

# Configuración del punto de acceso en modo de sabueso en los controladores inalámbricos Catalyst 9800

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración de AP en Modo Sniffer a través de la GUI](#)

[Configuración de AP en modo de sabueso mediante CLI](#)

[Configurar AP para escanear un canal a través de la GUI](#)

[Configure el AP para escanear un canal a través de CLI](#)

[Configuración de Wireshark para Recopilar la Captura de Paquetes](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

## Introducción

Este documento describe cómo configurar un punto de acceso (AP) en modo sniffer en un controlador inalámbrico Catalyst serie 9800 (WLC 9800) a través de la interfaz gráfica de usuario (GUI) o la interfaz de línea de comandos (CLI) y cómo recopilar una captura de paquetes (PCAP) a través del aire (OTA) con el punto de acceso del sabueso para resolver problemas y analizar comportamientos inalámbricos.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- 9800 Configuración WLC
- Conocimientos básicos en el estándar 802.11

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- AP 2802
- 9800 WLC Cisco IOS®-XE versión 17.3.2a
- Wireshark 3.X

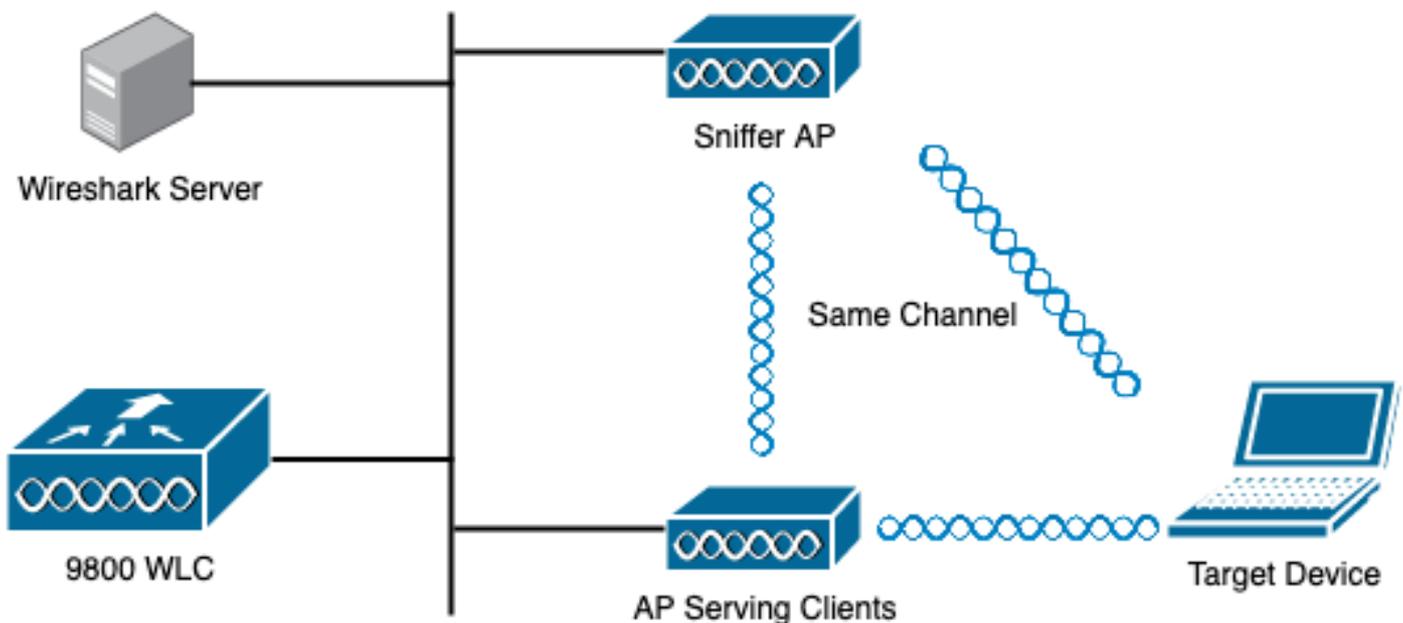
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configurar

Puntos a considerar:

- Se recomienda tener el punto de acceso del sabueso cerca del dispositivo de destino y el punto de acceso al que está conectado este dispositivo.
- Asegúrese de saber qué Canal y Ancho 802.11, el dispositivo cliente y el AP utilizan.

## Diagrama de la red



## Configuraciones

### Configuración de AP en Modo Sniffer a través de la GUI

Paso 1. En la GUI del WLC 9800, navegue hasta **Configuration > Wireless > Access Points > All Access Points**, como se muestra en la imagen.



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

Paso 2. Seleccione el AP que desea utilizar en el modo de sabueso. En la pestaña **General**, actualice el nombre del AP, como se muestra en la imagen.

Cisco Catalyst 9800-CL Wireless Controller 17.3.2a

Welcome admin

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

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

Paso 3. Verifique que el estado de administración esté habilitado y cambie el modo AP a sniffer, como se muestra en la imagen.

