Configuration du point d'accès en mode renifleur sur Catalyst 9800 WC

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Mises en garde
- Considérations conceptuelles
- Configurations
  - Configuration du point d'accès en mode renifleur via l'interface utilisateur graphique
    - Configuration du point d'accès en mode renifleur via CLI
  - Configuration du point d'accès pour analyser le canal souhaité via l'interface utilisateur graphique
  - Configurer le point d'accès pour analyser un canal via CLI
  - Configurer Wireshark pour collecter la capture de paquets
  - Autre point d'accès - Sniffer APs Switchport
  - Autre point de dérivation - EPC dans le 9800
- Vérifier
- Dépannage
- Informations connexes

Introduction

Ce document décrit comment configurer un point d'accès (AP) en mode renifleur sur un contrôleur sans fil de la gamme Catalyst 9800 (WLC 9800).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration WLC 9800

- Connaissances de base de la norme 802.11

Composants utilisés

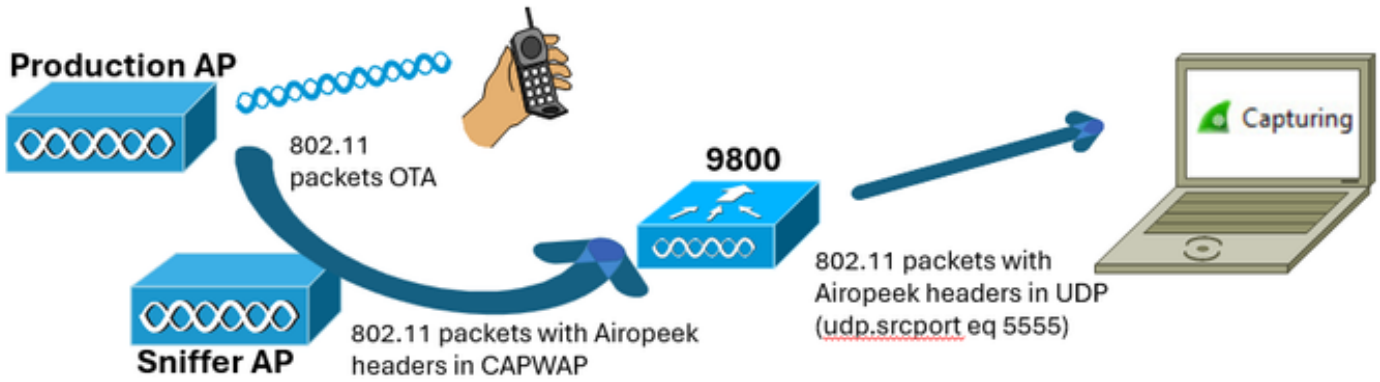
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- AP2802, AP C9130AXI
- Wireshark 3.4.4 ou version ultérieure
- 9800 WLC Cisco IOS® XE versions 17.3.2a et 26.1.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Un point d'accès en mode renifleur est un point d'accès relié à un contrôleur Catalyst 9800, dont la radio est dédiée à la réception de tous les paquets 802.11 sur un canal donné, et à la transmission de ces paquets avec un en-tête AiroPeek, dans CAPWAP, au 9800. Le 9800 transfère ces paquets analysés dans UDP (port source 5555, port de destination 5000) vers un périphérique de destination d'analyse IPv4, tel qu'un ordinateur exécutant Wireshark en mode proche. Ces paquets peuvent ensuite être analysés hors ligne.



Le point d'accès en mode renifleur peut être configuré via l'interface graphique utilisateur (GUI) ou l'interface de ligne de commande (CLI). Ce document couvre également la collecte d'une capture de paquets (PCAP) sur l'air (OTA) avec le point d'accès de l'analyseur pour dépanner et analyser

les comportements sans fil.

Mises en garde

N'utilisez pas la fonction AP Sniffer Mode si le Catalyst 9800 est connecté à l'infrastructure axée sur les applications (ACI) de Cisco avec apprentissage par défaut des terminaux. Le 9800 transmet ses paquets capturés 802.11 encapsulés UDP provenant de l'adresse IP de sortie des 9800, mais avec l'adresse MAC source définie sur l'adresse MAC de l'émetteur-récepteur de l'analyseur, avec un quartet d'ordre bas défini sur 0xF. Cela pose des problèmes car l'ACI voit la même adresse IP provenant de plusieurs adresses MAC ; voir l'ID de bogue Cisco CSCwa45713.

Considérations conceptuelles

Éléments à prendre en compte :

