

# Konfigurieren des Access Points im Sniffer-Modus auf den Catalyst Wireless Controllern der Serie 9800

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfiguration](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Konfigurieren des Access Points im Sniffer-Modus über die GUI](#)

[Konfigurieren des Access Points im Sniffer-Modus über die CLI](#)

[Konfigurieren des AP zum Scannen eines Kanals über die Benutzeroberfläche](#)

[Konfigurieren des AP zum Scannen eines Kanals über die CLI](#)

[Konfigurieren von Wireshark zum Erfassen der Paketerfassung](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird beschrieben, wie Sie einen Access Point (AP) im Sniffer-Modus auf einem Catalyst Wireless Controller der Serie 9800 (9800 WLC) über die grafische Benutzeroberfläche (GUI) oder die Befehlszeilenschnittstelle (CLI) konfigurieren und eine Packet Capture (PCAP) Over the Air (OTA) mit dem Sniffer AP erfassen, um Fehler zu beheben und das Verhalten von Wireless-Geräten zu analysieren.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration des 9800 WLC
- Grundkenntnisse des 802.11-Standards

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- AP 2802
- 9800 WLC Cisco IOS®-XE Version 17.3.2a
- Wireshark 3.x

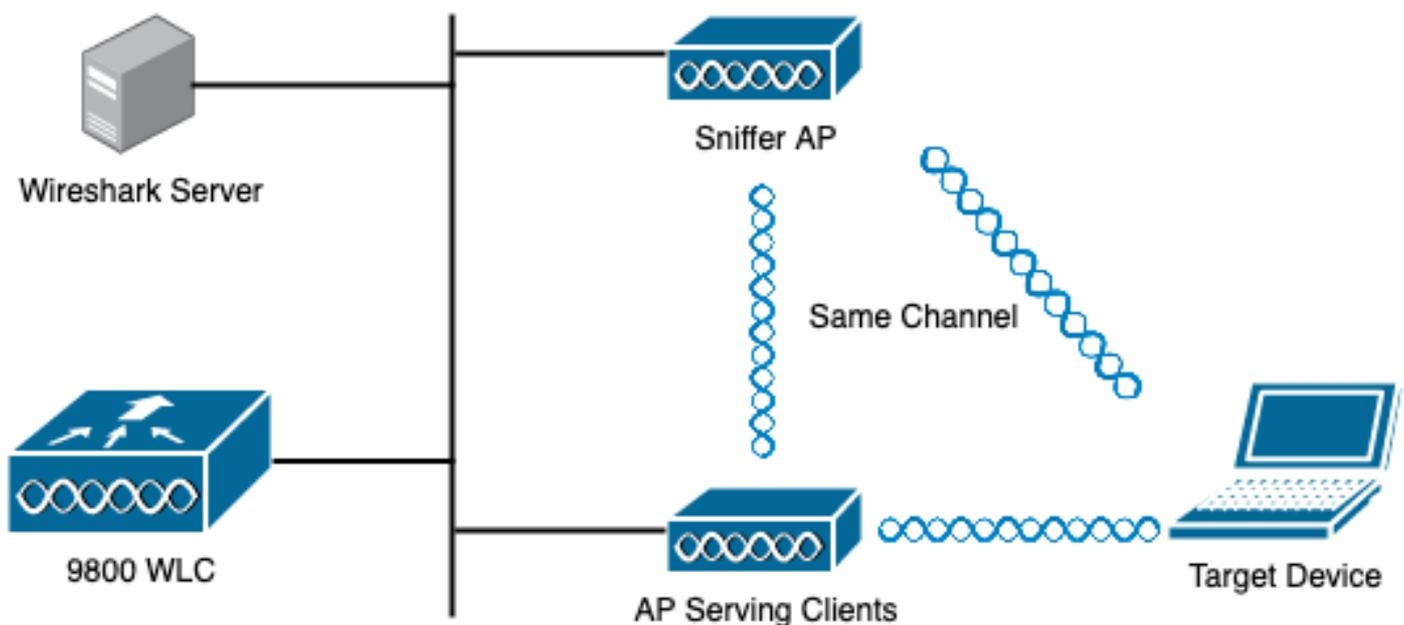
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konfiguration

Wichtige Punkte:

- Es wird empfohlen, den Sniffer-Access Point in der Nähe des Zielgeräts und des AP zu haben, mit dem das Gerät verbunden ist.
- Stellen Sie sicher, dass Sie wissen, welche 802.11-Kanäle und welche Breite, welches Client-Gerät und welcher AP verwendet werden.

## Netzwerkdiagramm



## Konfigurationen

### Konfigurieren des Access Points im Sniffer-Modus über die GUI

Schritt 1: Navigieren Sie auf der Benutzeroberfläche des 9800 WLC zu **Configuration > Wireless > Access Points > All Access Points (Konfiguration > Wireless > Access Points > Alle Access Points)**, wie im Bild gezeigt.



