تكوين نقطة الوصول في وضع sniffer على وحدات التحكم اللاسلكية Catalyst 9800

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
التكوين
الرسم التخطيطي للشبكة
التكوينات
تكلت AP في sniffer أسلوب عن طريق GUI
تكلت ap في sniffer أسلوب عن طريق CLI
تكوين نقطة وصول لمسح قناة عبر واجهة المستخدم الرسومية
تكوين نقطة الوصول لمسح قناة عبر CLI (واجهة سطر الأوامر)
تكوين Wireshark لجمع التقاط الحزمة
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
معلومات ذات صلة

المقدمة

يصف هذا وثيقة كيف أن يشكل منفذ نقطة (ap) في sniffer أسلوب على مادة حفازة 9800 sery السلكي جهاز تحكم (9800 WLC) من خلال الرسم مستعمل قران (gui) أو أمر خط قران (CLI) وكيف أن يجمع ربط قبض (PCAP) على الهواء (OTA) مع ال sniffer ap in order to تحريت وحللت السلكي تصرف.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين 9800 WLC
- معرفة أساسية بمعيار 802.11

المكونات المستخدمة

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

- نقطة الوصول 2802
- 9800 WLC Cisco IOS®-XE، الإصدار 17.3.2a
- Wireshark 3.x

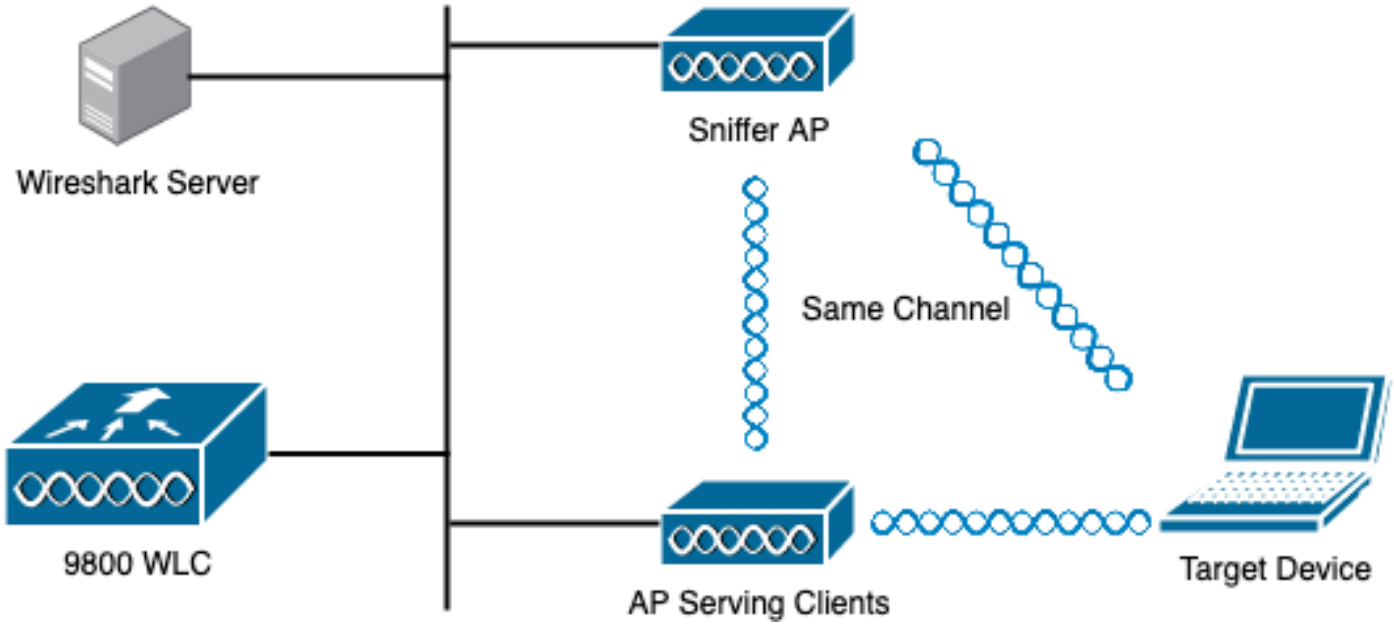
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

امور يجب التأمل فيها:

- يوصى بأن يكون نقطة الوصول sniffer قريبة من الجهاز المستهدف ونقطة الوصول التي يكون هذا الجهاز متصلا بها.
- تأكد من معرفة القناة 802.11 والعرض وجهاز العميل واستخدام نقطة الوصول.

