

Configurer le point d'accès en mode renifleur sur les contrôleurs sans fil Catalyst 9800

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configurer le point d'accès en mode renifleur via l'interface utilisateur graphique](#)

[Configurer le point d'accès en mode renifleur via CLI](#)

[Configurer le point d'accès pour analyser un canal via une interface utilisateur graphique](#)

[Configurer AP pour analyser un canal via CLI](#)

[Configuration de Wireshark pour collecter la capture de paquets](#)

[Vérification](#)

[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) via l'interface graphique utilisateur (GUI) ou l'interface de ligne de commande (CLI) et comment collecter une capture de paquets (PCAP) en vol (OTA) avec le point d'accès renifleur afin de dépanner et analyser les comportements sans fil.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration WLC 9800
- Connaissances de base dans la norme 802.11

Components Used

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

- AP 2802
- 9800 WLC Cisco IOS®-XE version 17.3.2a

- Wireshark 3.X

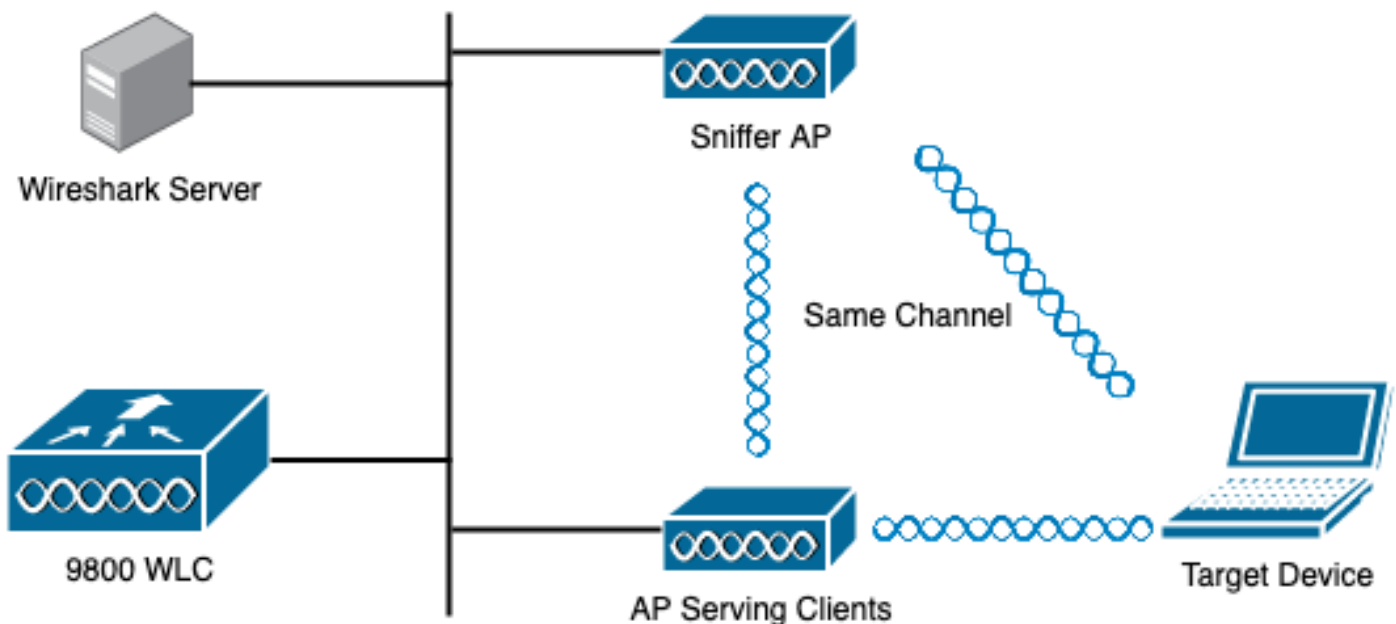
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Points à considérer :

- Il est recommandé d'avoir le point d'accès de renifleur proche du périphérique cible et du point d'accès auquel ce périphérique est connecté.
- Assurez-vous de connaître le canal et la largeur 802.11, le périphérique client et le point d'accès utilisés.

Diagramme du réseau



Configurations

Configurer le point d'accès en mode renifleur via l'interface utilisateur graphique

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



Q Search Menu Items

- Dashboard
- Monitoring >
- Configuration** >
- Administration >
- Licensing
- Troubleshooting

- Interface
 - Logical
 - Ethernet
 - Wireless
- Layer2
 - Discovery Protocols
 - VLAN
 - VTP
- Radio Configurations
 - CleanAir
 - High Throughput
 - Media Parameters
 - Network
 - Parameters
 - RRM
- Routing Protocols
 - Static Routing
- Security
 - AAA
 - ACL
 - Advanced EAP
 - PKI Management
 - Guest User
 - Local EAP
 - Local Policy

- Services
 - AireOS Config Translator
 - Application Visibility
 - Cloud Services
 - Custom Application
 - IOx
 - mDNS
 - Multicast
 - NetFlow
 - Python Sandbox
 - QoS
 - RA Throttle Policy
- Tags & Profiles
 - AP Join
 - EoGRE
 - Flex
 - Policy
 - Remote LAN
 - RF
 - Tags
 - WLANs
- Wireless**
 - Access Points**
 - Advanced
 - Air Time Fairness
 - Fabric

Étape 2. Sélectionnez le point d'accès à utiliser en mode renifleur. Sous l'onglet **Général**, mettez à jour le nom de l'AP, comme indiqué dans l'image.

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Blk M
2802-carcerva	AIR-AP2802I-B-K9	2	✓	172.16.0.125	ac

10 items per page

5 GHz Radios

2.4 GHz Radios

Edit AP

General Interfaces High Availability Inventory

General

AP Name* 2802-carcerva-sniffer

Location* default location

Base Radio MAC a03d.6f92.9400

Ethernet MAC 00a2.eedf.6114

Admin Status **ENABLED**

AP Mode Flex

Operation Status Registered

Étape 3. Vérifiez que l'état Admin est **Activé** et changez le **mode AP** en **Sniffer**, comme l'illustre l'image.

