

# Configurar o ponto de acesso no modo de farejador nos Catalyst 9800 Wireless Controllers

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configurar o AP no modo Sniffer via GUI](#)

[Configurar o AP no modo Sniffer via CLI](#)

[Configurar o AP para digitalizar um canal por meio da GUI](#)

[Configurar o AP para digitalizar um canal via CLI](#)

[Configurar o Wireshark para coletar a captura de pacote](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve como configurar um ponto de acesso (AP) no modo de farejador em um Catalyst 9800 Series Wireless Controller (9800 WLC) por meio da Interface Gráfica de Usuário (GUI) ou da Interface de Linha de Comando (CLI) e como coletar uma Captura de Pacote (PCAP - Packet Capture) Sobre o Ar (OTA - Packet Capture) com o AP de ffer para identificar e identificar problemas e analisar comportamentos sem fio.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de WLC 9800
- Conhecimento básico no padrão 802.11

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

- Wireshark 3.X

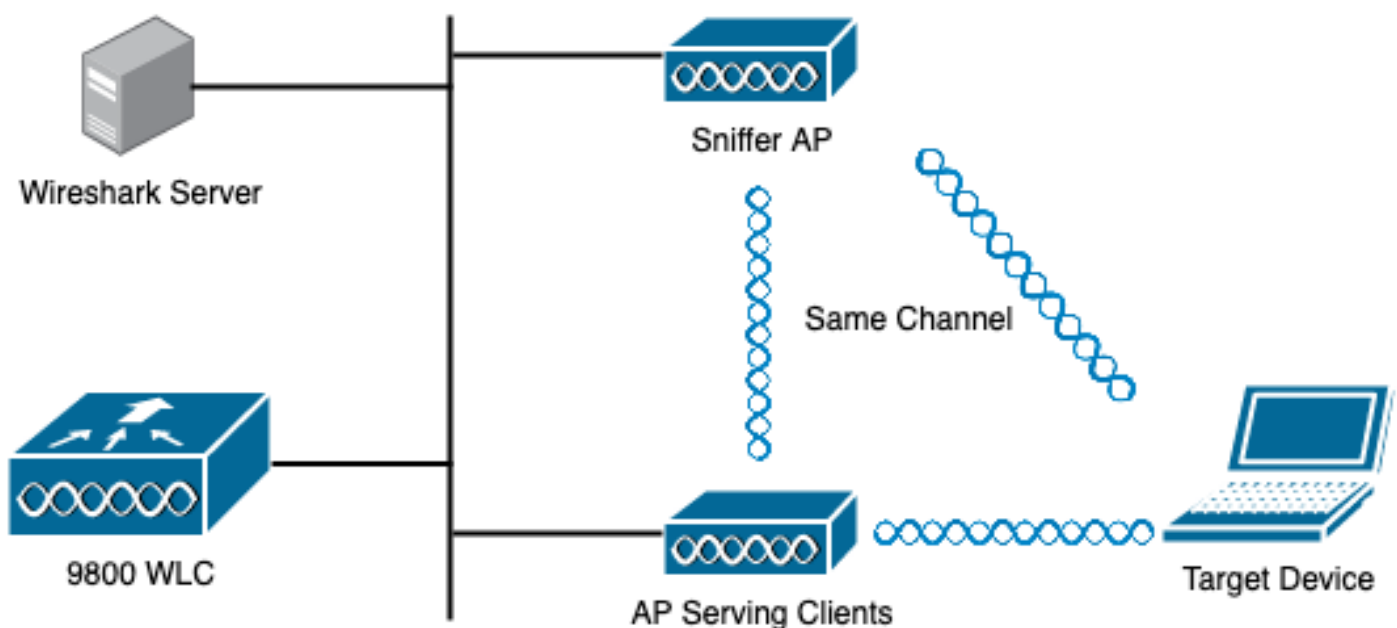
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

Pontos a serem considerados:

- Recomenda-se que o AP do farejador esteja próximo do dispositivo de destino e do AP ao qual esse dispositivo está conectado.
- Certifique-se de saber qual canal e largura 802.11, o dispositivo cliente e o AP usam.

## Diagrama de Rede



## Configurações

### Configurar o AP no modo Sniffer via GUI

Etapa 1. Na GUI do 9800 WLC, navegue para **Configuration > Wireless > Access Points > All Access Points**, como mostrado na imagem.



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

Etapa 2. Selecione o AP desejado para ser usado no modo sniffer. Na guia **Geral**, atualize o nome do AP, como mostrado na imagem.

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
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

Etapa 3. Verifique se **Admin Status** está **Habilitado** e altere o **AP Mode** para **Sniffer**, como mostrado na imagem.

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
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**