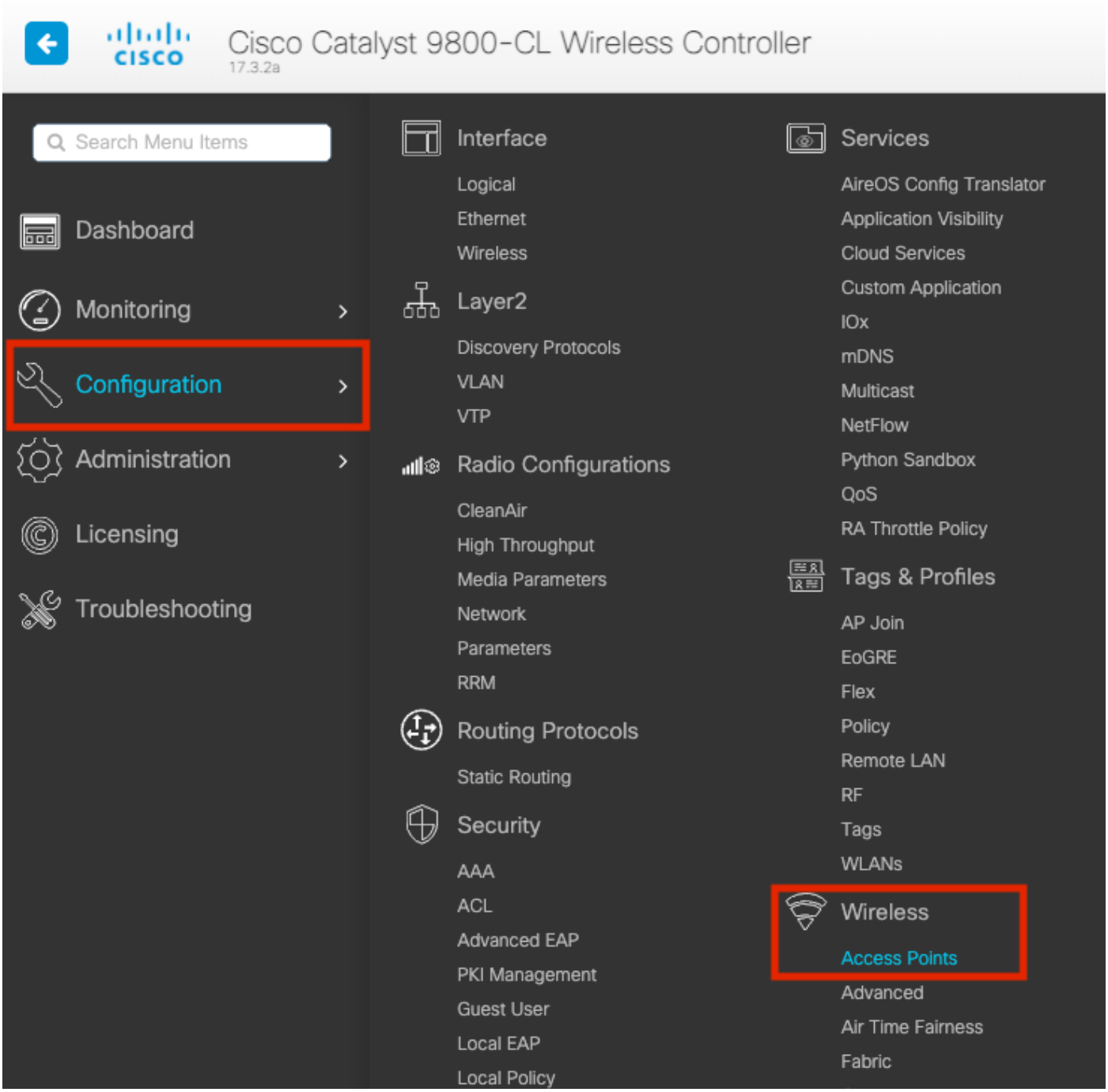
الرسم التخطيطي للشبكة



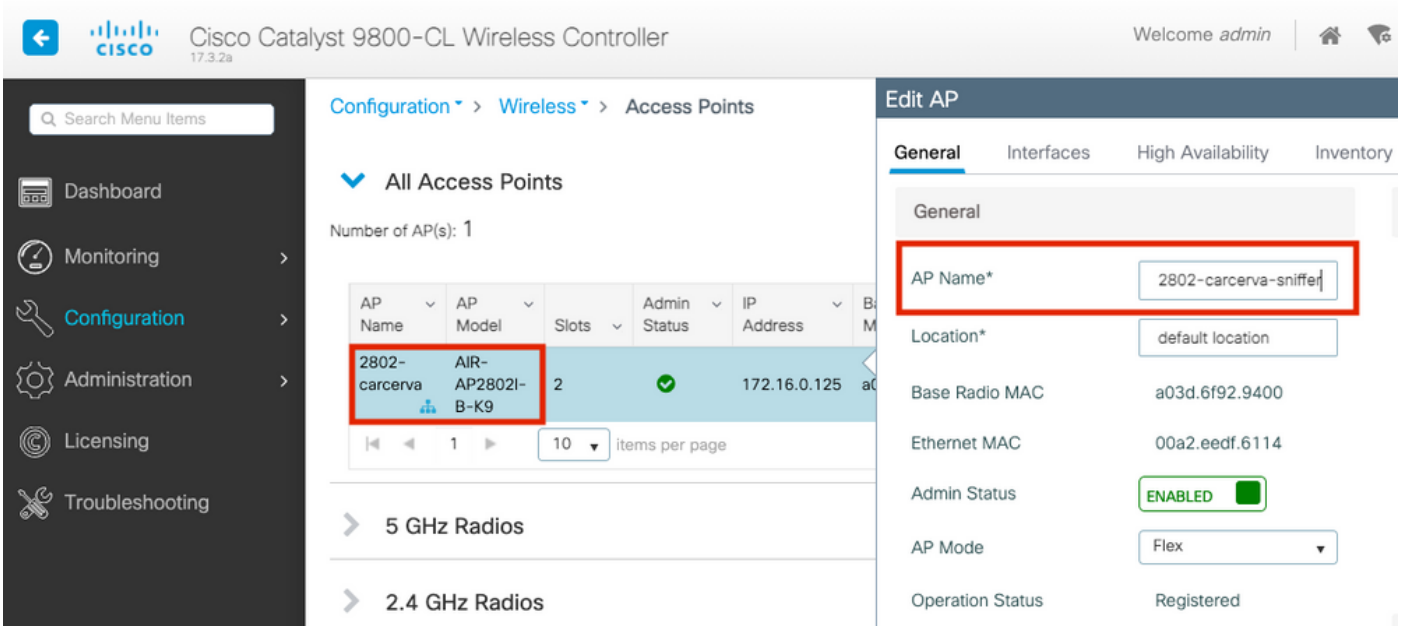
التكوينات

شكلت AP في sniffer أسلوب عن طريق GUI

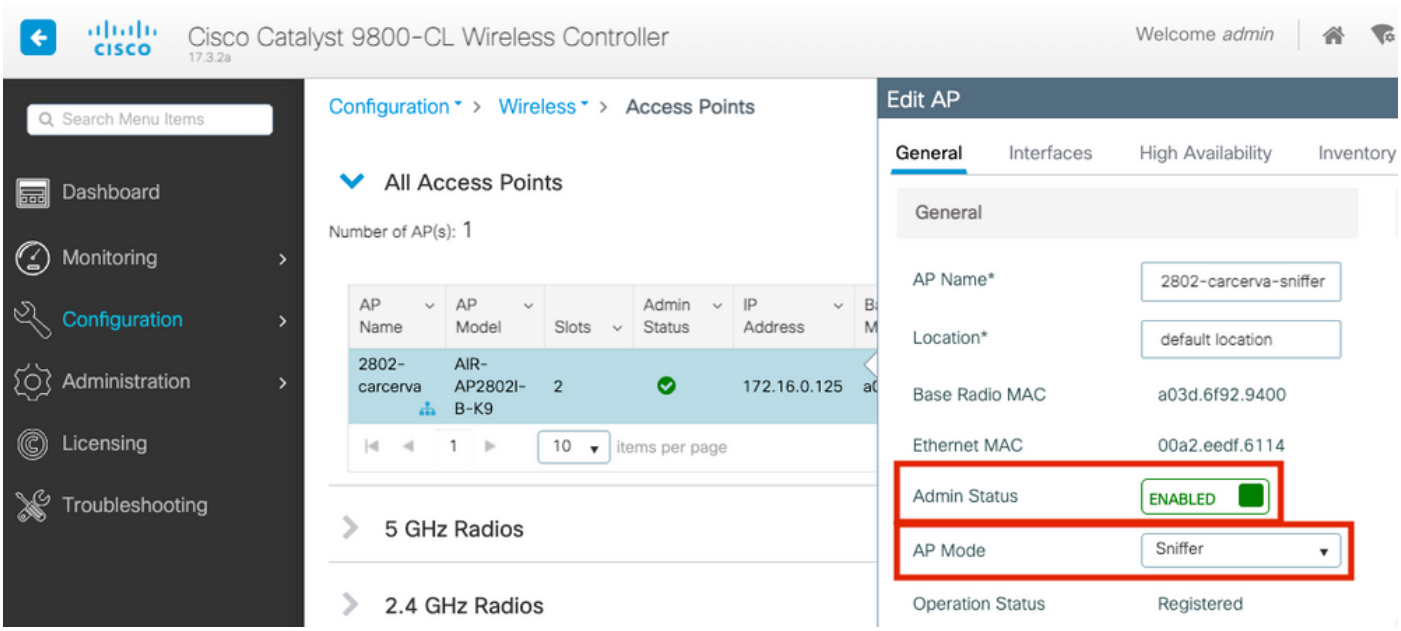
الخطوة 1. في واجهة المستخدم الرسومية (GUI) الخاصة بواجهة مستخدم الرسومات (WLC) طراز 9800، انتقل إلى **التكوين > السلكي > نقاط الوصول > جميع نقاط الوصول**، كما هو موضح في الصورة.



الخطوة 2. حدد نقطة الوصول التي ترغب في إستخدامها في وضع sniffer. على علامة التبويب **عام**، قم بتحديث اسم نقطة الوصول، كما هو موضح في الصورة.



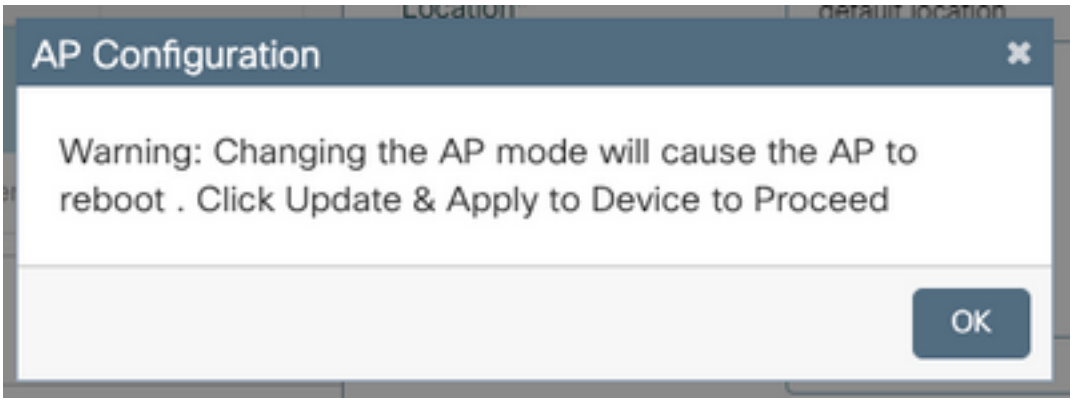
الخطوة 3. دقق **Admin وضع يمكن** غيرت **ال ap أسلوب** إلى **sniffer**، كما هو موضح في الصورة.