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Blk M
2802-carcerva	AIR-AP2802I-B-K9	2	✓	172.16.0.125	ac

10 items per page

5 GHz Radios

2.4 GHz Radios

Edit AP

General Interfaces High Availability Inventory

General

AP Name* 2802-carcerva-sniffer

Location* default location

Base Radio MAC a03d.6f92.9400

Ethernet MAC 00a2.eedf.6114

Admin Status **ENABLED**

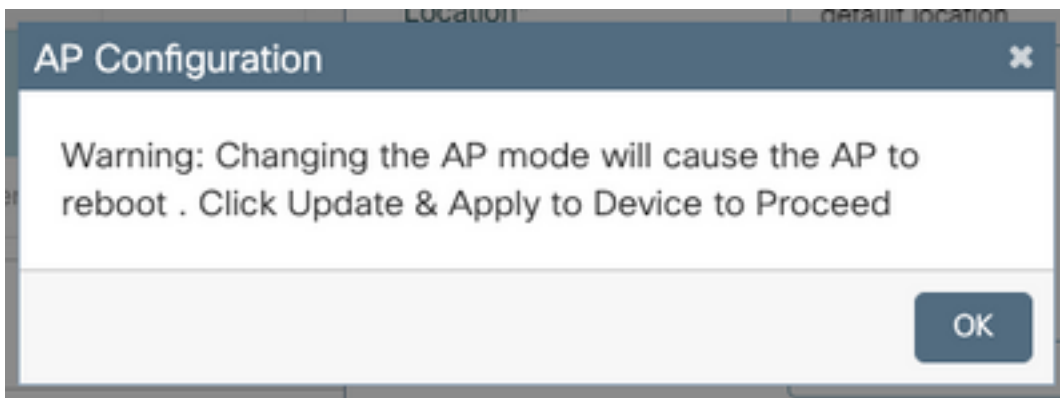
AP Mode Sniffer

Operation Status Registered

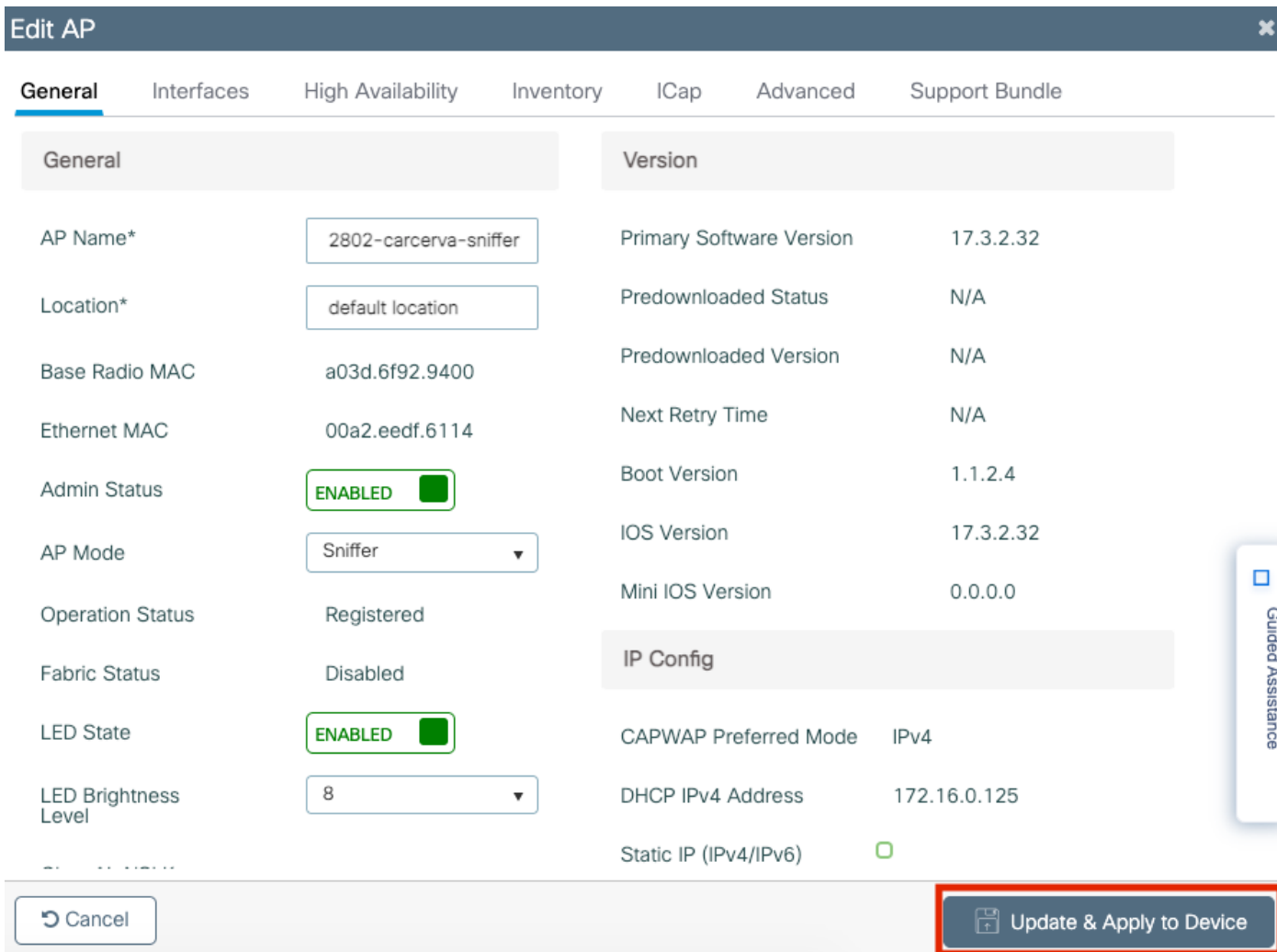
Une fenêtre contextuelle apparaît avec la note suivante :