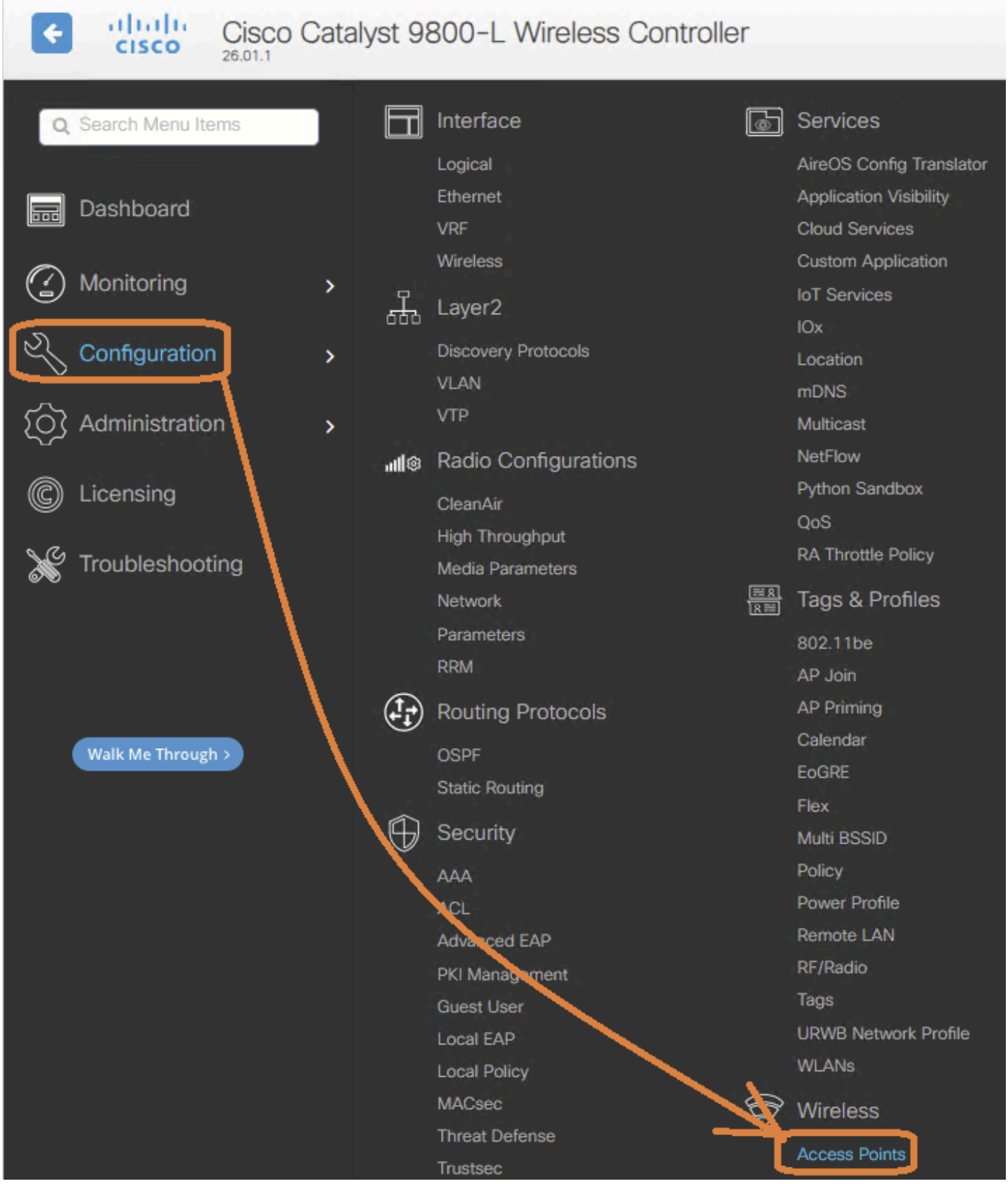
- Il est recommandé d'avoir le point d'accès du renifleur à proximité du périphérique cible et du point d'accès auquel le périphérique est connecté. Si le point d'accès du renifleur est éloigné des émetteurs, il ne peut pas démoduler la plupart des trames de données.
- Le point d'accès analyseur peut prendre en charge l'ensemble de modulation utilisé par les dispositifs d'émission et de réception en cours de test. Par exemple, si les périphériques testés utilisent 802.11ax, utilisez un point d'accès 802.11ax ou 802.11be pour détecter, et non un point d'accès 802.11ac tel qu'un point d'accès AP2802.

Remarque : Le point d'accès en mode renifleur n'est pas pris en charge sur le 9800-CL déployé sur un cloud public.

Configurations

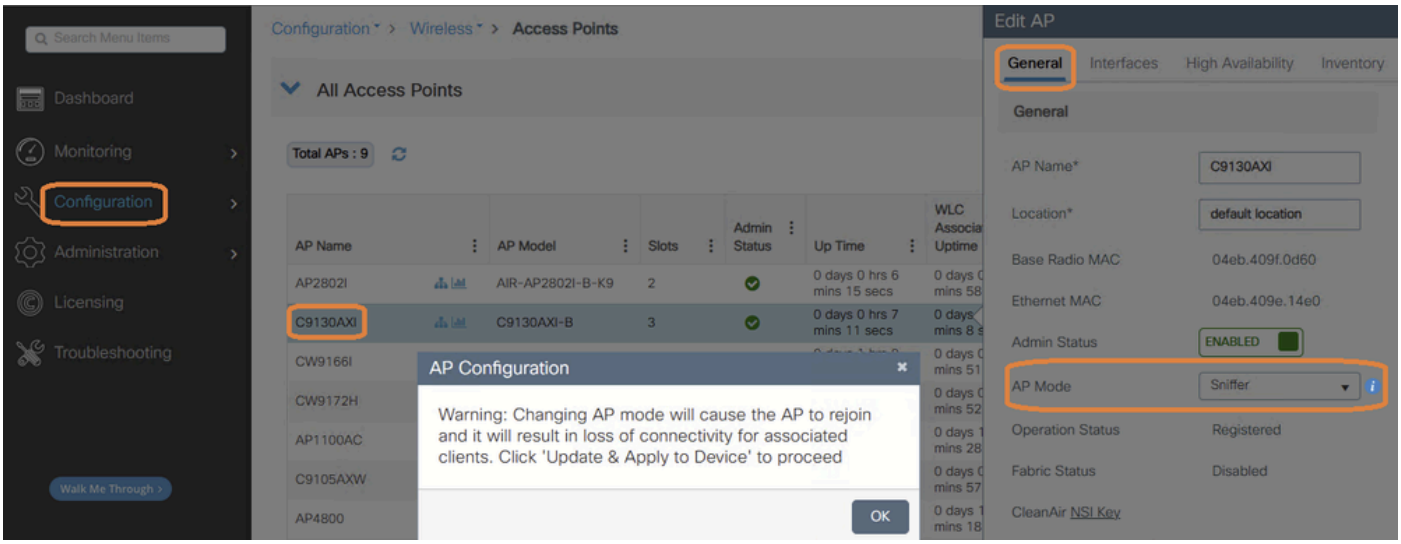
Configuration du point d'accès en mode renifleur via l'interface utilisateur graphique

1. Sur l'interface graphique utilisateur du WLC 9800, accédez à Configuration > Wireless > Access Points > All Access Points, comme indiqué dans l'image :



---

2. Sélectionnez le point d'accès à utiliser en mode renifleur. Dans l'onglet General, vérifiez que l'état Admin est ENABLED et définissez le mode AP sur Sniffer. Cliquez sur OK dans l'avertissement contextuel, puis sur Mettre à jour et appliquer au périphérique.