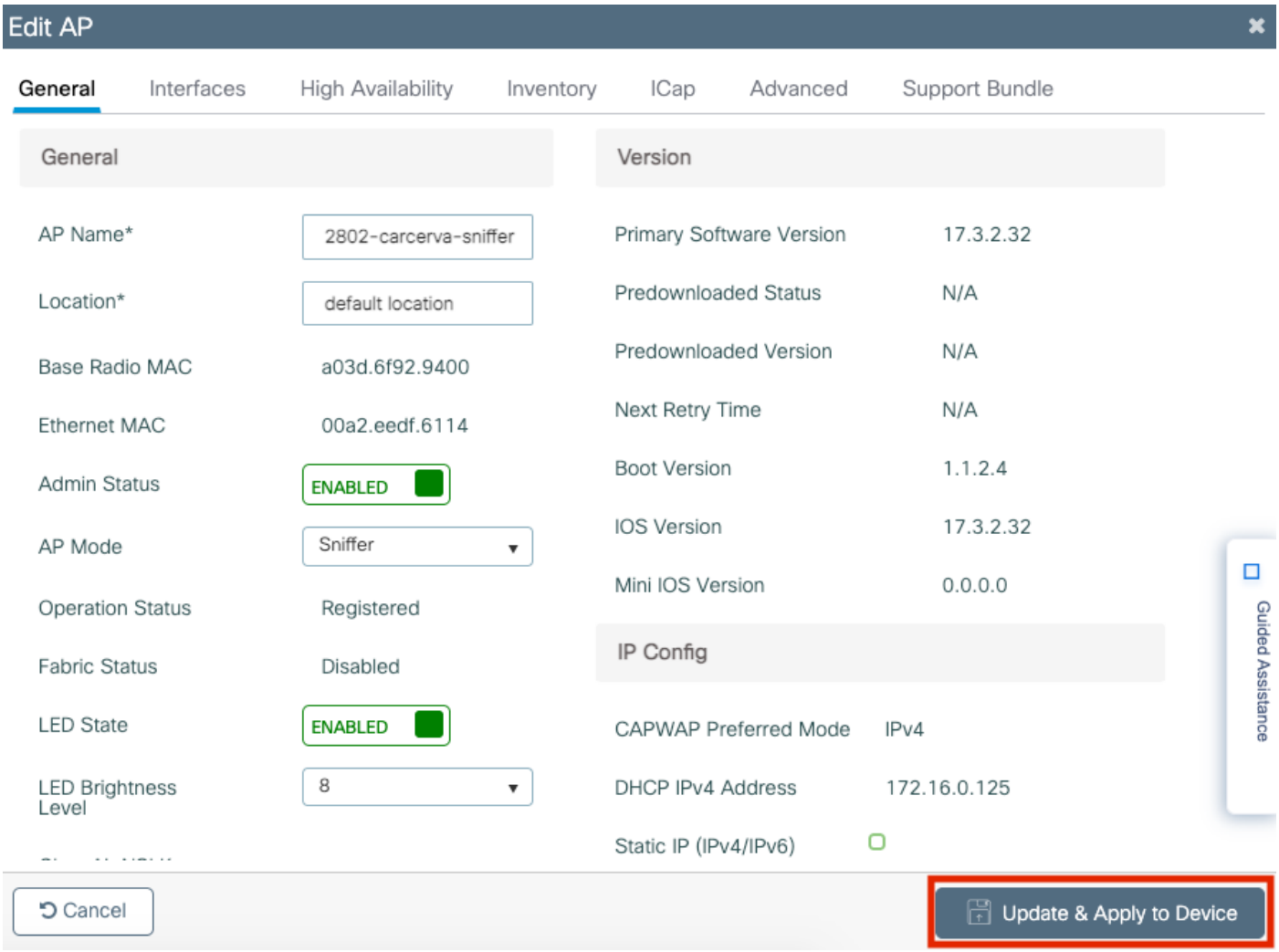
يظهر إطار منبثق مع الملاحظة التالية:

"تحذير: سيؤدي تغيير وضع نقطة الوصول إلى إعادة تمهيد نقطة الوصول. انقر فوق تحديث وتطبيق على الجهاز للمتابعة

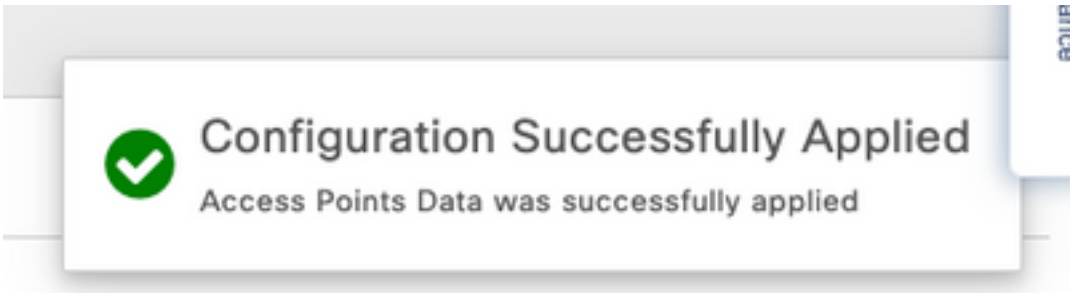
حدد **موافق**، كما هو موضح في الصورة.



الخطوة 4. انقر على **تحديث وتطبيق على الجهاز**، كما هو موضح في الصورة.



يظهر إطار منبثق لتأكيد التغييرات وثبات نقطة الوصول، كما هو موضح في الصورة.



شكلت ap في sniffer أسلوب عن طريق CLI

الخطوة 1. حدد نقطة الوصول التي ترغب في إستخدامها كوضع sniffer وتأخذ اسم نقطة الوصول.

الخطوة 2. قم بتعديل اسم نقطة الوصول.

يقوم هذا الأمر بتعديل اسم نقطة الوصول. حيث <AP-name> هو الاسم الحالي لنقطة الوصول.

```
carcerva-9k-upg#ap name <AP-name> name 2802-carcerva-sniffer
```

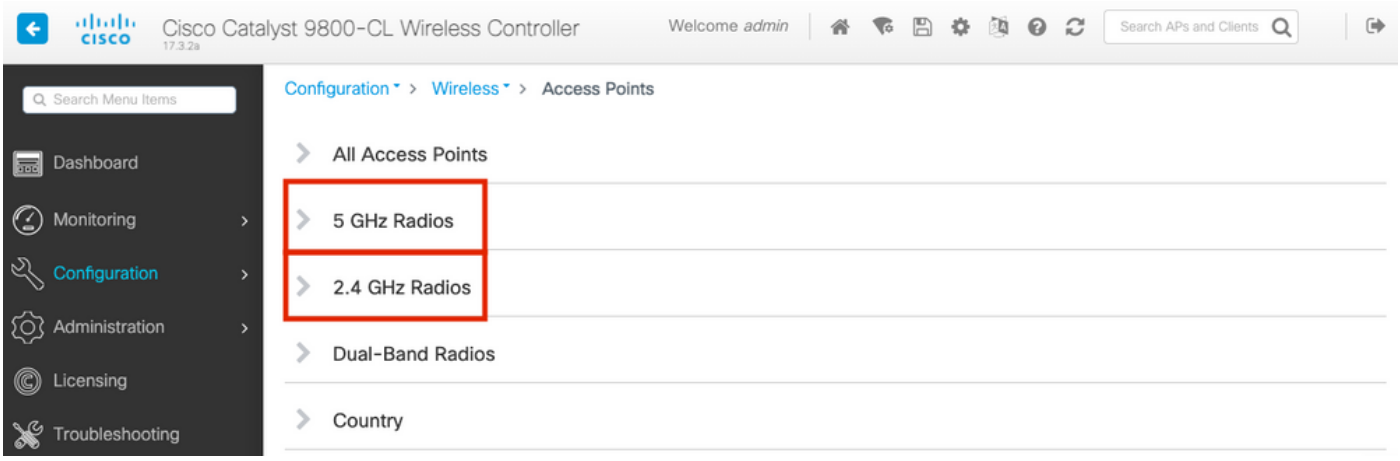
الخطوة 3. شكلت ال ap في sniffer أسلوب.

```
carcerva-9k-upg#ap name 2802-carcerva-sniffer mode sniffer
```

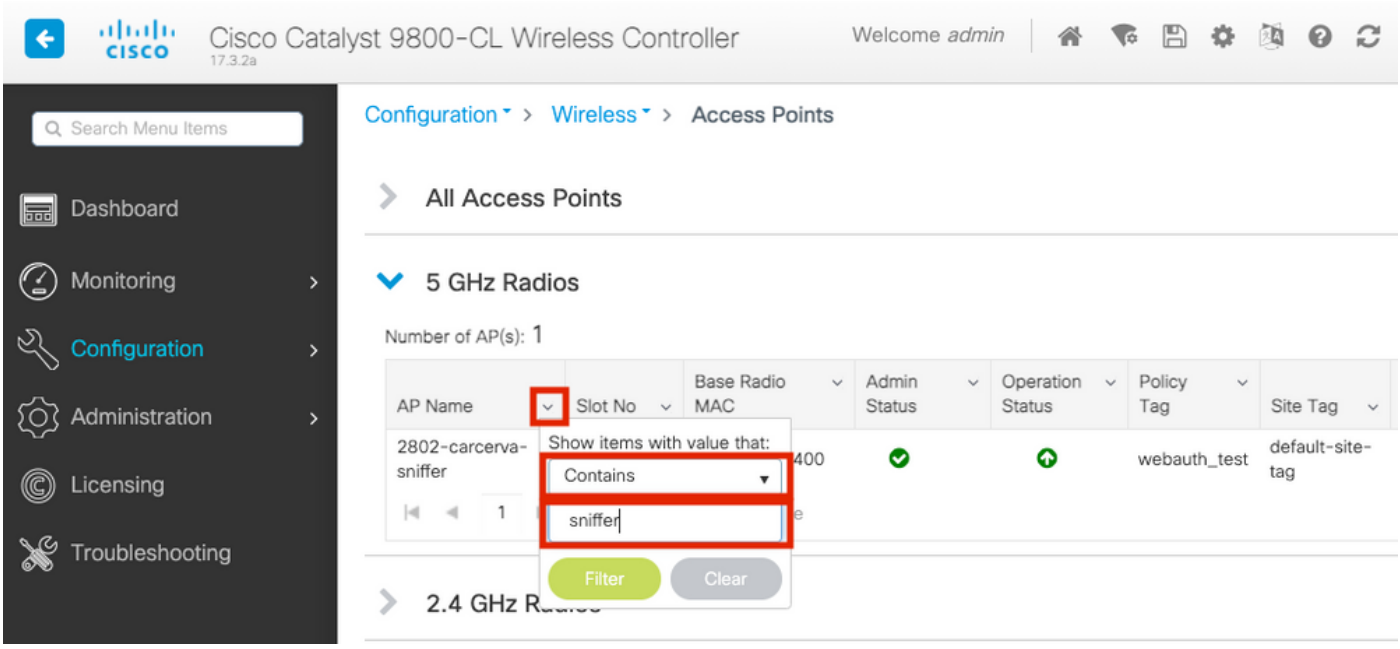
تكوين نقطة وصول لمسح قناة عبر واجهة المستخدم الرسومية

الخطوة 1. في واجهة المستخدم الرسومية WLC طراز 9800، انتقل إلى **التكوين > لاسلكي > نقاط الوصول**.

