تكوين أمان Wi-Fi 6E WLAN من الطبقة 2 والتحقق منه

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

أمان Wi-Fi 6e

WPA3

المستويات: أوضاع WPA3 ومفهوم

طاقات الوصول Cisco Catalyst Wi-Fi 6E APs

اعدادات الأمان المدعومة للعميل

التكوين

الرسم التخطيطي للشبكة

التكوينات

التكوين الأساسي

التحقق من الصحة

التحقق الأمني

WPA3 - AES(CCPM128) + OWE

WPA3 - AES(CCPM128) + Owe مع وضع الانتقال

WPA3-شخصي - AES(CCMP128) + SAE

WPA3-شخصي - AES(CCMP128) + SAE + FT

WPA3-Enterprise + AES(CCMP128) + 802.1x-SHA256 + FT

WPA3-مؤسسي + GCMP128 تشفير + Suiteb-1X

WPA3-مؤسسي + GCMP256 تشفير + Suiteb192-1X

قيمة الاستنتاجات الأمنية

استكشاف الأخطاء وإصلاحها

معلومات ذات صلة

المقدمة

يصف هذه الوثيقة كيفية تكوين شبكة Wi-Fi 6E WLAN من الطبقة 2 الآمنة وهي مزودة بأزواج مختلفة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وحدات التحكم في شبكة LAN اللاسلكية (WLC) 9800 من Cisco
- نقاط الوصول (APs) من Cisco التي تدعم Wi-Fi 6E.
- معيار IEEE 802. 11ax.
- الأدوات: Wireshark الإصدار 4.0.6

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى إصدارات البرامج والمكونات المادية التالية:

- WLC 9800-CL مع IOS® XE 17.9.3.
- APs C9136 و CW9162 و CW9164 و CW9166.
- عملاء Wi-Fi 6e:
  - Lenovo X1 Carbon Gen11 مع محول AX211 Wi-Fi 6 و 6E من Intel مع برنامج تشغيل إصدار 22.200.2(1).
  - مهايئ NetGear A8000 Wi-Fi 6 و 6E مع برنامج تشغيل v1(0.0.108)؛
  - Mobile Pixel 6a مع نظام التشغيل Android 13؛
  - الهاتف المحمول Samsung S23 مع نظام التشغيل Android 13.

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

معلومات أساسية

الشيء الرئيسي الذي يجب معرفته هو أن Wi-Fi 6E ليس معيارا جديدا تماما، بل هو امتداد. تعد شبكة Wi-Fi 6E في قاعدتها امتدادا لمعيار الاتصال اللاسلكي Wi-Fi 6 (802. 11ax) في مدى تردد الراديو الذي يبلغ 6 جيجاهرتز.

تعتمد Wi-Fi 6E على Wi-Fi 6 الذي يعد أحدث جيل من معايير Wi-Fi، ولكن أجهزة Wi-Fi 6E وتطبيقات Wi-Fi فقط يمكنها العمل في مدى موجات 6 جيجاهرتز.

أمان Wi-Fi 6e

يوفر Wi-Fi 6E تأمينا مع Wi-Fi Protected Access 3 (WPA3) وتشفير لاسلكي انتهازي (OWE) والذي يوجد توافق خلفي مع تأمين Open و WPA2.

يعد WPA3 وأمان Open المحسن إلزاميين الآن لاعتماد Wi-Fi 6e كما يتطلب Wi-Fi 6E إطار إدارة محمي (PMF) في كل من نقطة الوصول والعملاء.

عند تكوين SSID بتردد 6 جيجاهرتز، توجد متطلبات أمان معينة يجب تلبيتها:

- أمان WPA3 L2 مع OWE أو SAE أو 802.1x-SHA256
- تمكين إطار الإدارة المحمية؛
- لا يسمح بأي أسلوب تأمين L2 آخر، أي لا يوجد وضع مختلط ممكن.

WPA3

تم تصميم WPA3 لتحسين تأمين Wi-Fi من خلال تمكين مصادقة أفضل عبر WPA2، مما يوفر قوة تشفير موسعة ويزيد من مرونة الشبكات الحساسة.

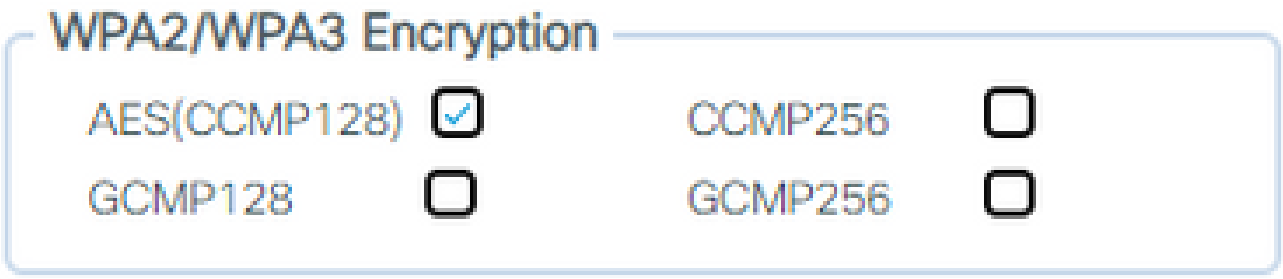
تتضمن المميزات الرئيسية لـ WPA3:

- يحمي إطار الإدارة المحمي (PMF)إطارات إدارة البث الأحادي والبث ويقوم بتشفير إطارات الإدارة للبث الأحادي. وهذا يعني أن أنظمة اكتشاف التسلل اللاسلكي ومنع التسلل اللاسلكي تتميز بقدر أقل من أساليب القوة الغاشمة لفرض سياسات العميل.
- تتيح المصادقة المتزامنة لمتكافئين (SAE)المصادقة المستندة إلى كلمة المرور وآلية الاتفاقية الأساسية. وهذا يحمي من هجمات القوة الغاشمة.
- الوضع الانتقالي هو وضع مختلط يمكن إستخدام WPA2 لتوصيل العملاء الذين لا يؤيدون WPA3.

يدور WPA3 حول التطوير والتوافق الأمنيين المستمرين وكذلك قابلية التشغيل البيني.
لا يوجد عنصر معلومات يعين WPA3 (مثل WPA2). يتم تعريف WPA3 بواسطة مجموعات AKM/Cipher Suite/PMF.

في تكوين شبكة WLAN رقم 9800، لديك 4 خوارزميات تشفير WPA3 مختلفة يمكنك إستخدامها.

تستند إلى بروتوكول الوضع العكسي/Galois (GCMP) ووضع العداد مع بروتوكول رمز مصادقة الرسائل المتسلسلة لتشفير (CCMP): AES (CCMP128) و CCMP256 و GCMP128 و GCMP256:

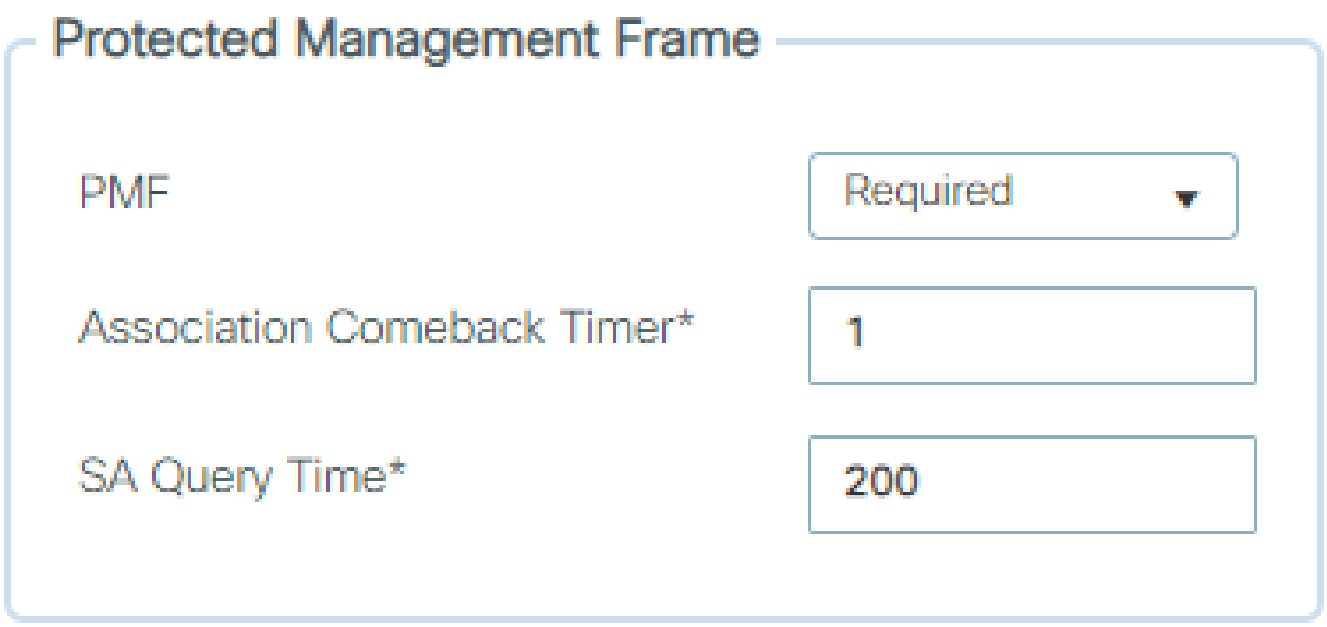


خيارات تشفير WPA2/3

الحشد

يتم تنشيط PMF على شبكة WLAN عند تمكين PMF.

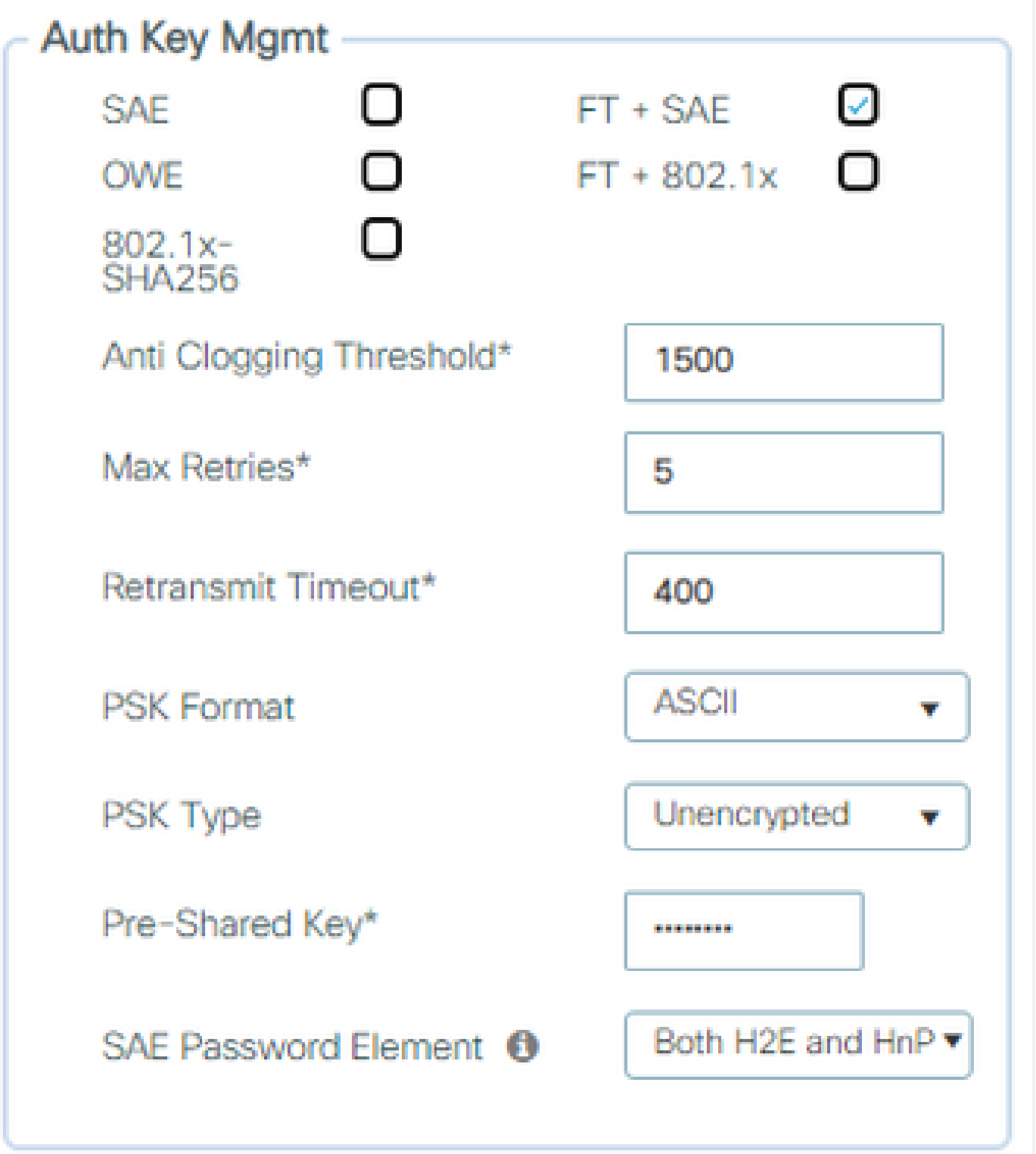
بشكل افتراضي، تكون إطارات الإدارة 802.11 غير مصدق عليها وبالتالي لا تكون محمية من الانتحال. إطار حماية إدارة البنية الأساسية (MFP) وإطارات الإدارة المحمية (PMF) بقدرة 802.11w توفر الحماية ضد مثل هذه الهجمات.



خيارات PMF

إدارة مفتاح المصادقة

هذه هي خيارات AKM المتاحة في إصدار 17.9.x:

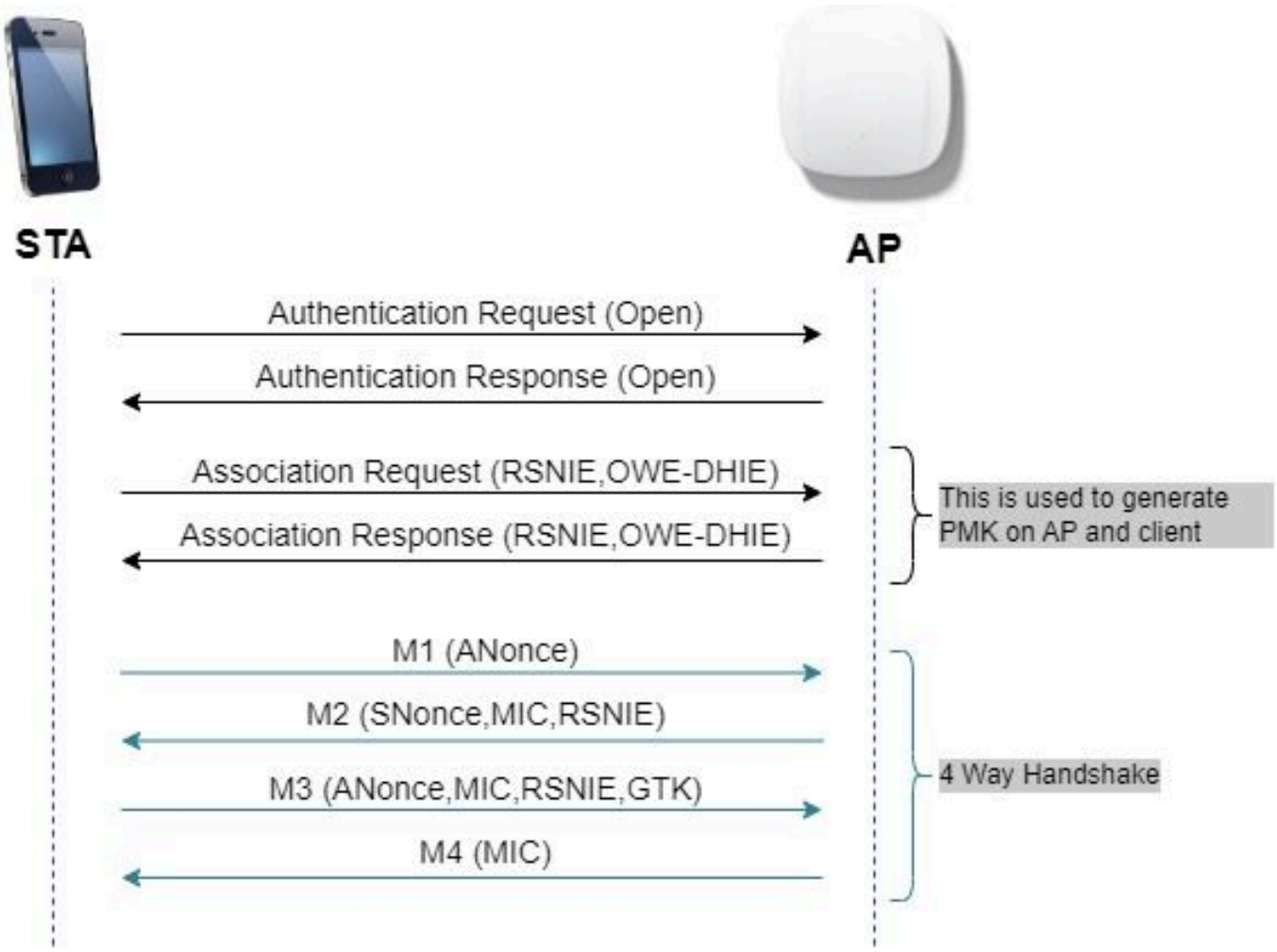


خيارات AKM

تستدانن

التشفير اللاسلكي الانتهازي (OWE) وه امتداد لمعيار IEEE 802. 11 الذي يوفر تشفير الوسيط اللاسلكي (IETF RFC 8110). إن الغرض من المصادقة المستندة إلى OWE وه تجنب فتح اتصال لاسلكي غير آمن بين نقاط الوصول والعملاء. يستخدم OWE تشفير قائم عل خوارزميات Diffie-Hellman لإعداد التشفير اللاسلكي. من خلال OWE، يقوم العميل ونقطة الوصول بتبادل مفاتيح Diffie-Hellman أثناء إجراء الوصول واستخدام المفاتح الرئيسي للحكمة (PMK) الناتج عن ذلك مع المصافحة الرباعية الإتجاه. يؤدي إستخدام OWE

إلى تحسين أمان الشبكة الالسلكية لعمليات النشر التي يتم فيها نشر الشبكات المفتوحة أو المشتركة المستندة إلى PSK.



تبادل إطارات الدبوي

نفس

يستخدم WPA3 مصادقة جديدة وآلية إدارة مفاتيح جديدة تسمى المصادقة المتزامنة للمساويين. ويتم تعزيز هذه الآلية أكثر من خلال إستخدام تجزئة SAE إلى عنصر (H2E).

SAE مع H2E إلزامي لـ WPA3 و Wi-Fi 6E.