Cisco Catalyst 9800-CL Wireless Controller 17.3.2a

Welcome admin

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

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**

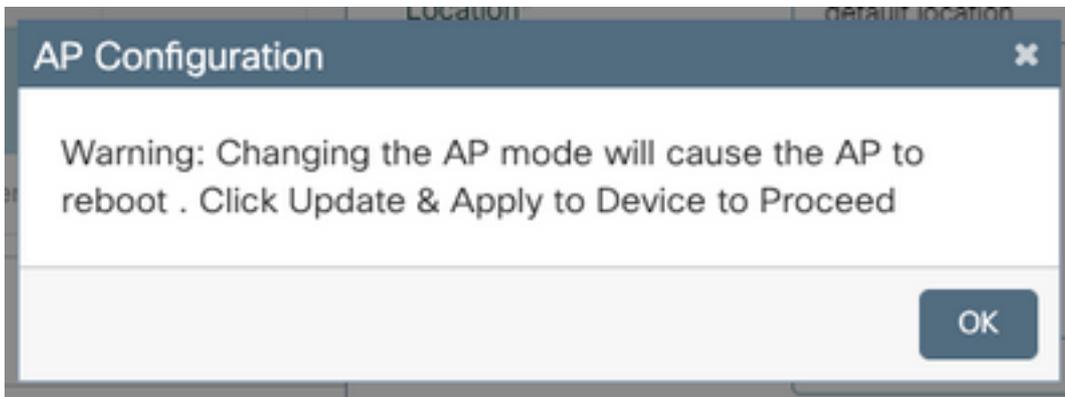
AP Mode Sniffer

Operation Status Registered

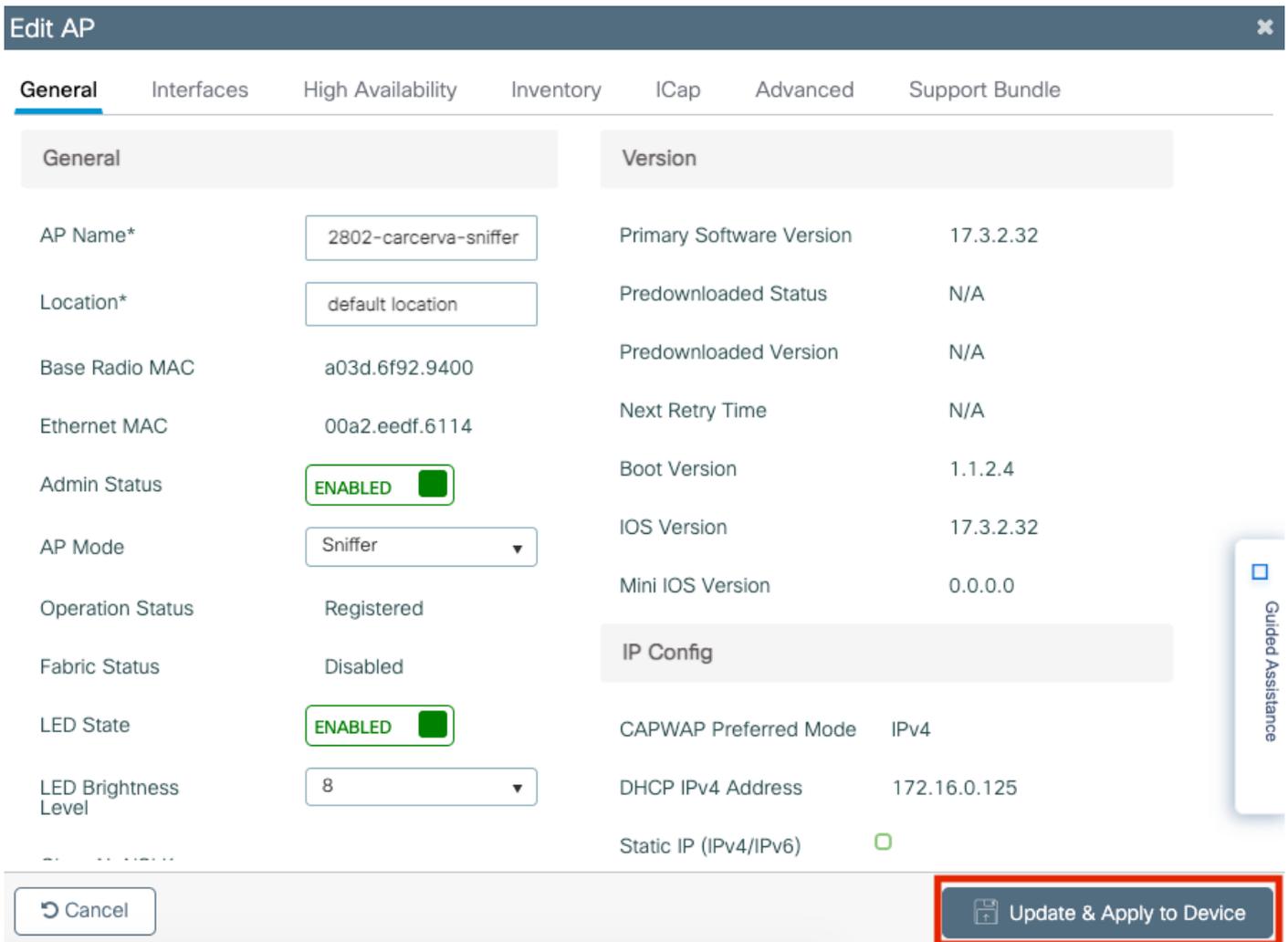
Aparece una ventana emergente con la siguiente nota:

"Advertencia: Si cambia el modo AP, el AP se reiniciará. Haga clic en Actualizar y aplicar al dispositivo para continuar".

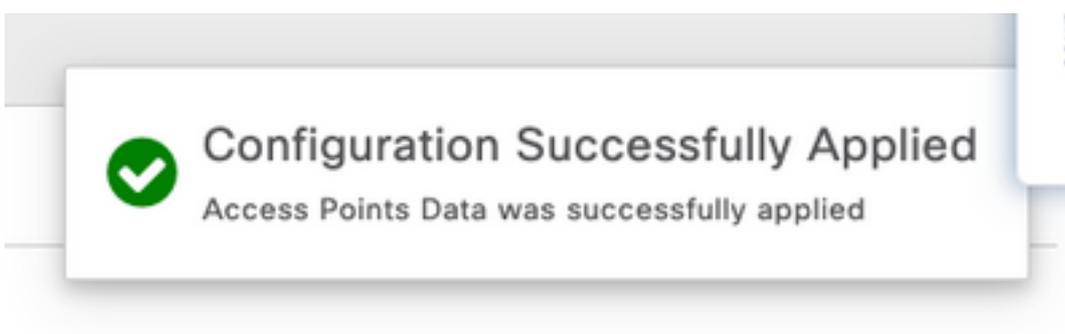
Seleccione **OK**, como se muestra en la imagen.



Paso 4. Haga clic en **Update & Apply to Device**, como se muestra en la imagen.



Aparece una ventana emergente para confirmar los cambios y los rebotes de AP, como se muestra en la imagen.



## Configuración de AP en modo de sabueso mediante CLI

Paso 1. Determine el AP que se desea utilizar como modo de sabueso y tome el nombre de AP.

Paso 2. Modifique el nombre AP.

Este comando modifica el nombre AP. Donde <AP-name> es el nombre actual del AP.

