# 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  |          | Interface  | 0           | Services   |   |
|--|----------|--|-------------|--|---|
| 📰 Dashboard  |          | Logical<br>Ethernet<br>Wireless  |             | AireOS Config Translator<br>Application Visibility<br>Cloud Services   | r |
| Monitoring   | › للله   | Layer2<br>Discovery Protocols  |             | Custom Application<br>IOx<br>mDNIS   |   |
| Configuration  | >        | VLAN<br>VTP  |             | Multicast<br>NetFlow   |   |
| <ul> <li>Administration</li> <li>Licensing</li> <li>Troubleshooting</li> </ul> | )<br>∎∎⊛ | Radio Configurations<br>CleanAir<br>High Throughput<br>Media Parameters<br>Network<br>Parameters<br>RRM<br>Routing Protocols<br>Static Routing | R<br>R<br>R | Python Sandbox<br>QoS<br>RA Throttle Policy<br>Tags & Profiles<br>AP Join<br>EoGRE<br>Flex<br>Policy<br>Remote LAN<br>RF |   |
|  | Ð        | Security<br>AAA<br>ACL<br>Advanced EAP<br>PKI Management<br>Guest User<br>Local EAP<br>Local Policy  | \$          | Tags<br>WLANS<br>Wireless<br>Access Points<br>Advanced<br>Air Time Fairness<br>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.

| Cisco Catal          | Welcome admin 🛛 🕷 🕏  |                  |                            |                             |         |                |                  |
|----------------------|--|------------------|----------------------------|-----------------------------|---------|----------------|------------------|
| Q. Search Menu Items | Configuration > Wir  | E                | Edit AP                    |                             |         |                |                  |
| Dashboard            | <ul> <li>All Access Point</li> <li>Number of AP(s): 1</li> </ul> |                  | General Interfaces General | High Availability Inventory |         |                |                  |
| ( Monitoring >       |  |                  | AP Name*                   | 2802-carcerva-sniffer       |         |                |                  |
| Configuration        | AP V AP Name Model   | Slots ~          | Admin ~<br>Status          | IP ~<br>Address             | B;<br>M | Location*      | default location |
| (Ò) Administration   | 2802- AIR-<br>carcerva AP2802I-<br>& B-K9                        | 2                | ۲                          | 172.16.0.125                | a       | Base Radio MAC | a03d.6f92.9400   |
| C Licensing          | < < 1 ⊳  | 10 🔻 it          | ems per page               |                             |         | Ethernet MAC   | 00a2.eedf.6114   |
| X Troubleshooting    | > 5 GHz Radios   |                  | Admin Status               |                             |         |                |                  |
|                      |  |                  |                            |                             | _       | AP Mode        | Flex v           |
|                      | > 2.4 GHz Radio  | Operation Status | Registered                 |                             |         |                |                  |

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

| Cisco Catal          | Cisco Catalyst 9800-CL Wireless Controller |                  |                            |                             |          |                       |                  |  |  |  |  |  |  |
|----------------------|--|------------------|----------------------------|-----------------------------|----------|-----------------------|------------------|--|--|--|--|--|--|
| Q. Search Menu Items | Configuration * > Wi                       |                  | Edit AP                    |                             |          |                       |                  |  |  |  |  |  |  |
| Dashboard            | V All Access Po<br>Number of AP(s): 1      |                  | General Interfaces General | High Availability Inventory |          |                       |                  |  |  |  |  |  |  |
| Monitoring >         |  |                  |                            |                             | AP Name* | 2802-carcerva-sniffer |                  |  |  |  |  |  |  |
| Configuration        | AP ~ AP<br>Name Model                      | Slots v          | Admin ~<br>Status          | IP ~<br>Address             | B;<br>M  | Location*             | default location |  |  |  |  |  |  |
| (O) Administration   | 2802- AIR-<br>carcerva AP2802I<br>dh B-K9  | 2                | ۲                          | 172.16.0.125                | a        | Base Radio MAC        | a03d.6f92.9400   |  |  |  |  |  |  |
| C Licensing          | ∈ ⊲ 1 ⊩                                    | 10 🔻 it          | tems per page              |                             |          | Ethernet MAC          | 00a2.eedf.6114   |  |  |  |  |  |  |
| X Troubleshooting    |  |                  |                            |                             | _        | Admin Status          |                  |  |  |  |  |  |  |
|                      | 5 GHz Radios                               |                  | AP Mode                    | Sniffer 🔹                   |          |                       |                  |  |  |  |  |  |  |
|                      | > 2.4 GHz Radi                             | 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.