"Avertissement : La modification du mode AP entraîne le redémarrage de l'AP. Cliquez sur Mettre à jour et appliquer au périphérique pour continuer. »

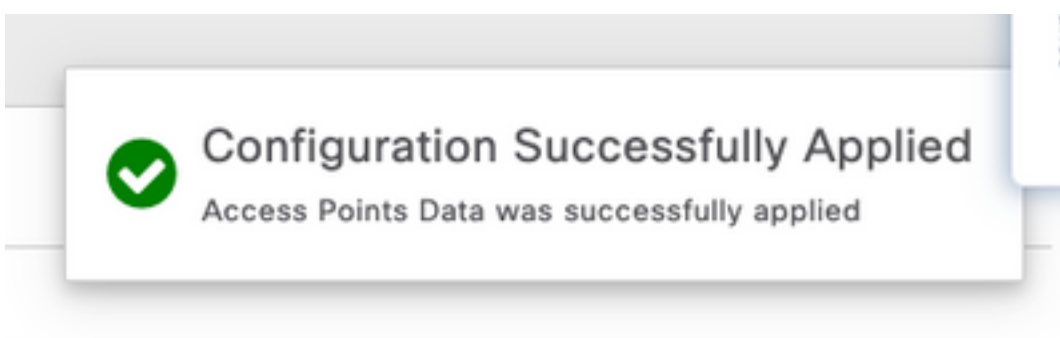
Sélectionnez **OK**, comme indiqué dans l'image.



Étape 4. Cliquez sur **Mettre à jour et appliquer au périphérique**, comme illustré dans l'image.



Une fenêtre contextuelle apparaît pour confirmer les modifications et le point d'accès rebondit, comme l'illustre l'image.



Configurer le point d'accès en mode renifleur via CLI

Étape 1. Déterminez le point d'accès à utiliser comme mode de renifleur et saisissez le nom du point d'accès.

Étape 2. Modifiez le nom du point d'accès.

Cette commande modifie le nom de l'AP. Où <AP-name> est le nom actuel de l'AP.

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

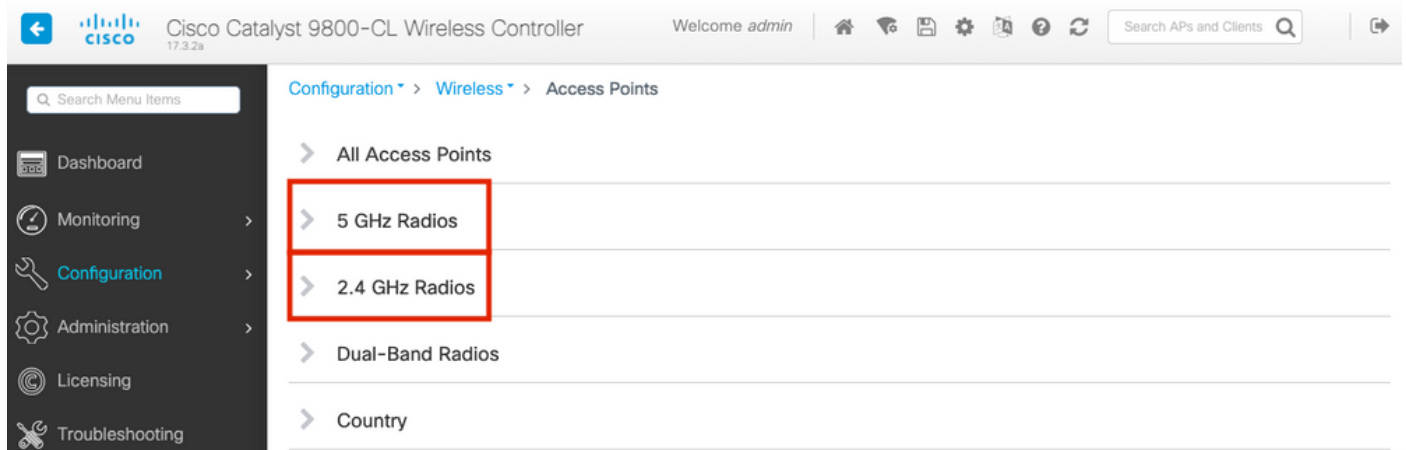
Étape 3. Configurez l'AP en mode Sniffer.

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

Configurer le point d'accès pour analyser un canal via une interface utilisateur graphique

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

Étape 2. Sur la page **Points d'accès**, affichez la liste de menu **Radios 5 GHz** ou **Radios 2,4 GHz**. Cela dépend du canal à analyser, comme le montre l'image.



Étape 2. Rechercher le point d'accès. Cliquez sur le bouton **flèche bas** pour afficher l'outil de recherche, sélectionnez **Contains** dans la liste déroulante et tapez le **nom de l'AP**, comme indiqué dans l'image.

Cisco Catalyst 9800-CL Wireless Controller 17.3.2a

Welcome admin

Configuration > Wireless > Access Points

All Access Points

5 GHz Radios

Number of AP(s): 1

AP Name	Slot No	Base Radio MAC	Admin Status	Operation Status	Policy Tag	Site Tag
2802-carcerva-sniffer		400	✓	↑	webauth_test	default-site-tag

Show items with value that: Contains
sniffer

Filter Clear

2.4 GHz Radios

Étape 3. Sélectionnez le point d'accès et cochez la case **Enable Sniffer** sous **Configure > Sniffer Channel Assignment**, comme indiqué dans l'image.

Cisco Catalyst 9800-CL Wireless Controller 17.3.2a

Welcome admin

Configuration > Wireless > Edit Radios 5 GHz Band

Configure Detail

All Access Points

5 GHz Radios

Number of AP(s): 1

AP Name "Contains"

AP Name: 2802-carcerva-sniffer

Antenna Mode: Omnidirectional

Antenna A: ✓

Antenna B: ✓

Antenna C: ✓

Antenna D: ✓

Antenna Gain: 10

Sniffer Channel Assignment

Enable Sniffing:

Sniff Channel: 36

Sniffer IP*: 172.16.0.190

Sniffer IP Status: Valid

Download Core Dump to bootflash

Cancel

Étape 4. Sélectionnez Channel dans la liste déroulante **Sniff Channel** et tapez l'adresse IP de l'analyseur (adresse IP du serveur avec Wireshark), comme indiqué dans l'image.