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

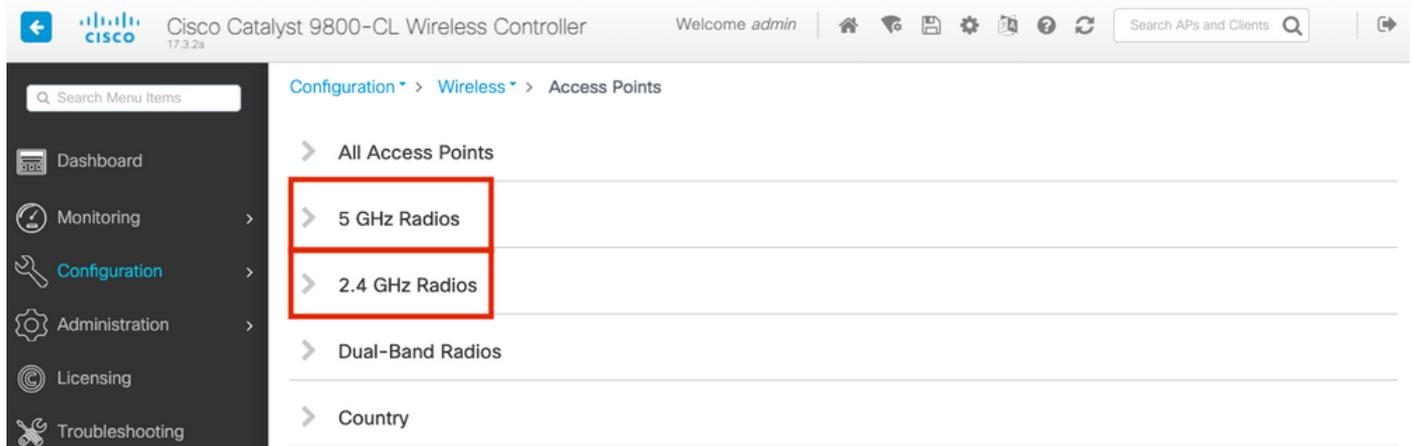
Paso 3. Configure el AP en el modo Sniffer.

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

## Configurar AP para escanear un canal a través de la GUI

Paso 1. En la GUI del WLC 9800, navegue hasta **Configuration > Wireless > Access Points**.

Paso 2. En la página **Puntos de acceso**, muestre la lista de menú **Radios de 5 GHz** o **Radios de 2,4 GHz**. Esto depende del canal que se desea escanear, como se muestra en la imagen.



Paso 2. Busque el AP. Haga clic en el botón **flecha abajo** para mostrar la herramienta de búsqueda, seleccione **Contiene** de la lista desplegable y escriba el **nombre AP**, como se muestra en la imagen.

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

Paso 3. Seleccione el AP y marque la casilla **Enable Sniffer** bajo **Configure > Sniffer Channel Assignment**, como se muestra en la imagen.

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	Omni
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

Paso 4. Seleccione el canal en la lista desplegable **Canal** del sniff y escriba la **dirección IP del sniffer** (dirección IP del servidor con Wireshark), como se muestra en la imagen.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration interface. The page title is "Edit Radios 5 GHz Band". The left sidebar contains navigation options: Dashboard, Monitoring, Configuration (highlighted), Administration, Licensing, and Troubleshooting. The main content area shows the configuration for a 5 GHz radio. The "Configure" tab is selected, and the "Sniffer Channel Assignment" section is visible. The "Sniff Channel" dropdown is set to 36, and the "Sniffer IP\*" field is set to 172.16.0.190. Both fields are highlighted with red boxes.

Antenna Mode	On/Off
Antenna A	<input checked="" type="checkbox"/>
Antenna B	<input checked="" type="checkbox"/>
Antenna C	<input checked="" type="checkbox"/>
Antenna D	<input checked="" type="checkbox"/>
Antenna Gain	10

Sniffer Channel Assignment

Enable Sniffing

Sniff Channel: 36

Sniffer IP\*: 172.16.0.190

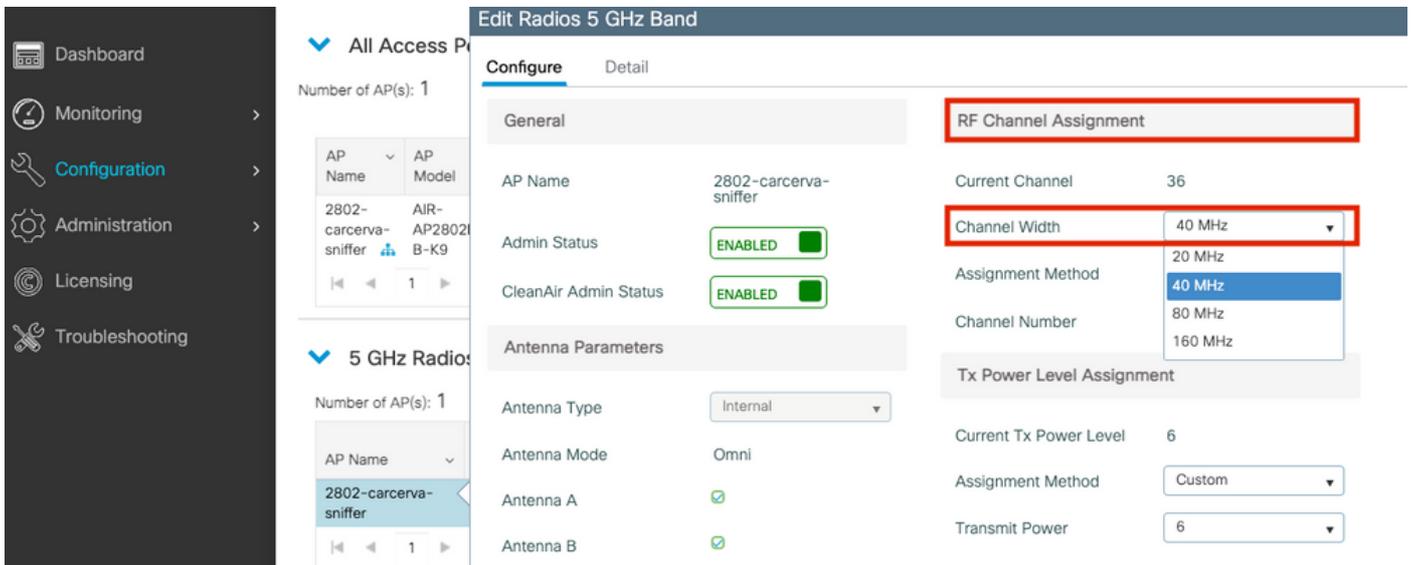
Sniffer IP Status: Valid

Download [Core Dump](#) to bootflash

Cancel

Paso 5. Seleccione el ancho de canal que el dispositivo de destino y el AP utilizan cuando están conectados.