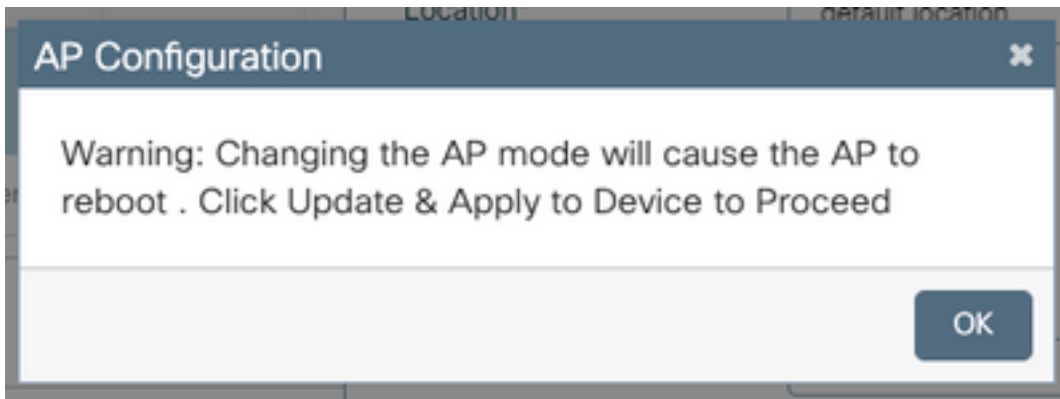
AP Mode Sniffer

Operation Status Registered

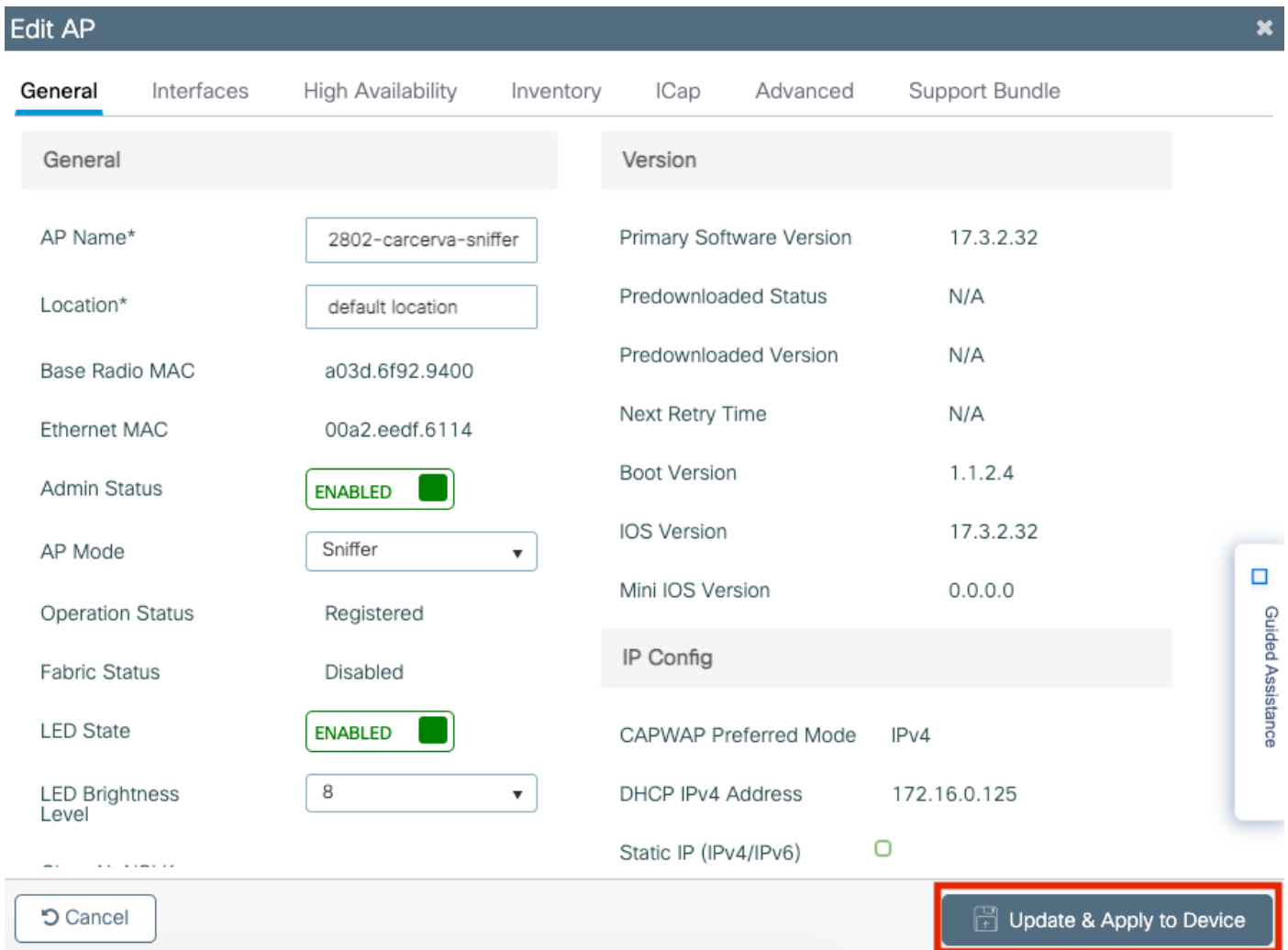
Uma janela pop-up é exibida com a próxima nota:

"aviso: Alterar o modo AP fará com que o AP seja reinicializado. Clique em Atualizar e aplicar ao dispositivo para continuar"

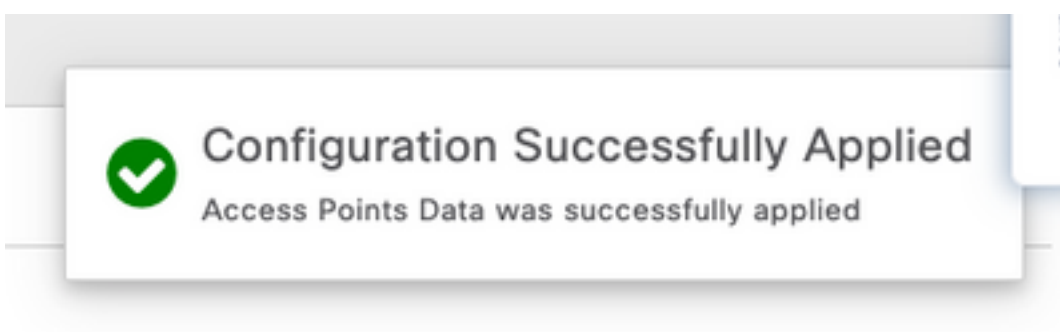
Selecione **OK**, como mostrado na imagem.



Etapa 4. Clique em **Atualizar e aplicar ao dispositivo**, conforme mostrado na imagem.



Um pop-up aparece para confirmar as alterações e o AP reflete, como mostrado na imagem.



## Configurar o AP no modo Sniffer via CLI

Etapa 1. Determine o AP desejado para ser usado como modo de farejador e pegue o nome do AP.

Etapa 2. Modifique o nome do AP.

Esse comando modifica o nome do AP. Onde <AP-name> é o nome atual do AP.