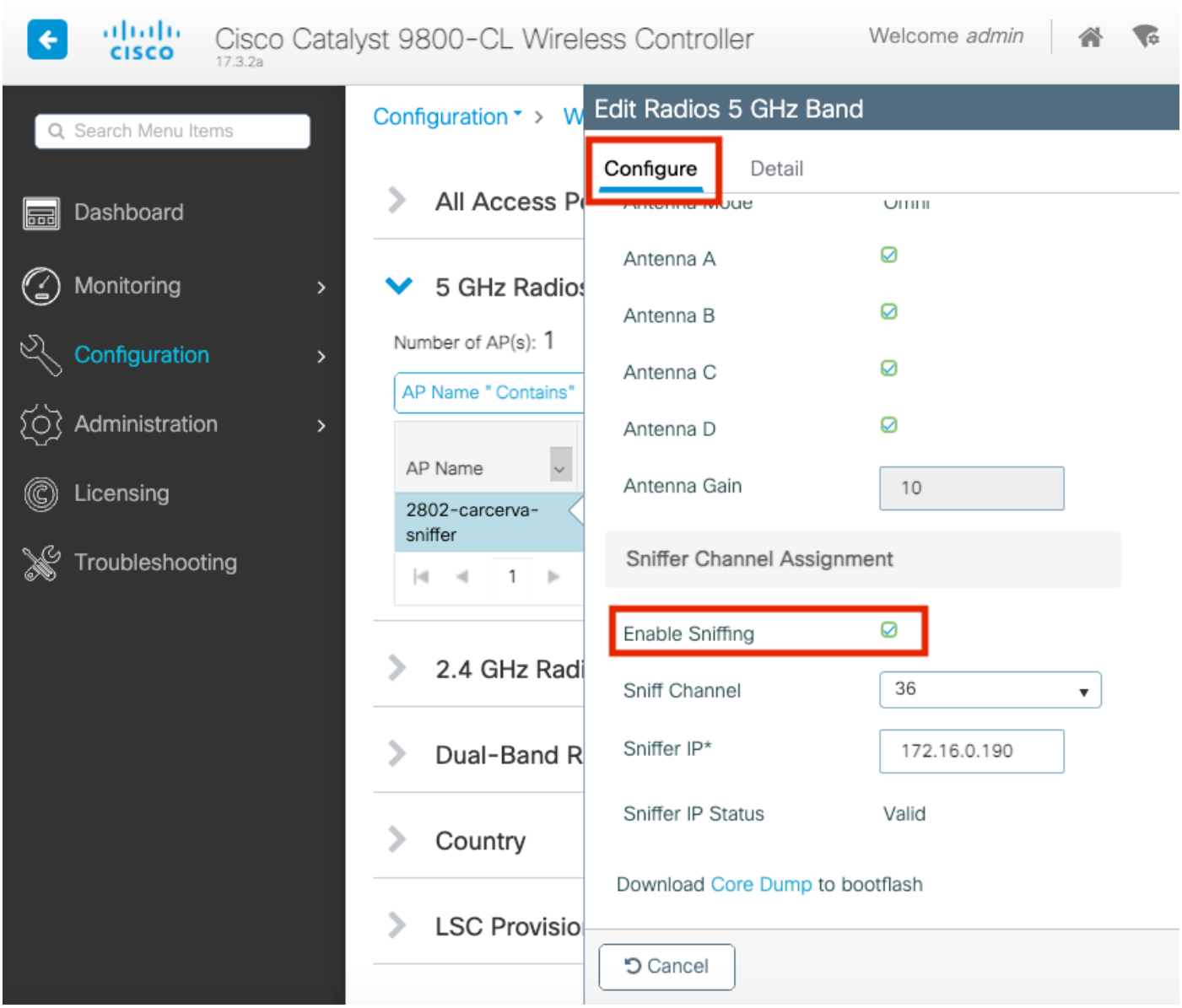
الخطوة 2. في صفحة **نقاط الوصول**، قم بعرض قائمة **أجهزة الراديو 5 جيجاهرتز** أو **أجهزة الراديو 2.4 جيجاهرتز**. يعتمد ذلك على القناة التي ترغب في المسح الضوئي، كما هو موضح في الصورة.



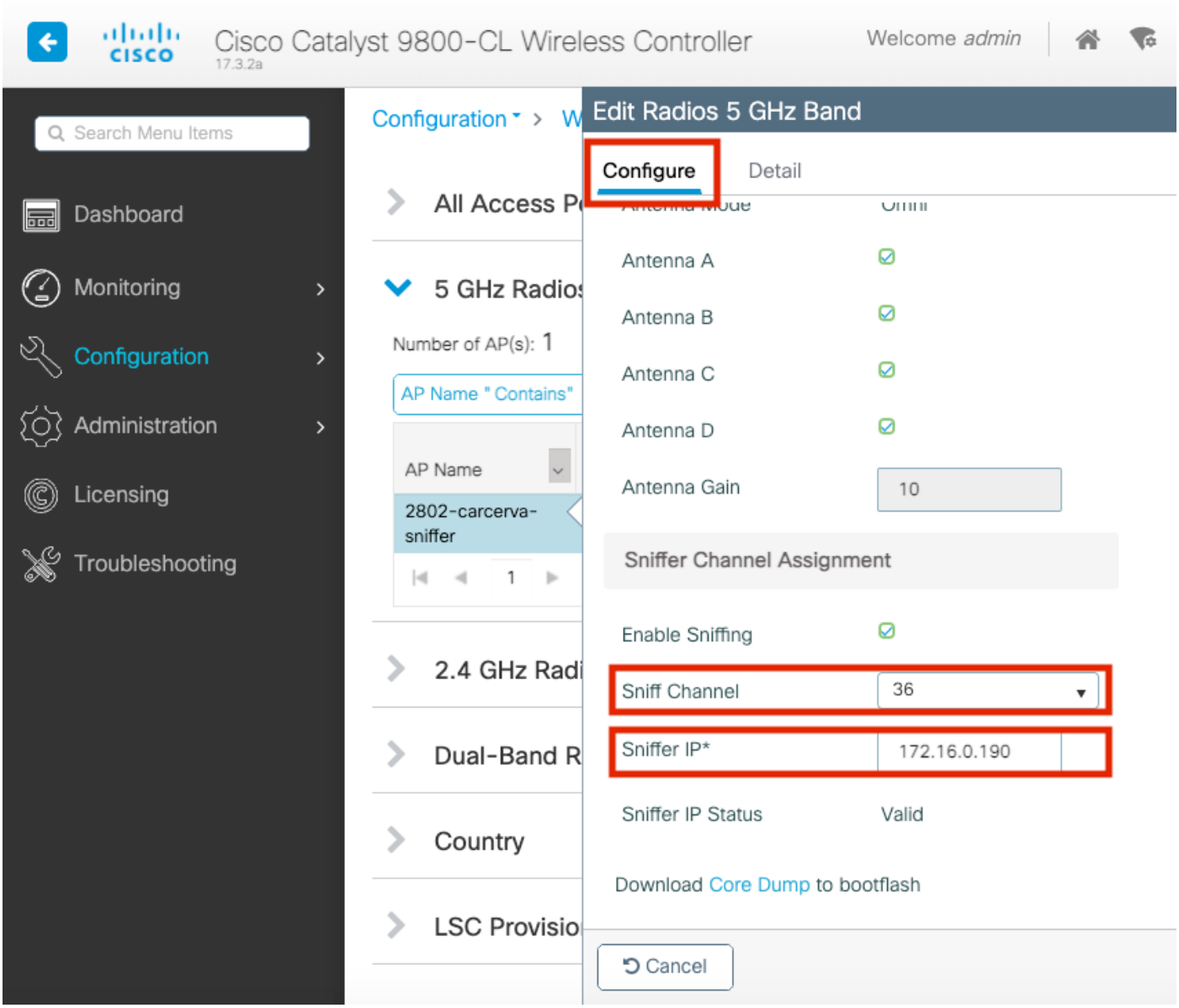
الخطوة 2. ابحث في نقطة الوصول. انقر على زر **السهم لأسفل** لعرض أداة البحث، وحدد **Contains** من القائمة المنسدلة، واكتب **اسم نقطة الوصول**، كما هو موضح في الصورة.