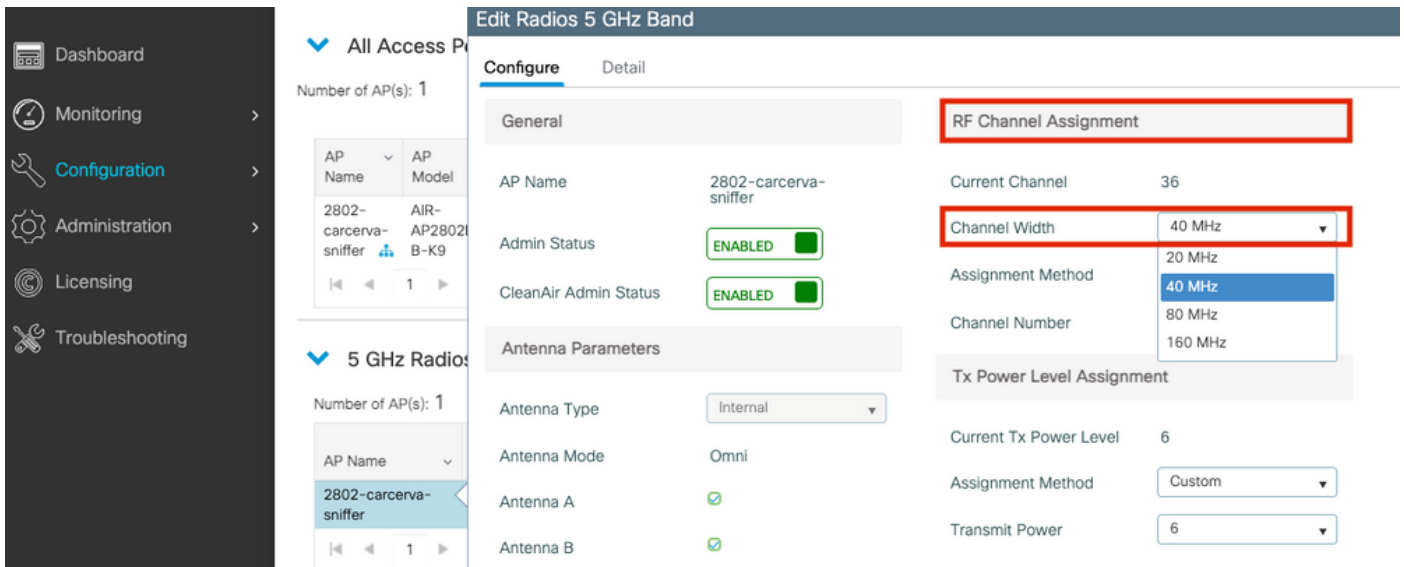
The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration interface. The page title is "Edit Radios 5 GHz Band". The "Configure" tab is selected. The "Sniffer Channel Assignment" section is highlighted, showing the following configuration:

Parameter	Value
Enable Sniffing	<input checked="" type="checkbox"/>
Sniff Channel	36
Sniffer IP*	172.16.0.190
Sniffer IP Status	Valid

At the bottom of the configuration area, there is a "Cancel" button.

Étape 5. Sélectionnez la **largeur de canal** que le périphérique cible et le point d'accès utilisent lorsqu'ils sont connectés.

Accédez à **Configure > RF Channel Assignment** afin de configurer ceci, comme illustré dans l'image.



Configurer AP pour analyser un canal via CLI

Étape 1. Activez l'analyse de canal sur l'AP. Exécutez cette commande :

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

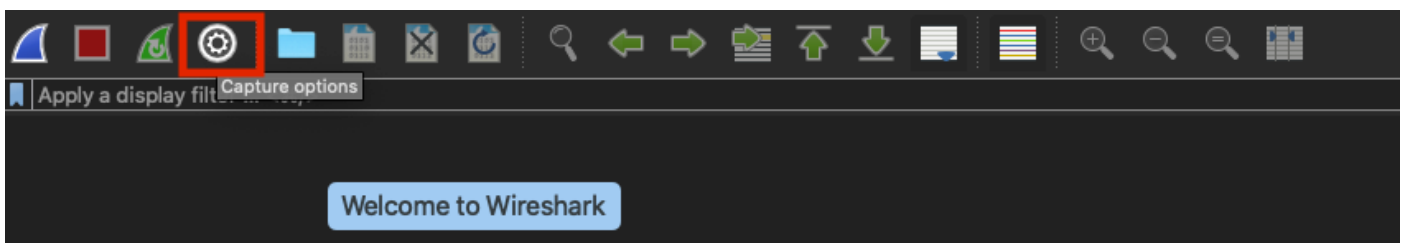
Exemple :