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

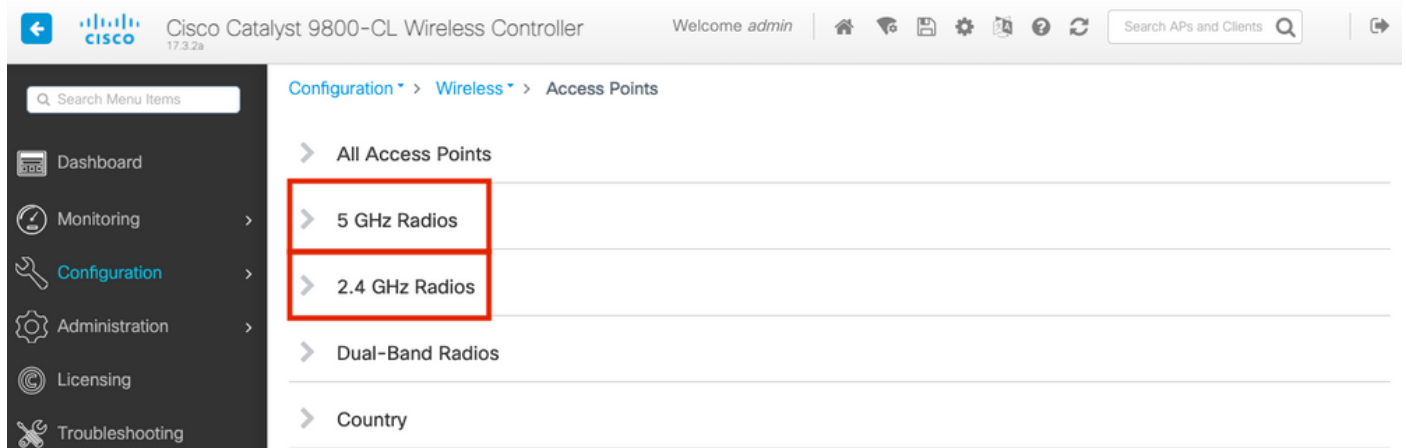
Etapa 3. Configure o AP no modo Sniffer.

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

## Configurar o AP para digitalizar um canal por meio da GUI

Etapa 1. Na GUI do 9800 WLC, navegue para **Configuration > Wireless > Access Points**.

Etapa 2. Na página **Pontos de acesso**, exiba a lista de menus **Rádios de 5 GHz** ou **Rádios de 2,4 GHz**. Isso depende do canal desejado para digitalização, como mostrado na imagem.



Etapa 2. Procure o AP. Clique no botão **seta para baixo** para exibir a ferramenta de pesquisa, selecione **Contém** na lista suspensa e digite o **nome do AP**, como mostrado na imagem.

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

Etapa 3. Marque o AP e marque a caixa de seleção **Enable Sniffer** em **Configure > Sniffer Channel Assignment**, como mostrado na imagem.

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

Etapa 4. Selecione o canal na lista suspensa **Sniff Channel** e digite o **Sniffer IP address** (Server IP address with Wireshark, endereço IP do servidor com Wireshark), como mostrado na imagem.

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 "5 GHz Radios" for the AP "2802-carcerva-sniffer". The "Sniffer Channel Assignment" section is expanded, showing the following settings:

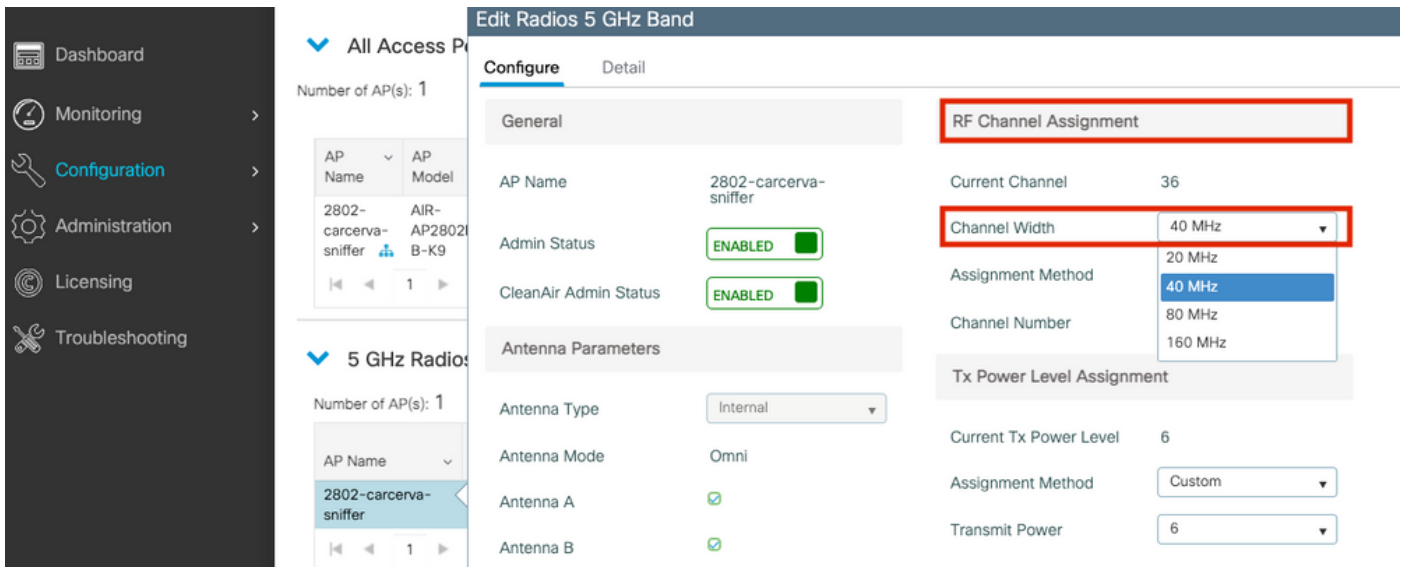
Parameter	Value
Enable Sniffing	<input checked="" type="checkbox"/>
Sniff Channel	36
Sniffer IP*	172.16.0.190
Sniffer IP Status	Valid

Buttons for "Cancel" and "Download Core Dump to bootflash" are visible at the bottom of the configuration panel.

Etapa 5. Selecione a largura do canal que o dispositivo de destino e o AP usam quando conectados.

Navegue até **Configurar > Atribuição de canal RF** para configurar isso, como mostrado na imagem.