الخطوة 3. حدد نقطة الوصول وحدد خانة الاختيار **enable sniffer** تحت **ال configure**>sniffer قناة تعيين، كما هو موضح في الصورة.

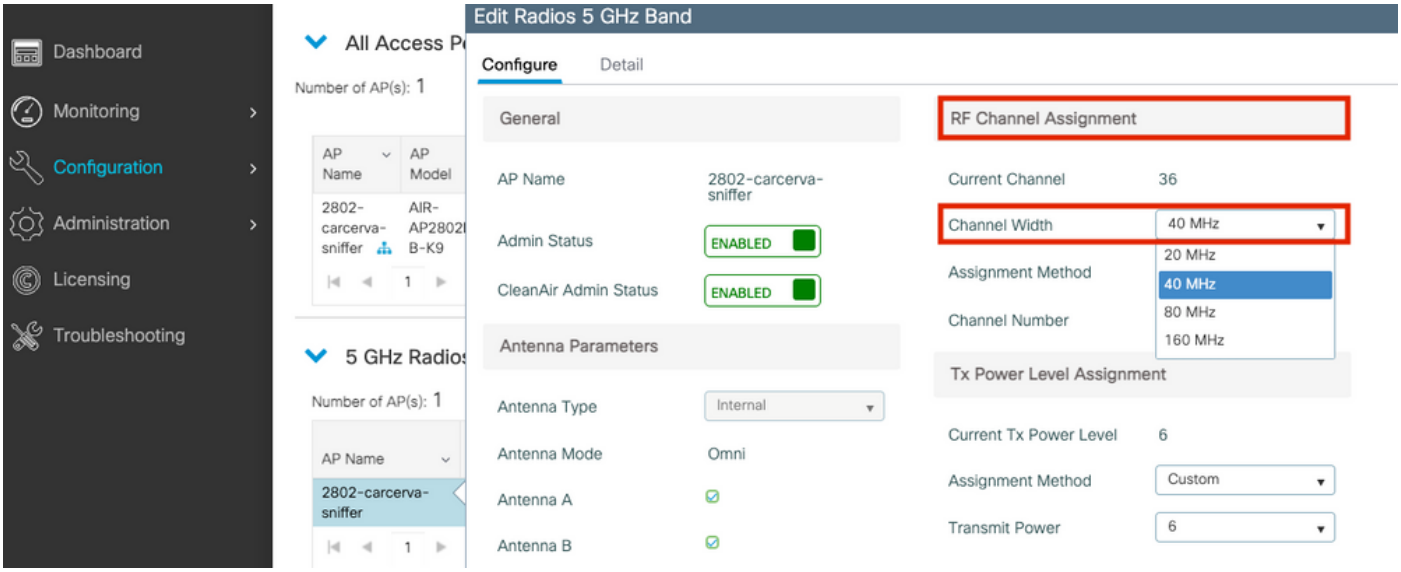


الخطوة 4. حدد القناة من القائمة المنسدلة **قناة** Sniff واكتب **عنوان IP لـ Sniffer** (عنوان IP للخادم مع Wireshark)، كما هو موضح في الصورة.



الخطوة 5. حدد **عرض القناة** الذي يستخدمه الجهاز المستهدف ونقطة الوصول عند التوصيل.

انتقل إلى **تكوين >تعيين قناة التردد اللاسلكي** لتكوين هذا، كما هو موضح في الصورة.



تكوين نقطة الوصول لمسح قناة عبر CLI (واجهة سطر الأوامر)

الخطوة 1. مكنت القناة sniff على ال ap. شغل هذا أمر:

```
carcerva-9k-upg#ap name <ap-name> sniff {dot11a for 5GHz | dot11bfor 2.4GHz | dual-band}
```

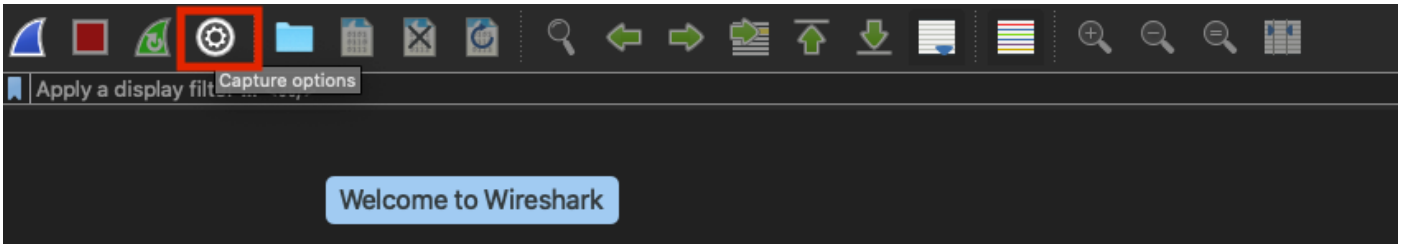
مثال:

```
carcerva-9k-upg#ap name 2802-carcerva-sniffer sniff dot11a 36 172.16.0.190
```

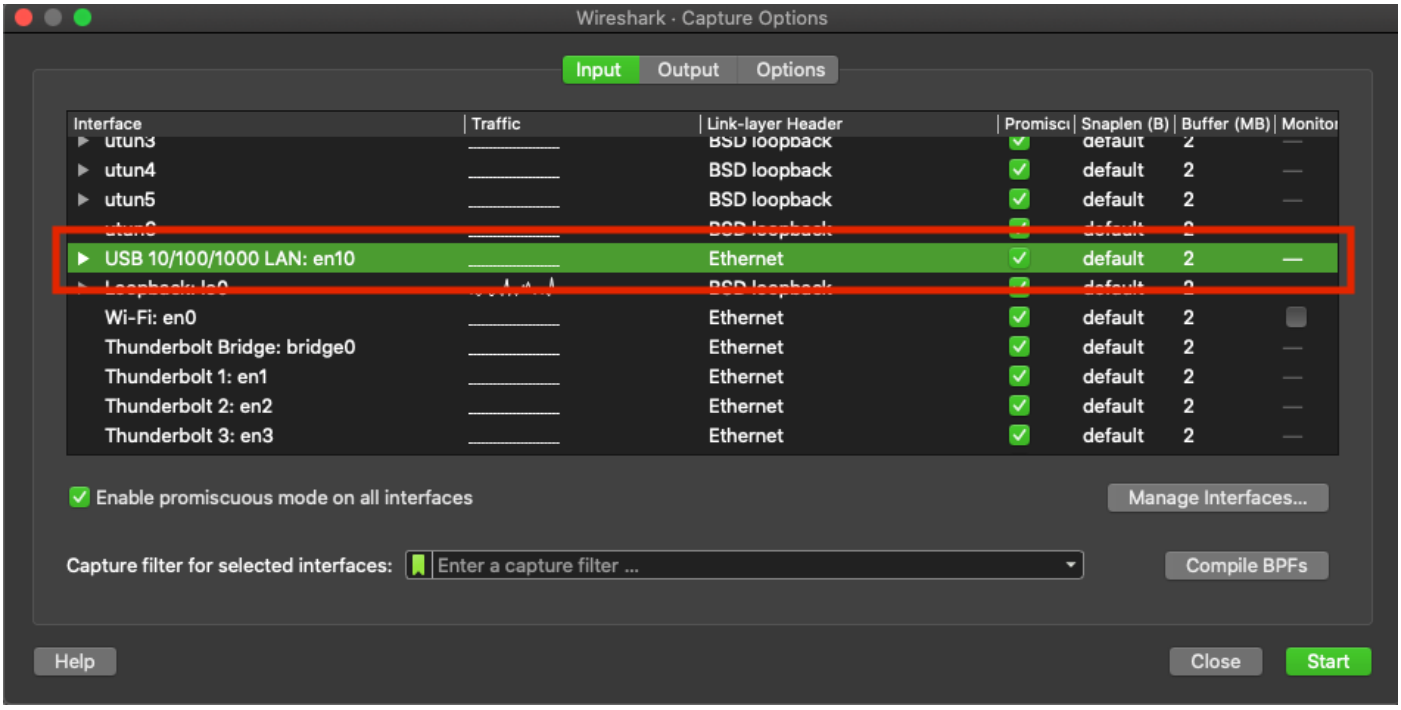
تكوين Wireshark لجمع التقاط الحزمة

الخطوة 1. إطلاق Wireshark.