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

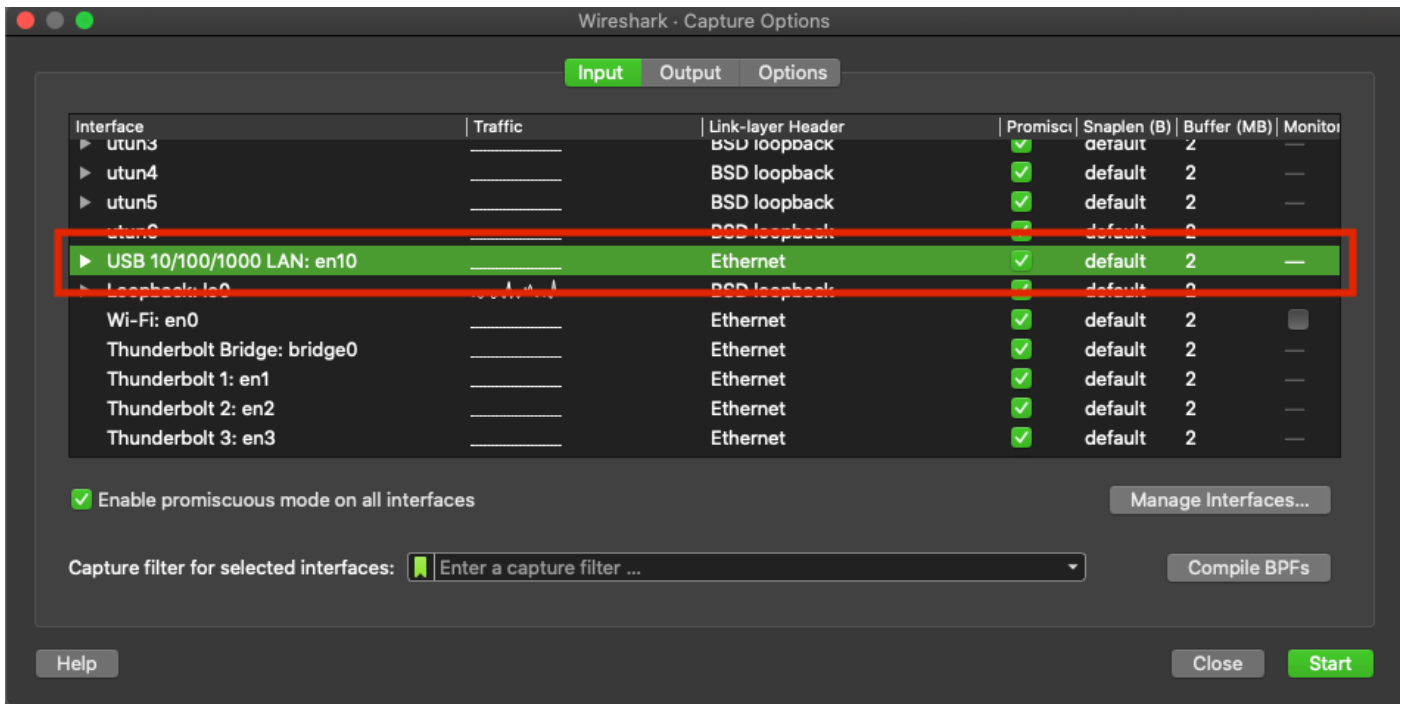
Configuration de Wireshark pour collecter la capture de paquets

Étape 1. Lancez Wireshark.

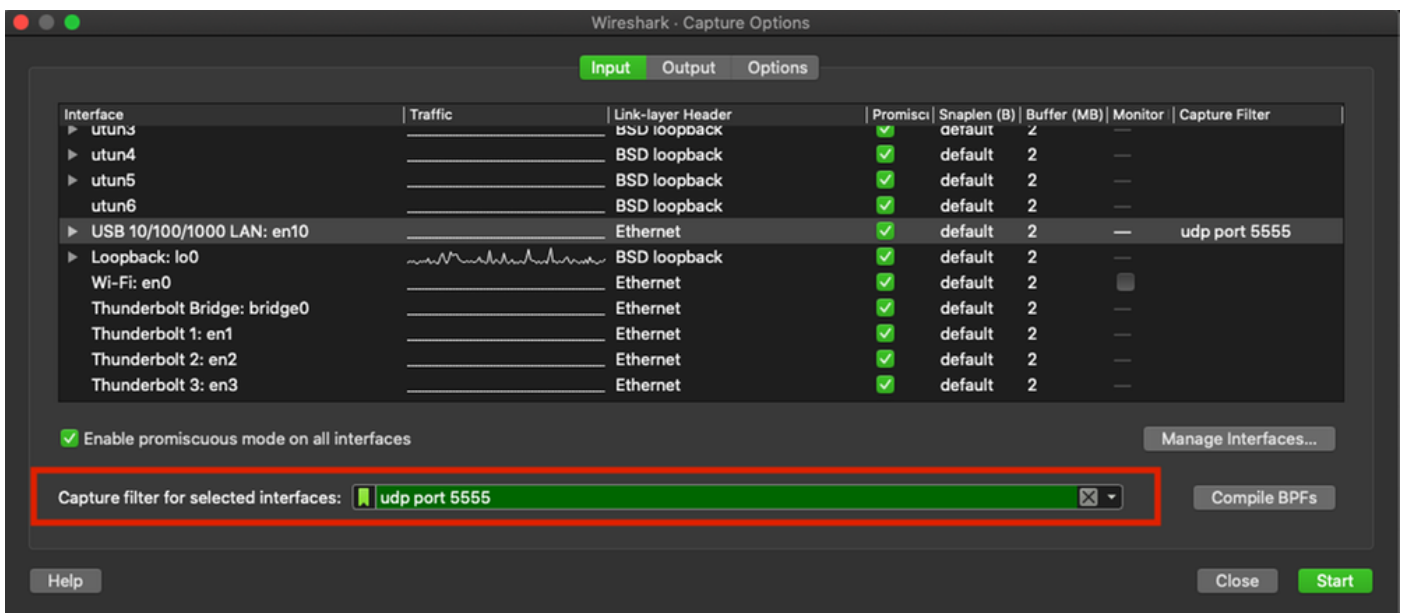
Étape 2. Sélectionnez l'icône de menu **Capture options** dans Wireshark, comme illustré dans l'image.