---

3. Le point d'accès se sépare puis se rejoint après quelques minutes.

Configuration du point d'accès en mode renifleur via CLI

1. Identifiez le point d'accès que vous souhaitez utiliser comme mode renifleur.

---

2. Configurez le point d’accès en mode renifleur.

```
<#root>
9800-L#

ap name C9130AXI mode sniffer
```

---

3. Le point d'accès se sépare puis se rejoint après quelques minutes.

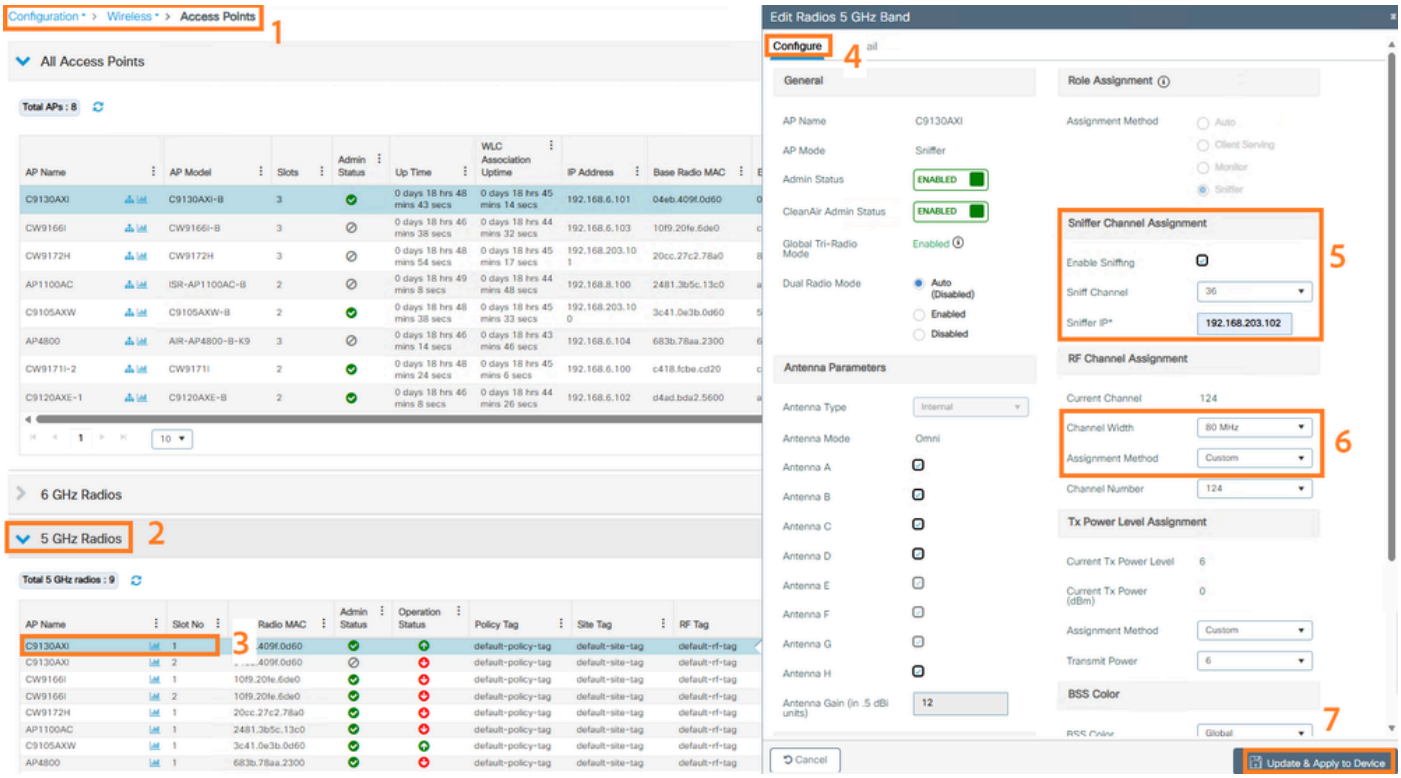
Configuration du point d'accès pour analyser le canal souhaité via l'interface utilisateur graphique

1. Dans Configuration > Wireless > Access Points (1), faites défiler la page vers le bas pour rechercher l'émetteur-récepteur de l'analyseur dans la bande souhaitée. Dans cet exemple, sous

5 GHz Radios (2), AP C9130AXI's Slot 1 radio (3). Configurez cette radio (4) pour activer l'analyse (5), en attribuant le canal souhaité à l'analyse et en entrant l'adresse IP du dispositif d'analyse.

---

2. Sous RF Channel Assignment (6), définissez la méthode d'affectation sur Custom, et définissez la largeur de canal souhaitée dans la liste déroulante. Cliquez sur Update and Apply to Device (7).



Configurer le point d'accès pour analyser un canal via CLI

1. Configurez le canal pour renifler sur le point d'accès et activez cette commande :

<#root>

9800-L#

ap name

<ap-name>

dot11 sniff

{24ghz | 5ghz | 6ghz}

slot

<slot> <channel> <Sniffer-IP-address>

Exemple :

<#root>

9800-L#

ap name C9130AXI dot11 5ghz slot 1 sniff 36 192.168.203.102

---

2. Configurez la largeur du canal :

<#root>

9800-L#

ap name

<ap-name>

dot11

{24ghz | 5ghz | 6ghz}

slot

<slot>

channel width

<width in MHz>

Exemple :

<#root>

9800-L#

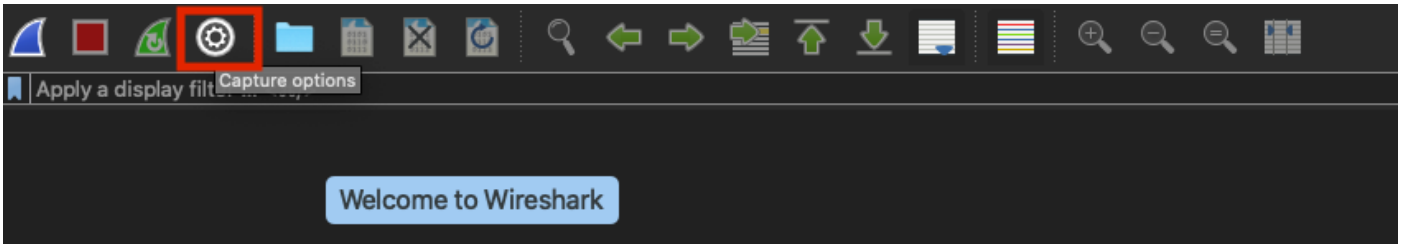
ap name C9130AXI dot11 5ghz slot 1 channel width 40

À ce stade, le point d'accès de l'analyseur capture les paquets de transmission et les envoie en CAPWAP au 9800. Le 9800 transmet ensuite les paquets détectés au périphérique de capture.