## Configurar o AP para digitalizar um canal via CLI

Etapa 1. Ative o farejador de canal no AP. Execute este comando:

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

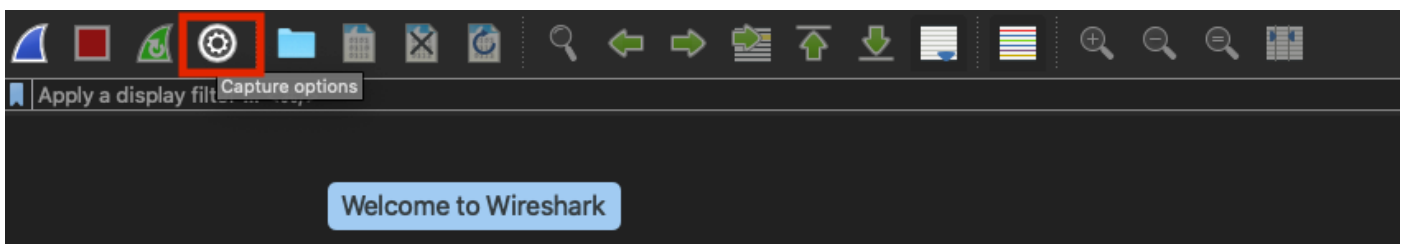
Exemplo:

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

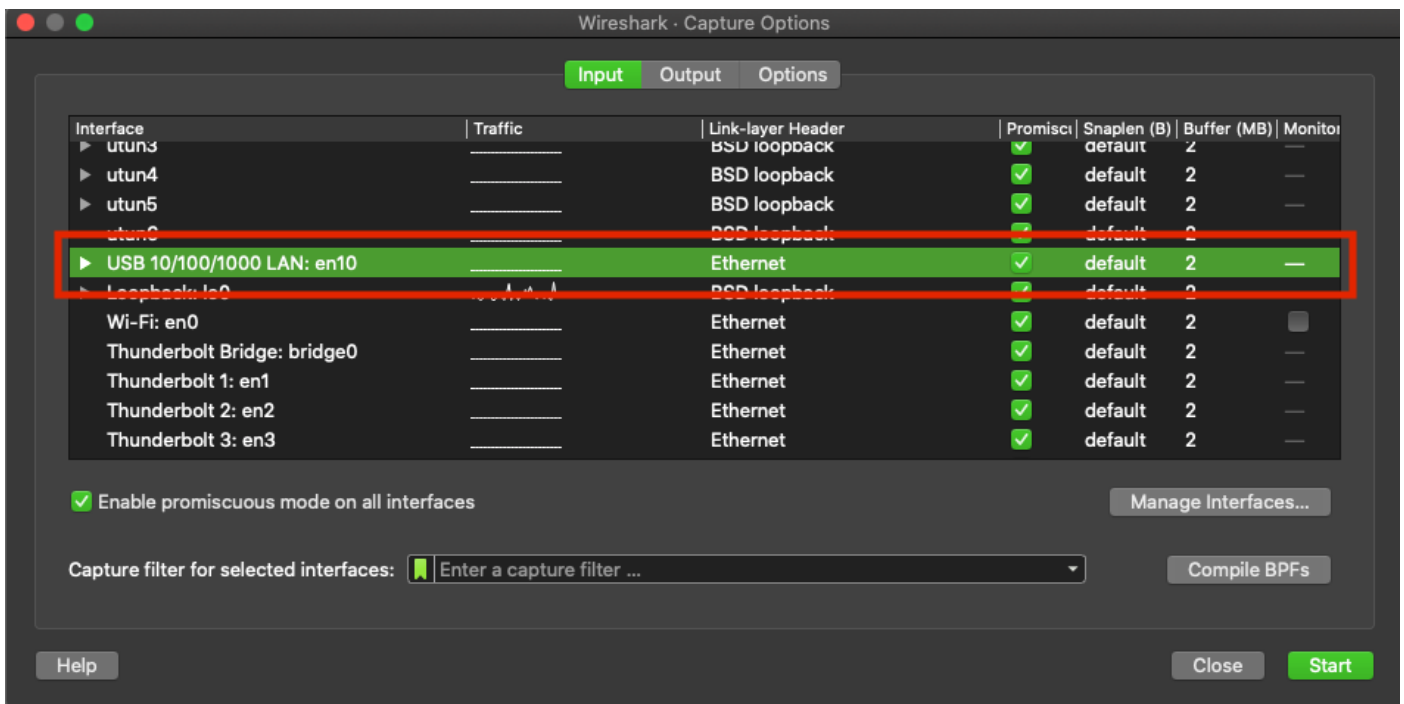
## Configurar o Wireshark para coletar a captura de pacote

Etapa 1. Inicie o Wireshark.

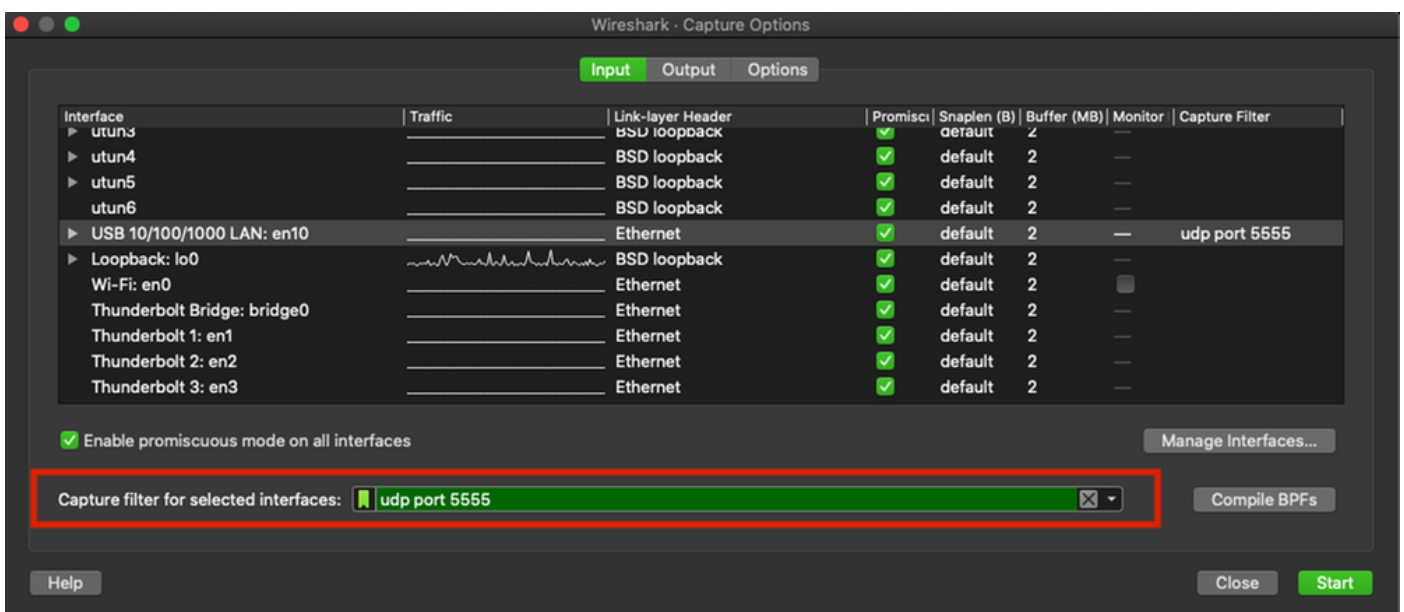
Etapa 2. Selecione o ícone do menu **Capture options** no Wireshark, como mostrado na imagem.