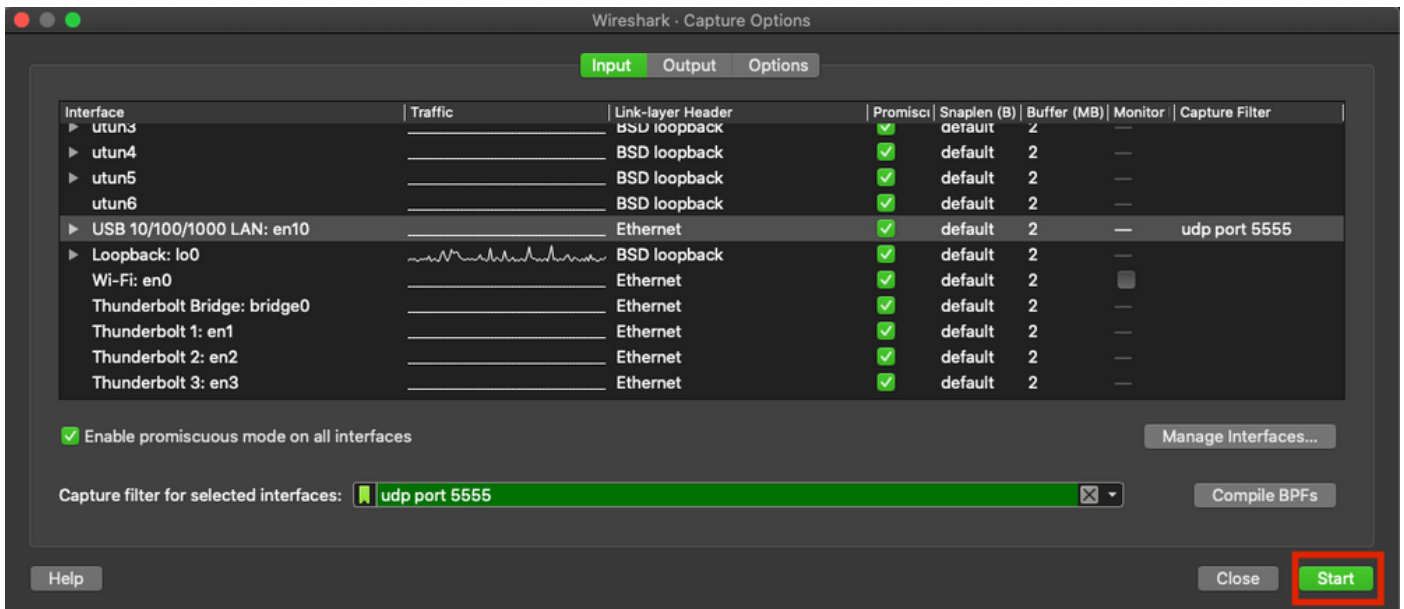
Étape 3. Cette action affiche une fenêtre contextuelle. Sélectionnez l'interface filaire dans la liste comme source de la capture, comme l'illustre l'image.



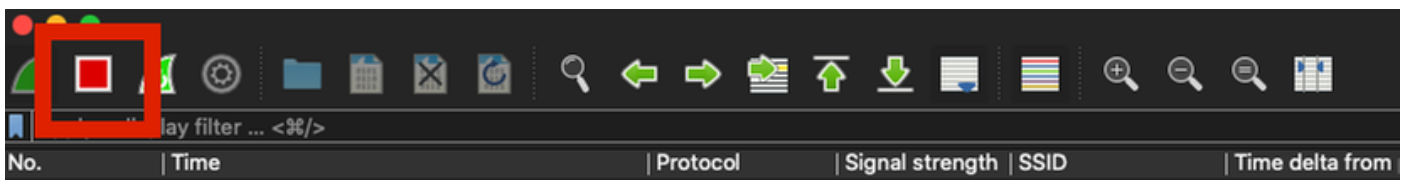
Étape 4. Sous le filtre Capture pour les interfaces sélectionnées : , tapez udp port 5555, comme indiqué dans l'image.



Étape 5. Cliquez sur Démarrer, comme illustré dans l'image.