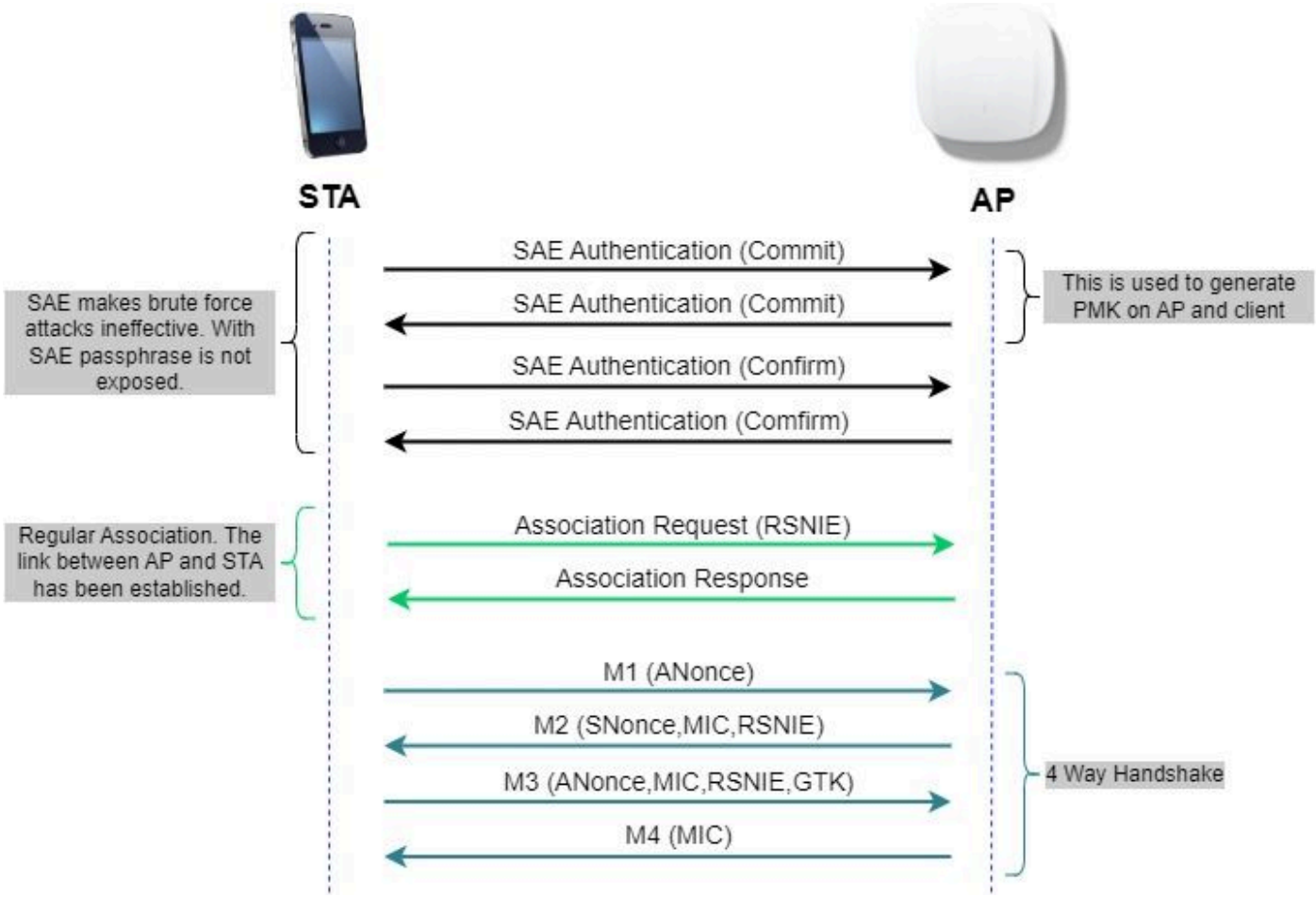
تستخدم SAE تشفير لوغاريتم منفصل لإجراء تبادل فعال بطريقة تؤدي إلى المصادقة المتبادلة باستخدام كلمة مرور قد تكون مقاومة لهجوم القاموس دون اتصال.

هجوم القاموس دون اتصال بالإنترنت وه المكان الذي يحاول فيه خصم تحديد كلمة مرور الشبكة عن طريق محاولة كلمات المرور الممكنة بدون المزيد من التفاعل مع الشبكة.

عندما يتصل العميل بنقطة الوصول، فإنه يجري تبادل SAE. وإذا نجحت، فإنها تنشئ كل مفتاح مشفر قوي، والذي يتم اشتقاق مفاتيح الجلسة منه. يدخل العميل ونقطة الوصول بشكل أساسي إلى مراحل الالتزام ثم يؤكدان.

وبمجرد وجود التزام، يمكن للعميل ونقطة الوصول الانتقال إلى حالات التأكيد في كل مرة يتم فيها إنشاء مفاتيح جلسة. وتستخدم هذه الطريقة السرية لإعادة التوجيه حيث يتمكن

الدخيل من فك مفتاح واحد ولكن ليس كل المفاتيح الأخرى.



تبادل إطارات SAE

تجزئة إلى عنصر (H2E)

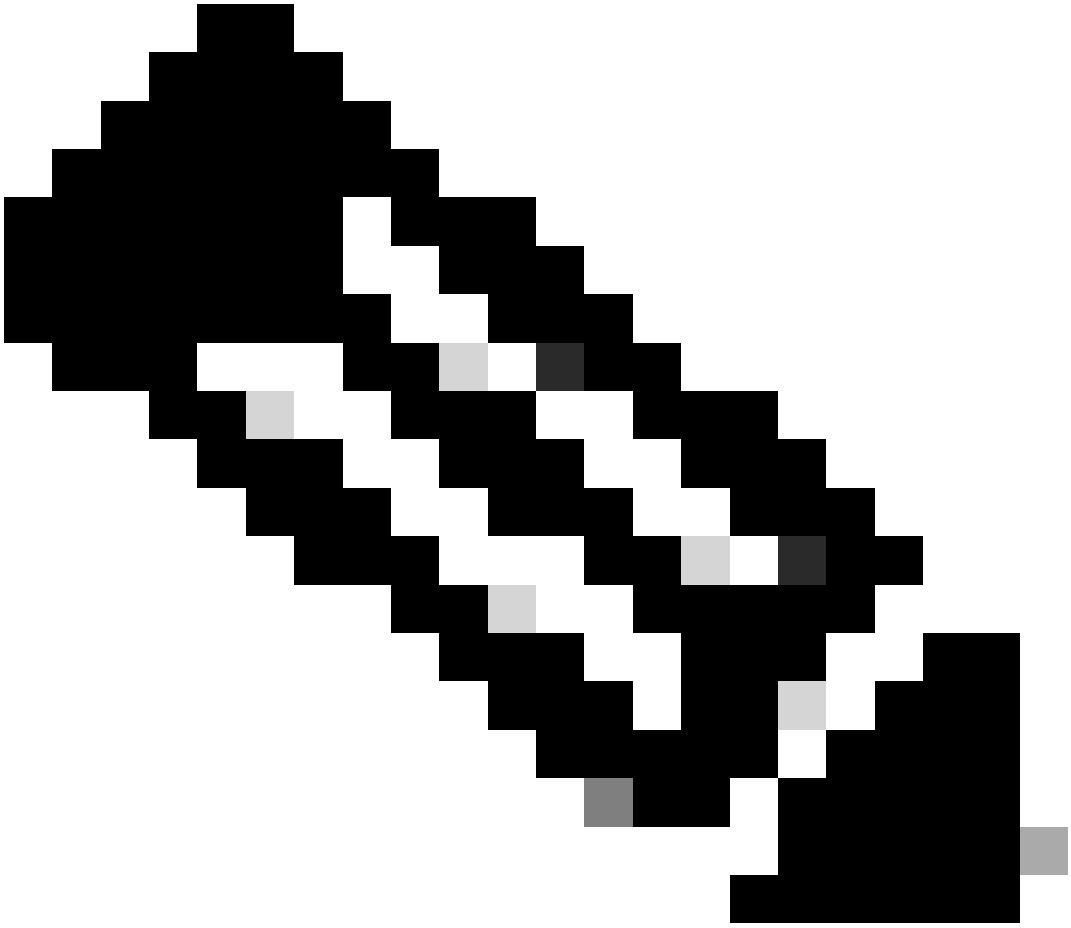
التجزئة إلى العنصر (H2E) هي طريقة عنصر كلمة مرور SAE جديد (PWE). في هذه الطريقة، يتم إنشاء PWE السري المستخدم في بروتوكول SAE من كلمة مرور.

عندما تقوم محطة (STA) تدعم H2E بتهيئة SAE باستخدام AP، فإنها تتحقق مما إذا كانت AP تدعم H2E. إذا كانت الإجابة بنعم، فإن نقطة الوصول تستخدم H2E لاستخلاص PWE باستخدام قيمة رمز الحالة المعرفة حديثا في رسالة SAE Commit.

إذا كان STA يستخدم ميزة الصيد والنقر (HNp)، فستظل عملية تبادل SAE بالكامل دون تغيير.

عند إستخدام H2E، يقسم اشتقاق PWE إلى هذه المكونات:

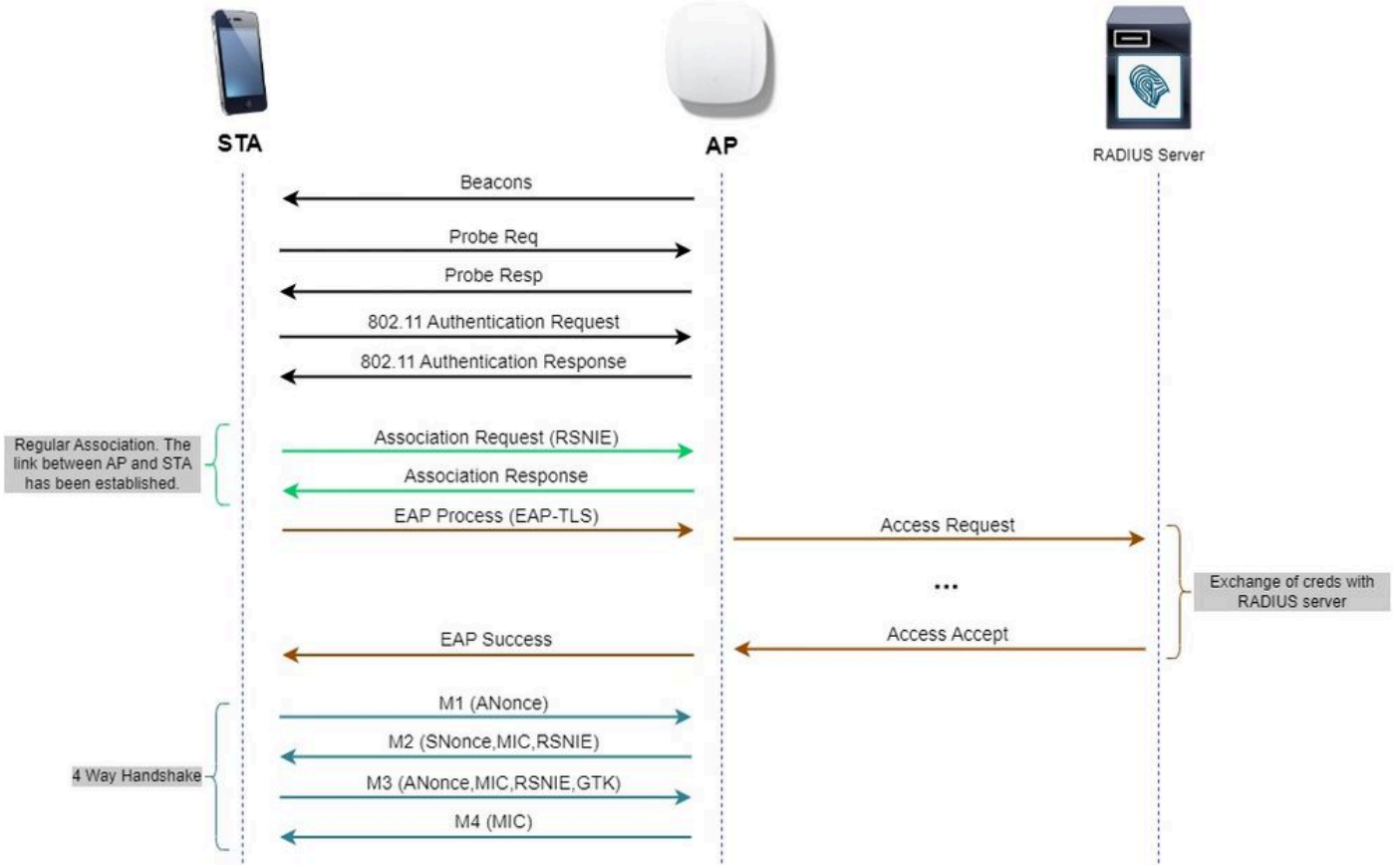
- اشتقاق عنصر وسيط سري (PT) من كلمة المرور. يمكن تنفيذ هذا دون اتصال عندما يتم تكوين كلمة المرور في البداية على الجهاز لكل مجموعة معتمدة.
- اشتقاق PWE من ال pt المخزن. يعتمد ذلك على المجموعة التي تم التفاوض عليها وعناوين MAC الخاصة بالأقران. يتم تنفيذ هذا في الوقت الحقيقي أثناء تبادل SAE.



ملاحظة: 6 جيجاهرتز تدعم فقط أسلوب SAE من التجزئة إلى العنصر PWE.

WPA-Enterprise المعروف باسم 802.1x

WPA3-Enterprise هو الإصدار الأكثر أمانا من WPA3 ويستخدم اسم مستخدم بالإضافة إلى كلمة مرور مركبة مع 802.1X لمصادقة المستخدم مع خادم RADIUS. بشكل افتراضي، يستخدم WPA3 تشفير 128-بت، لكنه يقدم أيضا تشفير تشفير قوة تشفير 192-بت قابل للتكوين إختياري، والذي يعطي حماية إضافية لأي شبكة ترسل بيانات حساسة.



تدفق الرسم التخطيطي للمؤسسة WPA3

مجموعة المستويات: أوضاع WPA3

- WPA3-شخصي
  - وضع WPA3-الشخصي فقط
    - يلزم توفر قواتا الحشد الشعبي
  - وضع الانتقال WPA3-الشخصي
    - قواعد التكوين: على نقطة الوصول، عند تمكين WPA2-شخصي، يجب أيضا تمكين وضع الانتقال WPA3-Personal بشكل افتراضي، ما لم يتم تجاوزه بشكل صريح من قبل المسؤول للعمل في وضع WPA2-Personal فقط

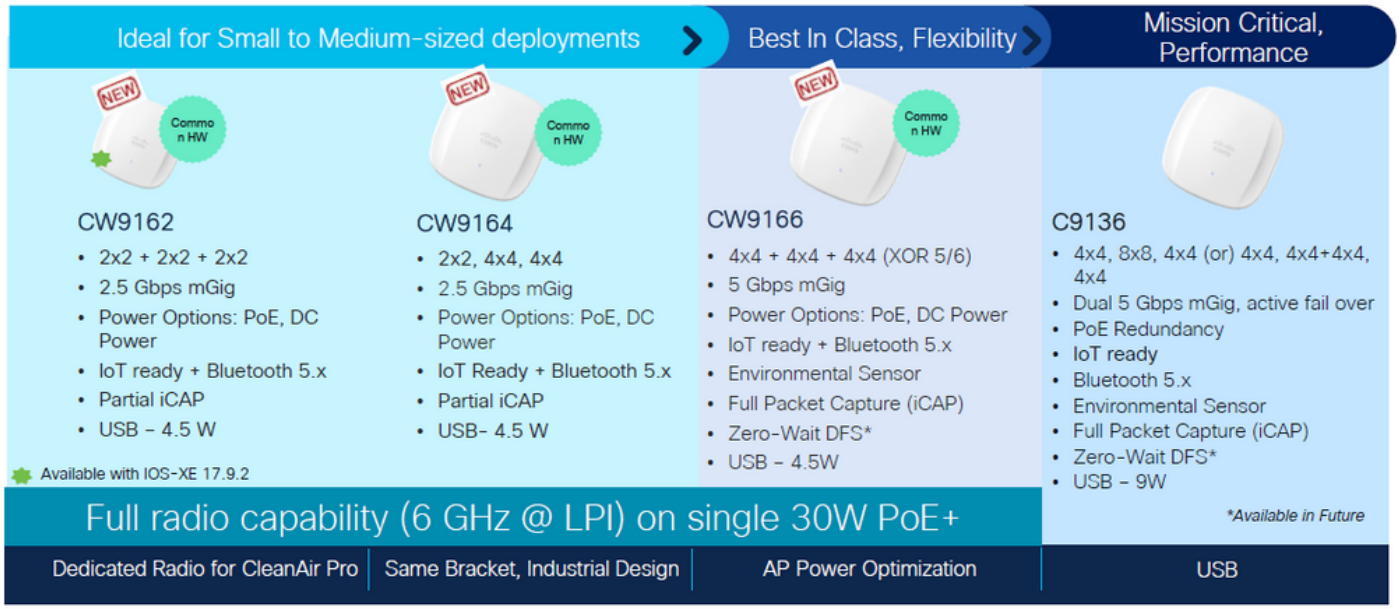
- WPA3-مؤسسي
  - وضع WPA3-مؤسسي فقط
    - يتم التفاوض على PMF لجميع إتصالات WPA3
  - وضع الانتقال WPA3-Enterprise
    - يتم التفاوض على PMF لاتصال WPA3
    - PMF إختياري لاتصال WPA2
  - وضع WPA3-Enterprise Suite-B "192-bit" المتوافق مع خوارزمية الأمان القومي التجاري (CNSA)
    - أكثر من مجرد الحكومة الفيدرالية
    - مجموعات شفرة التشفير المتناسقة لتجنب التكوين الخاطئ
    - إضافة GCMP و ECCP لوظائف التشفير والتجزئة الأفضل (SHA384)
    - يلزم توفر قواتا الحشد الشعبي

- يكون تأمين WPA3 192-بت حصريا ل EAP-TLS، مما يتطلب شهادات على كل من المعطى وخادم RADIUS.
- لاستخدام WPA3 الإصدار 192 بت على مستوى المؤسسة، يجب أن تستخدم خوادم RADIUS أحد شفرات EAP المسموح بها:

  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

لمعرفة المزيد حول المعلومات التفصيلية حول تنفيذ WPA3 في شبكات WLAN من Cisco، بما في ذلك مصفوفة توافق أمان العميل، يرجى الاستماع بحرية التحقق من دليل نشر WPA3.

نقاط الوصول Cisco Catalyst Wi-Fi 6E APs



نقاط وصول Wi-Fi 6e

إعدادات الأمان المدعومة للعملاء

يمكنك العثور على المنتج الذي يدعم WPA3-Enterprise باستخدام باحث منتجات وفي صفحة لتحالف WiFi.

في أجهزة Windows يمكنك التحقق من إعدادات التأمين التي يدعمها المحول باستخدام الأمر netsh wlan show drivers".