| Edit AP            |                    |                   |                       |               |               |                |                  | ×       |
|--------------------|--------------------|-------------------|-----------------------|---------------|---------------|----------------|------------------|---------|
| General            | Interfaces         | High Availability | Inventory             | lCap          | Advanced      | Support Bundle |                  |         |
| General            |                    |                   |                       | Version       |               |                |                  |         |
| AP Name            | *                  | 2802-carcerva-sn  | 2802-carcerva-sniffer |               |               | 17.3.2.32      |                  |         |
| Location*          | ,                  | default location  |                       | Predownloa    | aded Status   | N/A            |                  |         |
| Base Rad           | io MAC             | a03d.6f92.9400    |                       | Predownloa    | aded Version  | N/A            |                  |         |
| Ethernet I         | MAC                | 00a2.eedf.6114    | Next Retry            | Time          | N/A           |                |                  |         |
| Admin St           | atus               | ENABLED           |                       | Boot Versio   | n             | 1.1.2.4        |                  |         |
| AP Mode            |                    | Sniffer           | •                     | IOS Versior   | 1             | 17.3.2.32      |                  |         |
| Operatior          | n Status           | Registered        |                       | Mini IOS Ve   | ersion        | 0.0.0.0        |                  | Gui     |
| Fabric Sta         | atus               | Disabled          |                       | IP Config     |               |                |                  | ded Ass |
| LED State          | LED State          |                   | ENABLED               |               | referred Mode | IPv4           |                  | istance |
| LED Brigh<br>Level | LED Brightness 8 • |                   |                       | DHCP IPv4     | Address       | 172.16.0.125   |                  |         |
|                    |                    |                   |                       | Static IP (IP | v4/IPv6)      | 0              |                  |         |
| Cance              | I                  |                   |                       |               |               | 📑 Update       | e & Apply to Dev | vice    |

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 Catal          | yst 9800-CL Wireless Controller Welcome admin 🛛 💣 🔞 🚱 😂  |
|----------------------|--|
| Q. Search Menu Items | Configuration > Wireless > Access Points   |
| n Dashboard          | > All Access Points  |
| Monitoring >         | ✓ 5 GHz Radios   |
| Configuration        | Number of AP(s): 1   |
| ∫ Administration >   | AP Name Slot No v MAC Status Status Tag Site Tag v   |
| © Licensing          | 2802-carcerva- Show items with value that:<br>sniffer Contains V 400 O webauth_test default-site-<br>tag |
| X Troubleshooting    | > 2.4 GHz R  |

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

| Cisco Catal          | yst 9800–CL Wirele  | ess Controller          | Welcome admin 🛛 😭 📢 |
|----------------------|---------------------|-------------------------|---------------------|
| Q Search Menu Items  | Configuration - > W | Edit Radios 5 GHz Band  | b                   |
| 📰 Dashboard          | > All Access P      | , atterna moue          | UIIII               |
| Monitoring >         | ✓ 5 GHz Radios      | Antenna A               | Ø                   |
|                      | Number of AP(s): 1  | Antenna B               | Ø                   |
|                      | AP Name " Contains" | Antenna C               | $\oslash$           |
| {O} Administration → | AP Name             | Antenna D               | Ø                   |
| © Licensing          | 2802-carcerva-      | Antenna Gain            | 10                  |
| ₩ Troubleshooting    | sniffer<br> ◀ ◀ 1 ► | Sniffer Channel Assignn | nent                |
|                      |                     | Enable Sniffing         | Ø                   |
|                      | 2.4 GHz Radi        | Sniff Channel           | 36 🔻                |
|                      | > Dual-Band R       | Sniffer IP*             | 172.16.0.190        |
|                      | > Country           | Sniffer IP Status       | Valid               |
|                      | ISC Provisio        | Download Core Dump to b | ootflash            |
|                      |                     | 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.