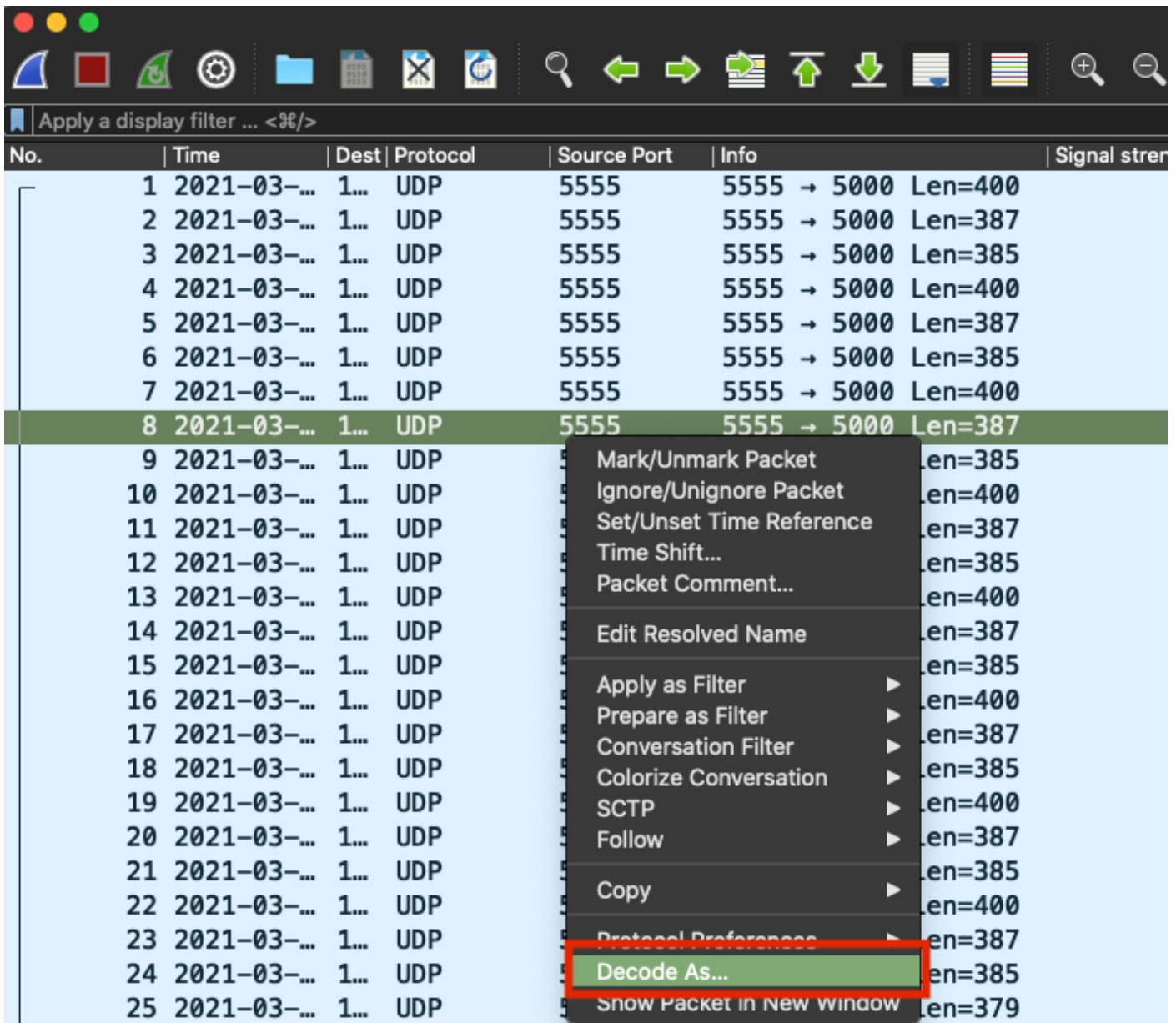


Étape 6. Attendez que Wireshark recueille les informations requises et sélectionnez le bouton **Arrêter** de Wireshark, comme l'illustre l'image.

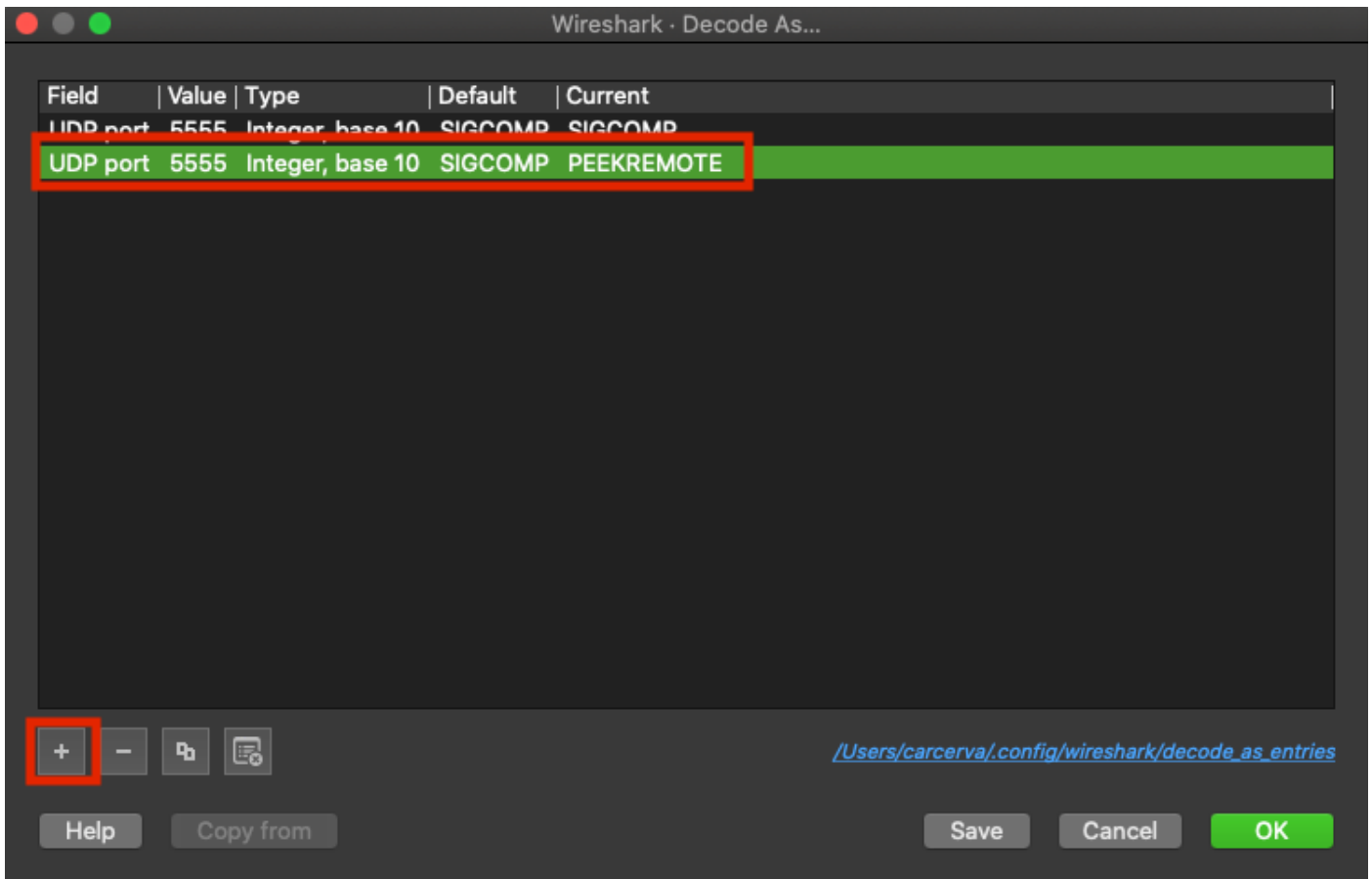


Astuce : Si le WLAN utilise un chiffrement tel que la clé prépartagée (PSK), assurez-vous que la capture intercepte la connexion en quatre étapes entre le point d'accès et le client souhaité. Cela peut être fait si le PCAP OTA démarre avant que le périphérique ne soit associé au WLAN ou si le client est déauthentié et réauthentié pendant l'exécution de la capture.

Étape 7. Wireshark ne décode pas automatiquement les paquets. Afin de décoder les paquets, sélectionnez une ligne dans la capture, cliquez avec le bouton droit de la souris pour afficher les options, puis sélectionnez **Décoder sous...**, comme indiqué dans l'image.



Étape 8. Une fenêtre contextuelle s'affiche. Sélectionnez le bouton Ajouter et ajoutez une nouvelle entrée, sélectionnez les options suivantes : **Port UDP de Field, 5555 de Value, SIGCOMP de Default et PEEKREMOTE de Current**, comme l'illustre l'image.