Navegue hasta **Configurar > Asignación de Canal RF** para configurar esto, como se muestra en la imagen.



## Configure el AP para escanear un canal a través de CLI

Paso 1. Habilite el sniff del canal en el AP. Ejecute este comando:

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

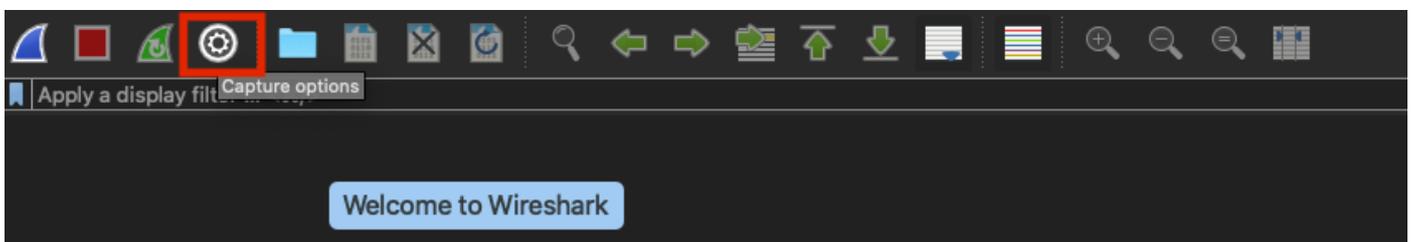
Ejemplo:

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

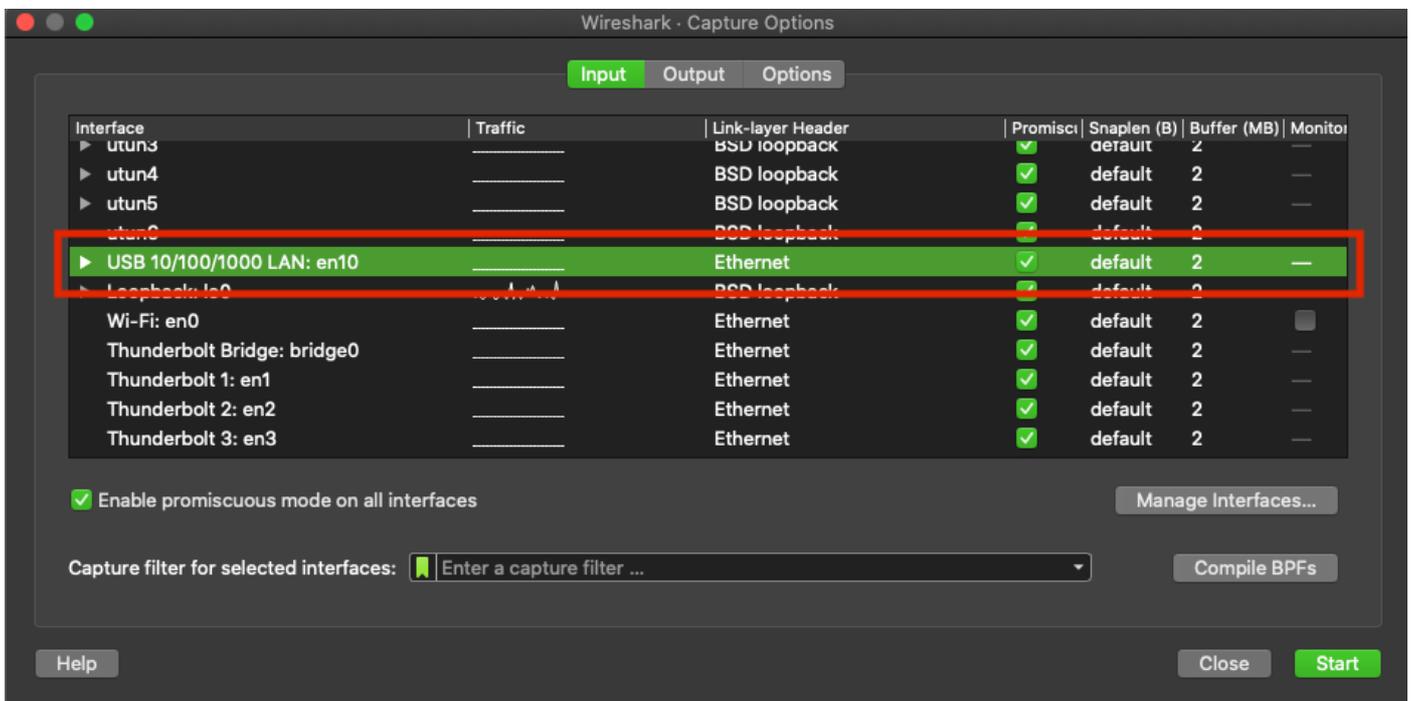
## Configuración de Wireshark para Recopilar la Captura de Paquetes

Paso 1. Inicie Wireshark.