| Cisco Catal          | yst 9800-CL Wireless Controller      | Welcome admin 🛛 🏠 🕵 |
|----------------------|--------------------------------------|---------------------|
| Q, Search Menu Items | Configuration -> W Edit Radios 5 GHz | : Band              |
| 📰 Dashboard          | > All Access P                       | Unini               |
| Monitoring >         | Antenna A S GHz Radios               | Ø                   |
|                      | Antenna B<br>Number of AP(s): 1      | $\oslash$           |
|                      | AP Name " Contains"                  | Ø                   |
| Administration   >   | Antenna D                            | Ø                   |
| C Licensing          | AP Name Antenna Gain                 | 10                  |
| X Troubleshooting    | Sniffer Channel A                    | ssignment           |
|                      | Enable Sniffing                      | Ø                   |
|                      | Sniff Channel                        | 36 🗸                |
|                      | > Dual-Band R Sniffer IP*            | 172.16.0.190        |
|                      | Sniffer IP Status                    | Valid               |
|                      | Download Core Dum                    | np to bootflash     |
|                      | > LSC Provisio                       |                     |

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.

|                    |                                       | Edit Radios 5 GHz Band |                |                        |                   |  |  |  |  |  |  |  |  |
|--------------------|---------------------------------------|------------------------|----------------|------------------------|-------------------|--|--|--|--|--|--|--|--|
| Dashboard          | <ul> <li>All Access Period</li> </ul> | Configure Detail       |                |                        |                   |  |  |  |  |  |  |  |  |
| Monitoring >       | Number of AP(s): 1                    | General                |                | RF Channel Assignment  |                   |  |  |  |  |  |  |  |  |
| Configuration      | AP ~ AP<br>Name Model                 | AP Name                | 2802-carcerva- | Current Channel        | 36                |  |  |  |  |  |  |  |  |
| (O) Administration | 2802- AIR-<br>carcerva- AP28021       | Admin Status           |                | Channel Width          | 40 MHz 🔻          |  |  |  |  |  |  |  |  |
| C Licensing        |                                       | CleanAir Admin Status  |                | Assignment Method      | 20 MHz<br>40 MHz  |  |  |  |  |  |  |  |  |
| 💥 Troubleshooting  | ✓ 5 GHz Padio                         | Antenna Parameters     |                | Channel Number         | 80 MHz<br>160 MHz |  |  |  |  |  |  |  |  |
|                    | Number of AP(s): 1                    | Antenna Type           | Internal v     | Tx Power Level Assignm | lent              |  |  |  |  |  |  |  |  |
|                    | AP Name 🗸                             | Antenna Mode           | Omni           | Current Tx Power Level | 6                 |  |  |  |  |  |  |  |  |
|                    | 2802-carcerva-<br>sniffer             | Antenna A              | Ø              | Assignment Method      | Custom            |  |  |  |  |  |  |  |  |
|                    |                                       | Antenna B              | Ø              | Transmit Power         | <u>ь</u>          |  |  |  |  |  |  |  |  |

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.