هنا يمكنك الاطلاع على إخراج صفيفات التخزين طراز AX211 من Intel:

```
C:\Users\tantunes>netsh wlan show drivers

Interface name: Wi-Fi

    Driver                    : Intel(R) Wi-Fi 6E AX211 160MHz
    Vendor                    : Intel Corporation
    Provider                  : Intel
    Date                      : 3/9/2023
    Version                   : 22.200.2.1
    INF file                  : oem151.inf
    Type                      : Native Wi-Fi Driver
    Radio types supported     : 802.11b 802.11g 802.11n 802.11a 802.11ac 802.11ax
    FIPS 140-2 mode supported : Yes
    802.11w Management Frame Protection supported : Yes
    Hosted network supported  : No
    Authentication and cipher supported in infrastructure mode:
                                Open            None
                                Open            WEP-40bit
                                Open            WEP-104bit
                                Open            WEP
                                WPA-Enterprise  TKIP
                                WPA-Enterprise  CCMP
                                WPA-Personal    TKIP
                                WPA-Personal    CCMP
                                WPA2-Enterprise TKIP
                                WPA2-Enterprise CCMP
                                WPA2-Personal   TKIP
                                WPA2-Personal   CCMP
                                Open            Vendor defined
                                WPA3-Personal   CCMP
                                Vendor defined  Vendor defined
                                WPA3-Enterprise 192 Bits GCMP-256
                                OWE             CCMP
                                WPA3-Enterprise CCMP
                                WPA3-Enterprise TKIP
    Number of supported bands : 3
                                2.4 GHz [ 0 MHz - 0 MHz]
                                5 GHz   [ 0 MHz - 0 MHz]
                                6 GHz   [ 0 MHz - 0 MHz]
    IHV service present       : Yes
    IHV adapter OUI           : [00 00 00], type: [00]
    IHV extensibility DLL path: C:\WINDOWS\System32\DriverStore\FileRepository\netwtw6e.inf_amd64_eda979fbdedea064\IntelIHVRouter12.dll
```

اخراج Windows ل _netsh wlan show driver_ للعميل AX211

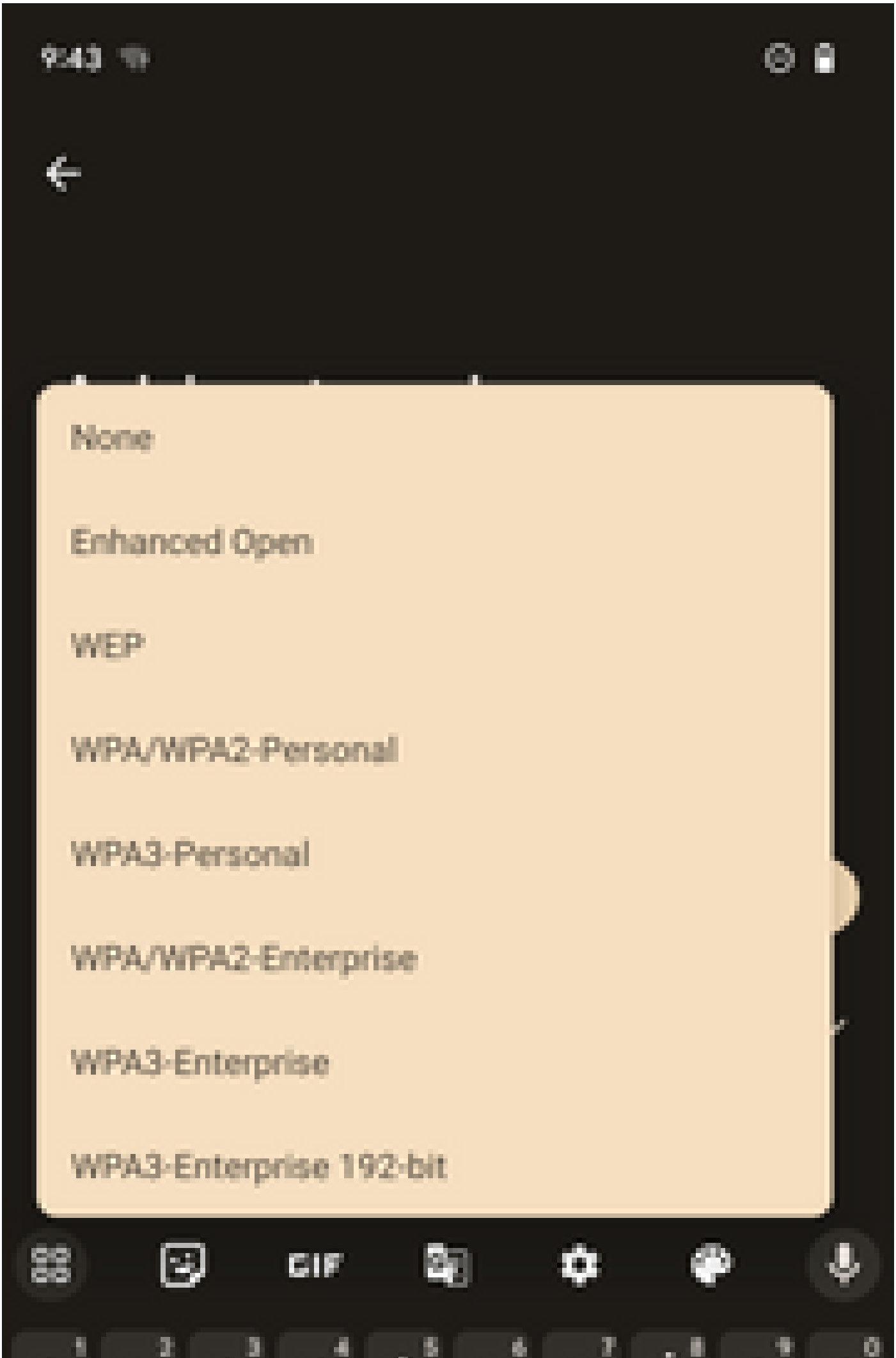
Netgear A8000:

```
Interface name: A8000_NETGEAR

    Driver                     : NETGEAR A8000 WiFi 6 & 6E Adapter
    Vendor                     : NETGEAR Inc.
    Provider                   : MediaTek, Inc.
    Date                       : 11/25/2022
    Version                    : 1.0.0.108
    INF file                   : oem9.inf
    Type                       : Native Wi-Fi Driver
    Radio types supported      : 802.11b 802.11a 802.11g 802.11n 802.11ac 802.11ax
    FIPS 140-2 mode supported : Yes
    802.11w Management Frame Protection supported : Yes
    Hosted network supported  : No
    Authentication and cipher supported in infrastructure mode:
                                Open             None
                                Open             WEP-40bit
                                Open             WEP-104bit
                                Open             WEP
                                WPA-Enterprise   TKIP
                                WPA-Enterprise   CCMP
                                WPA3-Personal    CCMP
                                OWE              CCMP
                                WPA-Personal     TKIP
                                WPA-Personal     CCMP
                                WPA2-Enterprise  TKIP
                                WPA2-Enterprise  CCMP
                                WPA2-Personal    TKIP
                                WPA2-Personal    CCMP
    Number of supported bands : 3
                                2.4 GHz [ 0 MHz - 0 MHz]
                                5 GHz   [ 0 MHz - 0 MHz]
                                6 GHz   [ 0 MHz - 0 MHz]
    IHV service present        : Yes
    IHV adapter OUI            : [00 00 00], type: [00]
    IHV extensibility DLL path: C:\WINDOWS\system32\mtkihvux.dll
    IHV UI extensibility ClSID: {00000000-0000-0000-0000-000000000000}
    IHV diagnostics CLSID      : {00000000-0000-0000-0000-000000000000}
    Wireless Display Supported: Yes (Graphics Driver: Yes, Wi-Fi Driver: Yes)
```

إخراج Windows لـ _NetSH WLAN show driver_ لـ NetGear A8000s للعميل

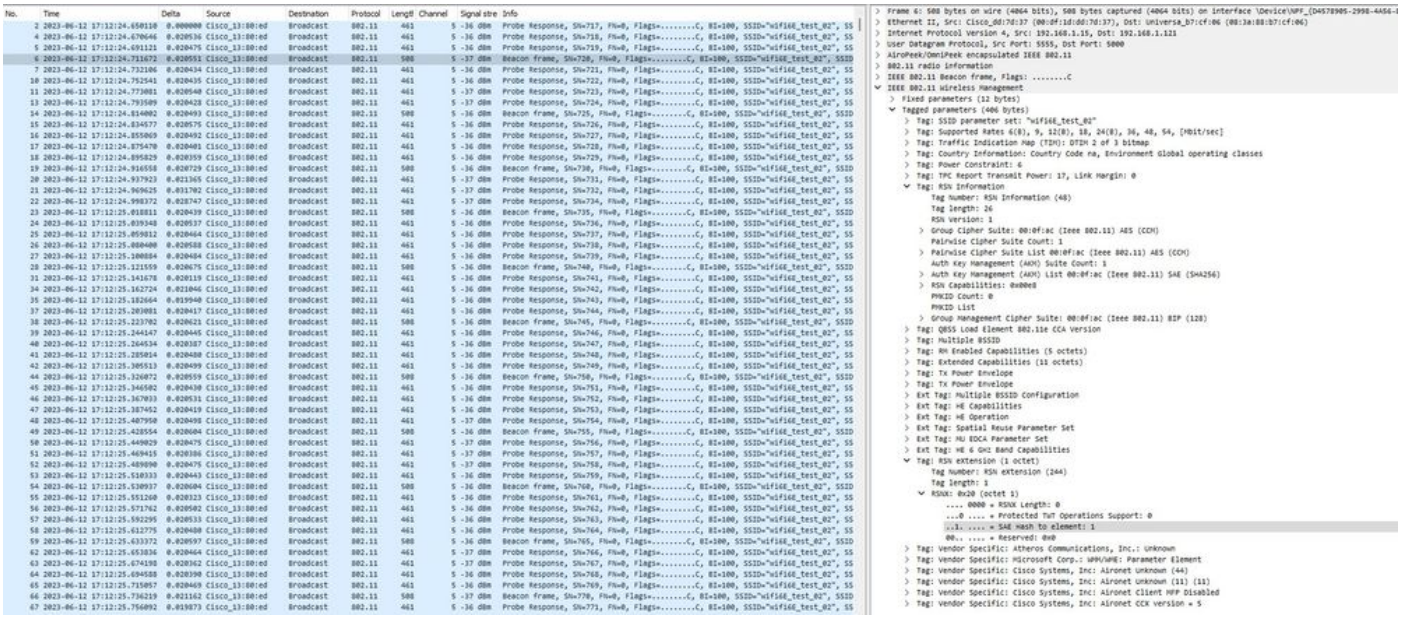
أندرويد بيكسل 6a:


9:43
None
Enhanced Open
WEP
WPA/WPA2-Personal
WPA3-Personal
WPA/WPA2-Enterprise
WPA3-Enterprise
WPA3-Enterprise 192-bit
GIF

: ضع في اعتبارك أنه غير مسموح بالاصطياد والنقر باستخدام السياسة
اللاسلكية بتردد 6 جيجاهيرتز. عندما تقوم بتكوين شبكة WLAN فقط بسرعة 6
جيجاهرتز، يجب عليك تحديد عنصر كلمة مرور H2E SAE.

عرض على واجهة المستخدم الرسومية (GUI) الخاصة بإعدادات أمان WLAN:

التحقق من أجهزة الإرشاد OTA:

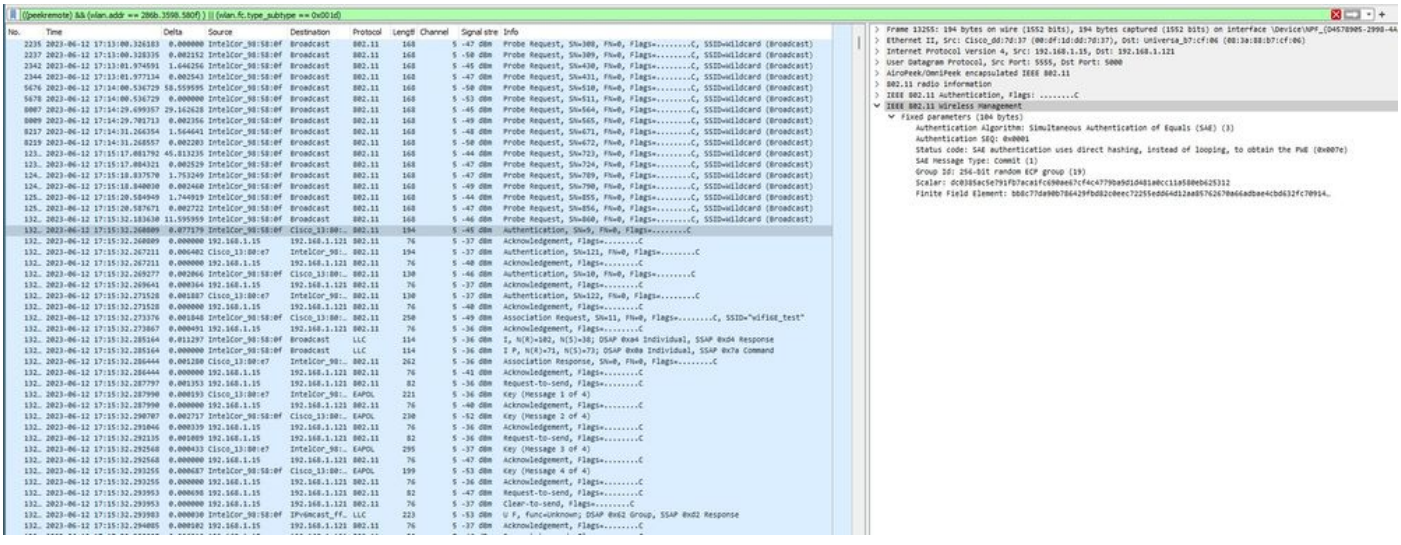


WPA3 SAE Beacons

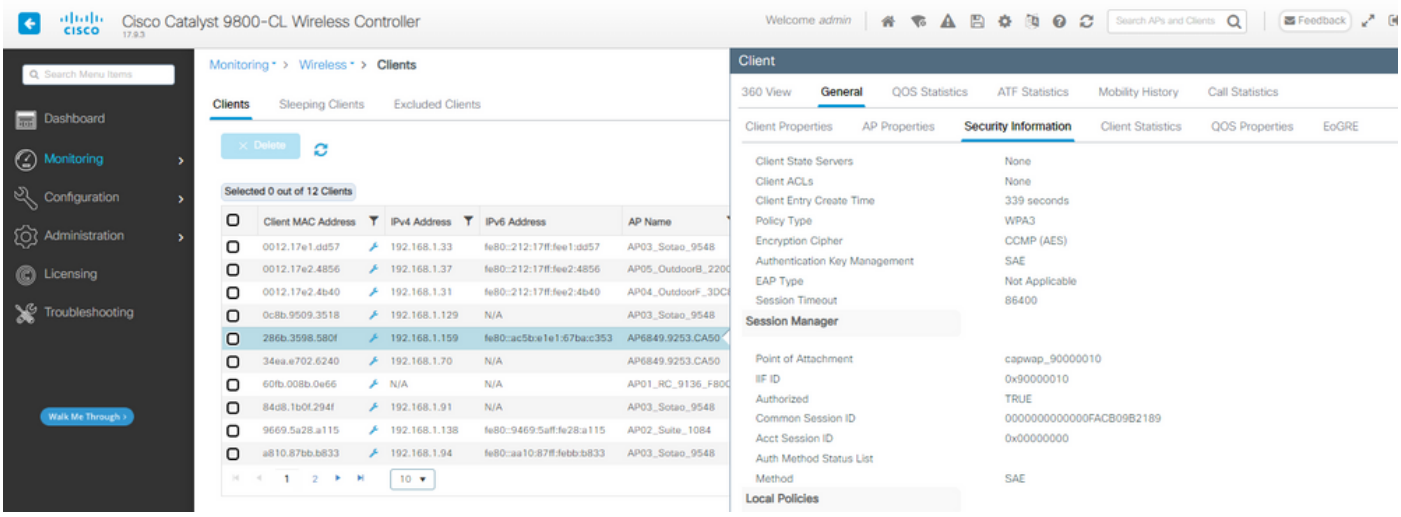
هنا يمكن أن نشاهد عملاء Wi-Fi 6e الذين يربطون:

مجموعة الشرائح Intel AX211

الاتصال OTA مع التركيز على معلومات RSN من العميل:

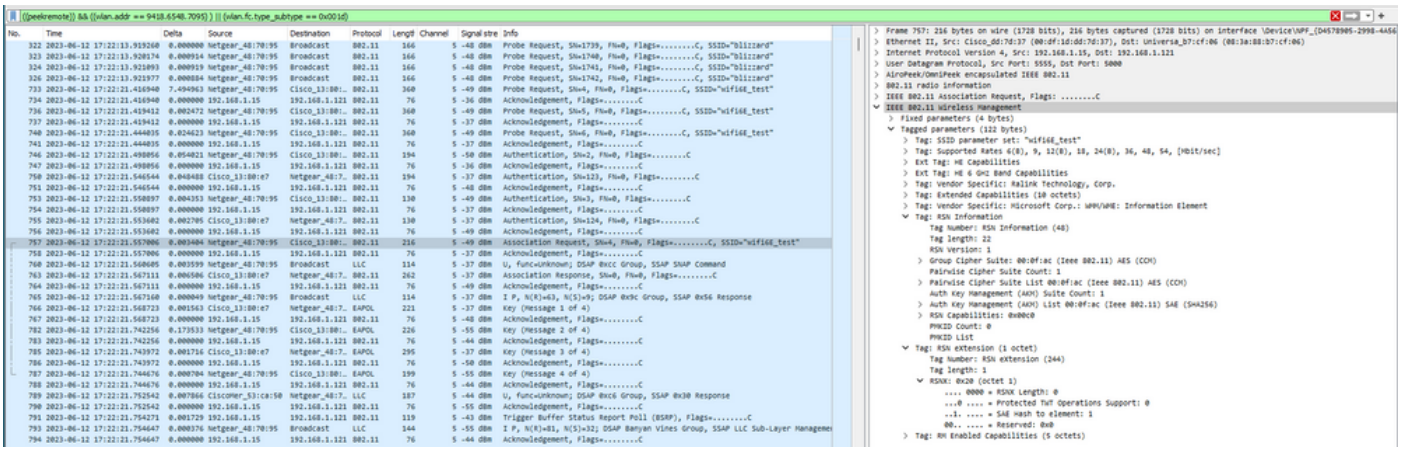


تفاصيل العميل في WLC:

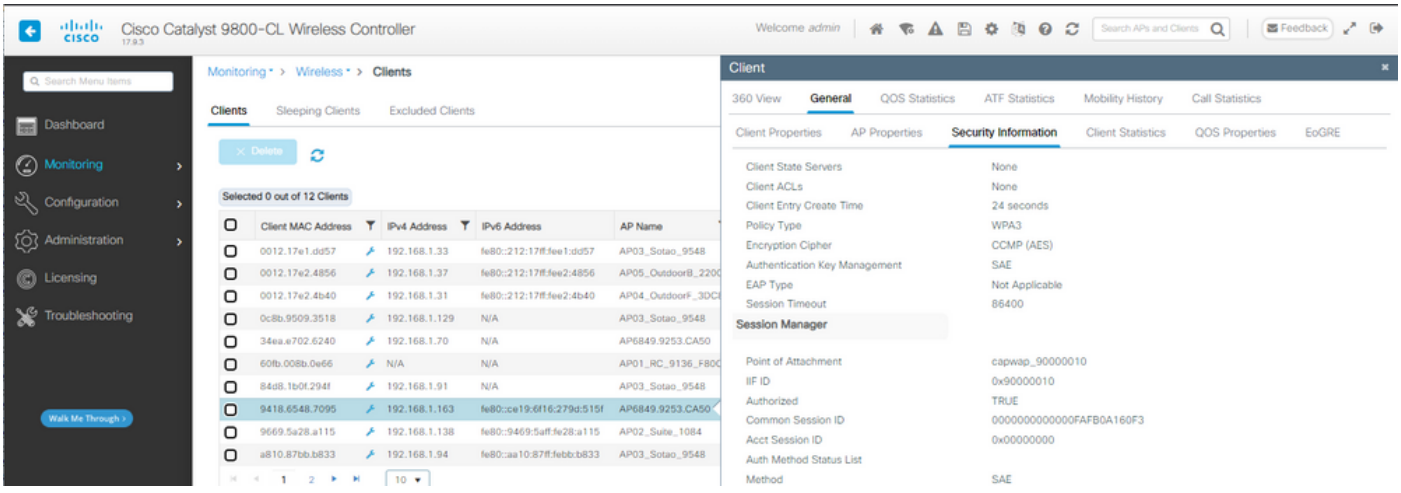


NetGear A8000

الاتصال OTA مع التركيز على معلومات RSN من العميل:

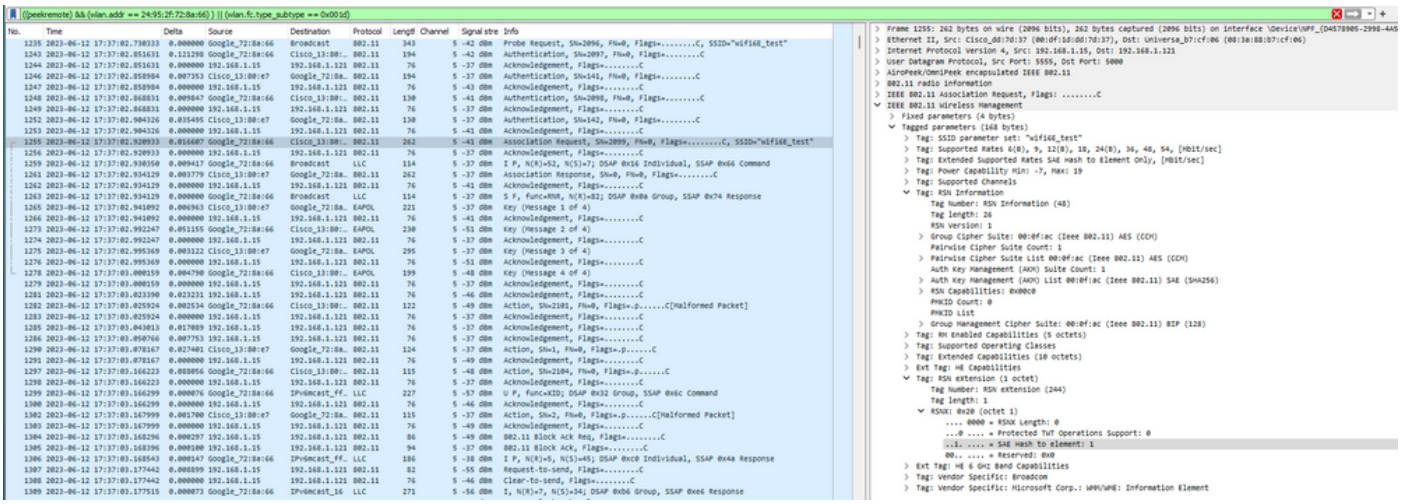


تفاصيل العميل في WLC:

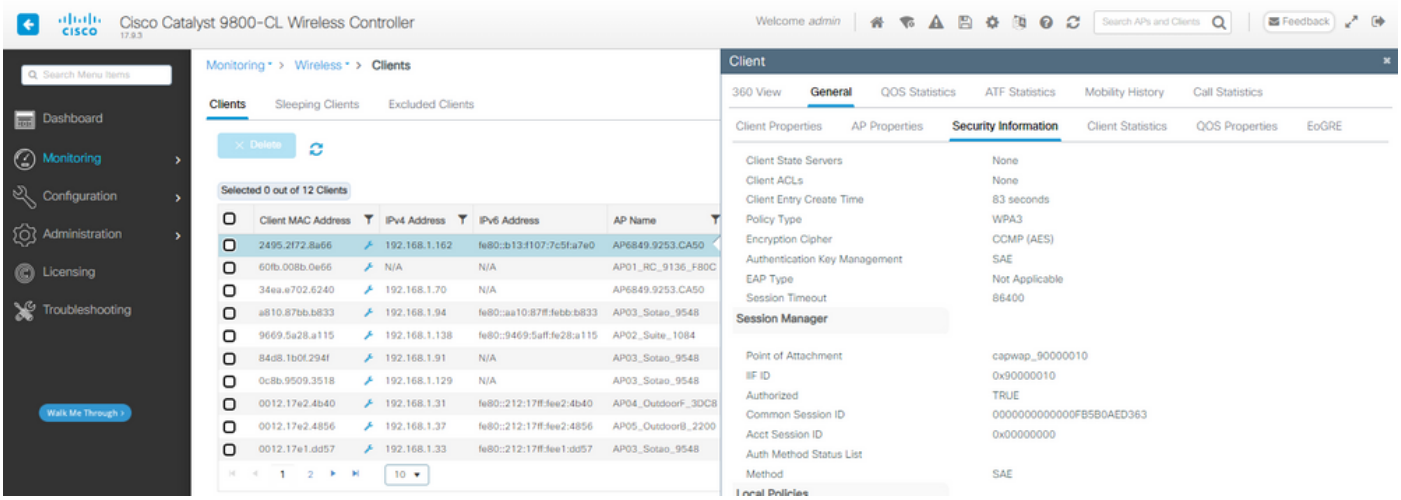


بيكسل 6a

الاتصال OTA مع التركيز على معلومات RSN من العميل:

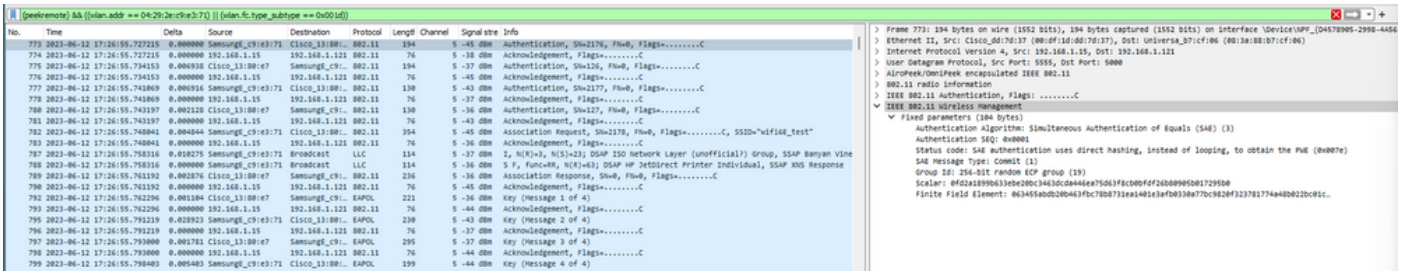


تفاصيل العميل في WLC:

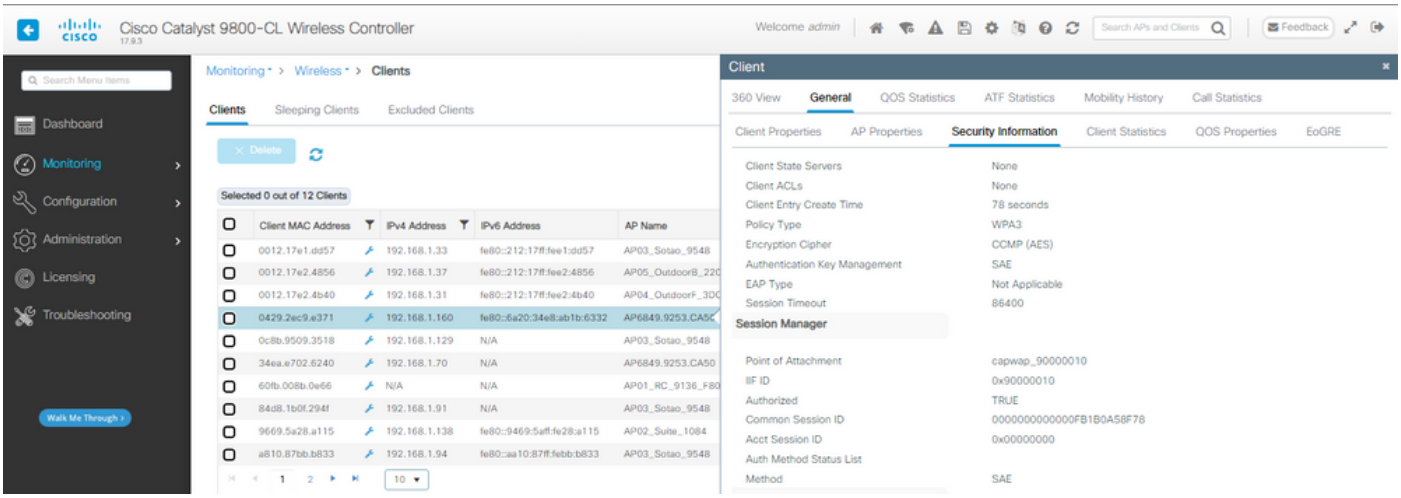


سامسونج إس 23

الاتصال OTA مع التركيز على معلومات RSN من العميل:

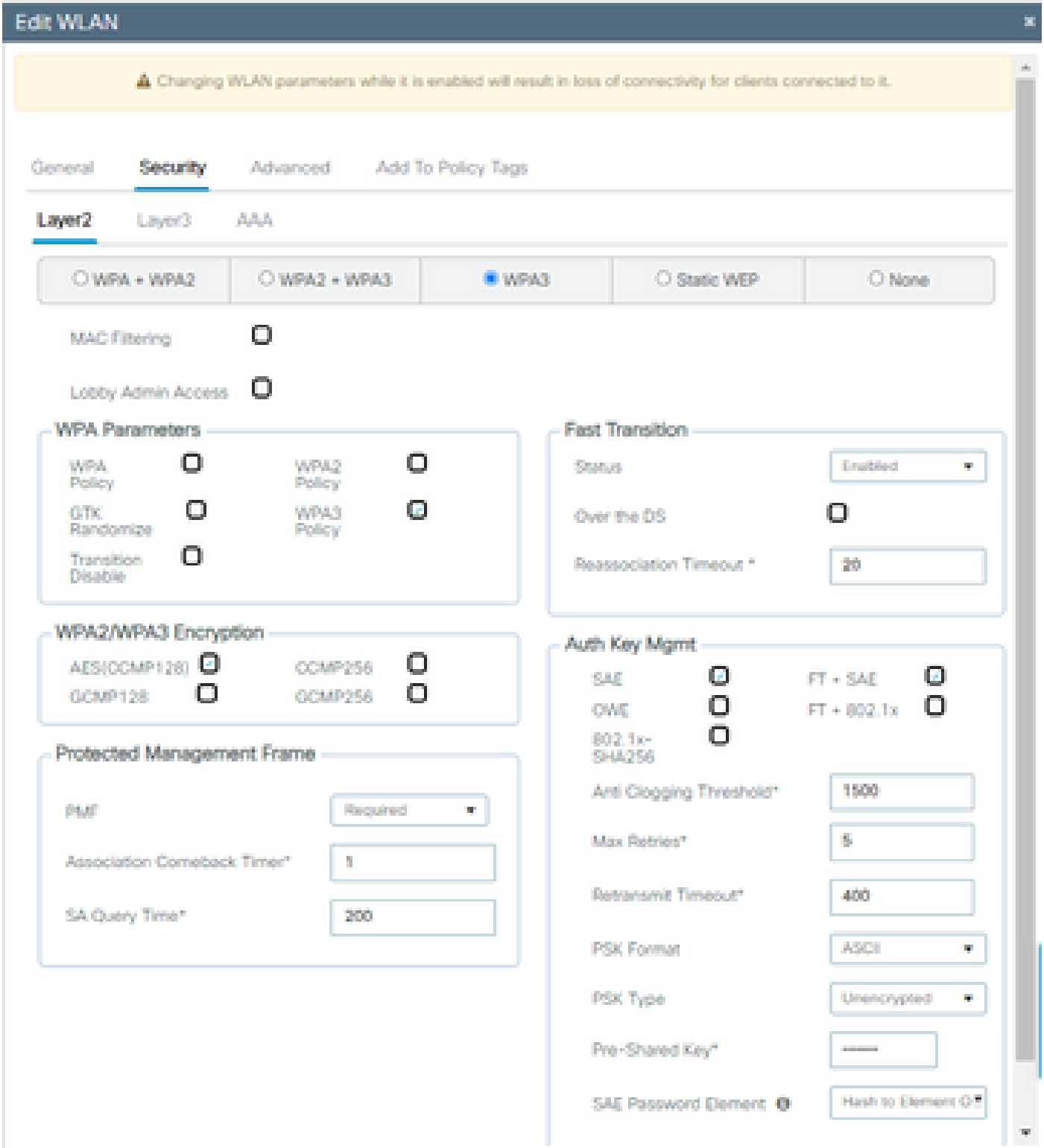


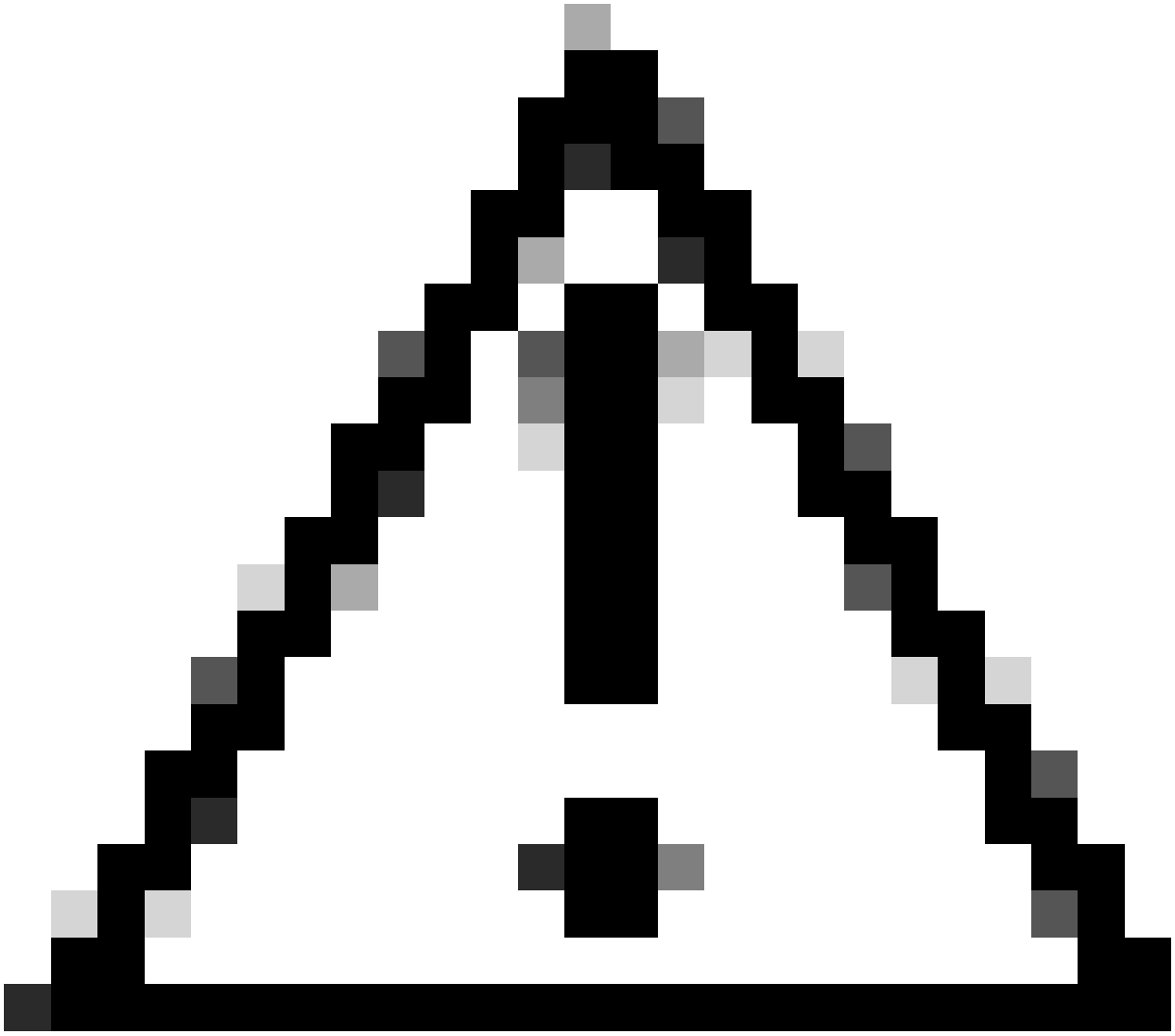
تفاصيل العميل في WLC:



WPA3-شخصي - AES(CCMP128) + SAE + FT

تكوين أمان WLAN:

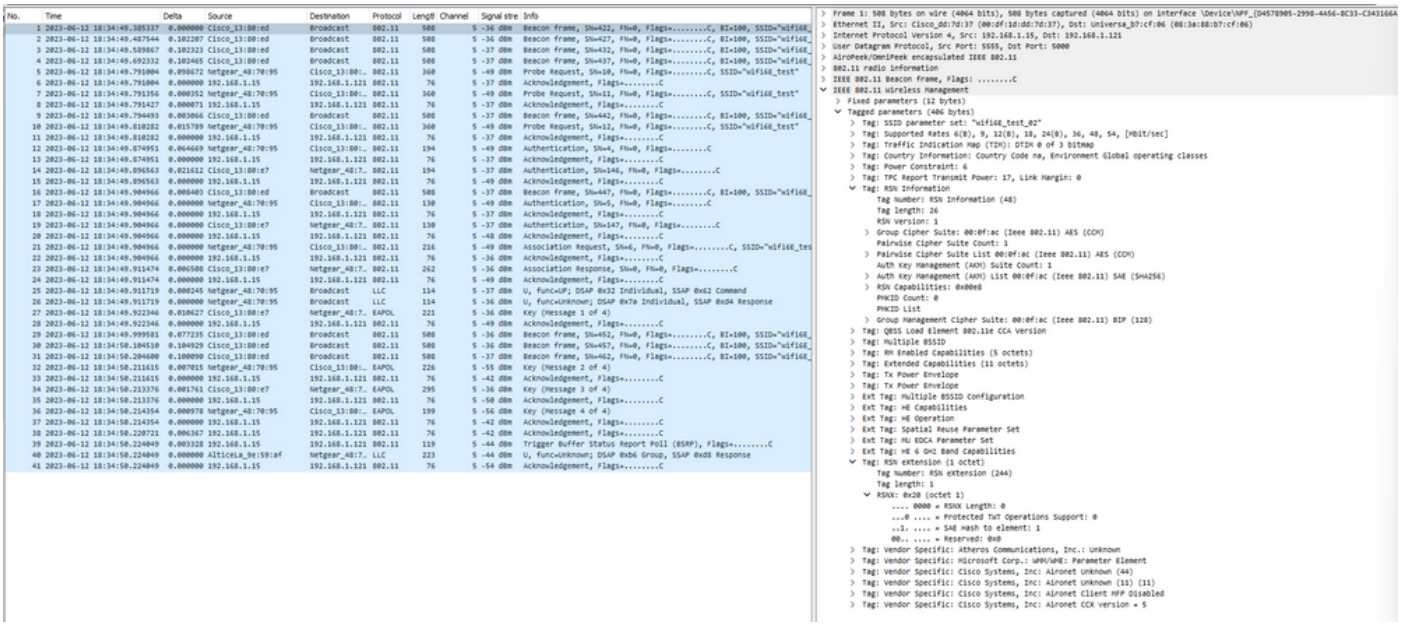

Edit WLAN
Changing WLAN parameters while it is enabled will result in loss of connectivity for clients connected to it.
General
Security
Advanced
Add To Policy Tags
Layer2
Layer3
AAA
WPA + WPA2
WPA2 + WPA3
WPA3
Static WEP
None
MAC Filtering
Lobby Admin Access
WPA Parameters
WPA Policy
WPA2 Policy
GTK Randomize
WPA3 Policy
Transition Disable
WPA2/WPA3 Encryption
AES(CCMP128)
CCMP256
GCMP128
GCMP256
Protected Management Frame
PMF
Required
Association Comeback Timer*
1
SA Query Time*
200
Fast Transition
Status
Enabled
Over the DS
Reassociation Timeout *
20
Auth Key Mgmt
SAE
FT + SAE
OWE
FT + 802.1x
802.1x-SHA256
Anti Clogging Threshold*
1500
Max Retries*
5
Retransmit Timeout*
400
PSK Format
ASCII
PSK Type
Unencrypted
Pre-Shared Key*
SAE Password Element
Hash to Element (H



تحذير: في إدارة مفاتح المصادقة، تسمح عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بتحديد FT+SAE دون تمكين SAE، ومع ذلك فقد لوحظ أن العملاء غير قادرين على الاتصال. قم دائما بتمكين كل خانتي الاختيار SAE و FT+SAE إذا كنت تريد إستخدام SAE مع الانتقال السريع.