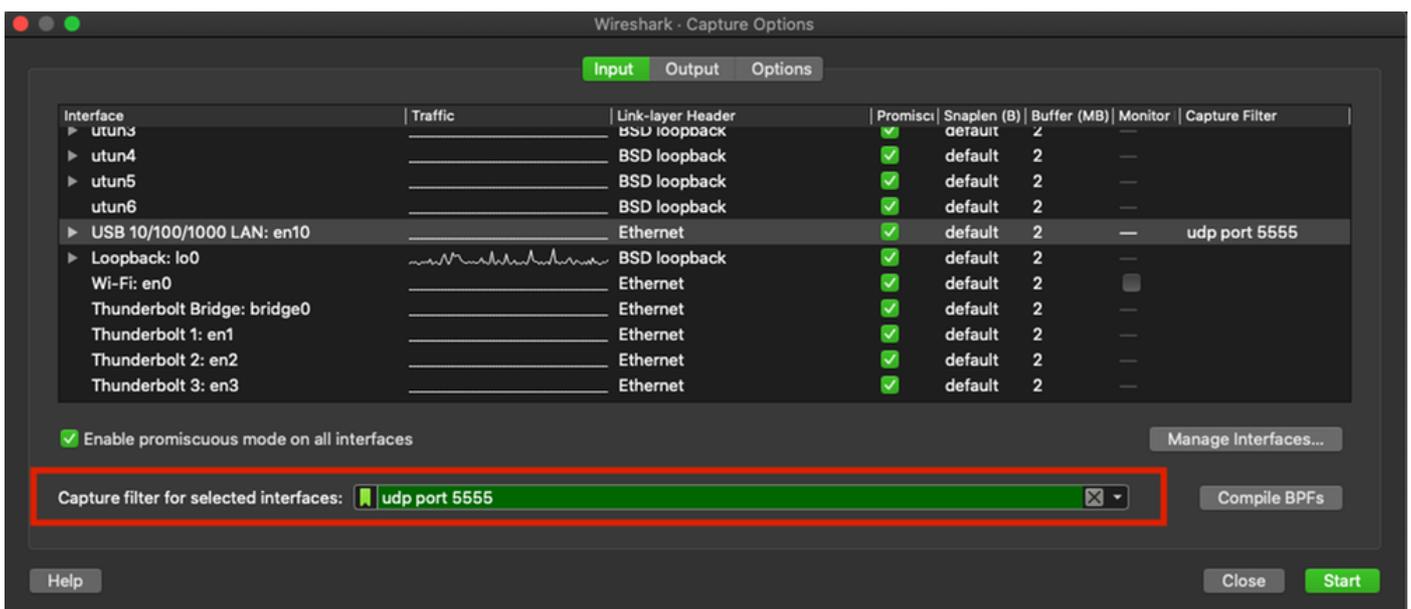
Paso 2. Seleccione el icono del menú **Opciones de captura** de Wireshark, como se muestra en la imagen.



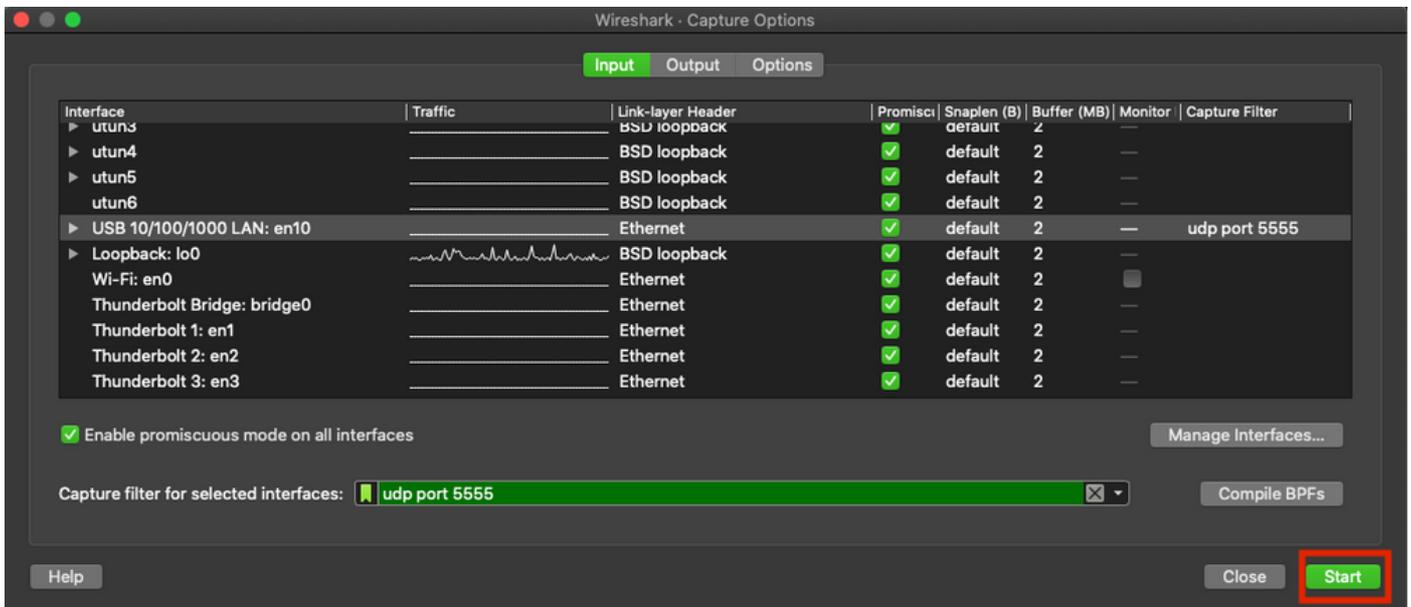
Paso 3. Esta acción muestra una ventana emergente. Seleccione la interfaz con cables de la lista como el origen de la captura, como se muestra en la imagen.



Paso 4. Bajo el filtro Capturar para las interfaces seleccionadas: , escriba **udp port 5555**, como se muestra en la imagen.



Paso 5. Haga clic en Inicio, como se muestra en la imagen.