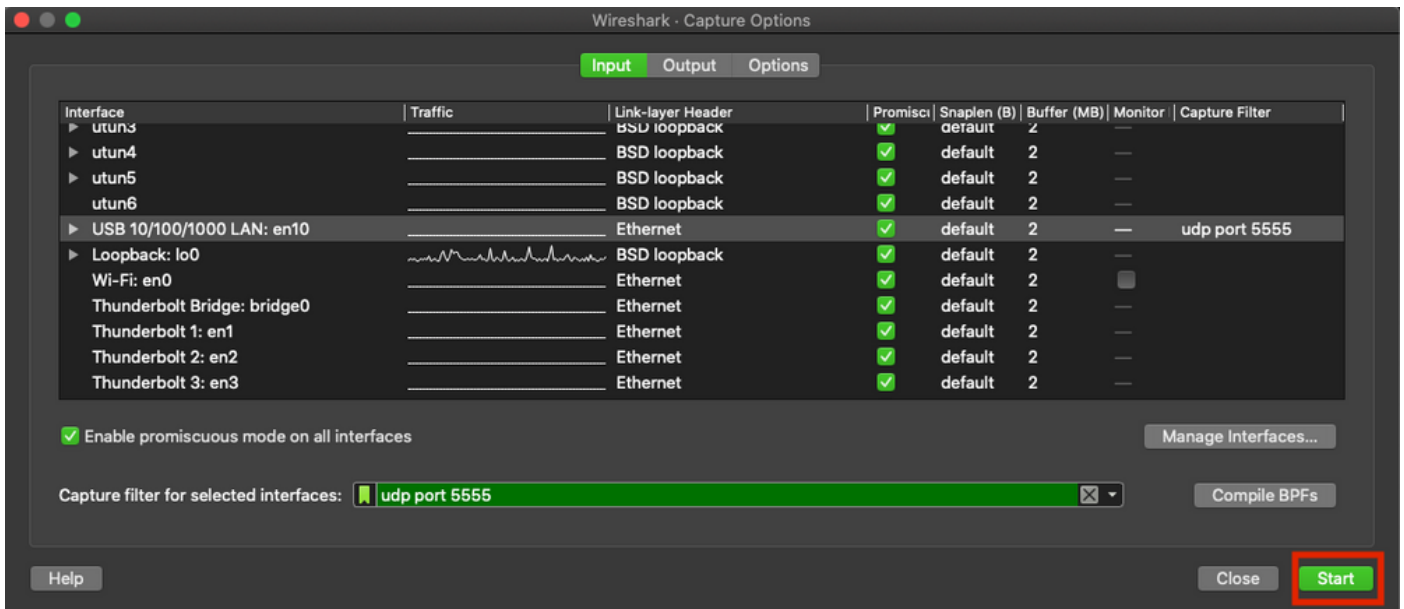
Etapa 3. Esta ação exibe uma janela pop-up. Selecione a Interface com fio na lista como a origem da captura, como mostrado na imagem.



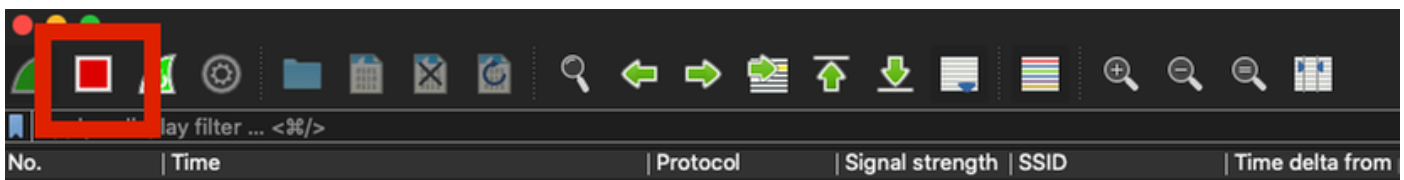
Etapa 4. No filtro Capturar para interfaces selecionadas: caixa de campo, digite udp port 5555, como mostrado na imagem.



Etapa 5. Clique em Iniciar, conforme mostrado na imagem.