عرض على واجهة المستخدم الرسومية (GUI) الخاصة بإعدادات أمان WLAN:

التحقق من أجهزة الإرشاد OTA:

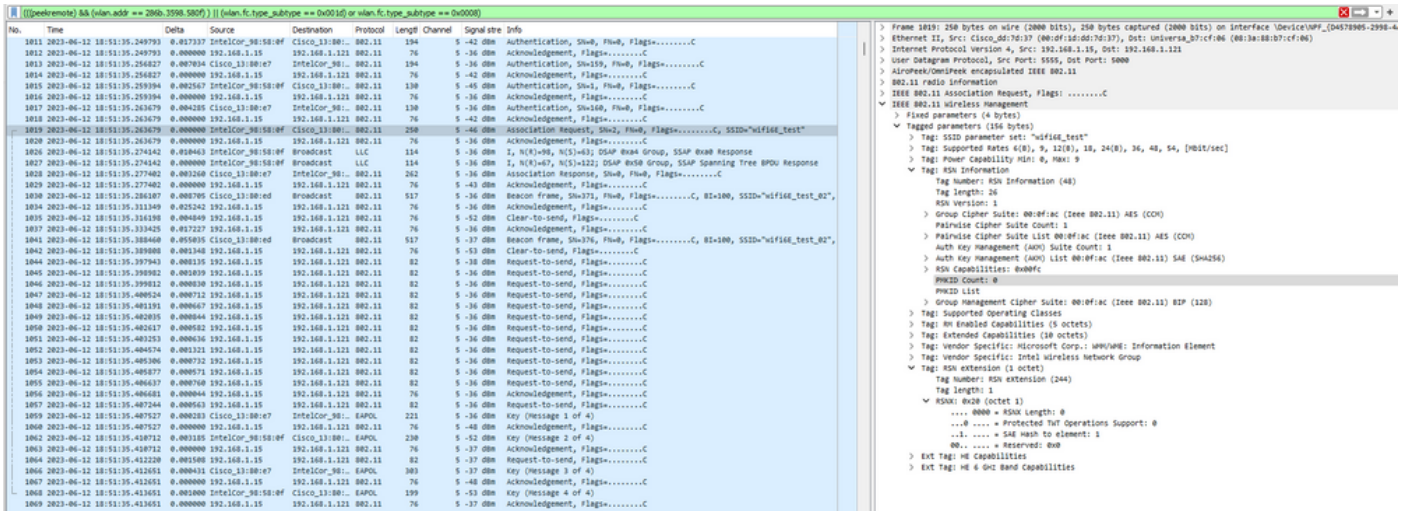


WPA3 SAE + أجهزة توجيه FT

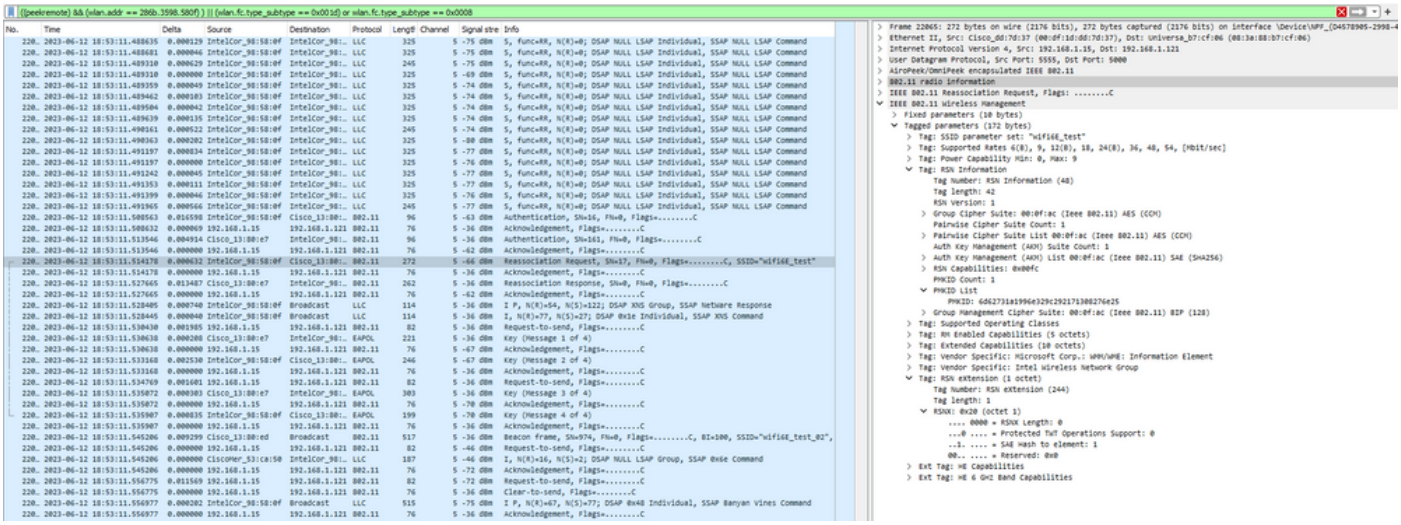
هنا يمكن أن نشاهد عملاء Wi-Fi 6e الذين يربطون:

مجموعة الشرائح Intel AX211

الاتصال OTA مع التركيز على معلومات RSN من العميل:

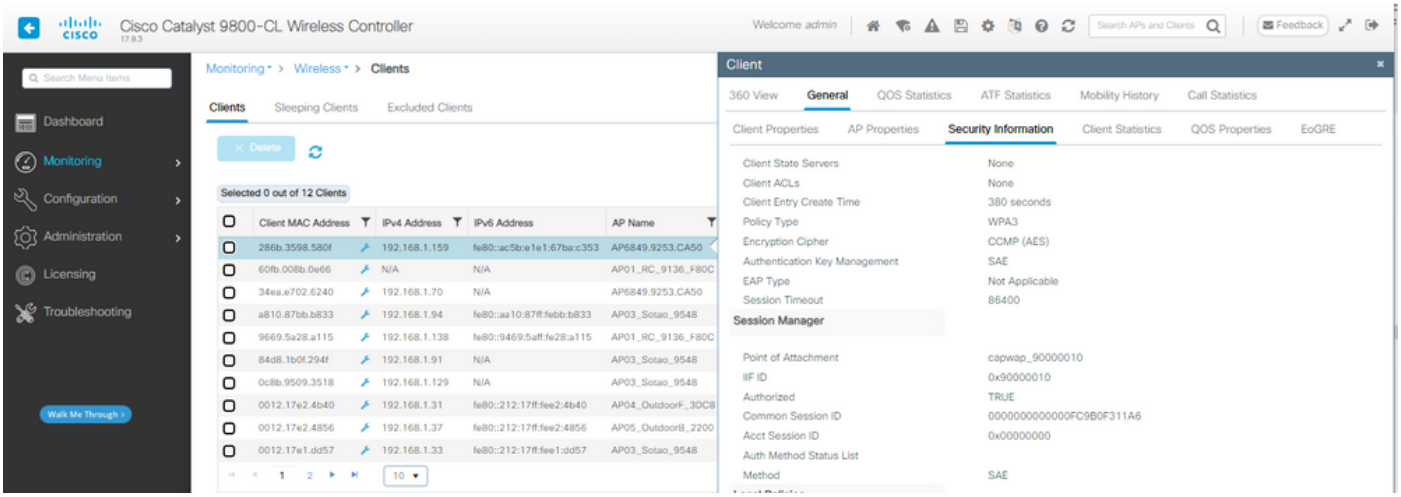


حدث تجوال حيث يمكنك رؤية PMKID:



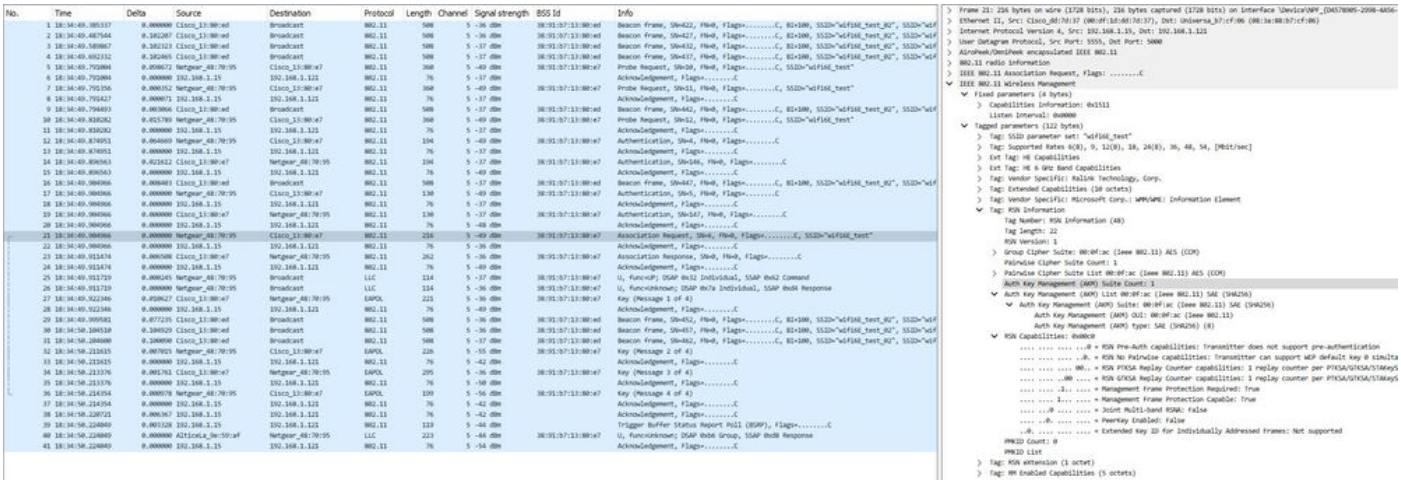
WPA3 SAE + طلب إعادة تعيين FT

تفاصيل العميل في WLC:



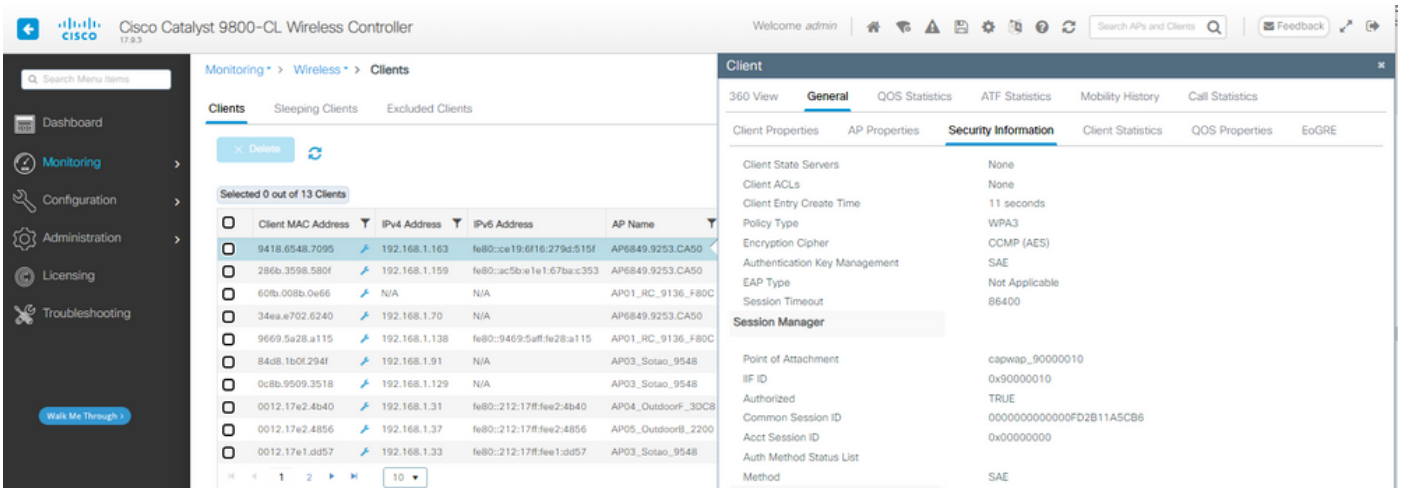
NetGear A8000

الاتصال OTA مع التركيز على معلومات RSN من العميل. التوصيل الأولي:



س س س

تفاصيل العميل في WLC:



بيكسل 6a

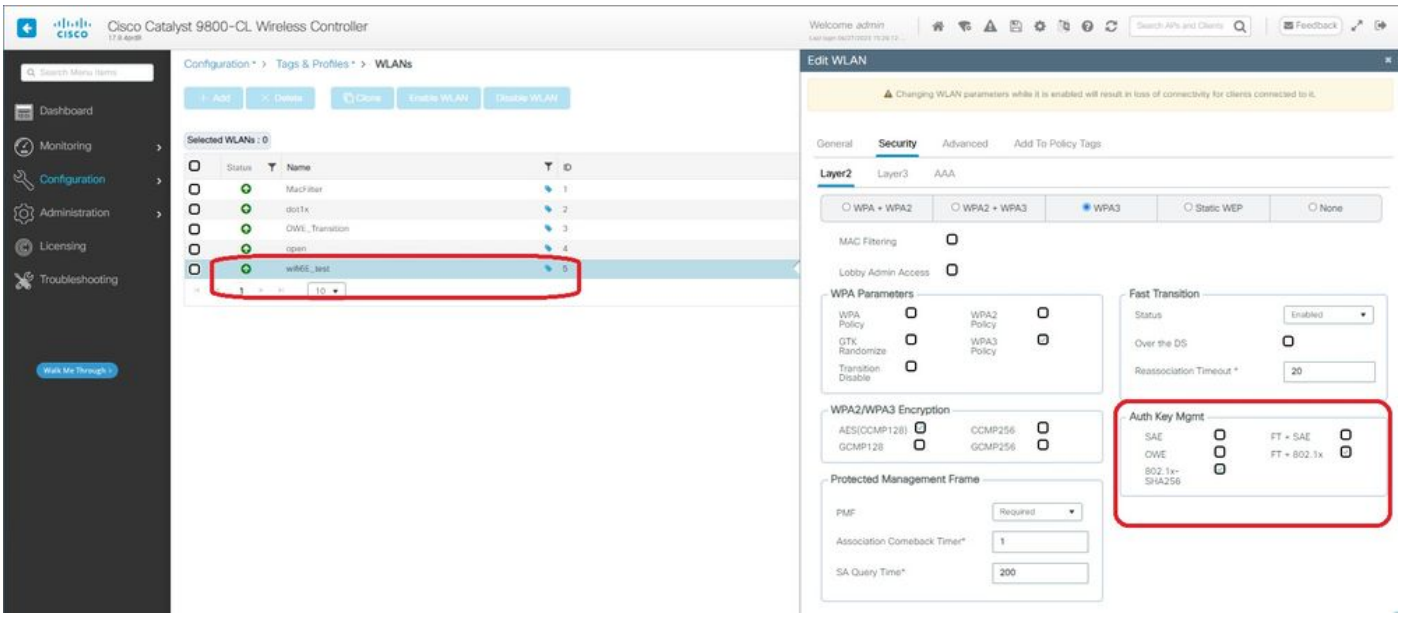
تعذر على الجهاز التجول عند تمكين FT.

سامسونج إس 23

تعذر على الجهاز التجول عند تمكين FT.

WPA3-Enterprise + AES(CCMP128) + 802.1x-SHA256 + FT

تكوين أمان WLAN:



WPA3 Enterprise 802.1x-SHA256 + تكوين أمان FTWLAN

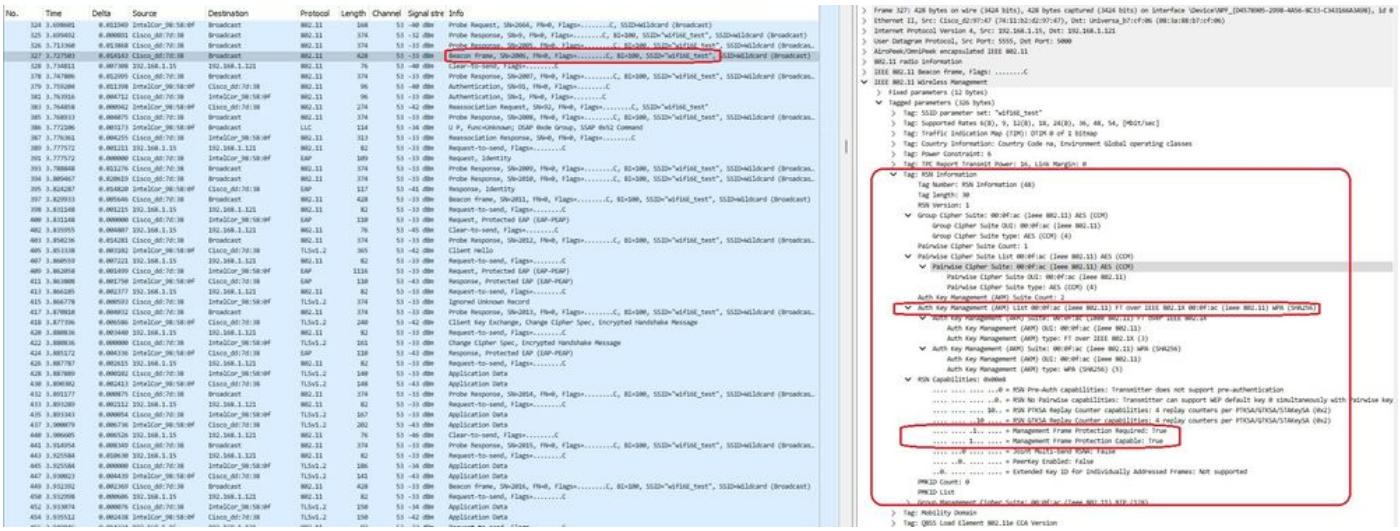
عرض على واجهة المستخدم الرسومية (GUI) الخاصة بإعدادات أمان WLAN:

هنا يستطيع رأيت ال ISE Live سجل مقياس سرعة ظهر ال يصدق قادم من كل أداة:

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Profile	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device
				Identity	Endpoint ID	Endpoint Profile	Authentication	Authorization	Authorization	IP Address	Network Device
Jun 27, 2023 01:52:38.130 PM			0	tantunes	04:29:2E:C9:E3:71		WirelessDot...	WirelessDot...	PermitAccess		
Jun 27, 2023 01:52:38.130 PM				tantunes	04:29:2E:C9:E3:71		WirelessDot...	WirelessDot...	PermitAccess		eWLC-9800-01
Jun 27, 2023 01:51:53.850 PM			0	tantunes	24:95:2F:72:8A:66	Unknown	WirelessDot...	WirelessDot...	PermitAccess		
Jun 27, 2023 01:51:53.850 PM				tantunes	24:95:2F:72:8A:66	Unknown	WirelessDot...	WirelessDot...	PermitAccess		eWLC-9800-01
Jun 27, 2023 01:50:58.679 PM			0	tantunes	94:18:65:48:70:95	Netgear-Device	WirelessDot...	WirelessDot...	PermitAccess		
Jun 27, 2023 01:50:58.679 PM				tantunes	94:18:65:48:70:95	Netgear-Device	WirelessDot...	WirelessDot...	PermitAccess		eWLC-9800-01
Jun 27, 2023 01:50:43.883 PM				tantunes	94:18:65:48:70:95	Netgear-Device	WirelessDot...	WirelessDot...	PermitAccess		eWLC-9800-01
Jun 27, 2023 01:50:42.877 PM			0	tantunes	28:6B:35:98:58:0F	Intel-Device	WirelessDot...	WirelessDot...	PermitAccess		
Jun 27, 2023 01:50:42.877 PM				tantunes	28:6B:35:98:58:0F	Intel-Device	WirelessDot...	WirelessDot...	PermitAccess		eWLC-9800-01

سجلات ISE المباشرة

المنارات OTA تبدو هكذا:

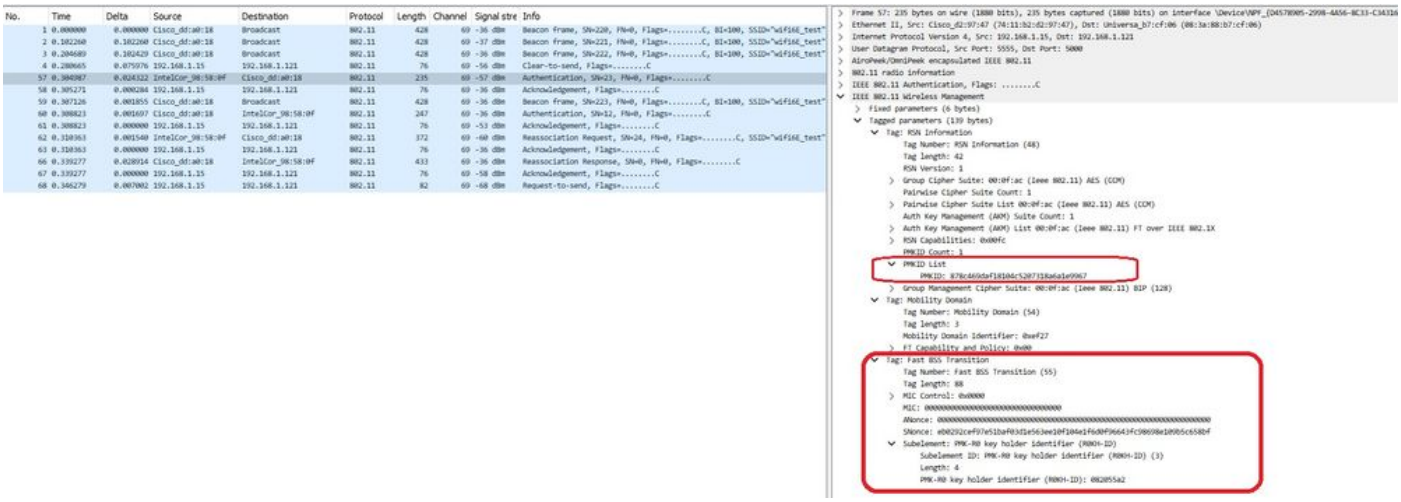


WPA3 Enterprise 802.1x +FT Beacon

هنا يمكن أن نشاهد عملاء Wi-Fi 6e الذين يربطون:

مجموعة الشرائح Intel AX211

الاتصال OTA مع التركيز على معلومات RSN من العميل على حدث تجوال:

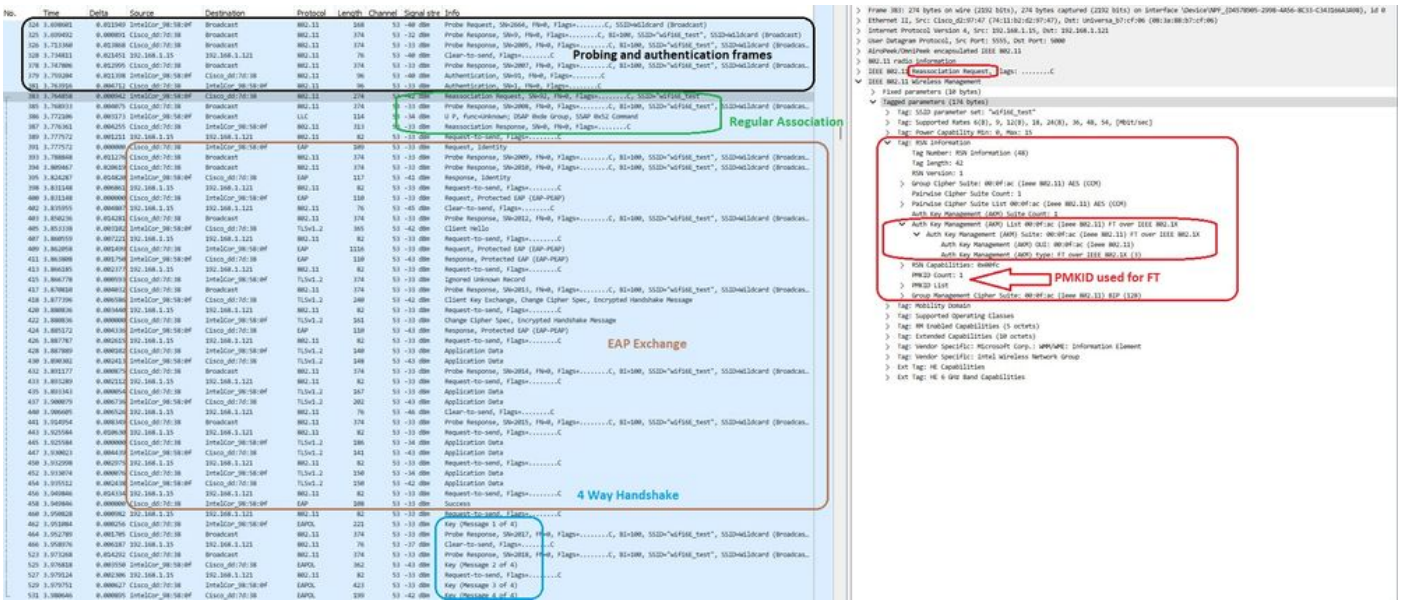


حدث تجوال WPA3 Enterprise 802.1x + FT

يحدث سلوك مثير للاهتمام إذا قمت بحذف العميل يدويا من الشبكة المحلية اللاسلكية

(من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) على سبيل المثال). يستلم العميل إطار إلغاء اقتران ولكنه يحاول إعادة الاتصال بنفس نقطة الوصول ويستخدم إطار إعادة اقتران يتبعه تبادل EAP كامل لأن تفاصيل العميل تم حذفها من نقطة الوصول/WLC.

وهذا هو أساسا نفس الإطار التبادلي كما في عملية اقتران جديدة. هنا يمكنك رؤية تبادل الإطارات:



تدفق اتصال WPA3 Enterprise 802.1x + FT AX211

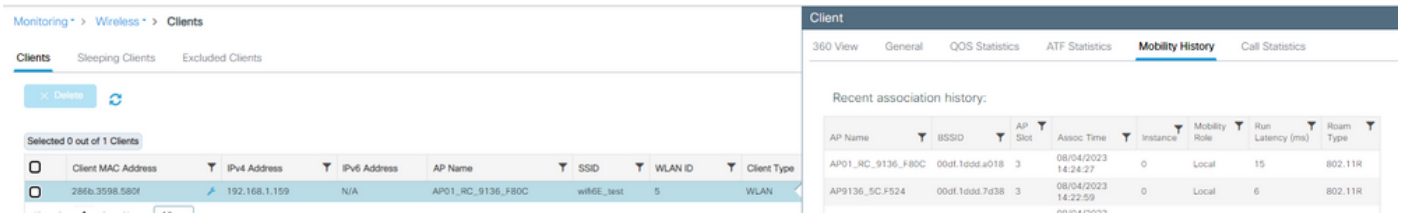
تفاصيل العميل في WLC:

تفاصيل عميل WPA3 Enterprise 802.1x + FT

لقد تم إختبار هذا العميل أيضا باستخدام تقنية FT عبر نظام DS، كما تمكن من التجوال باستخدام معيار 802. 11r:

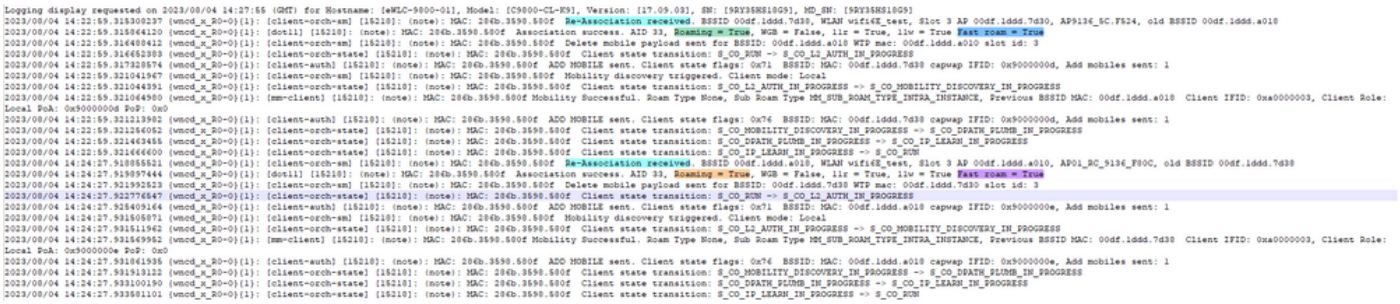
AX211 الجتواال مع FT عبر DS

يمكننا أيضا مشاهدة أحداث الجتواال في FT:



WPA3 Enterprise مع FT

وتعقب العميل من WLC:

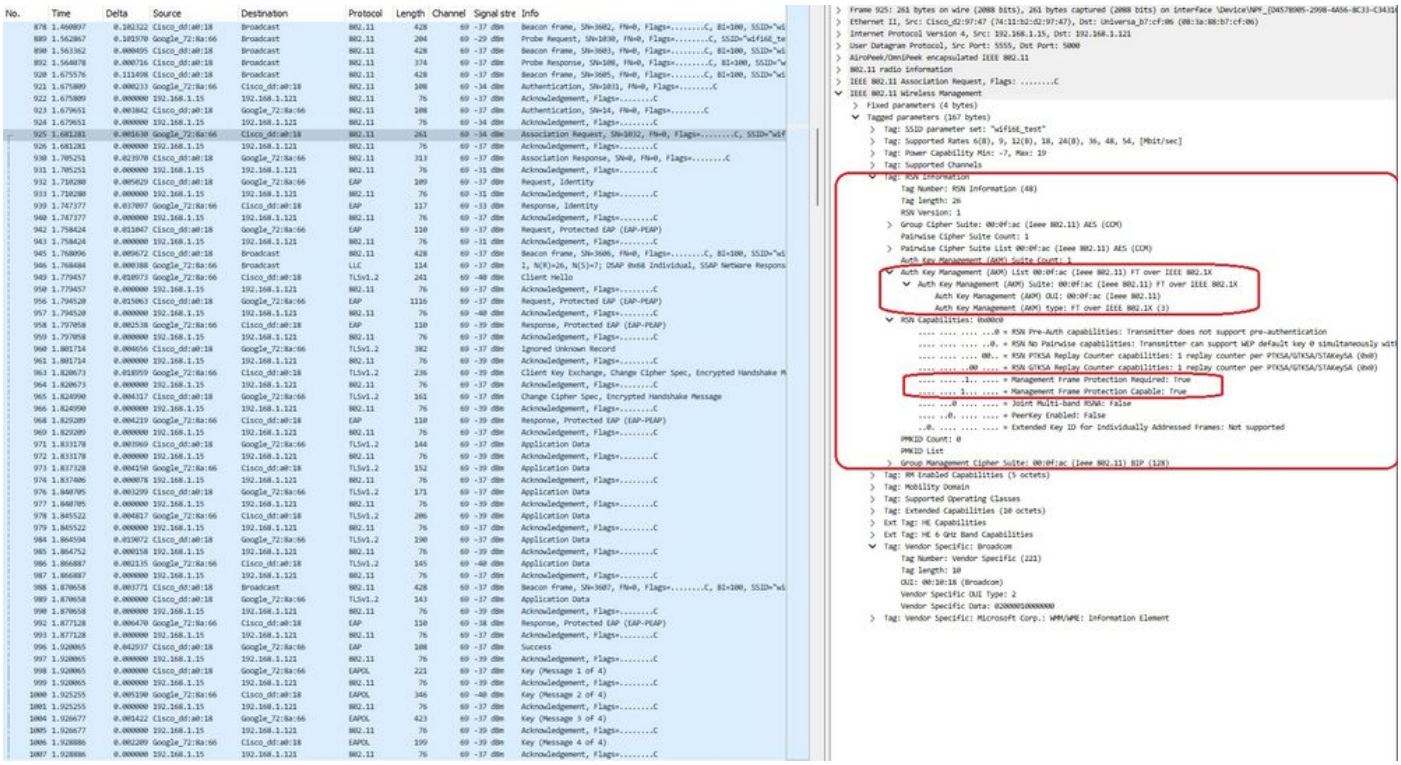


NetGear A8000

WPA3-Enterprise غير معتمد على هذا العميل.

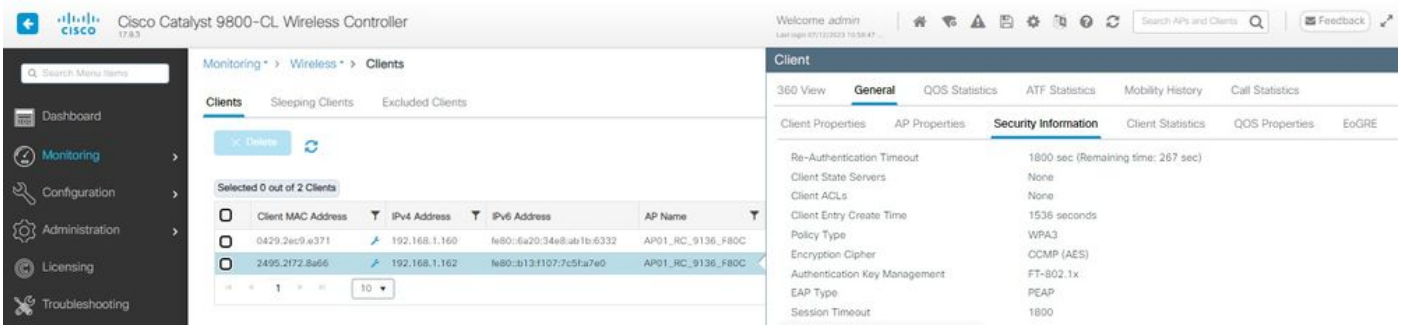
بيكسل 6a

الاتصال OTA مع التركيز على معلومات RSN من العميل:



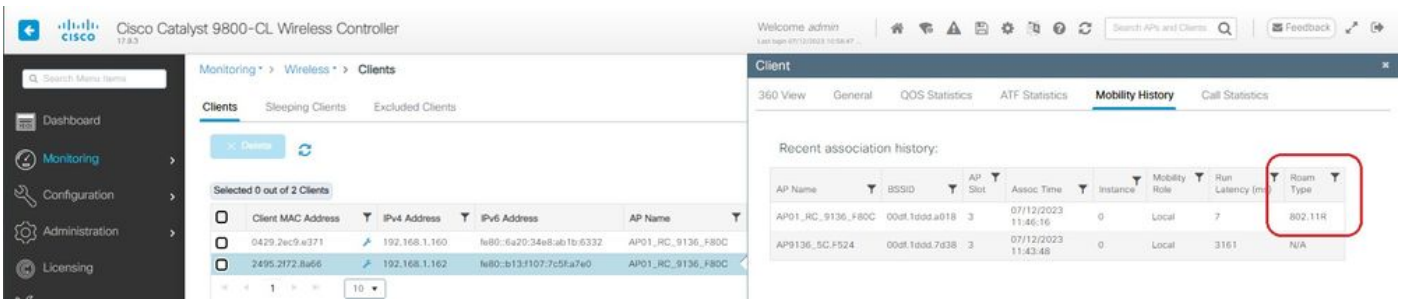
WPA3 Enterprise 802.1x + FT Pixel6a الاقتران

تفاصيل العميل في WLC:



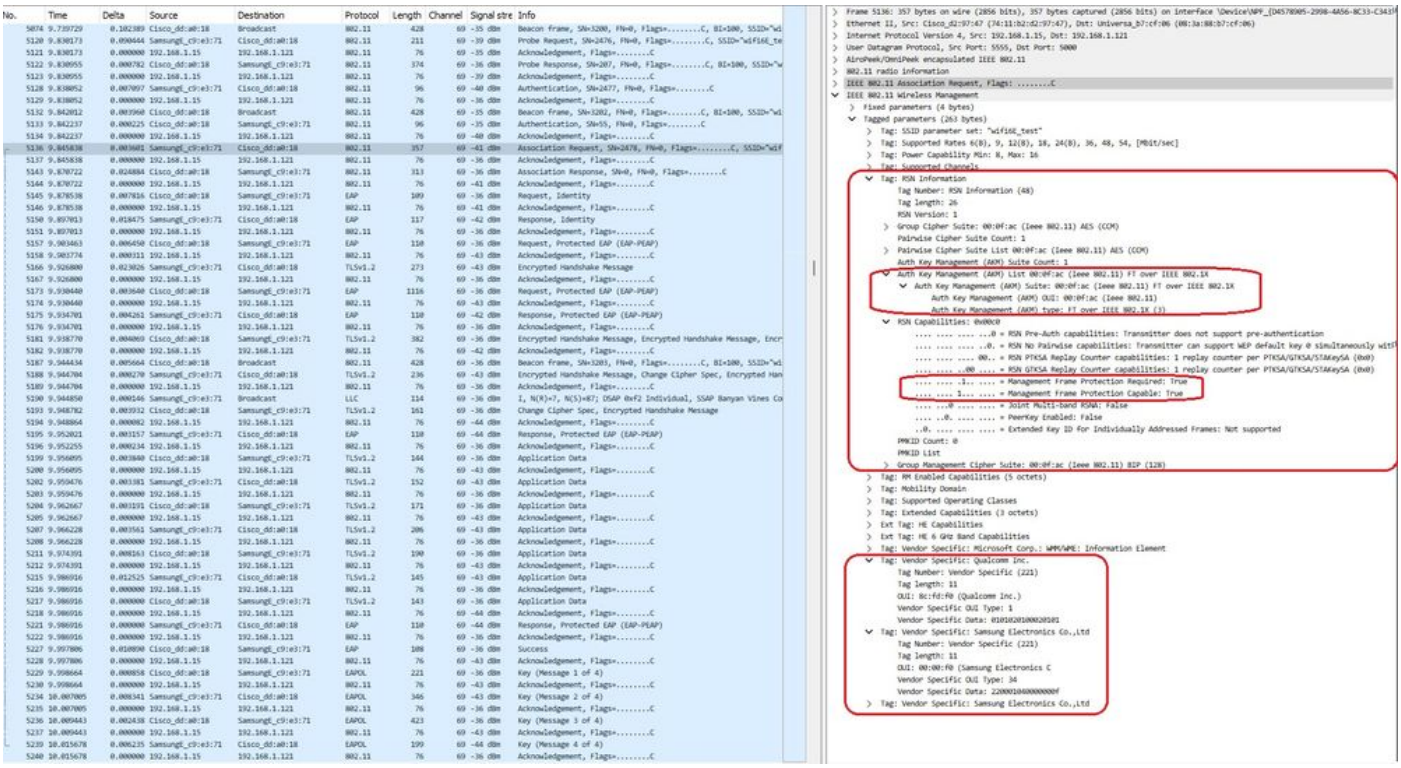
WPA3 Enterprise 802.1x + FT Pixel6a تفاصيل العميل

ركز على نوع التجوال عبر الهواء حيث يمكننا رؤية نوع التجوال 802. 11R:



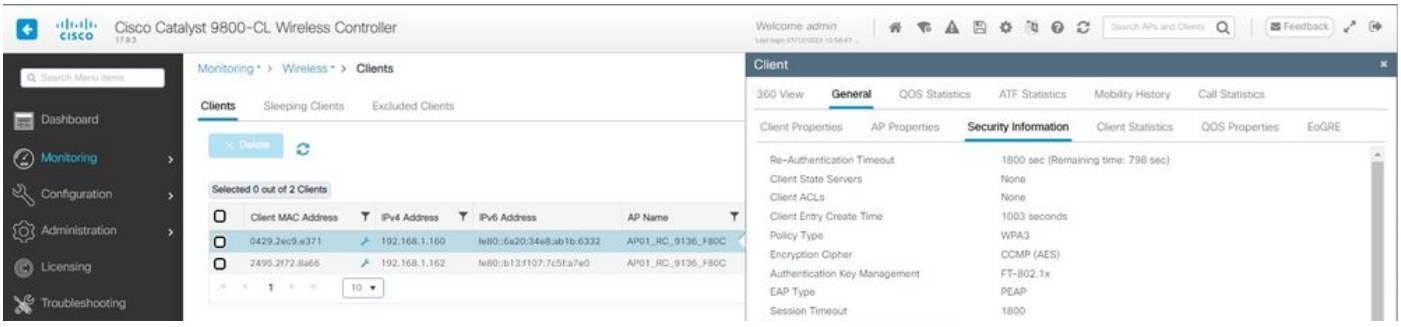
سامسونج إس 23

التصال OTA مع التركيز على معلومات RSN من العميل:



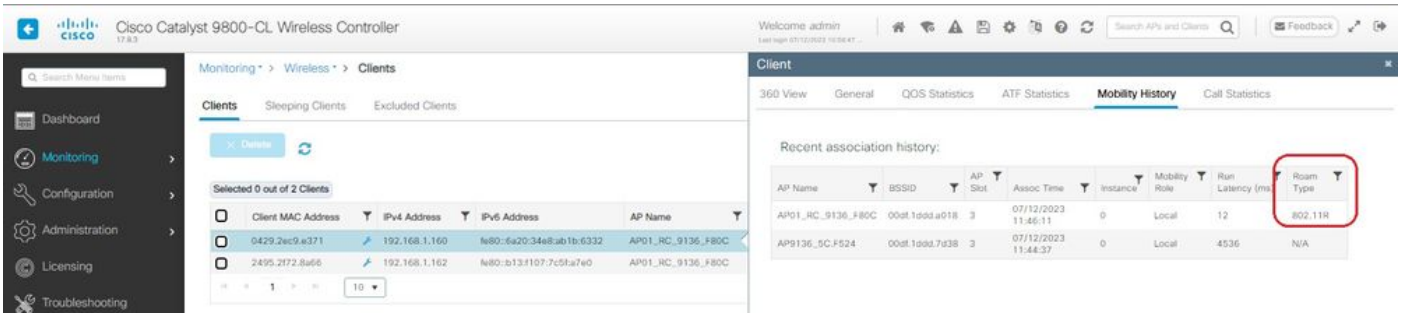
حدث تجوال S23 FToTA

تفاصيل العميل في WLC:



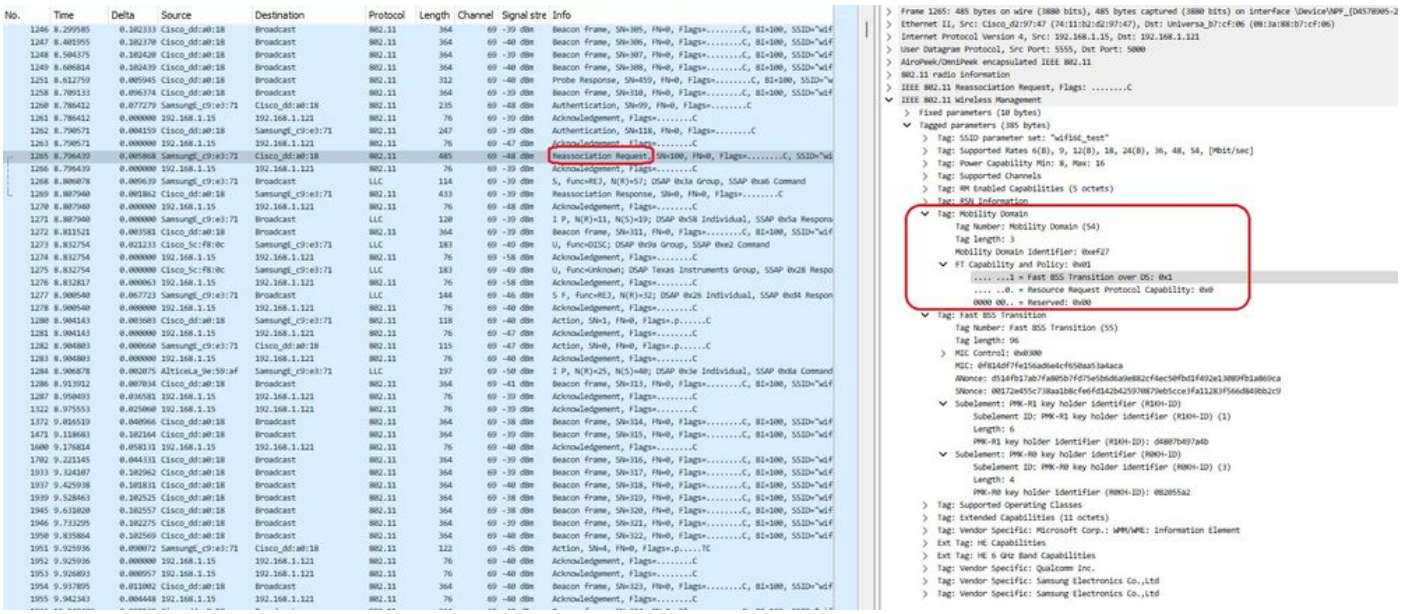
خصائص عميل S23

ركز على نوع التجوال عبر الهواء حيث يمكننا رؤية نوع التجوال 802. 11R:



S23 Roaming Type 802.11R

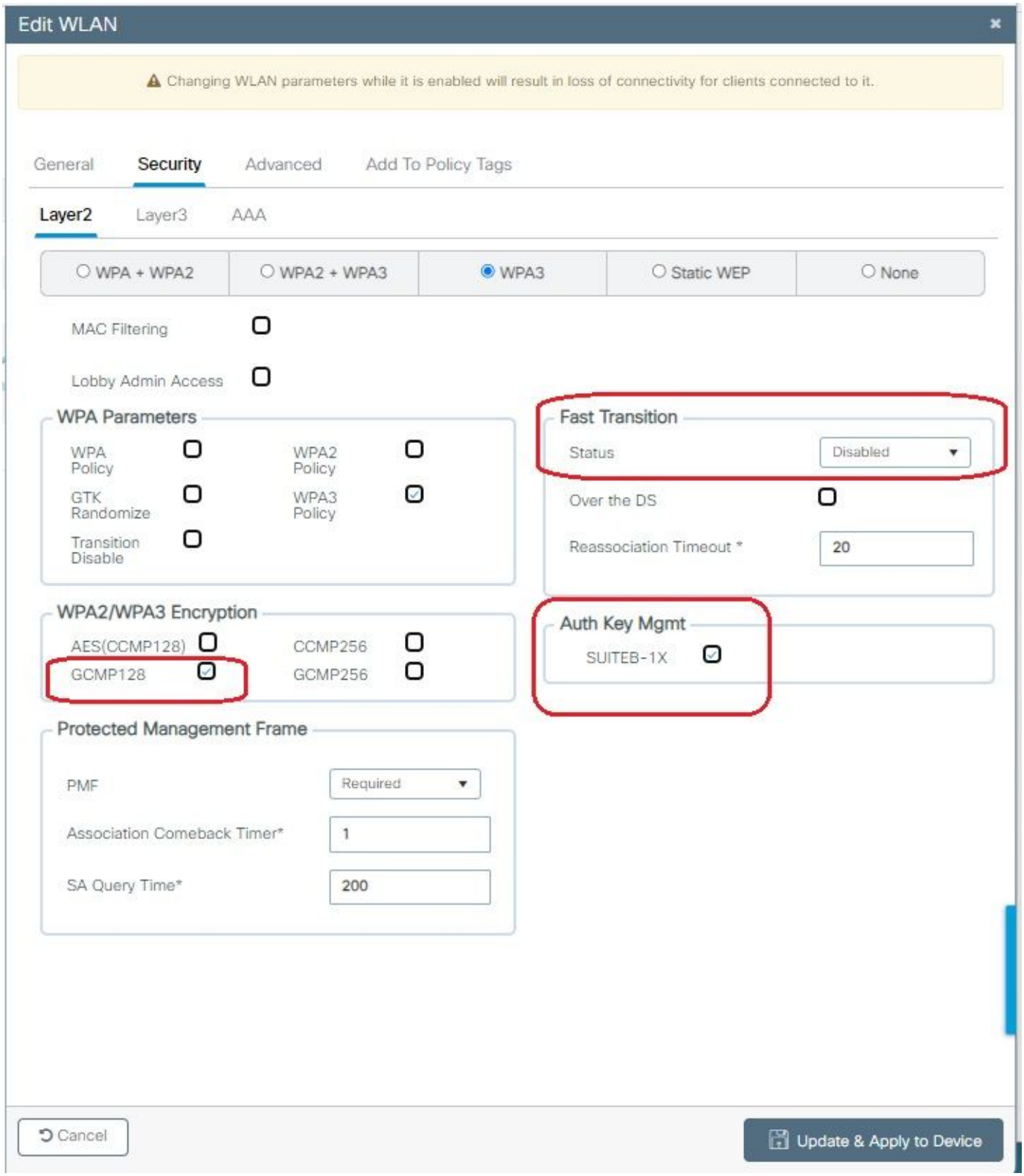
لقد تم إختبار هذا العميل أيضا باستخدام تقنية FT عبر نظام DS، كما تمكن من التجوال باستخدام معيار 802. 11r:



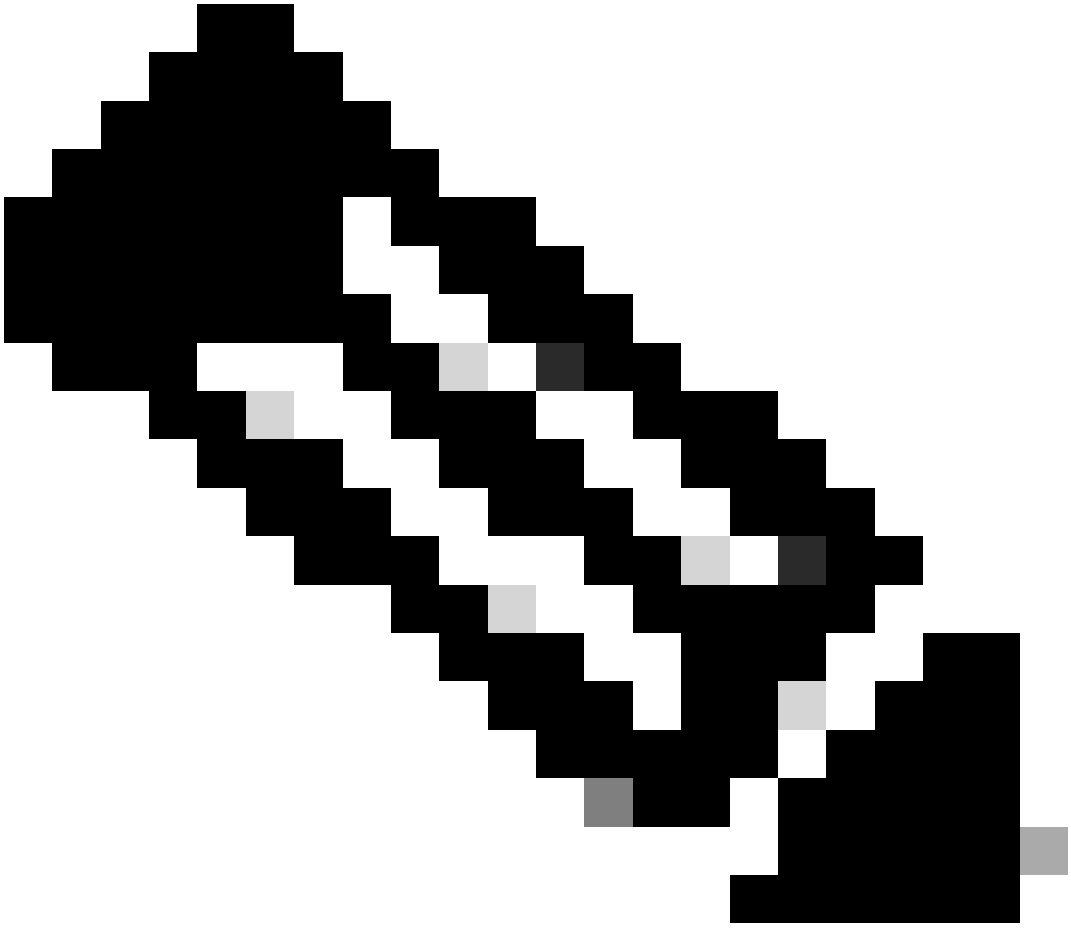
مزج S23 Roaming FToDS

WPA3-مؤسسي + GCMP128 تشفير + Suiteb-1X

تكوين أمان WLAN:



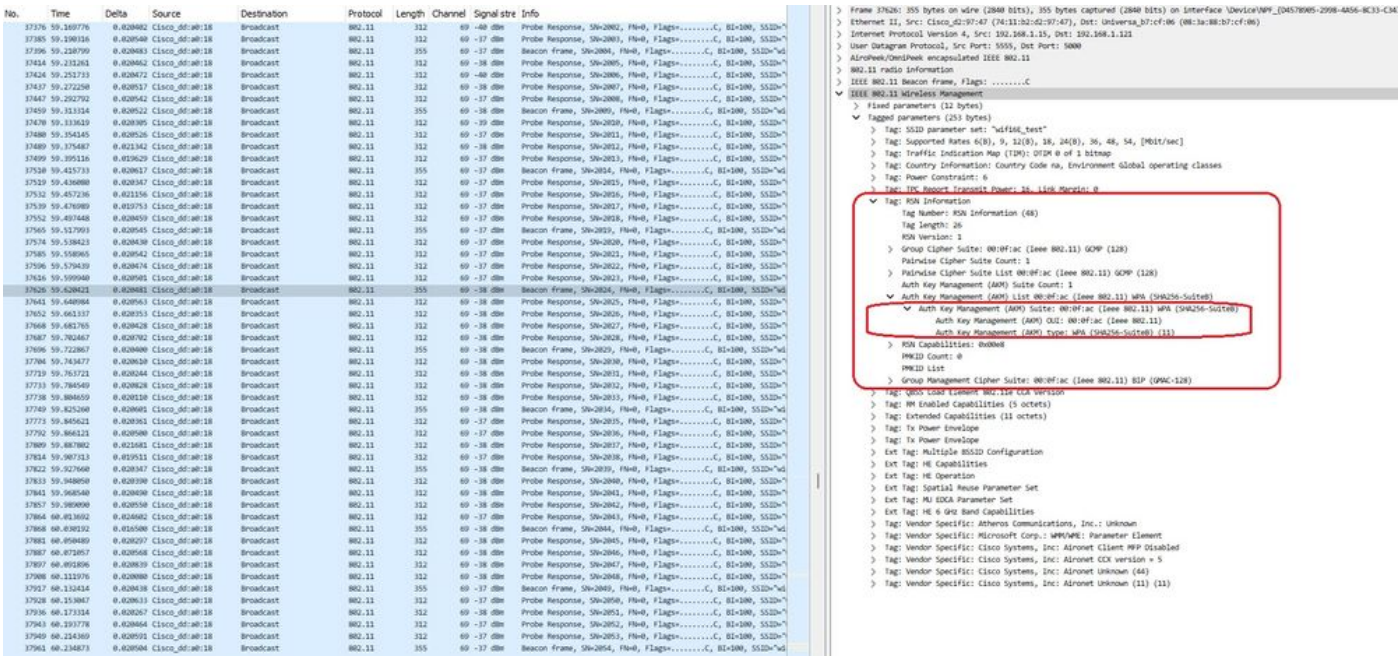
تكوين الأمان WPA3 Enterprise SuiteB-1X



ملاحظة: لا يتم دعم ft في SUITEB-1X

عرض على واجهة المستخدم الرسومية (GUI) الخاصة بإعدادات أمان WLAN:

التحقق من أجهزة الإرشاد OTA:

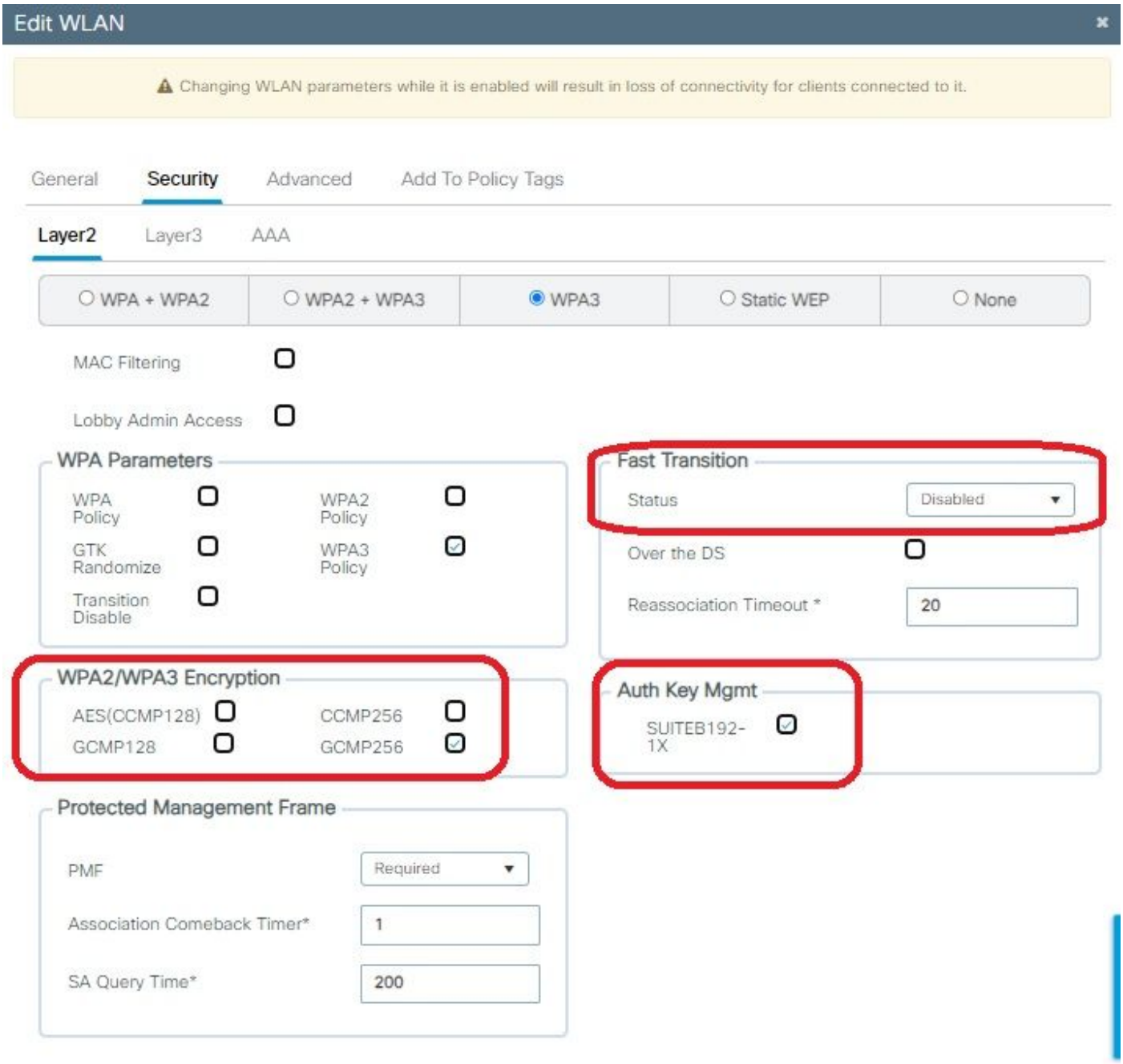


WPA3 Enterprise SuiteB-1X Beacon

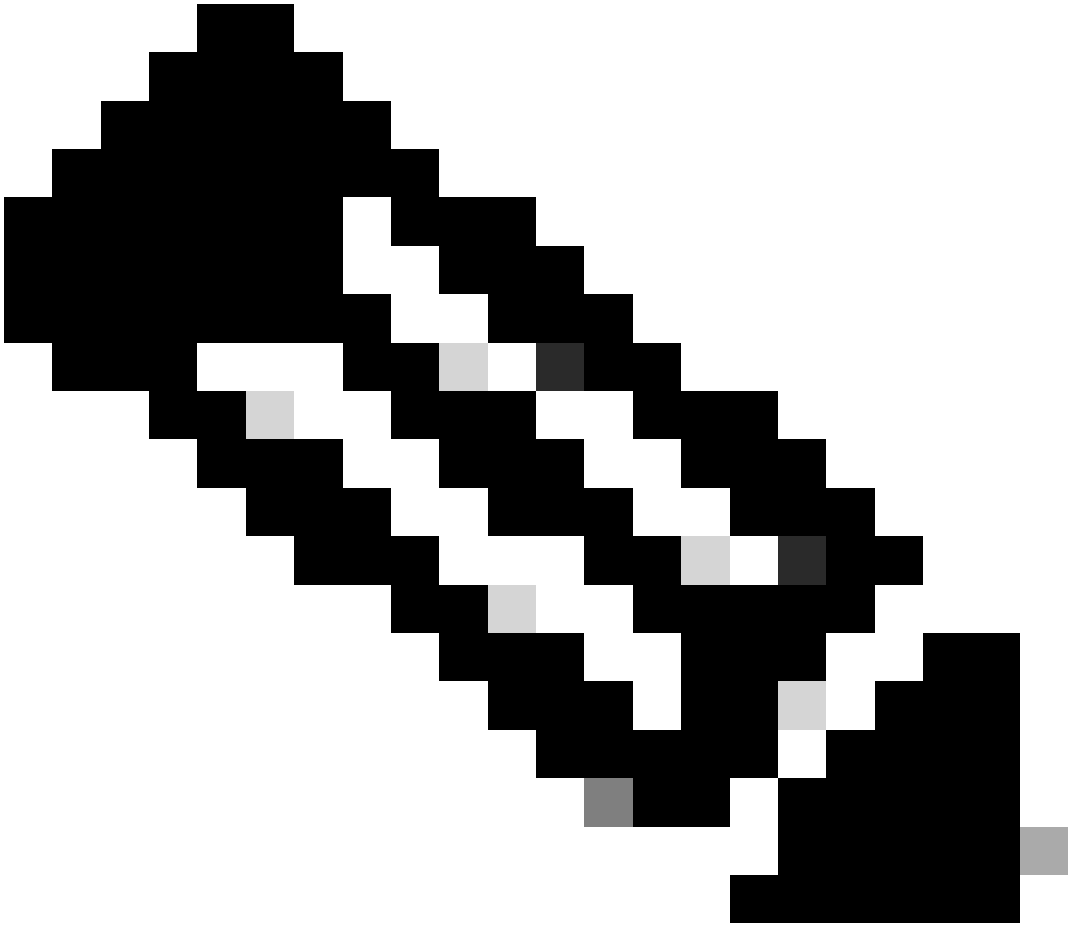
لم يتمكن أي من العملاء الذين تم إختباره من الاتصال بشبكة WLAN باستخدام SuiteB-1X مما يؤكد أن ال شيء يدعم طريقة الأمان هذه.