| • |                |   |                            | Wiresha   | rk · Cap | oture Options    |   |                |                           |           |
|---|----------------|---|----------------------------|-----------|----------|------------------|---|----------------|---------------------------|-----------|
|   |                |   |                            | Input     | Outpu    | t Options        |   |                |                           |           |
|   | in<br>P        | terface<br>▶ utun⊰                            | Traffic                    |           | L<br>    | ink-layer Header | Promise   | si Snaplen (B) | Buffer (MB)               | Monitor   |
|   |                | vtun4   |                            |           | E        | BSD loopback     |   | default        | 2                         |           |
|   | ┢              | ▶ utun5                                       |                            |           | E        | BSD loopback     |   | default        | 2                         |           |
|   |                | - ttan0                                       |                            |           |          | 20D laspbask     |   | default        | 2                         |           |
|   | ►              | <ul> <li>USB 10/100/1000 LAN: en10</li> </ul> |                            |           | E        | Ethernet         | <ul> <li>✓</li> </ul>   | default        | 2                         | -         |
|   | -              | Loopbook: IoO                                 |                            |           |          | PCD loophools    |   | defeult        | 2                         |           |
|   |                | Wi-Fi: en0                                    |                            |           | E        | Ethernet         | Sec.  | default        | 2                         |           |
|   |                | Thunderbolt Bridge: bridge0                   |                            |           | E        | Ethernet         | Image: A start and a start and a start a st | default        | 2                         |           |
|   |                | Thunderbolt 1: en1                            |                            |           | E        | Ethernet         | Solution  | default        | 2                         |           |
|   |                | Thunderbolt 2: en2                            |                            |           | E        | Ethernet         | <b>V</b>  | default        | 2                         |           |
|   |                | Thunderbolt 3: en3                            |                            |           | E        | Ethernet         | <b>V</b>  | default        | 2                         |           |
|   | <b>∨</b><br>Ca | Enable promiscuous mode on all interface      | i <b>s</b><br>ter a captur | re filter |          |                  |   | Man:           | age Interfac<br>Compile B | es<br>PFs |
| ŀ | lelj           | p   |                            |           |          |                  |   |                | Close                     | Start     |

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

| Interface   | Traffic                                      | Link-layer Header | Promisc  | ı  Snaplen (B) | Buffer (MB) | Monitor | Capture Filter                   |
|---|--|-------------------|----------|----------------|-------------|---------|----------------------------------|
| ■ utuna   |  | BSD loopback      | <u> </u> | detault        | 2           |         |                                  |
| ▶ utun4   |  | BSD loopback      | <u> </u> | default        | 2           |         |                                  |
| ▶ utun5   |  | BSD loopback      | <u> </u> | default        | 2           |         |                                  |
| utun6   |  | BSD loopback      |          | default        | 2           |         |                                  |
| USB 10/100/1000 LAN: er   |  | Ethernet          | <u> </u> | default        | 2           |         | udp port 5555                    |
| Loopback: Io0   | Muhahhan Marin                               | BSD loopback      | <u> </u> | default        | 2           |         |                                  |
| Wi-Fi: en0  |  | Ethernet          | <u> </u> | default        | 2           |         |                                  |
| Thunderbolt Bridge: bridg                                       | je0  | Ethernet          | <u> </u> | default        | 2           |         |                                  |
| Thunderbolt 1: en1  | · · · · · · · · · · · · · · · · · · ·        | Ethernet          | <u> </u> | default        | 2           |         |                                  |
| Thunderbolt 2: en2  |  | Ethernet          |          | default        | 2           |         |                                  |
| Thunderbolt 3: en3  |  | Ethernet          | S        | default        | 2           |         |                                  |
| Enable promiscuous mode Capture filter for selected integration | on all interfaces<br>rfaces: 📕 udp port 5555 |                   |          |                |             |         | anage Interfaces<br>Compile BPFs |