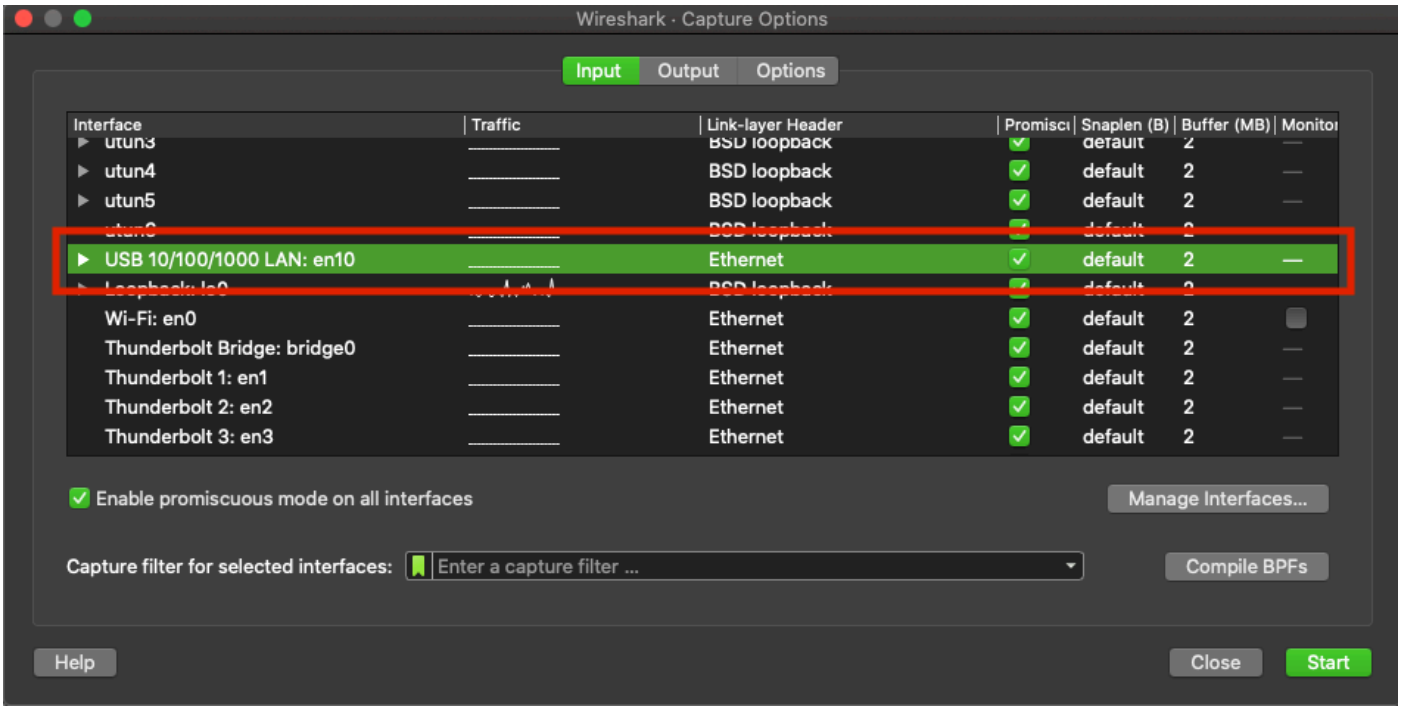
Configurer Wireshark pour collecter la capture de paquets

1. Lancez Wireshark.

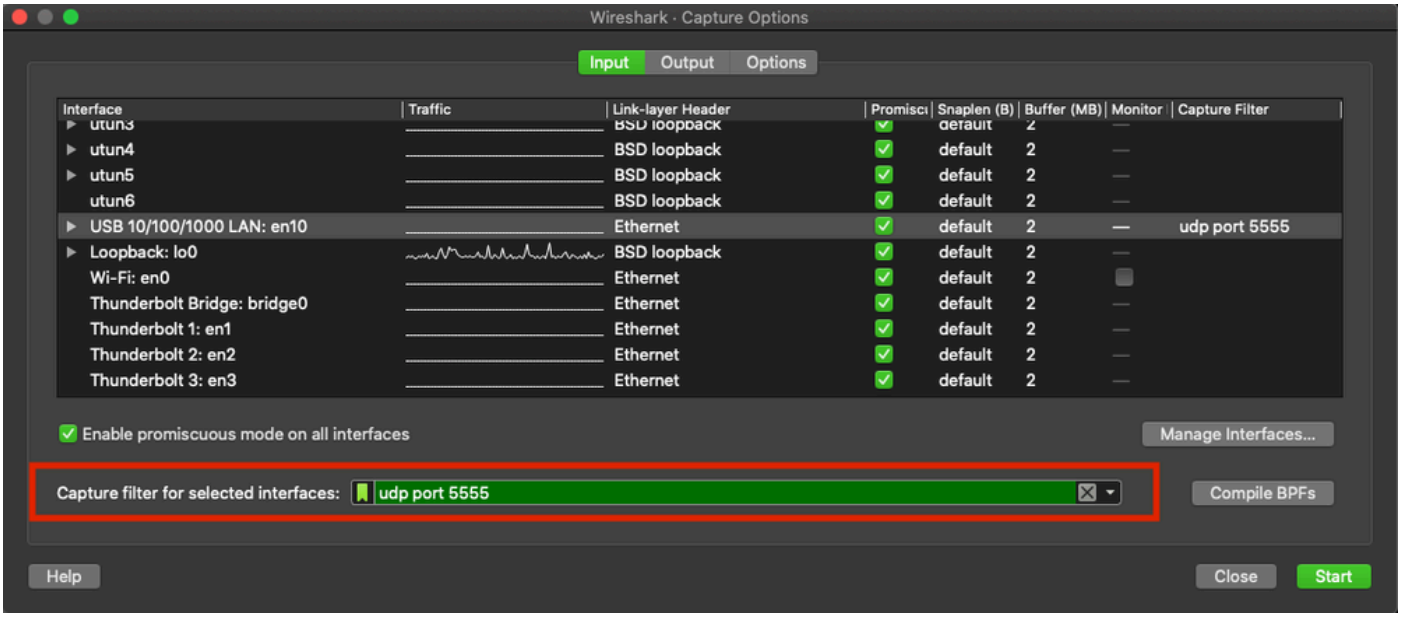
2. Sélectionnez l'icône du menu Options de capture dans Wireshark :



3. Cette action affiche une fenêtre contextuelle. Sélectionnez l'interface filaire dans la liste comme source de la capture. Assurez-vous que l'option Promiscuous est cochée.