WPA3-مؤسسي + GCMP256 تشفير + Suiteb192-1X

تكوين أمان WLAN:



إعدادات تأمين WPA3 Enterprise Suiteb192-1x

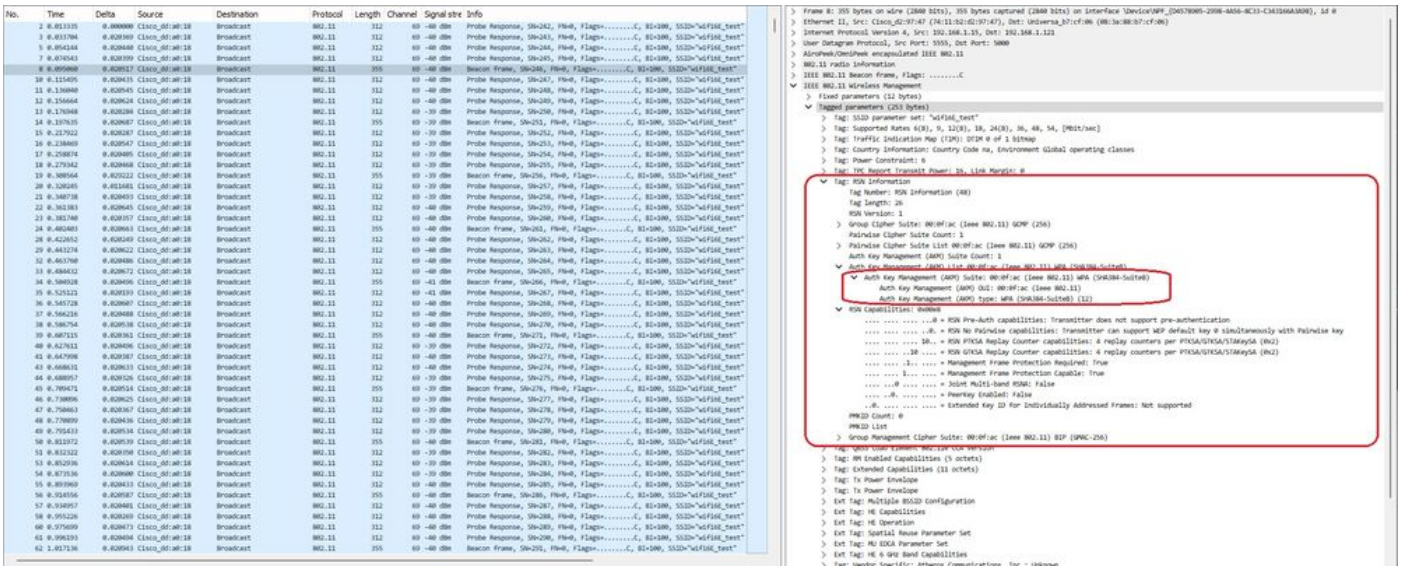


ملاحظة: لا يتم دعم ft مع GCMP256+SUITEB192-1X.

WLAN على قائمة شبكات WLAN الخاصة بواجهة مستخدم الرسومات (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC):

WLAN المستخدمة للاختبارات

التحقق من أجهزة الإرشاد OTA:

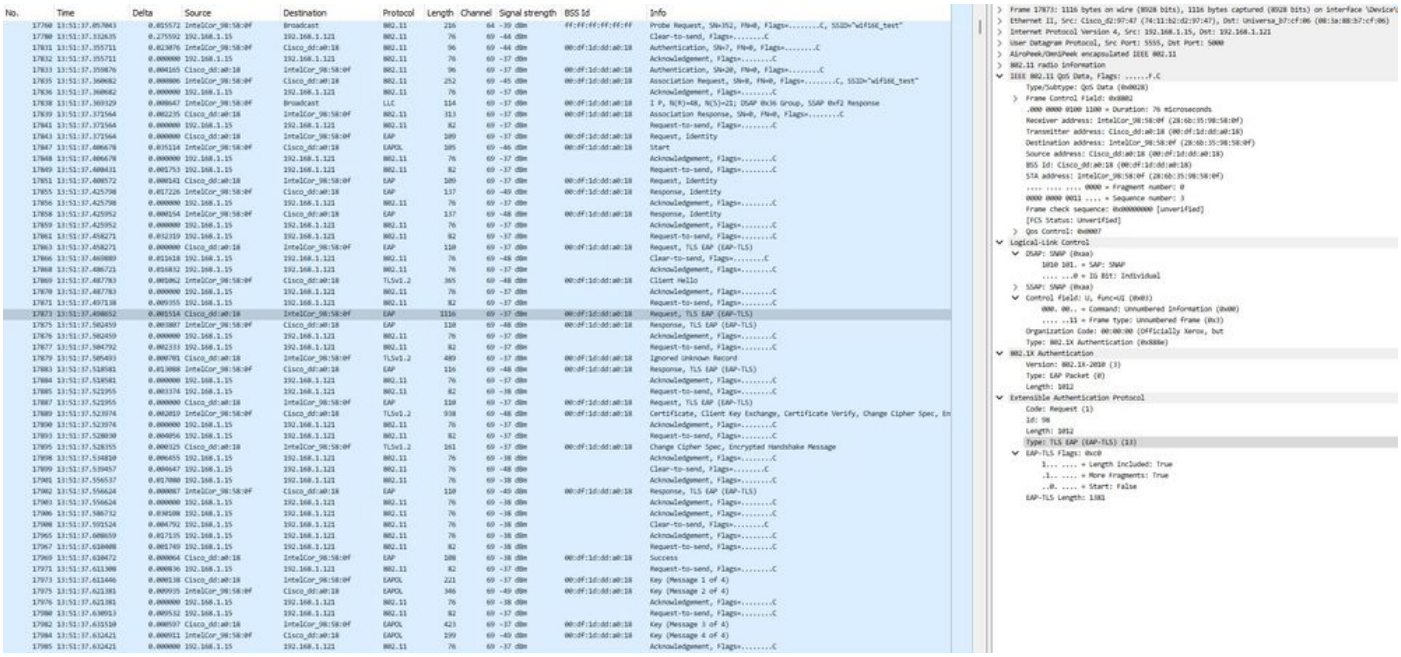


WPA3 Enterprise Suiteb192-1x Beacons

هنا يمكن أن نشاهد عملاء Wi-Fi 6e الذين يربطون:

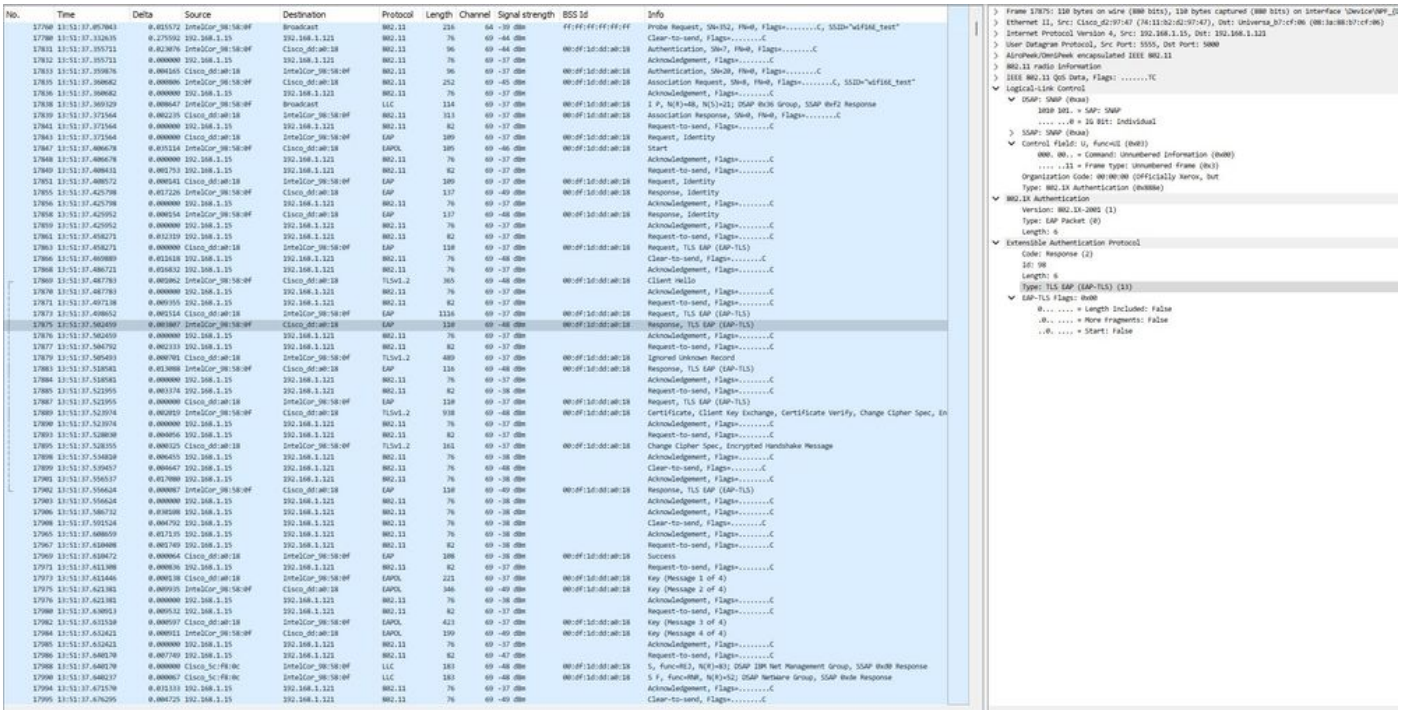
مجموعة الشرائح Intel AX211

الاتصال OTA مع التركيز على معلومات RSN من العميل:



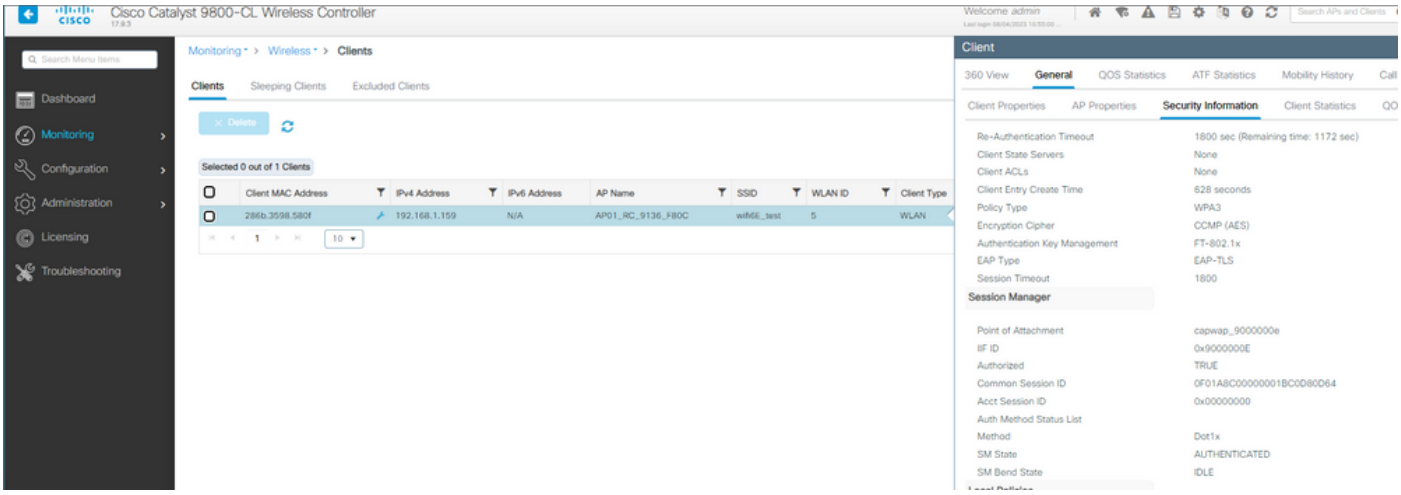
WPA3 Enterprise مع اقتران EAP-TLS بمعلومات عميل AX211 من Intel و RSN

وتبادل EAP-TLS:



WPA3 Enterprise مع EAP-TLS مع عميل Intel AX211 وتركيز EAP-TLS

تفاصيل العميل في WLC:



تفاصيل WPA3 Enterprise مع عميل EAP-TLS

NetGear A8000

WPA3-Enterprise غير معتمد على هذا العميل.

بيكسل 6a

في تاريخ كتابة هذا المستند، لم يتمكن هذا العميل من الاتصال بـ WPA3 Enterprise باستخدام EAP-TLS.

وهذه مسألة من جانب العميل يجري العمل عليها، وبمجرد حلها، يتعين تحديث هذه الوثيقة.

سامسونج إس 23

في تاريخ كتابة هذا المستند، لم يتمكن هذا العميل من الاتصال بـ WPA3 Enterprise باستخدام EAP-TLS.

وهذه مسألة من جانب العميل يجري العمل عليها، وبمجرد حلها، يتعين تحديث هذه الوثيقة.

الاستنتاجات الأمنية

بعد كل الاختبارات السابقة، هذه هي الاستنتاجات النهائية:

البروتوكول	تشفير	AKM	شفرة AKM	أسلوب EAP	FT-OverTA	FT-overDS	مجموعة الشرائح Intel AX211	سامسونج/جوجل أندرويد
تستدانن	AES-CCMP128	تستدانن	غير موجود.	غير موجود.	غير موجود	غير موجود	مدعوم	مدعوم
نفس	AES-CCMP128	SAE (H2E فقط)	SHA256	غير موجود.	مدعوم	مدعوم	مدعوم: H2E فقط و FT-OTA	مدعوم: H2E فقط. فشل FT. فشل FT-oDS.
المؤسسات	AES-CCMP128	802.1x-SHA256	SHA256	PEAP/FAST/TLS	مدعوم	مدعوم	الدعم: SHA256 و FT-OTA/ODS غير مدعوم: EAP-FAST	مدعوم: SHA256 و FT-OTA و FT-ODS (S23) غير مدعوم: EAP-FAST و FT-oDS (Pixel6a)
المؤسسات	GCMP128	SuiteB-1x	SHA256-SuiteB	PEAP/FAST/TLS	غير مدعوم	غير مدعوم	غير مدعوم	غير مدعوم
المؤسسات	GCMP256	سويت بي-192	SHA384-SuiteB	TLS	غير مدعوم	غير مدعوم	NA/TBD	NA/TBD

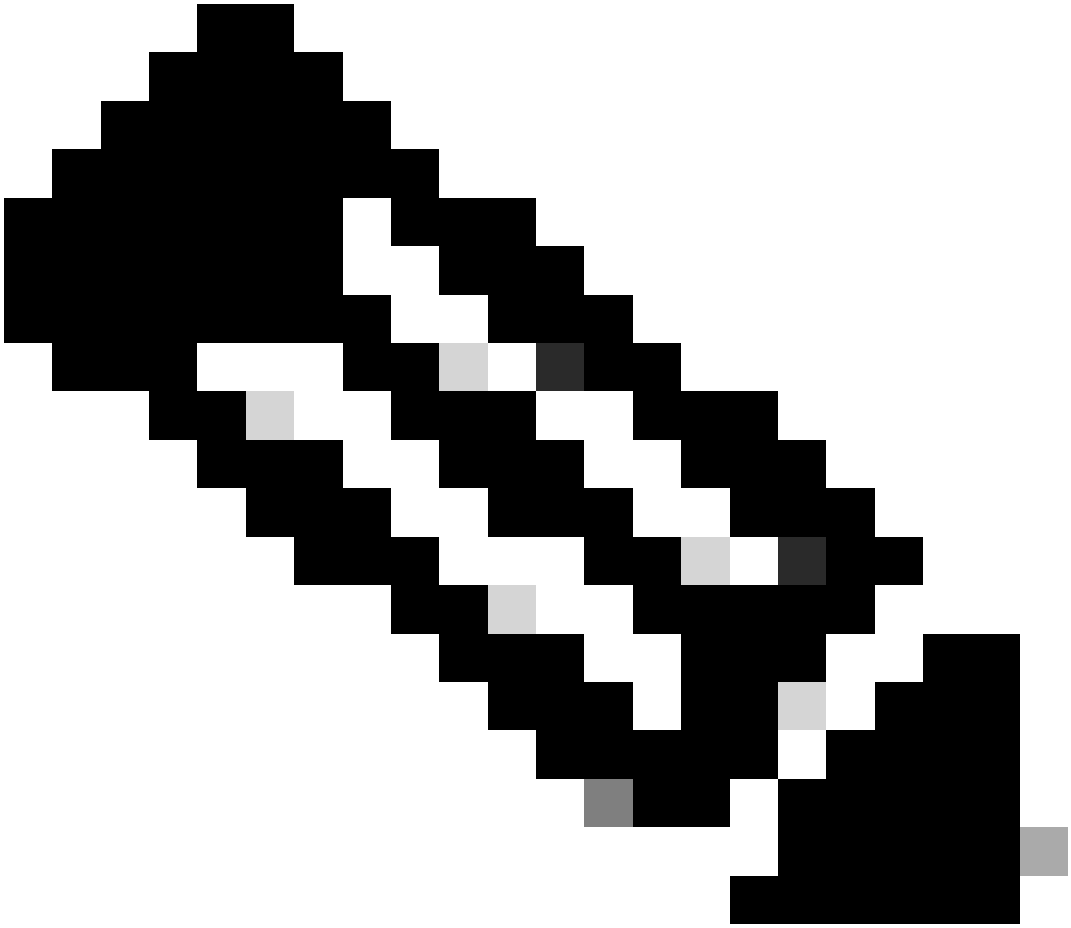
استكشاف الأخطاء وإصلاحها

استند أستكشاف الأخطاء وإصلاحها المستخدم في هذا المستند إلى المستند عبر الإنترنت:

أستكشاف أخطاء نقاط الوصول (APs) وإصلاحها

المبدأ التوجيهي العام لاستكشاف الأخطاء وإصلاحها هو تجميع تتبع RA في وضع تصحيح الأخطاء من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) باستخدام عنوان MAC للعميل للتأكد من اتصال العميل باستخدام جهاز MAC وليس عنوان MAC عشوائي.

على أستكشاف أخطاء Air وإصلاحها، تكون التوصية إستخدام نقطة الوصول في وضع sniffer التقاط حركة مرور البيانات على قناة نقطة الوصول التي يقوم العميل بخدمتها.



ملاحظة: ارجع إلى معلومات مهمة حول أوامر تصحيح الأخطاء قبل أن تستخدم أوامر debug.

معلومات ذات صلة

ما هو Wi-Fi 6E؟

ما هو Wi-Fi 6e؟ مقابل Wi-Fi 6

نظرة سريعة على Wi-Fi 6e

Wi-Fi 6e: الفصل الرائع التالي في تقرير Wi-Fi الأبيض

Cisco Live - إنشاء شبكة السلكية من الجيل التالي باستخدام نطاق وصول Catalyst Wi-Fi 6e

دليل تكوين برنامج Cisco Catalyst 9800 Series Wireless Controller Software، الإصدار 17.9.x

دليل نشر WPA3

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).