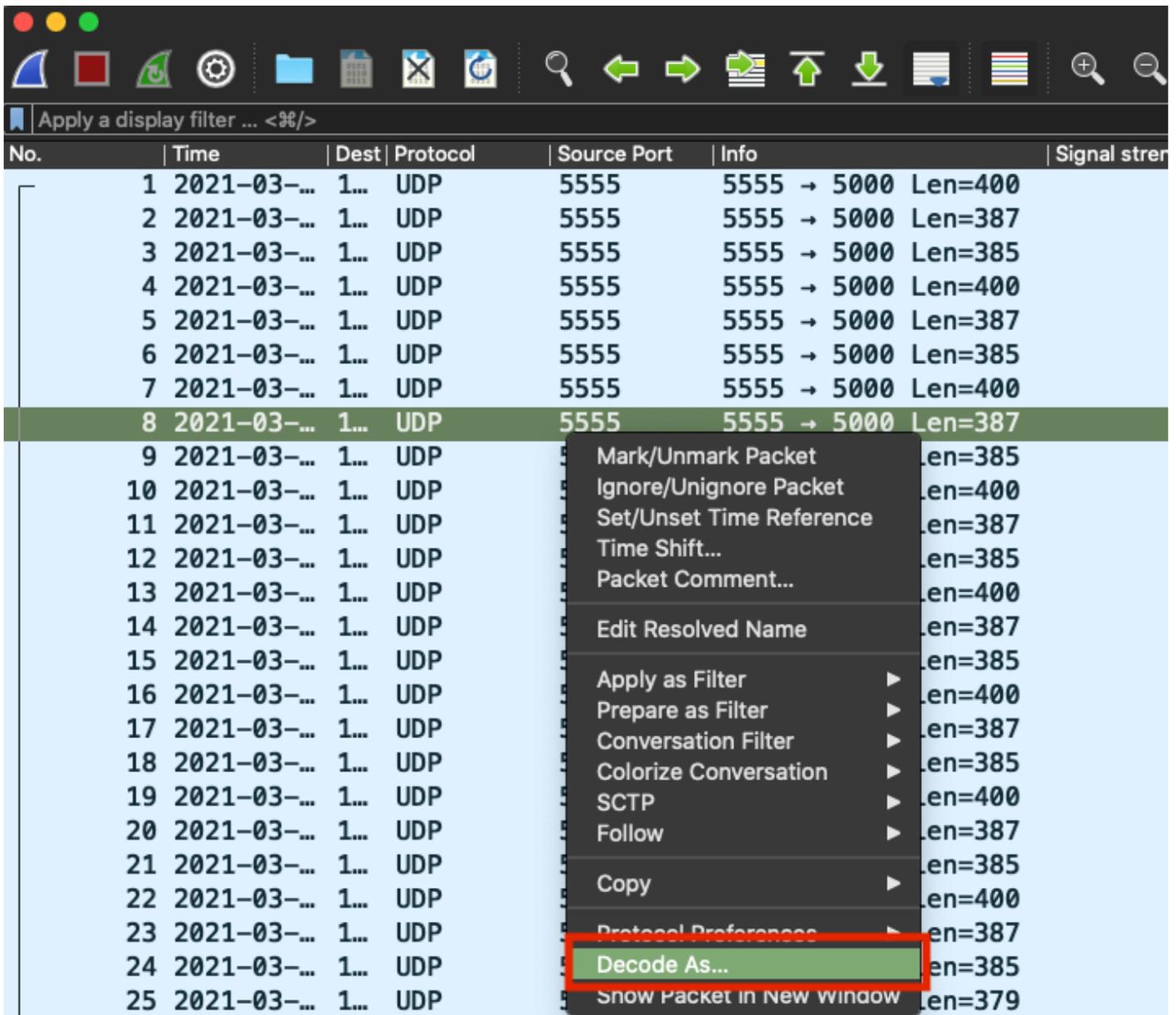


Paso 6. Espere a que Wireshark recopile la información requerida y seleccione el botón **Detener** de Wireshark, como se muestra en la imagen.