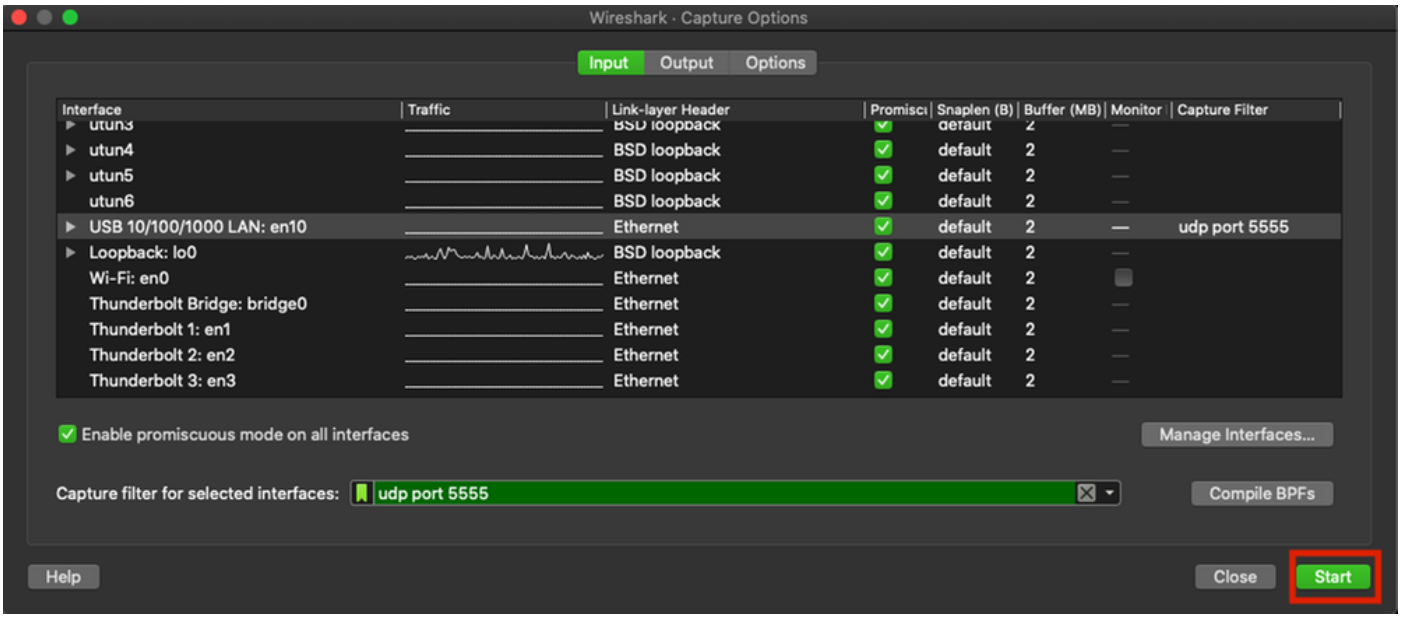


4. Dans la zone Filtre de capture pour les interfaces sélectionnées, tapez udp port 5555 comme indiqué dans l'image :



---

5. Cliquez sur Démarrer.



---

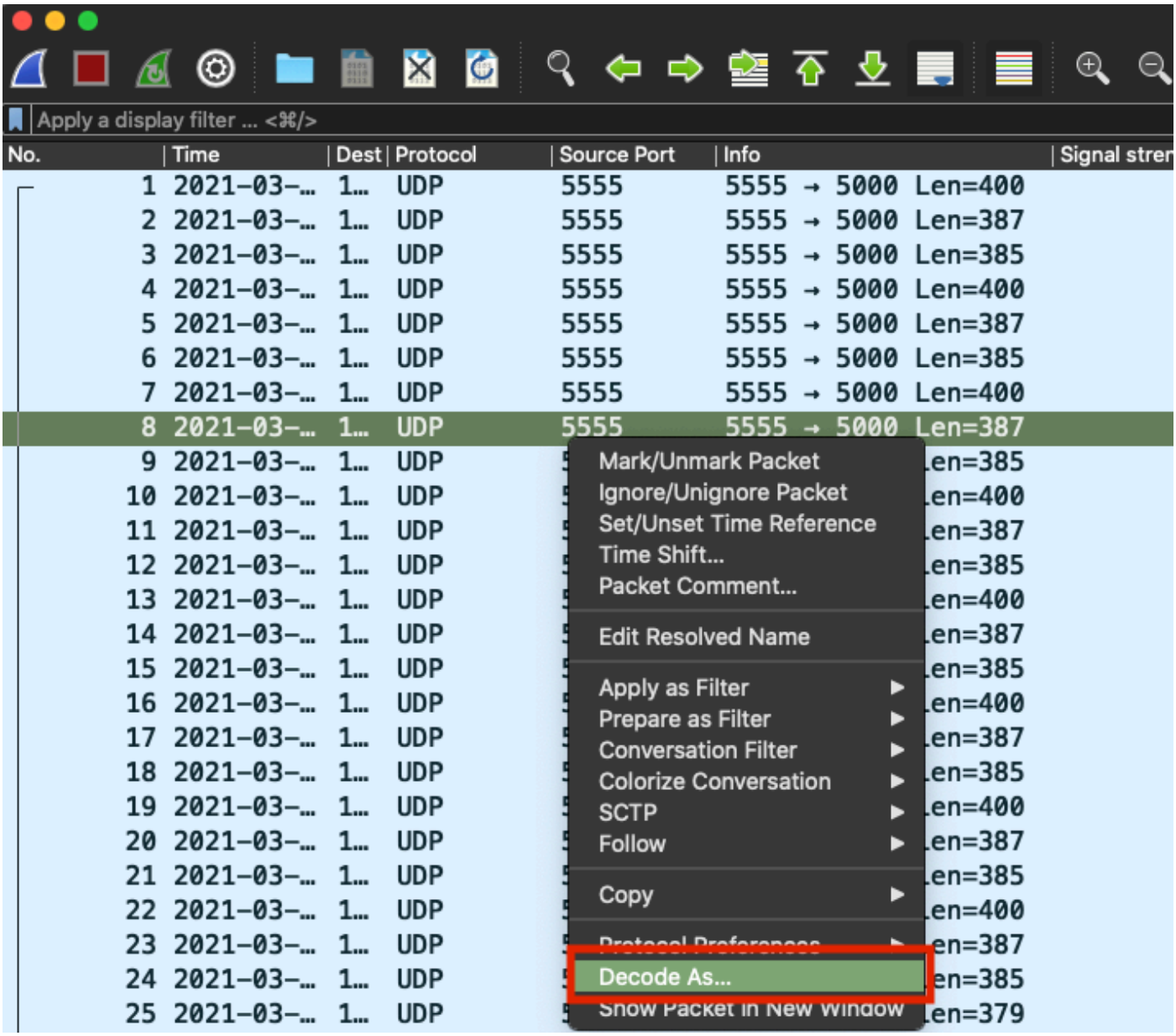
6. Attendez que Wireshark recueille les informations requises et sélectionnez le bouton Arrêter dans Wireshark.



Conseil : Si le WLAN utilise un cryptage tel que la clé pré-partagée (PSK), assurez-vous que la capture intercepte la connexion en quatre étapes entre le point d'accès et le client souhaité. Cela peut être effectué si le PCAP OTA démarre avant que le périphérique ne soit associé au WLAN ou si le client est désauthentifié et réauthentifié pendant l'exécution de la capture.