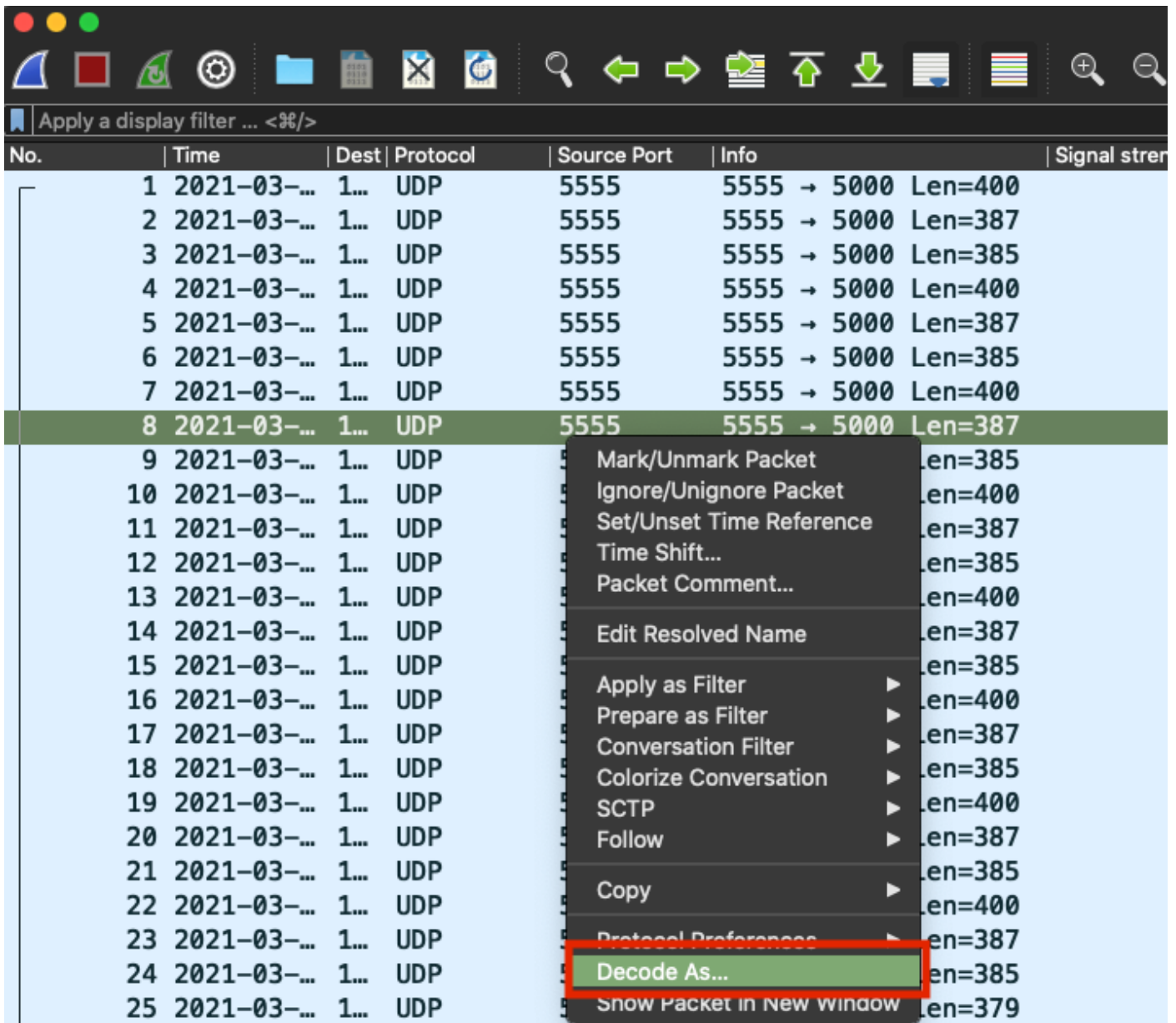


Etapa 6. Aguarde o Wireshark coletar as informações necessárias e selecione o botão **Parar** no Wireshark, como mostrado na imagem.