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

| •        |   | ١           | Wireshar | k ∙ Captur | e Options |          |             |             |         |                   |
|----------|---|-------------|----------|------------|-----------|----------|-------------|-------------|---------|-------------------|
|          |   |             | Input    | Output     | Options   |          |             |             |         |                   |
| Int      | erface                                      | Traffic     | Link-la  | yer Header |           | Promisci | Snaplen (B) | Buffer (MB) | Monitor | Capture Filter    |
|          | utun4                                       |             | BSD      | oopback    |           |          | default     | 2           |         |                   |
| ►        | utun5                                       |             | BSD      | oopback    |           |          | default     | 2           |         |                   |
|          | utun6                                       |             | _ BSD I  | oopback    |           |          | default     | 2           |         |                   |
|          | USB 10/100/1000 LAN: en10                   |             | Ether    | net        |           |          | default     | 2           |         | udp port 5555     |
| ►        | Loopback: Io0                               |             | BSD I    | oopback    |           | <b>N</b> | default     | 2           |         |                   |
|          | Wi-Fi: en0                                  |             | Ether    | net        |           |          | default     | 2           |         |                   |
|          | Thunderbolt Bridge: bridge0                 |             | Ether    | net        |           |          | default     | 2           |         |                   |
|          | Thunderbolt 1: en1                          |             | Ether    | net        |           |          | default     | 2           |         |                   |
|          | Thunderbolt 2: en2                          |             | _ Ether  | net        |           |          | default     | 2           |         |                   |
|          | Thunderbolt 3: en3                          |             | Ether    | net        |           | <b>S</b> | default     | 2           |         |                   |
| <b>~</b> | Enable promiscuous mode on all interface    | S           |          |            |           |          |             |             |         | Manage Interfaces |
| Caj      | oture filter for selected interfaces: 📕 udj | p port 5555 |          |            |           |          |             | ×           | •       | Compile BPFs      |
| elp      |   |             |          |            |           |          |             |             |         | Close             |

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 déauthentifié et réauthentifié 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.