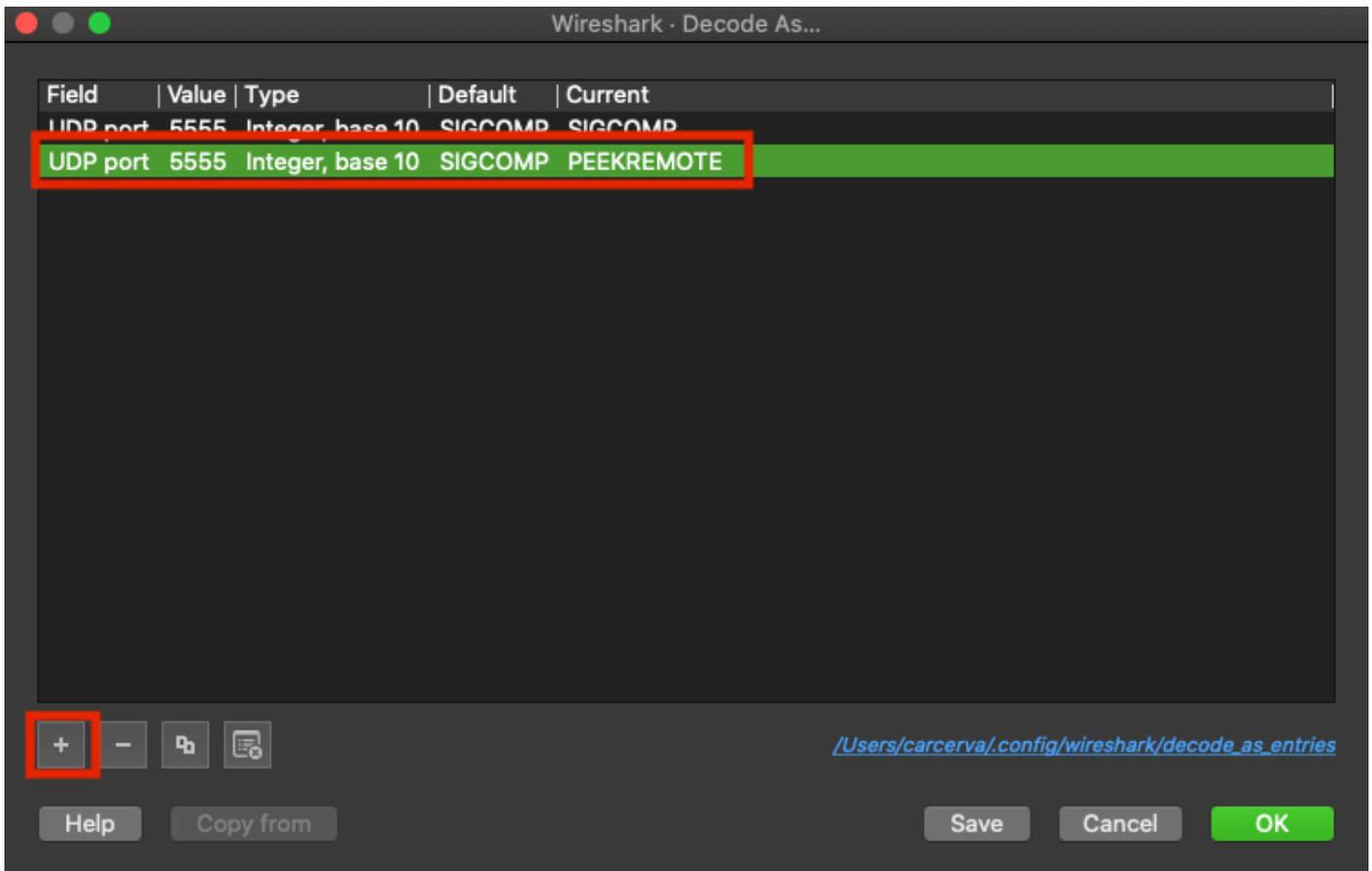


**Consejo:** Si la WLAN utiliza el cifrado como la clave precompartida (PSK), asegúrese de que la captura detecta el intercambio de señales de cuatro direcciones entre el AP y el cliente deseado. Esto se puede hacer si el PCAP OTA se inicia antes de que el dispositivo esté asociado con la WLAN o si el cliente se desautentica y se reautentica mientras se ejecuta la captura.

Paso 7. Wireshark no decodifica los paquetes automáticamente. Para decodificar los paquetes seleccione una línea de la captura, utilice el clic derecho para mostrar las opciones, y seleccione **Decodificar como...**, como se muestra en la imagen.



Paso 8. Aparece una ventana emergente. Seleccione el botón Add (Agregar) y agregue una nueva entrada. Seleccione estas opciones: Puerto UDP de Field, 5555 de Value, SIGCOMP de Default, y PEEKREMOTE de Current, como se muestra en la imagen.



Paso 9. Click OK. Los paquetes se descodifican y están listos para iniciar el análisis.

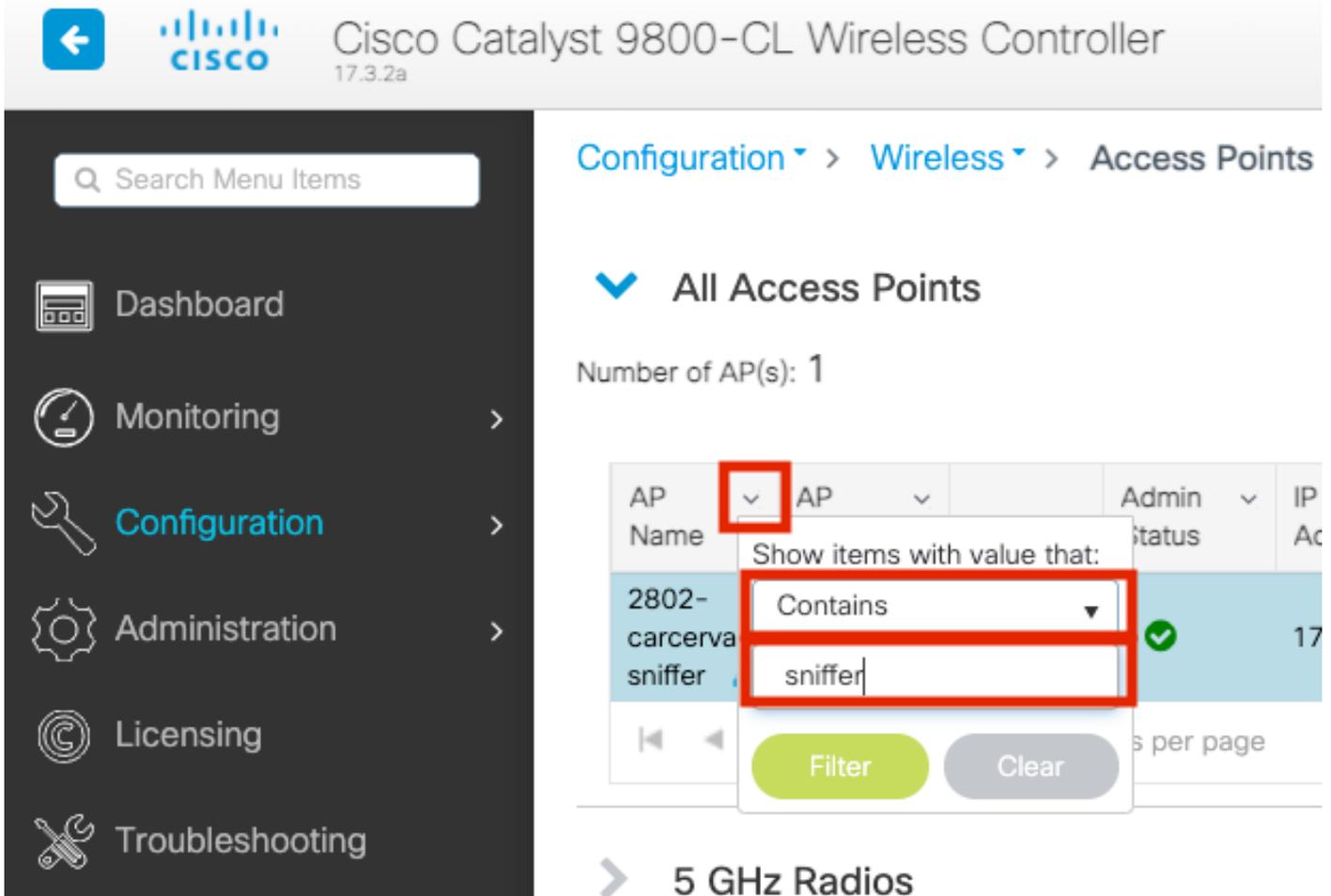
## Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