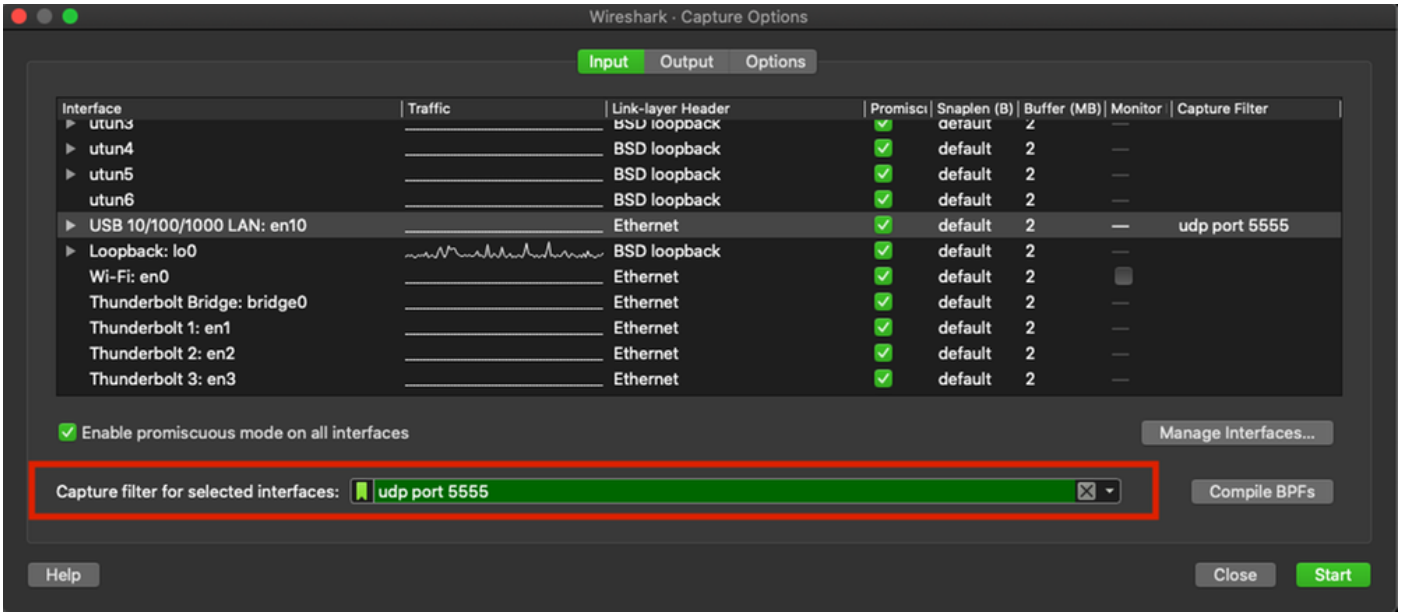
الخطوة 2. حدد أيقونة قائمة **خيارات الالتقاط** من Wireshark، كما هو موضح في الصورة.



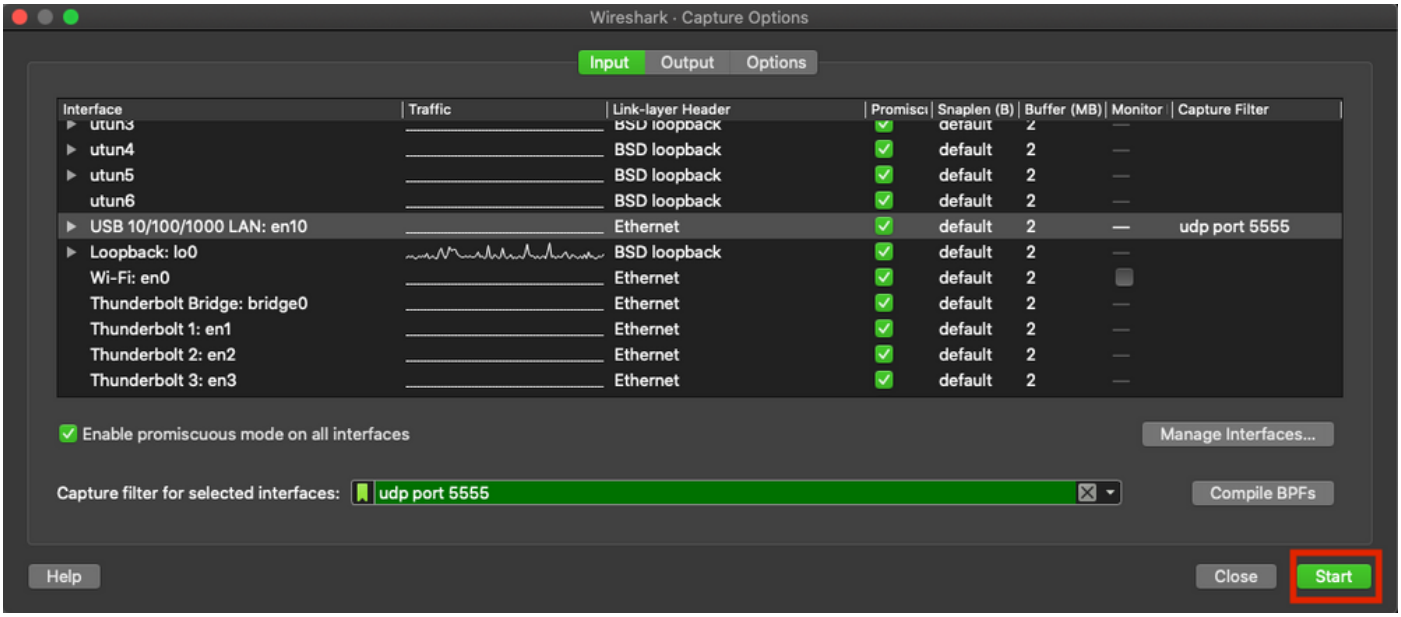
الخطوة 3. يعرض هذا الإجراء نافذة منبثقة. حدد الواجهة السلكية من القائمة كمصدر للالتقاط، كما هو موضح في الصورة.



الخطوة 4. تحت **مرشح الالتقاط للواجهات المحددة:** مربع الحقل، اكتب **udp port 555**، كما هو موضح في الصورة.



الخطوة 5. انقر على **بدء**، كما هو موضح في الصورة.

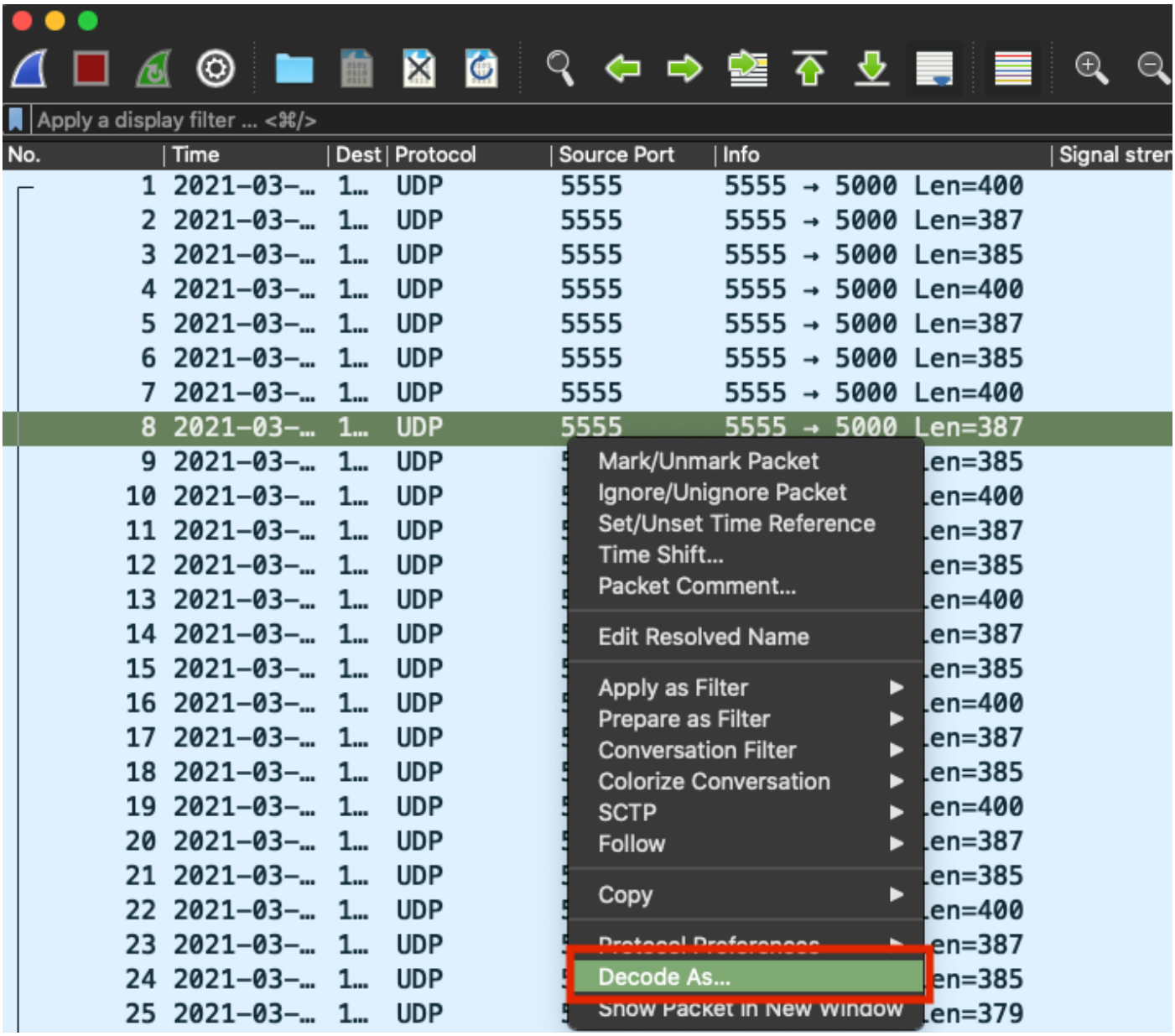


الخطوة 6. انتظر حتى يقوم Wireshark بجمع المعلومات المطلوبة وحدد زر **إيقاف** من Wireshark، كما هو موضح في الصورة.