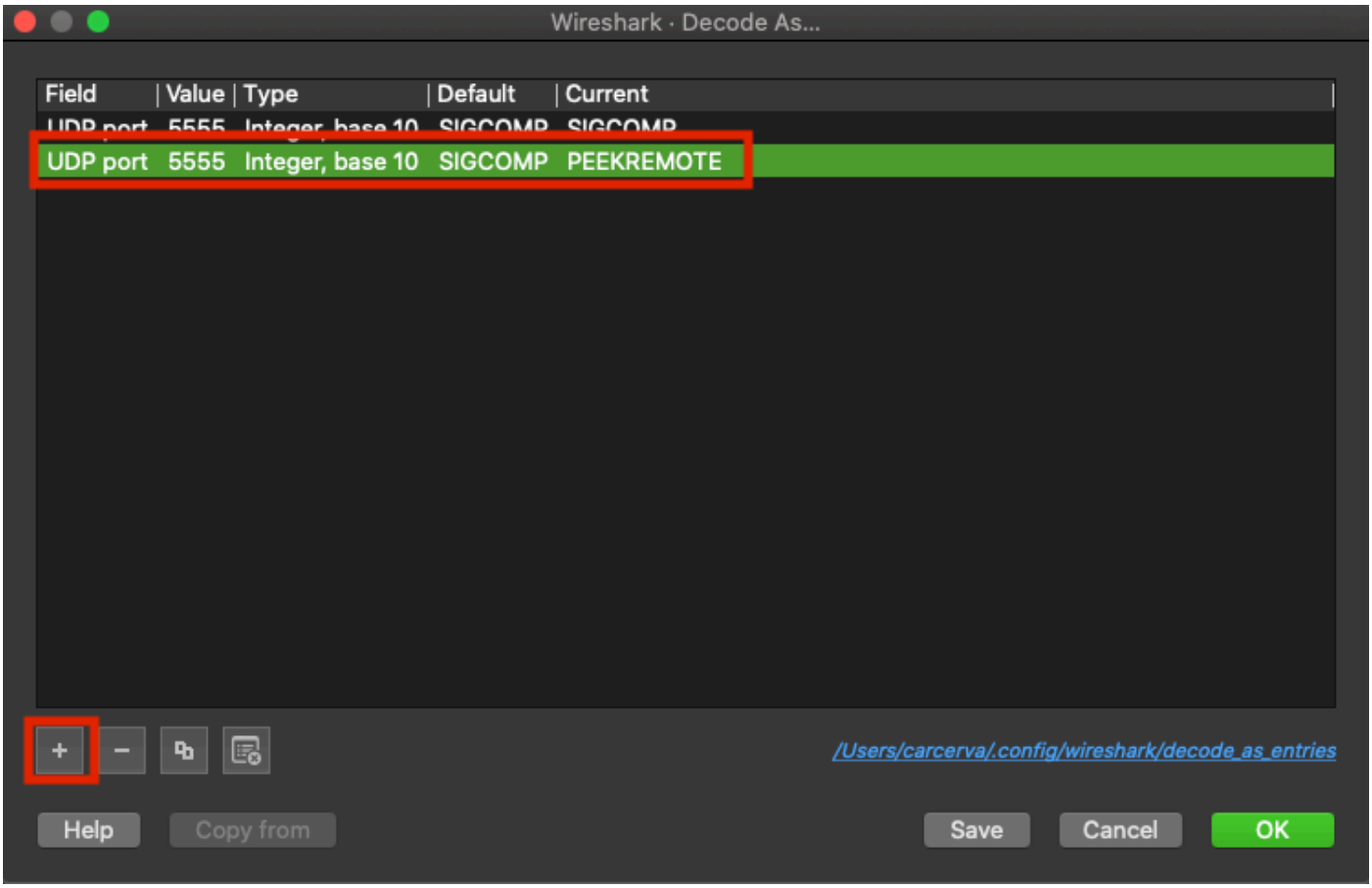
---

7. Wireshark ne décode pas automatiquement les paquets. Pour décoder les paquets, sélectionnez une ligne dans la capture, puis cliquez avec le bouton droit pour afficher les options et sélectionnez Décoder comme...



---

8. Une fenêtre contextuelle apparaît, sélectionnez le bouton Ajouter en cliquant sur le signe + et ajoutez une nouvelle entrée. Sélectionnez ces options : Port UDP de Field, 555 de Value, SIGCOMP de Default et PEEKREMOTE de Current.



---

9. Cliquez sur OK. Les paquets sont décodés et prêts à commencer l'analyse.

Autre point d'accès - Sniffer APs Switchport

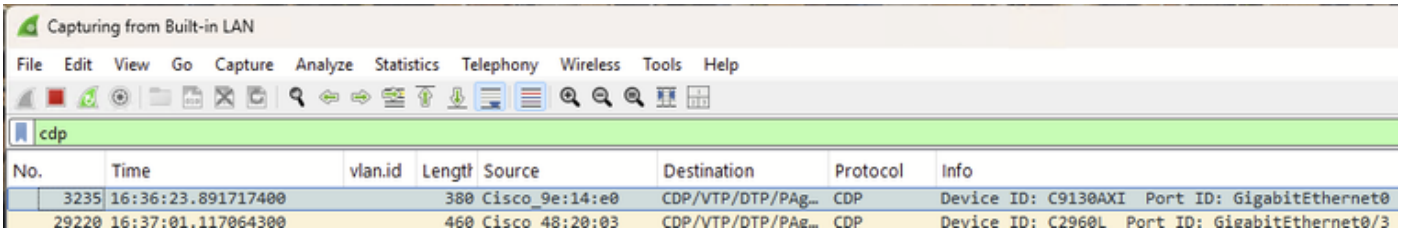
Au lieu de capturer les paquets détectés provenant du contrôleur, vous pouvez étendre le port de commutation des points d'accès Sniffer à un analyseur câblé. Cette commande capture les paquets 802.11 au format Airopeek encapsulés dans CAPWAP. Si la liaison CAPWAP entre le point d'accès et le 9800 est perdante, cela permet d'éviter la perte.

Sur le 9800, vous pouvez exécuter la commande show ap name <APNAME> cdp neighbors pour rechercher le nom de commutateur, l'adresse IP et le port de commutation des points d'accès. Câblez un analyseur de réseau local (tel qu'un PC ou un MacBook avec interface LAN) à un port de commutation libre sur le commutateur des points d'accès. Exécutez Wireshark et mettez-le en mode de proximité pour capturer tous les paquets reçus de ce port de commutateur, conformément aux instructions ci-dessus. Sur le commutateur, exécutez des commandes comme celles-ci, pour étendre les points d'accès :

```
switch(config)#monitor session 1 source interface Gi0/3
```

```
switch(config)#monitor session 1 destination interface Gi0/19
```

Où Gi0/3 est le port de commutation des AP analyseurs et GI0/19 est le port de commutation dans lequel l'analyseur de réseau local est détecté. Pour valider sur l'analyseur de réseau local qu'il collecte avec succès l'étendue à partir du port de commutation des AP, vous pouvez filtrer les paquets capturés sur cdp :



Autre point de dérivation - EPC dans le 9800

Une autre option consiste à capturer les paquets détectés via Embedded Packet Capture (EPC) dans le 9800. Cette méthode est pratique car elle ne nécessite pas de périphérique renifleur supplémentaire pour la capture.