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

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Afin de confirmer que l'AP est en mode Sniffer à partir de l'interface utilisateur graphique 9800 :

Étape 1. Sur l'interface graphique du WLC 9800, accédez à **Configuration > Wireless > Access Points > All Access Points**.

Étape 2. Recherchez le point d'accès. Cliquez sur le bouton fléché vers le bas pour afficher l'outil de recherche, sélectionnez **Contains** dans la liste déroulante et tapez le nom de l'AP, comme indiqué dans l'image.



Search Menu Items



Dashboard



Monitoring



Configuration



Administration



Licensing



Troubleshooting

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP	Admin Status	IP Address
2802-carcerva-sniffer	sniffer	<input checked="" type="checkbox"/>	172.16.0.125

Show items with value that: Contains sniffer

Filter Clear

> 5 GHz Radios

Étape 3. Vérifiez que l'état Admin est coché en vert et que le mode AP est Sniffer, comme l'illustre l'image.



Search Menu Items

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Base Radio MAC	AP Mode	Operation Status	Configuration Status	Policy Tag	Site Tag
2802-carcerva-sniffer	AIR-AP2802I-B-K9	2	<input checked="" type="checkbox"/>	172.16.0.125	a03d.6f92.9400	Sniffer	Registered	Healthy	webauth_test	default-site-tag

10 items per page

1 - 1 of 1 access points

Afin de confirmer que l'AP est en mode Sniffer à partir de l'interface de ligne de commande 9800. Exécutez ces commandes :

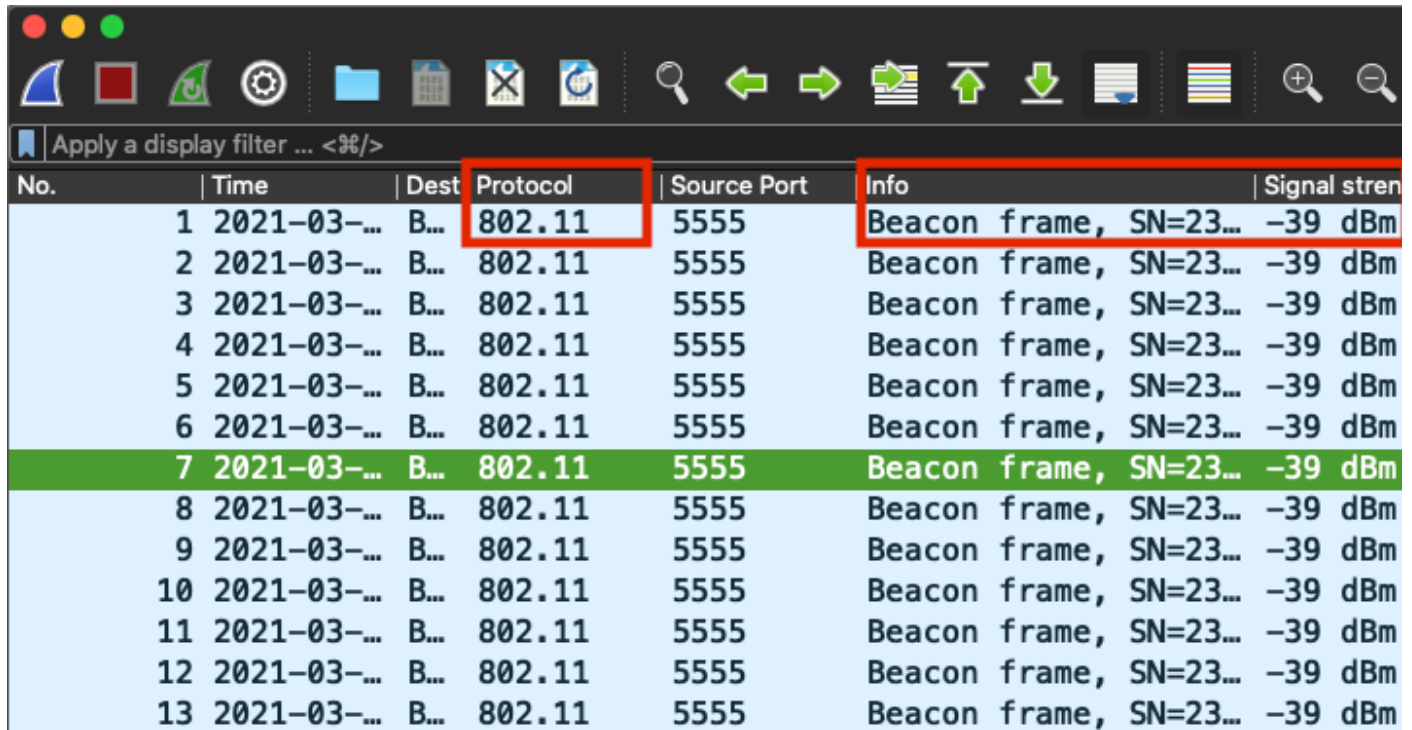
```
carcerva-9k-upg#show ap name 2802-carcerva-sniffer config general | i Administrative  
Administrative State : Enabled
```

```
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

Afin de confirmer que les paquets sont décodés sur Wireshark. Le protocole passe de UDP à 802.11 et des trames Beacon sont visibles, comme le montre l'image.



No.	Time	Dest	Protocol	Source Port	Info	Signal stren
1	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
2	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
3	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
4	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
5	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
6	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
7	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
8	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
9	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
10	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
11	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
12	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm
13	2021-03-...	B...	802.11	5555	Beacon frame, SN=23...	-39 dBm

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

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

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

Informations connexes

- [Guide de configuration du logiciel du contrôleur sans fil de la gamme Cisco Catalyst 9800, Cisco IOS XE Amsterdam 17.3.x - Chapitre : Mode Sniffer](#)
- [Notions de base de la norme sans fil 802.11](#)
- [Support et documentation techniques - Cisco Systems](#)