| 4 |       |          |        | 0    |      | 0101 | ×     | 6   | Q   |         | ⇒       |           | $\overline{\mathbf{e}}$ | <u> </u> | -   |     |    | Ð     | Q       |
|---|-------|----------|--------|------|------|------|-------|-----|-----|---------|---------|-----------|-------------------------|----------|-----|-----|----|-------|---------|
|   | Apply | y a disp | lay fi | lter | <%/> |      |       |     |     |         |         |           |                         |          |     |     |    |       |         |
| Ν | о.    |          | Tin    | ne   |      | Dest | Proto | col | Sou | irce Po | ort     | Info      |                         |          |     |     |    | Signa | l strer |
| ٢ | _     | 1        | 20     | 21-  | -03  | 1    | UDP   |     | 55  | 55      |         | 5555      | ; →                     | 5000     | Len | =4  | 00 |       |         |
|   |       | 2        | 20     | 21-  | -03  | 1    | UDP   |     | 55  | 55      |         | 5555      | ; →                     | 5000     | Len | =3  | 87 |       |         |
|   |       | 3        | 20     | 21-  | -03  | 1    | UDP   |     | 55  | 55      |         | 5555      | ; →                     | 5000     | Len | =3  | 85 |       |         |
|   |       | 4        | 20     | 21-  | -03  | 1    | UDP   |     | 55  | 55      |         | 5555      | ; →                     | 5000     | Len | =4  | 00 |       |         |
|   |       | 5        | 20     | 21-  | -03  | 1    | UDP   |     | 55  | 55      |         | 5555      | ; →                     | 5000     | Len | =3  | 87 |       |         |
|   |       | 6        | 20     | 21-  | -03  | 1    | UDP   |     | 55  | 55      |         | 5555      | ; →                     | 5000     | Len | =3  | 85 |       |         |
|   |       | 7        | 20     | 21-  | -03  | 1    | UDP   |     | 55  | 55      |         | 5555      | ; →                     | 5000     | Len | =4  | 00 |       |         |
|   |       | 8        | 20     | 21-  | -03  | 1    | UDP   |     | 55  | 55      |         | 5555      | j →                     | 5000     | Len | =3  | 87 |       |         |
|   |       | 9        | 20     | 21-  | -03  | 1    | UDP   |     | -   | Mark    | /Unma   | ark Pac   | ket                     |          | .en | =3  | 85 |       |         |
|   |       | 10       | 20     | 21-  | -03  | 1    | UDP   |     | 1   | Ignor   | e/Uni   | gnore F   | Pack                    | et       | .en | =4  | 00 |       |         |
|   |       | 11       | 20     | 21-  | -03  | 1    | UDP   |     | 1   | Set/L   | Shift   | Time R    | erer                    | ence     | .en | =3  | 87 |       |         |
|   |       | 12       | 20     | 21-  | -03  | 1    | UDP   |     | -   | Pack    | et Cor  | <br>nment |                         |          | .en | =3  | 85 |       |         |
|   |       | 13       | 20     | 21-  | -03  | 1    | UDP   |     |     | - uen   | 0.001   |           |                         |          | .en | =4  | 00 |       |         |
|   |       | 14       | 20     | 21-  | -03  | 1    | UDP   |     | -   | Edit I  | Resolv  | ed Nar    | me                      |          | .en | =3  | 87 |       |         |
|   |       | 15       | 20     | 21-  | -03  | 1    | UDP   |     |     | Apply   | v as Fi | ilter     |                         | •        | .en | =3  | 85 |       |         |
|   |       | 16       | 20     | 21-  | -03  | 1    | UDP   |     |     | Prepa   | are as  | Filter    |                         | •        | .en | =4  | 00 |       |         |
|   |       | 17       | 20     | 21-  | -03  | 1    | UDP   |     |     | Conv    | ersati  | on Filte  | er                      | Þ        | .en | =3  | 87 |       |         |
|   |       | 18       | 20     | 21-  | -03  | 1    | UDP   |     | -   | Color   | rize Co | onversa   | atior                   | 1 Þ      | .en | =3  | 85 |       |         |
|   |       | 19       | 20     | 21-  | -63  | 1    | UDP   |     | 1   | SCTF    | >       |           |                         | Þ        | .en | =4  | 00 |       |         |
|   |       | 20       | 20     | 21-  | -63  | 1    | UDP   |     | -   | Follo   | w       |           |                         | •        | .en | =3  | 87 |       |         |
|   |       | 21       | 20     | 21-  | -63  | 1    | UDP   |     |     | Copy    |         |           |                         | •        | len | =3  | 85 |       |         |
|   |       | 22       | 20     | 21-  | -63  | 1    | UDP   |     | -   |         |         |           |                         |          | en  | =4  | 00 |       |         |
|   |       | 23       | 20     | 21-  | -63  | 1    | UDP   |     | F   | Droto   | ide As  | referen   | 200                     |          | en  | 5=1 | 87 |       |         |
|   |       | 24       | 20     | 21-  | -63  | 1    | UDP   |     |     | Deco    |         |           | 014/-1                  | MIDGON   | len | 5=1 | 85 |       |         |
|   |       | 25       | 20     | 21-  | -03  | 1    | UDP   |     | 1   | Show    | Раск    |           | ew \                    | andow    | len | =3  | /9 |       |         |

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. Click 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. Rechercher 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.

.1 1.1 1. Cisco Catalyst 9800-CL Wireless Controller **CISCO** 17.3.2a Configuration >> Wireless >> Access Points Q Search Menu Items All Access Points Dashboard == Number of AP(s): 1 Monitoring > AP AP Admin IP Configuration > Name tatus Ac Show items with value that: 2802-Contains Ŧ Administration > carcerva 17 sniffer sniffer Licensing 4 -4 s per page Troubleshooting 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.