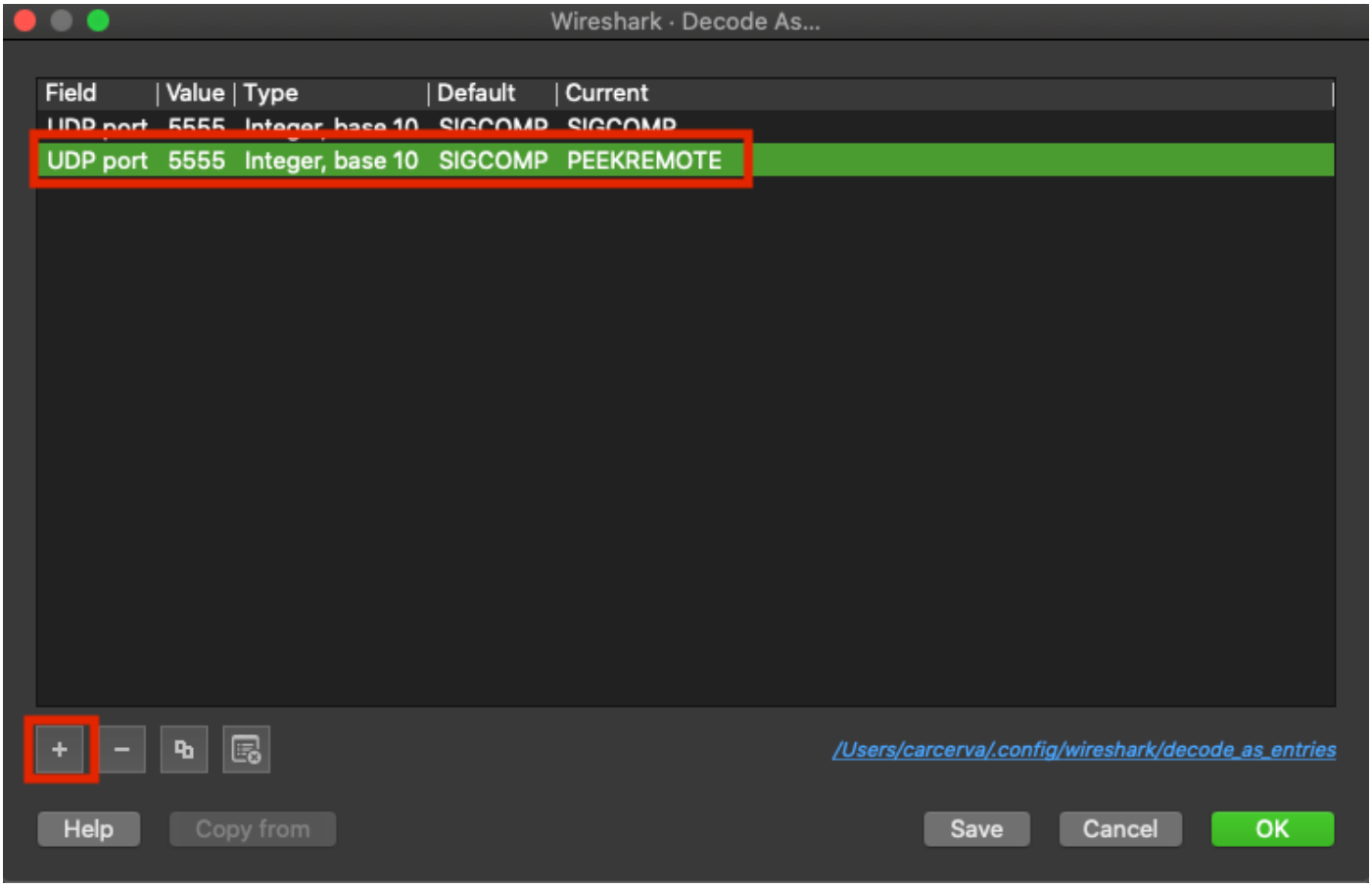
تلميح: إذا كانت الشبكة المحلية اللاسلكية (WLAN) تستخدم التشفير مثل المفتاح المشترك مسبقا (PSK)، فتأكد من أن المالتقاط يصيد مصافحة الاتصال الرباعية الإتجاه بين نقطة الوصول والعميل المطلوب. ويمكن القيام بذلك إذا بدأ تشغيل OTA PCAP قبل اقتران الجهاز بالشبكة المحلية اللاسلكية (WLAN) أو إذا كان العميل غير مصدق عليه وأعيد مصادقته أثناء تشغيل المالتقاط.

الخطوة 7. الى يقوم Wireshark بفك ترميز الحزم تلقائيا. من أجل فك ترميز الحزم، حدد سطر من المالتقاط، أستخدم النقر بزر الماوس الأيمن لعرض الخيارات، وحدد **فك الترميز كـ..**، كما هو

موضح في الصورة.



الخطوة 8. تظهر نافذة منبثقة. حدد زر الإضافة وقم بإضافة مدخل جديد، حدد هذه الخيارات: PEEKREMOTE من المنفذ UDP من الحقل، 5555 من القيمة، و SIGCOMP من الافتراضي، كما هو موضح في الصورة.



الخطوة 9. وانقر فوق **OK**. يتم فك ترميز الحزم وتكون جاهزة لبدء التحليل.

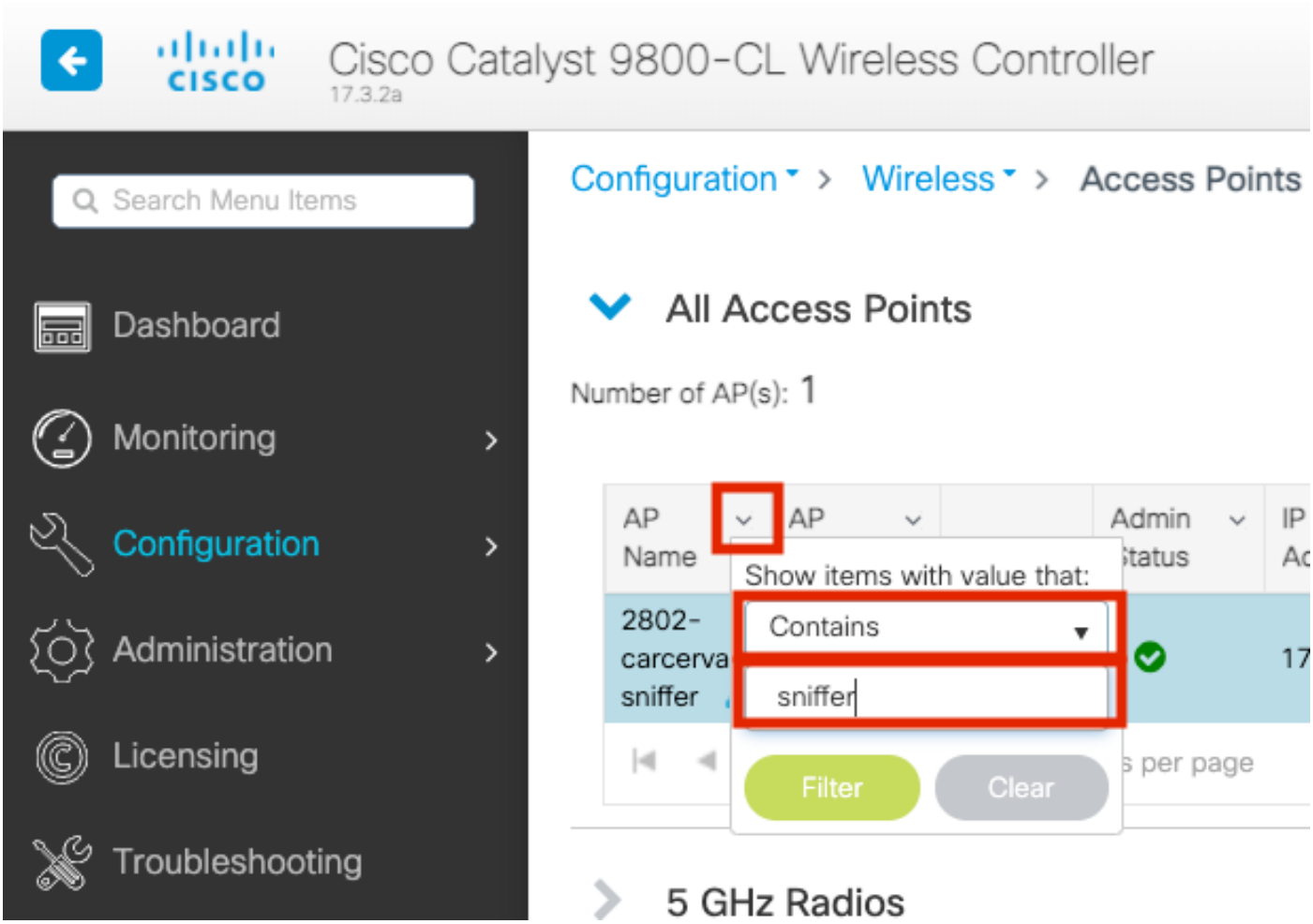
التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