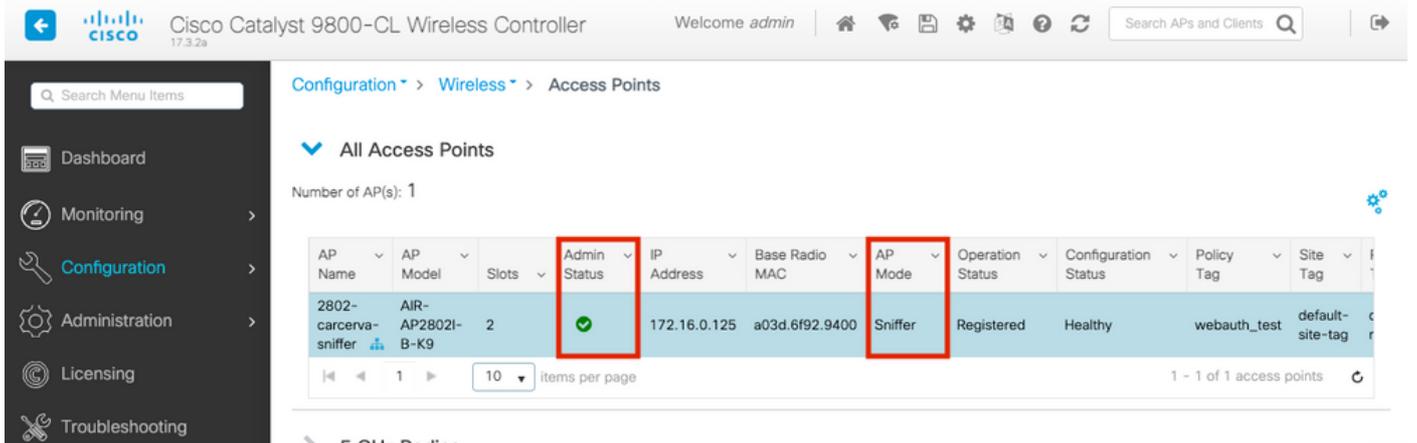
Para confirmar que el AP está en modo Sniffer desde la GUI 9800:

Paso 1. En el 9800 WLC GUI navegue a **Configuration > Wireless > Access Points > All Access Points**.

Paso 2. Busque el AP. Haga clic en el botón de flecha hacia abajo para mostrar la herramienta de búsqueda, seleccione **Contiene** de la lista desplegable y escriba el nombre AP, como se muestra en la imagen.



Paso 3. Verifique que el Estado de administración esté con la marca de verificación en verde y que el Modo AP sea sniffer, como se muestra en la imagen.



Para confirmar que el AP está en el modo Sniffer de la CLI 9800. Ejecute estos comandos:

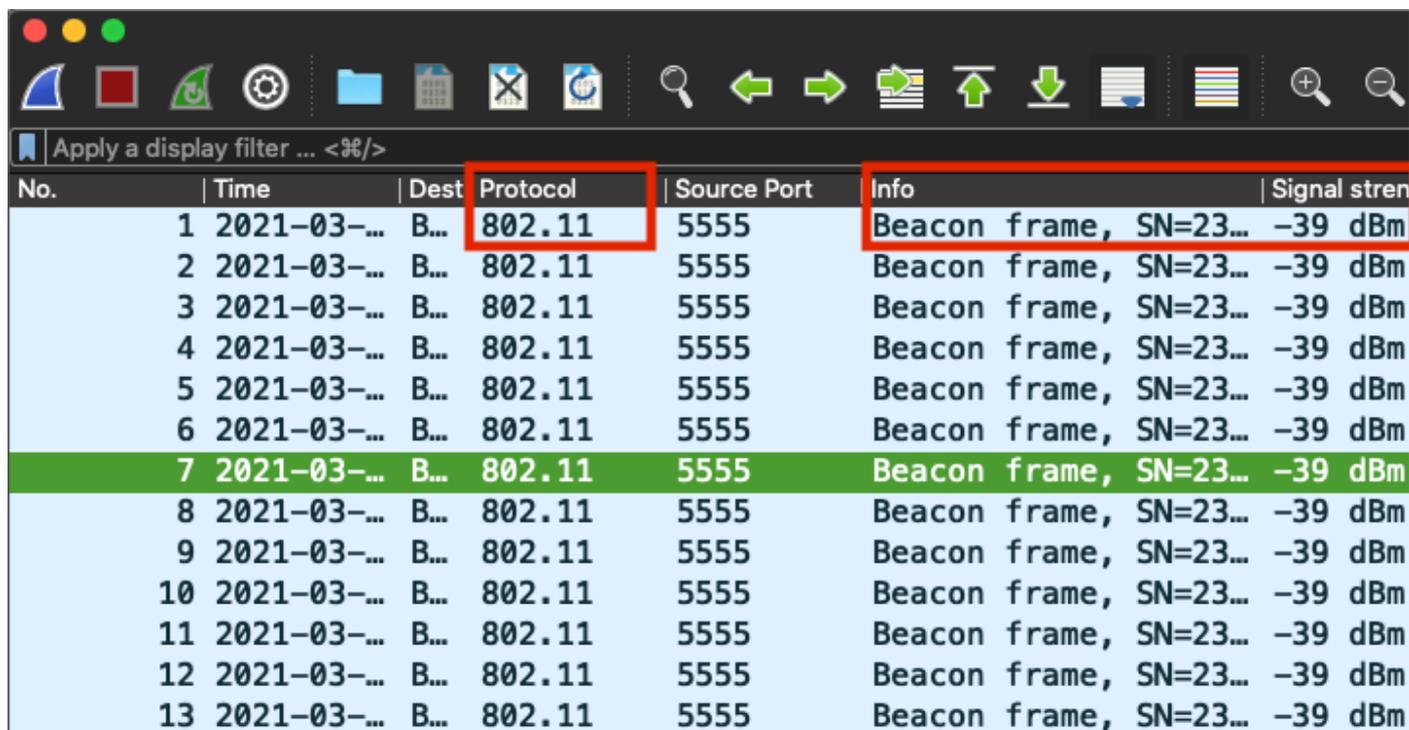
```
carcerva-9k-upg#show ap name 2802-carcerva-sniffer config general | i Administrative
Administrative State : Enabled
```

```
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

Para confirmar que los paquetes se decodifican en Wireshark. El protocolo cambia de UDP a 802.11 y se ven **tramas de baliza**, como se muestra en la imagen.



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

## Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Problema: Wireshark no recibe ningún dato del AP.

Solución: La interfaz de gestión inalámbrica (WMI) debe poder acceder al servidor Wireshark. Confirme el alcance entre el servidor Wireshark y el WMI desde el WLC.

## Información Relacionada

- [Guía de Configuración de Cisco Catalyst 9800 Series Wireless Controller Software, Cisco IOS XE Amsterdam 17.3.x - Capítulo: Modo de sabueso](#)
- [Aspectos básicos de la manipulación inalámbrica 802.11](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)