| ¢ | cisco Cisco                   | o Catalyst         | 9800-C                          | L Wireles                | ss Contro | oller             | Welcome         | e admin 🛛 😭         | <b>•</b>     | ¢ 🕸 0                 | Search               | APs and Clients | ג                    | ۲      |
|---|-------------------------------|--------------------|---------------------------------|--------------------------|-----------|-------------------|-----------------|---------------------|--------------|-----------------------|----------------------|-----------------|----------------------|--------|
| Q | Search Menu Items             | C                  | onfiguration                    | n≛> Wire                 | eless*>   | Access Poi        | ints            |                     |              |                       |                      |                 |                      |        |
|   | Dashboard   All Access Points |                    |                                 |                          |           |                   |                 |                     |              |                       |                      |                 |                      |        |
|   | Monitoring                    | Number of AP(s): 1 |                                 |                          |           |                   |                 |                     |              |                       |                      |                 |                      | \$     |
| Ľ | Configuration                 | >                  | AP ~<br>Name                    | AP ~<br>Model            | Slots ~   | Admin v<br>Status | IP ~<br>Address | Base Radio ~<br>MAC | AP ↓<br>Mode | Operation ~<br>Status | Configuration Status | Policy ~<br>Tag | Site ~<br>Tag        | E T    |
| Ś | Administration                | >                  | 2802-<br>carcerva-<br>sniffer 🚠 | AIR-<br>AP2802I-<br>B-K9 | 2         | ۰                 | 172.16.0.125    | a03d.6f92.9400      | Sniffer      | Registered            | Healthy              | webauth_test    | default-<br>site-tag | c<br>r |
| C | Licensing                     |                    | <b> 4 4</b>                     | 1 ⊩                      | 10 🔻 it   | ems per page      | •               |                     |              |                       |                      | - 1 of 1 access | points               | c      |
| × | Troubleshooting               |                    | E CU                            | Dadiaa                   |           |                   |                 |                     |              |                       |                      |                 |                      |        |

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.

| •                           |  |    |           |      |        |     |     |          |     |        |        |       |       |         |
|-----------------------------|--|----|-----------|------|--------|-----|-----|----------|-----|--------|--------|-------|-------|---------|
|                             |  | ø  | © 🖿       |      | ×      | 6   | Q   | <b>(</b> | •   | 警 쥼    | · 🕹 🛛  |       | Ð     | Q       |
| Apply a display filter <発/> |  |    |           |      |        |     |     |          |     |        |        |       |       |         |
| No.                         |  |    | Time      | Dest | Protoc | :ol | Sou | irce Po  | ort | Info   |        |       | Signa | l stren |
|                             |  | 1  | 2021–03–… | B    | 802.   | 11  | 55  | 55       |     | Beacon | frame, | SN=23 | -39   | dBm     |
|                             |  | 2  | 2021–03–… | B    | 802.   | 11  | 55  | 55       |     | Beacon | frame, | SN=23 | -39   | dBm     |
|                             |  | 3  | 2021–03–… | B    | 802.   | 11  | 55  | 55       |     | Beacon | frame, | SN=23 | -39   | dBm     |
|                             |  | 4  | 2021–03–… | В    | 802.   | 11  | 55  | 55       |     | Beacon | frame, | SN=23 | -39   | dBm     |
|                             |  | 5  | 2021–03–… | B    | 802.   | 11  | 55  | 55       |     | Beacon | frame, | SN=23 | -39   | dBm     |
|                             |  | 6  | 2021–03–… | B    | 802.   | 11  | 55  | 55       |     | Beacon | frame, | SN=23 | -39   | dBm     |
|                             |  | 7  | 2021–03–… | В    | 802.   | 11  | 55  | 55       |     | Beacon | frame, | SN=23 | -39   | dBm     |
|                             |  | 8  | 2021–03–… | B    | 802.   | 11  | 55  | 55       |     | Beacon | frame, | SN=23 | -39   | dBm     |
|                             |  | 9  | 2021–03–… | B    | 802.   | 11  | 55  | 55       |     | Beacon | frame, | SN=23 | -39   | dBm     |
|                             |  | 10 | 2021-03   | B    | 802.   | 11  | 55  | 55       |     | Beacon | frame, | SN=23 | -39   | dBm     |
|                             |  | 11 | 2021–03–… | B    | 802.   | 11  | 55  | 55       |     | Beacon | frame, | SN=23 | -39   | dBm     |
|                             |  | 12 | 2021-03   | B    | 802.   | 11  | 55  | 55       |     | Beacon | frame, | SN=23 | -39   | dBm     |
|                             |  | 13 | 2021-03   | B    | 802.   | 11  | 55  | 55       |     | 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