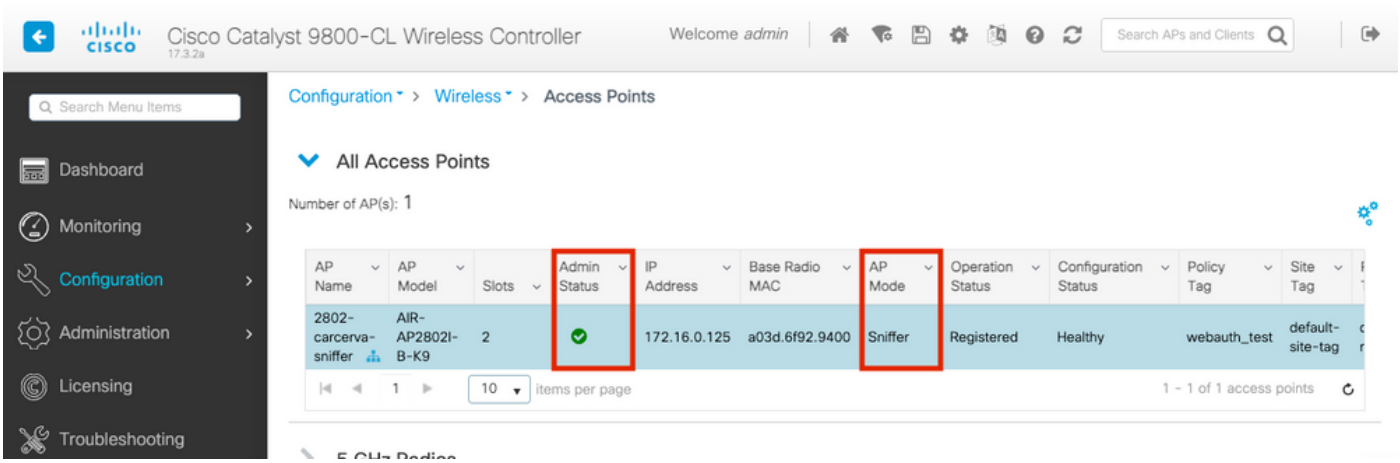
in order to أكدت ال ap في sniffer أسلوب من ال 9800 gui:

الخطوة 1. في واجهة المستخدم الرسومية (GUI) لبرنامج 9800 WLC، انتقل إلى **التكوين > السلكي > نقاط الوصول > جميع نقاط الوصول**.

الخطوة 2. ابحث في نقطة الوصول. انقر زر السهم لأسفل لعرض أداة البحث، وحدد **إحتواء** من القائمة المنسدلة، واكتب اسم نقطة الوصول، كما هو موضح في الصورة.



الخطوة 3. دقق **Admin** وضع مع **الـ checkmark in green** والـ **ap** أسلوب هو **sniffer**، كما هو موضح في الصورة.



in order to أكدت الـ ap في sniffer أسلوب من الـ 9800 CLI. قم بتشغيل هذه الأوامر:

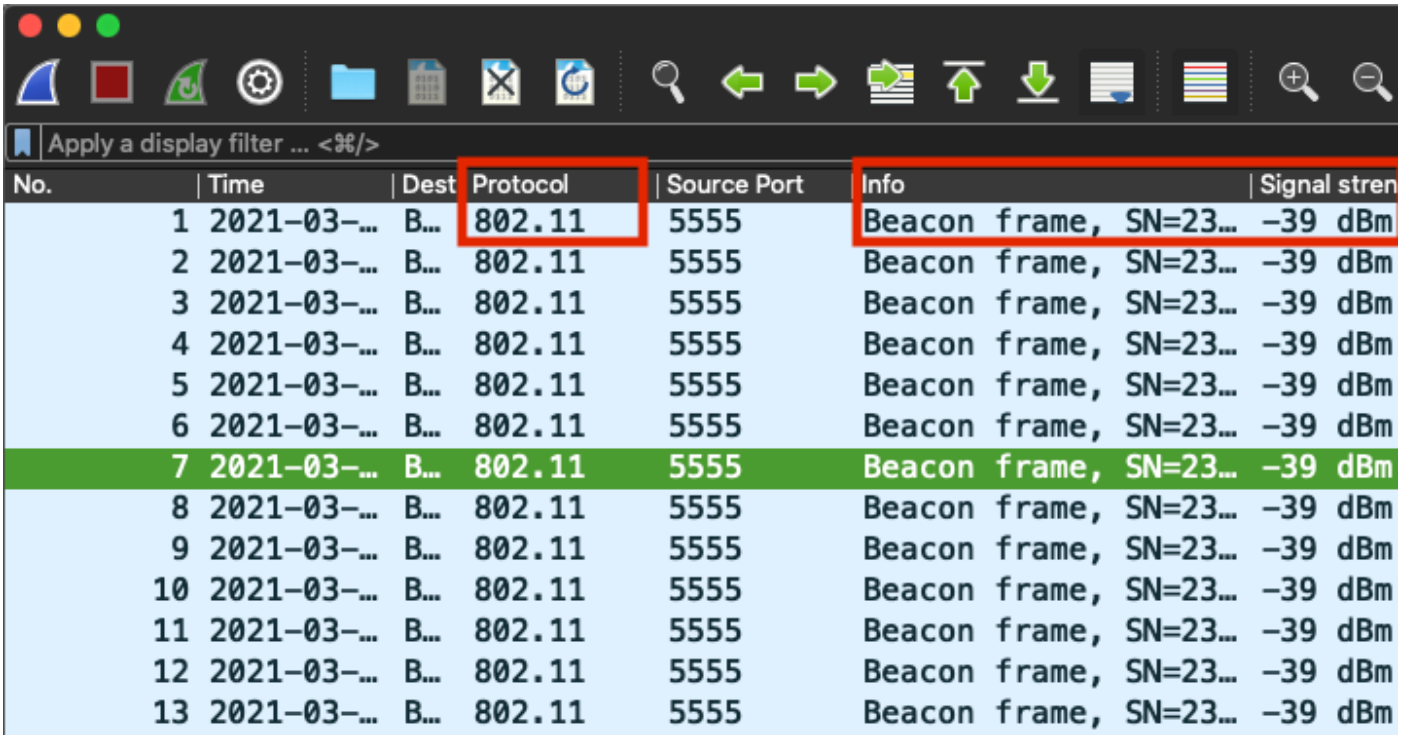
```
carcerva-9k-upg#show ap name 2802-carcerva-sniffer config general | i Administrative
Administrative State : Enabled

carcerva-9k-upg#show ap name 2802-carcerva-sniffer config general | i AP Mode
AP Mode : Sniffer

carcerva-9k-upg#show ap name 2802-carcerva-sniffer config dot11 5Ghz | i Sniff
AP Mode : Sniffer
Sniffing : Enabled
Sniff Channel : 36
```

```
Sniffer IP : 172.16.0.190
Sniffer IP Status : Valid
Radio Mode : Sniffer
```

لتأكيد فك ترميز الحزم على Wireshark. يتغير البروتوكول من **UDP** إلى **802.11** وهناك ترى **إطارات Beacon**، كما هو موضح في الصورة.



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكن إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

المشكلة: لا يتلقى Wireshark أي بيانات من نقطة الوصول.

الحل: يجب أن يكون خادم Wireshark قابلا للوصول إليه بواسطة واجهة الإدارة اللاسلكية (WMI). الرجاء تأكيد إمكانية الوصول بين خادم Wireshark و WMI من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

معلومات ذات صلة

- [دليل تكوين برنامج Cisco Catalyst 9800 Series Wireless Controller Software، Cisco IOS XE Amsterdam، الإصدار 17.3.x - الفصل: وضع Sniffer]
- [أساسيات مراقبة 802.11 اللاسلكية]
- [الدعم التقني والمستندات - Cisco Systems]

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).