---

1. Dans l'interface graphique utilisateur, accédez à Troubleshooting > Packet Capture.

---

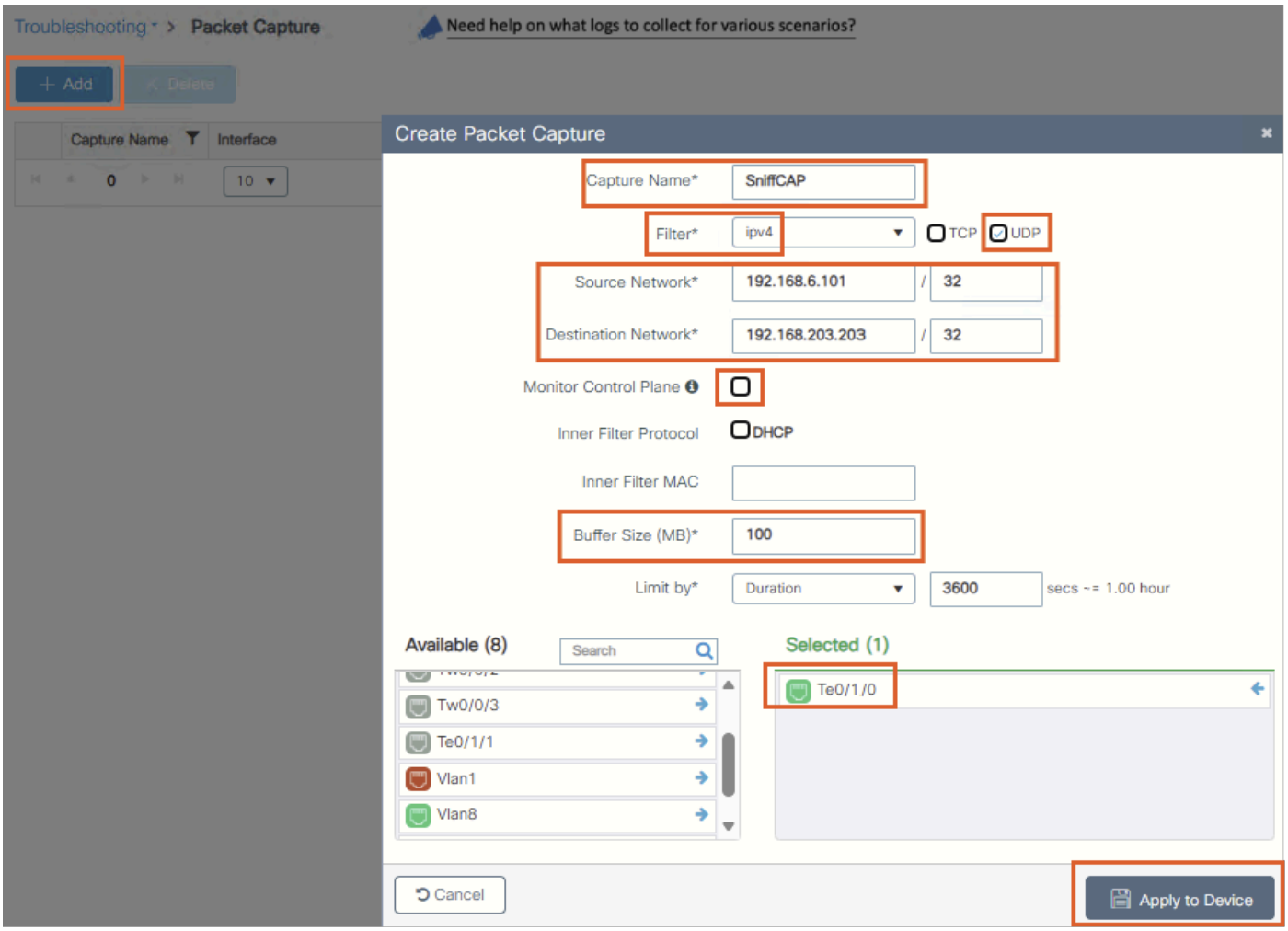
2. Ajoutez un point de capture en lui donnant un nom de capture.

---

3. Configurez un filtre IPv4, en faisant correspondre le protocole UDP avec la source, l'adresse IP du point d'accès et la destination, l'adresse WMI des années 9800. Décochez la case Monitor Control Plane.

---

4. Augmentez la taille de la mémoire tampon au maximum (100 Mo) et sélectionnez l'interface WMI et cliquez sur Apple to Device.



---

5. Ensuite, dans la liste Nom de la capture, cliquez sur Démarrer pour le point de capture que vous venez de créer. Lorsque l'événement qui vous intéresse est capturé, cliquez sur Stop, puis sur Export.

---

6. Vous pouvez exporter vers votre bureau, puis ouvrir le fichier dans Wireshark. Comme avec la méthode switchport span du point d'accès ci-dessus, la capture contient des trames 802.11 au format Aeropeek dans UDP (port source 5555) dans CAPWAP.

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement. Pour confirmer que le point d'accès est en mode Sniffer à partir de l'interface utilisateur graphique du 9800 :

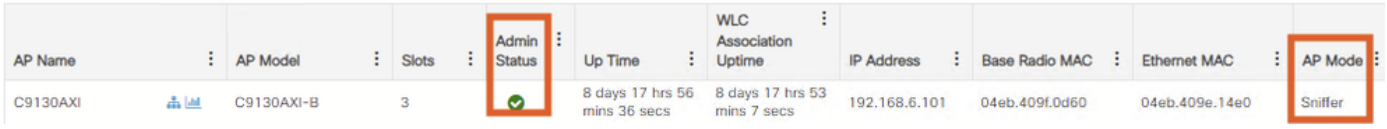
---

1. Dans l'interface graphique utilisateur du WLC 9800, accédez à Configuration > Wireless >

Access Points > All Access Points.

