتوقع إصلاحها، وبالتالي الوصي بذلك إذا كانت هذه WLAN حاجة العملاء المحتملين الذين سيتم إستخدامهم على شبكة WLAN هذه فعلية لذلك.

- من المهم جدا أن تفهم أنه يتم تطوير طرق التواصل الآمنة بسرعة من أجل تسريع عملية التواصل على الشبكة المحلية اللاسلكية (WLAN) عندما تنتقل بين نقاط الوصول إذا كان هناك تأمين ممكن للشبكة المحلية اللاسلكية (WLAN)/SSID. في حالة عدم وجود تأمين، الإدارة إطارات بتبديل الوصول نقطة الوصول، حيث توقع شيء للتعجيل، يوجد الي إطارات البيانات إرسال قبل الوصول نقطة من العميل ومصادقة مفتوحة نظام مصادقة مفتوحة من العميل ونقطة الوصول بطلب إعادة الدمج والاستجابة إلعادة التعيين). لذلك، الي يمكن أن يتحرك هذه بشكل أسرع. إذا كانت واجهت مشاكل التواصل بدون تأمين، الفشل في التواصل، فقط تحسين التواصل سريع لتحسين مراقبة WLAN/SSID وتصميم إعداد إذا كان مهم للتأكد من طرق للتنقل بالتبعية بين الخلايا تغطية نقطة الوصول.
- يتم تنفيذ 802.11r/ft مع WPA2-PSK من أجل تسريع أحداث التواصل بهذا التأمين وتجنب المصافحة الرباعية الإتجاه، كما هو موضح ضمن قسم 802.11r.
- ولكل من الطرق مزايا وعيوب، ولكن في النهاية، يجب عليك التحقق دائما مما إذا كانت محطات العميل اللاسلكية تدعم الطريقة المحددة التي تريد تنفيذها، وما إذا كانت البنية الأساسية للشبكة المحلية اللاسلكية (WLAN) من Cisco تدعم جميع الطرق المتاحة. ومن ثم، يجب عليك تحديد أفضل الطرق التي يدعمها العملاء اللاسلكيون بالفعل والتي تتصل بالشبكة المحلية اللاسلكية (WLAN)/SSID المحددة. على سبيل المثال، في بعض عمليات النشر، يمكنك إنشاء شبكة WLAN/SSID باستخدام CCKM ولكن ليس Cisco Wireless IP (التي تدعم WPA2/AES باستخدام CCKM)، ثم شبكة WLAN/SSID أخرى مع WPA2/AES عبر 802.11r/FT للعملاء اللاسلكيين الذين يدعمون طريقة التواصل السريع الآمن (أو يستخدمون OKC، إذا كان هذا ما يتم دعمه).
- إذا لم يدعم العملاء اللاسلكي أي من طرق التواصل السريعة التأمين المتاحة، فقد تحتاج إلى قبول حقيقة أن هؤلاء العملاء يمكنهم دائما تجربة التأخيرات الموضحة في هذا المستند عند التواصل بين نقاط الوصول على شبكة WLAN/SSID مع أمان 802.1X/EAP (الذي يمكن أن يتسبب في حالات انقطاع في تطبيقات/خدمات العميل).
- يتم دعم جميع الطرق، باستثناء SKC (WPA2 PMKID Caching)، للتواصل الآمن السريع بين نقاط الوصول التي تديرها وحدات تحكم الشبكة المحلية اللاسلكية (WLCs) مختلفة (التواصل بين وحدات التحكم)، طالما أنها موجودة على نفس مجموعة التنقل.
- يدعم CUWN بشكل كامل جميع طرق التواصل السريعة التأمين المختلفة المغطاة في هذه المادة عند إستخدام مصادقة 802. 1X/EAP لـ WPA/WPA2. الي يدعم CUWN التواصل السريع الآمن على الطرق التي تعمل مع WPA2-RSN (CCKM، PMKID Caching/SKC، OKC/PKC) عند إستخدام PSK (WPA2-Personal)، حيث الي تكون هناك حاجة غالبا لطرق التواصل السريع. ومع ذلك، يدعم CUWN التواصل السريع والآمن في حالة WPA2-ft (802.11r) مع PSK كما هو موضح أيضا في هذه المقالة.

معلومات ذات صلة

- [دليل نشر التحويل السريع لـ 802.11r BSS]
- [الدعم التقني والتنزيلات من Cisco]

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).