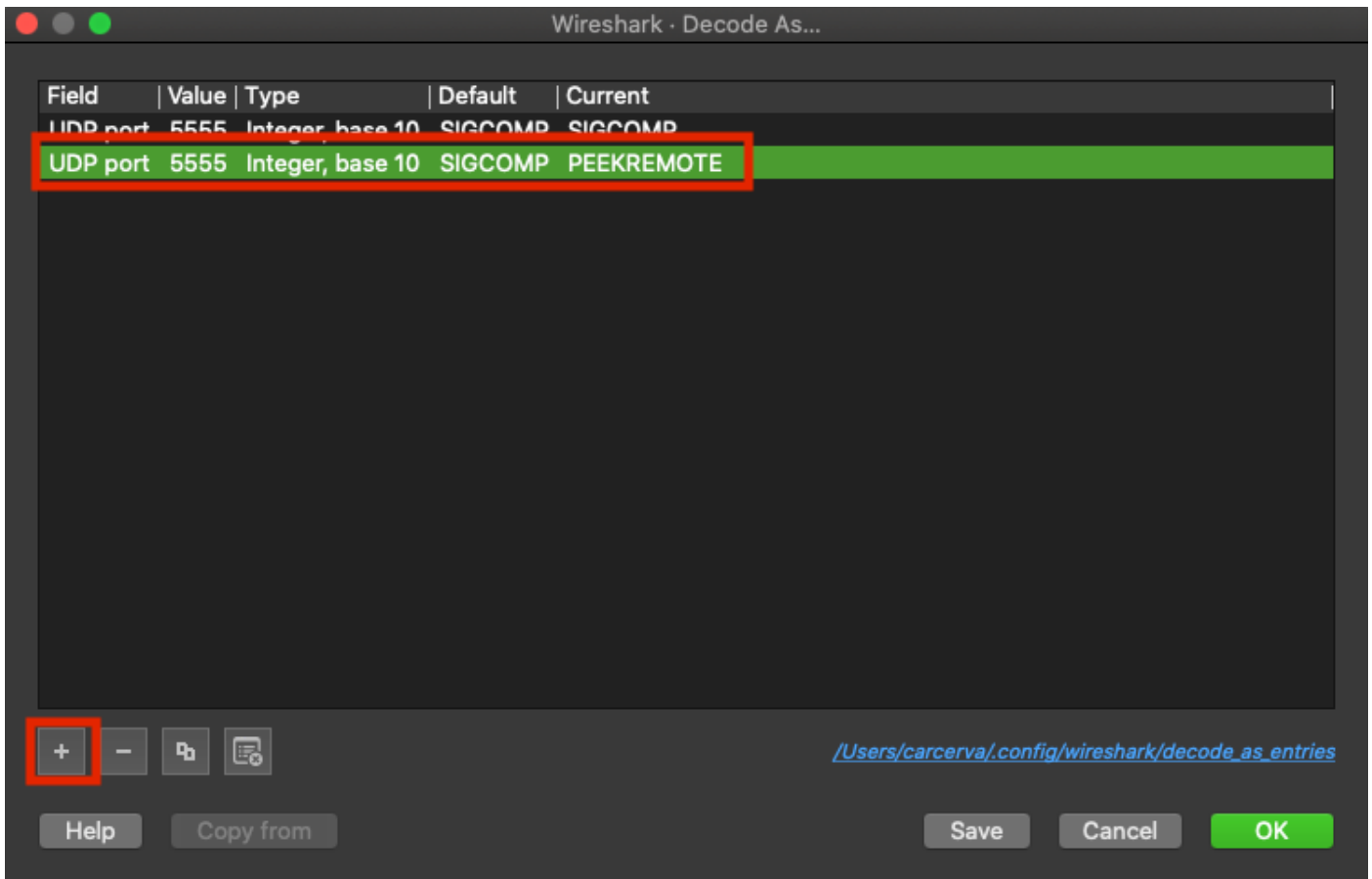


**Tip:** Se a WLAN usar criptografia como chave pré-compartilhada (PSK), assegure-se de que a captura capture o handshake de quatro vias entre o AP e o cliente desejado. Isso pode ser feito se o PCAP OTA for iniciado antes do dispositivo ser associado à WLAN ou se o cliente for desautenticado e reautenticado enquanto a captura é executada.

Passo 7. O Wireshark não decodifica os pacotes automaticamente. Para decodificar os pacotes, selecione uma linha da captura, clique com o botão direito do mouse para exibir as opções e selecione **Decodificar como...**, como mostrado na imagem.



Etapa 8. Uma janela pop-up é exibida. Selecione o botão adicionar e adicione uma nova entrada, selecione estas opções: **Porta UDP do Field, 5555 from Value, SIGCOMP from Default e PEEKREMOTE from Current**, como mostrado na imagem.



Etapa 9. Click **OK**. Os pacotes são decodificados e estão prontos para iniciar a análise.

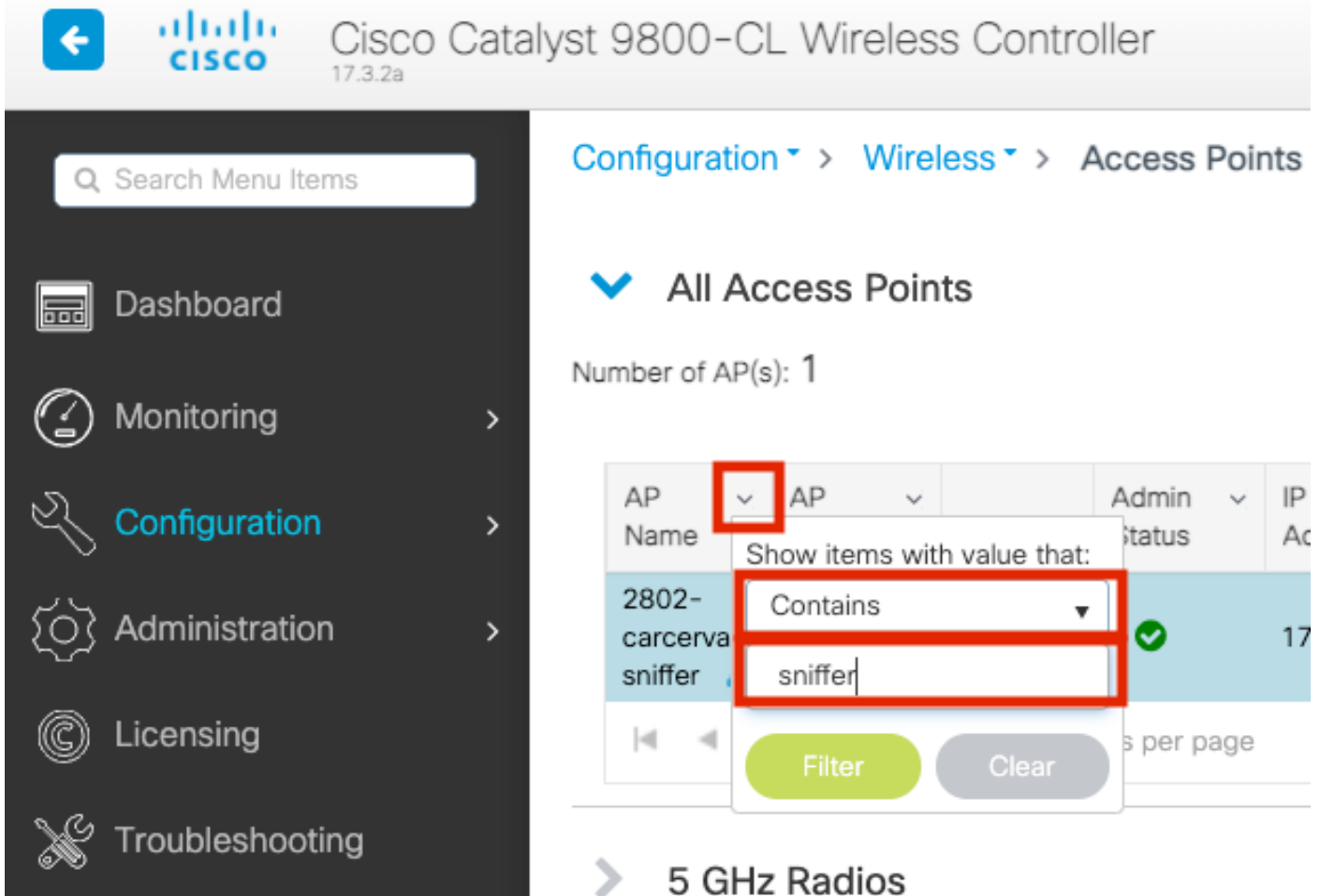
## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