---

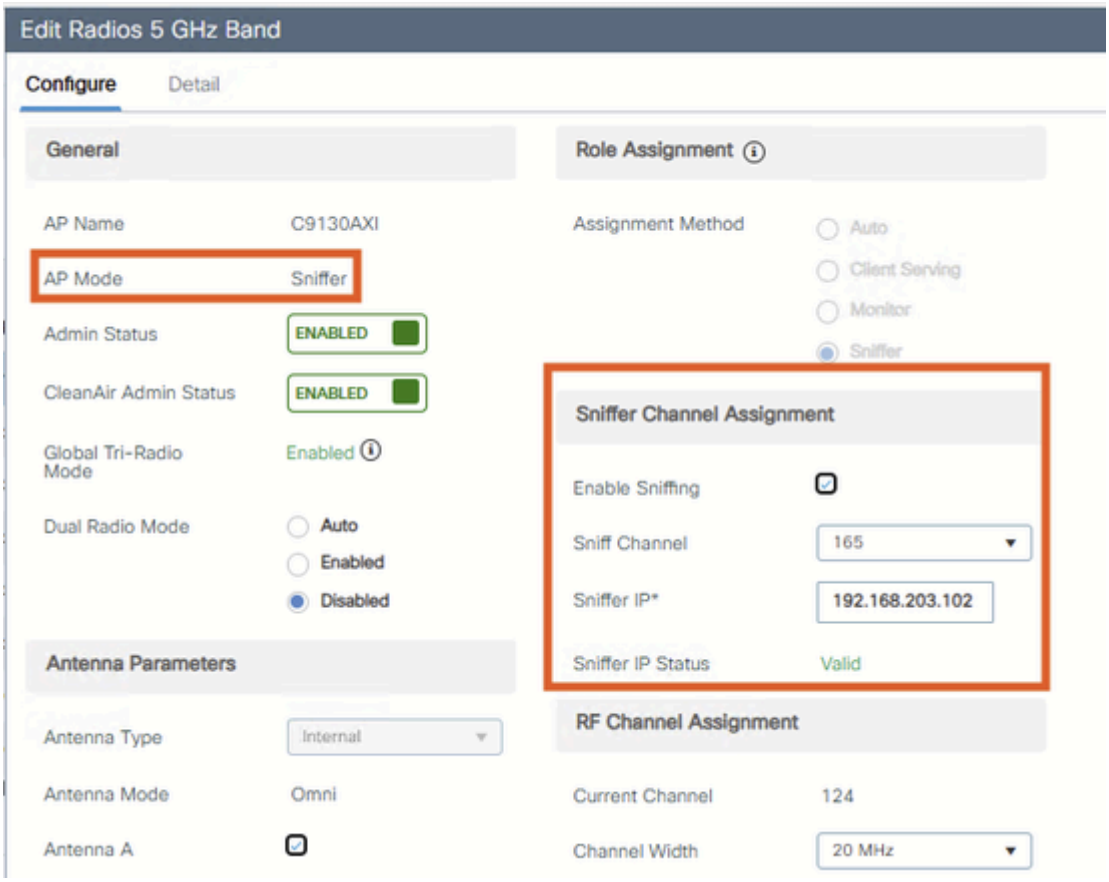
2. Trouvez l'AP renifleur ; Vérifiez que l'état Admin est vert et que le mode AP affiche Sniffer.



AP Name	AP Model	Slots	Admin Status	Up Time	WLC Association Uptime	IP Address	Base Radio MAC	Ethernet MAC	AP Mode
C9130AXI	C9130AXI-B	3		8 days 17 hrs 56 mins 36 secs	8 days 17 hrs 53 mins 7 secs	192.168.6.101	04eb.409f.0d60	04eb.409e.14e0	Sniffer

---

3. Recherchez l'émetteur-récepteur des points d'accès renifleurs. Vérifiez que l'analyse est activée et que l'affectation de canal est définie comme souhaité. Vérifiez que l'état IP du renifleur est correct, ce qui indique que le 9800 dispose d'une connectivité IP.



---

4. Pour confirmer que le point d'accès est en mode Sniffer à partir de l'interface de ligne de commande du 9800, exécutez les commandes suivantes :

<#root>

9800-L#

```
show ap name C9130AXI config general | include Administrative
```

```
Administrative State : Enabled
```

9800-L#

```
show ap name C9130AXI config general | include Sniff
```

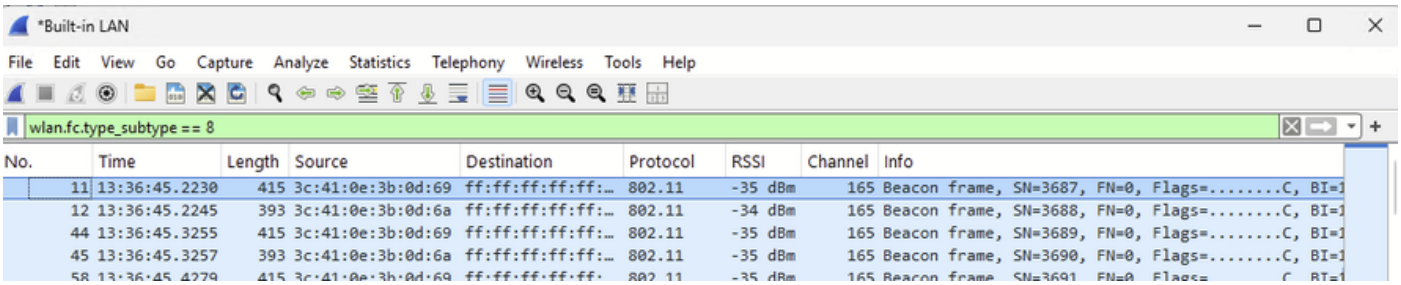
```
AP Mode : Sniffer
```

9800-L#

```
show ap name C9130AXI config dot11 5Ghz | include Sniff
AP Mode : Sniffer
Sniffing : Enabled
Sniff Channel : 165
Sniffer IP : 192.168.203.102
Sniffer IP Status : Valid
Radio Mode : Sniffer
Radio Role : Sniffer
```

---

5. Pour confirmer que Wireshark décode correctement les trames 802.11 et que le point d'accès de l'analyseur a été positionné à proximité des périphériques concernés, filtrez les balises 802.11 (wlan.fc.type_subtype == et affichez le RSSI (wlan_radio.signal_dbm) :



Dépannage

Problème : Wireshark ne reçoit aucune donnée du point d'accès.

Solution : Le serveur Wireshark doit être accessible à partir de l'interface de gestion sans fil (WMI). Vérifiez l'accessibilité entre le serveur Wireshark et le WMI à partir du WLC.

Informations connexes

- Analyse et dépannage de l’analyseur de réseau sans fil 802.11
- Assistance et documentation techniques - Cisco Systems

- Guide de configuration du logiciel du contrôleur sans fil de la gamme Cisco Catalyst 9800, Cisco IOS XE Amsterdam 17.18.x - Chapitre : Mode renifleur

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.