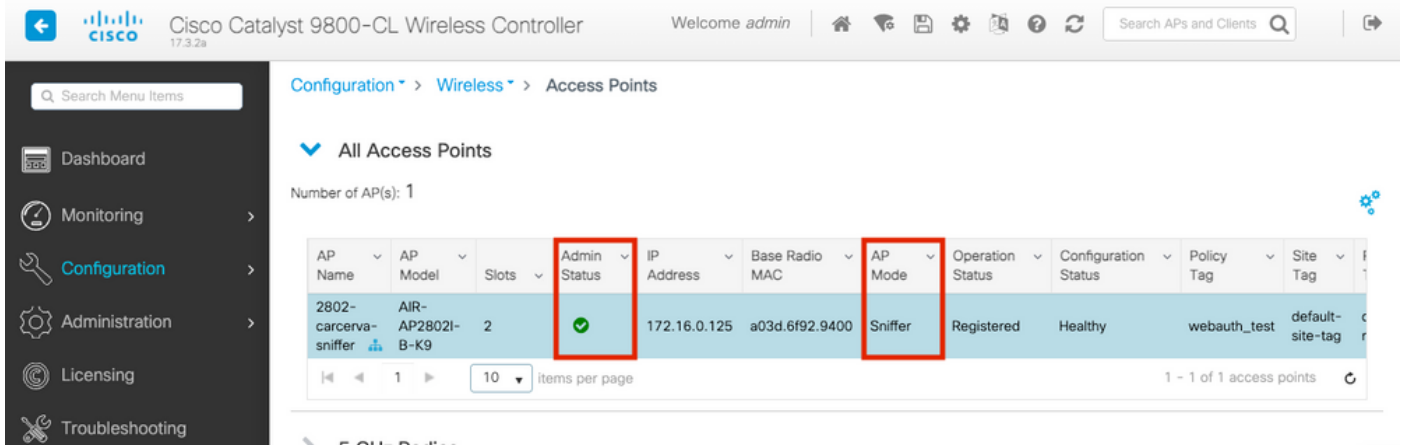
Para confirmar se o AP está no modo Sniffer na GUI do 9800:

Etapa 1. Na GUI do 9800 WLC, navegue para **Configuration > Wireless > Access Points > All Access Points**.

Etapa 2. Procure o AP. Clique no botão de seta para baixo para exibir a ferramenta de pesquisa, selecione **Contém** na lista suspensa e digite o nome do AP, como mostrado na imagem.



Etapa 3. Verifique se o **status Admin** está com a **marca de seleção em verde** e se o modo AP é **Sniffer**, como mostrado na imagem.



Para confirmar se o AP está no modo Sniffer da CLI 9800. Execute estes comandos:

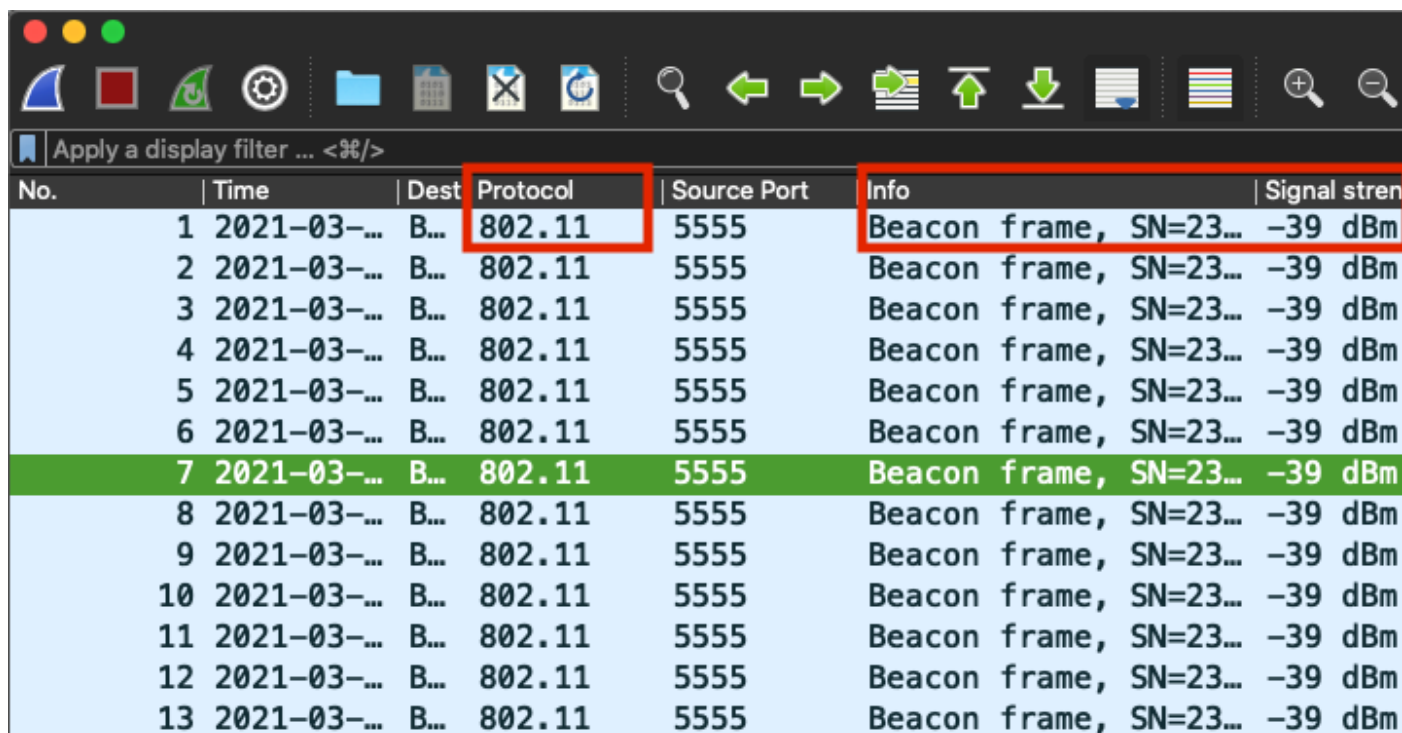
```
carcerva-9k-upg#show ap name 2802-carcerva-sniffer config general | i Administrative
Administrative State : Enabled
```

```
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 se os pacotes estão decodificados no Wireshark. O protocolo muda de **UDP** para **802.11** e há quadros **Beacon**, como mostrado na imagem.



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

Esta seção disponibiliza informações para a solução de problemas de configuração.

Problema: O Wireshark não recebe nenhum dado do AP.

Solução: O servidor do Wireshark deve estar acessível pela Interface de Gerenciamento Sem Fio (WMI - Wireless Management Interface). Confirme a acessibilidade entre o servidor Wireshark e a WMI da WLC.

## Informações Relacionadas

- [Guia de configuração do software Cisco Catalyst 9800 Series Wireless Controller, Cisco IOS XE Amsterdam 17.3.x - Capítulo: Modo de farejador](#)
- [Fundamentos do 802.11 Wireless Sniffing](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)