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

Schritt 2: Wählen Sie den AP aus, der im Sniffer-Modus verwendet werden soll. Aktualisieren Sie auf der Registerkarte **Allgemein** den Namen des Access Points, wie im Bild gezeigt.

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

Schritt 3: Überprüfen Sie, ob der **Admin-Status aktiviert** ist und ändern Sie den **AP-Modus in Sniffer**, wie im Bild gezeigt.

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**

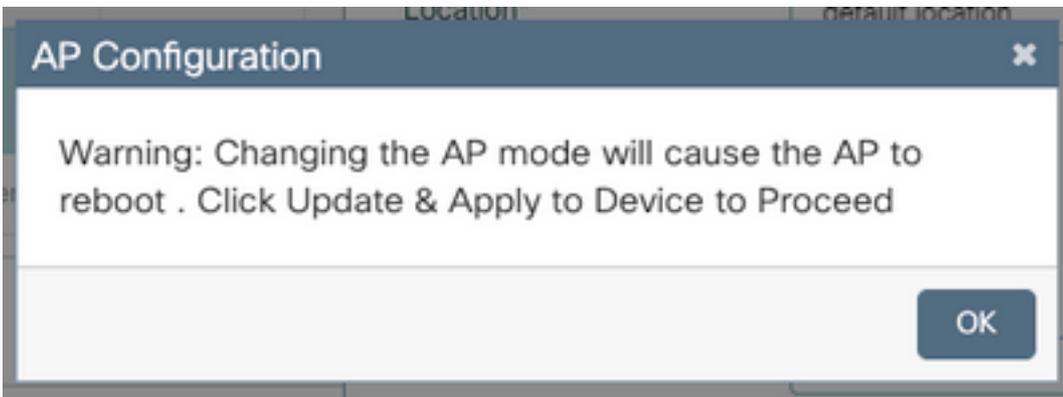
AP Mode Sniffer

Operation Status Registered

Ein Popup-Fenster wird mit dem nächsten Hinweis angezeigt:

"Warnung: Wenn Sie den AP-Modus ändern, wird der Access Point neu gestartet. Klicken Sie auf Aktualisieren und auf Gerät anwenden, um fortzufahren."

Wählen Sie **OK**, wie im Bild gezeigt.



Schritt 4: Klicken Sie auf **Aktualisieren und auf Gerät anwenden**, wie im Bild gezeigt.

Edit AP

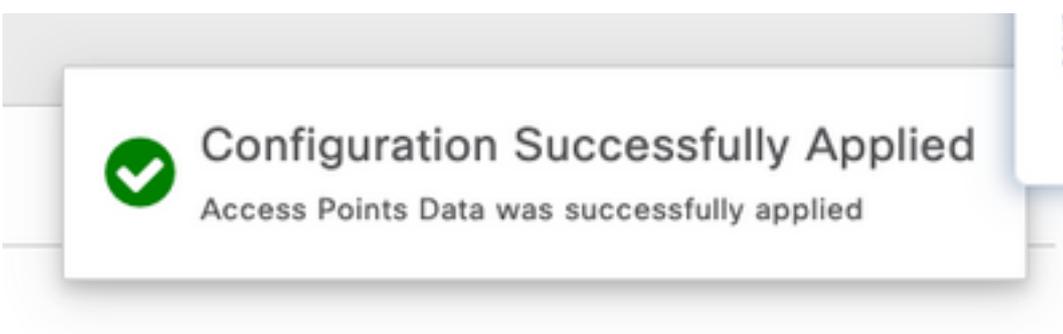
General Interfaces High Availability Inventory ICap Advanced Support Bundle

General		Version	
AP Name*	2802-carcerva-sniffer	Primary Software Version	17.3.2.32
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	a03d.6f92.9400	Predownloaded Version	N/A
Ethernet MAC	00a2.eedf.6114	Next Retry Time	N/A
Admin Status	ENABLED <input checked="" type="checkbox"/>	Boot Version	1.1.2.4
AP Mode	Sniffer ▼	IOS Version	17.3.2.32
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	IP Config	
LED State	ENABLED <input checked="" type="checkbox"/>	CAPWAP Preferred Mode	IPv4
LED Brightness Level	8 ▼	DHCP IPv4 Address	172.16.0.125
		Static IP (IPv4/IPv6)	<input type="checkbox"/>

Cancel Update & Apply to Device

Guided Assistance

Ein Popup-Fenster wird angezeigt, um die Änderungen zu bestätigen und der Access Point springt, wie im Bild gezeigt.



## Konfigurieren des Access Points im Sniffer-Modus über die CLI

Schritt 1: Bestimmen Sie den AP, der als Sniffer-Modus verwendet werden soll, und greifen Sie den AP-Namen zu.

Schritt 2: Ändern Sie den Namen des Access Points.

Mit diesem Befehl wird der AP-Name geändert. wobei <AP-Name> der aktuelle Name des Access Points ist.

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

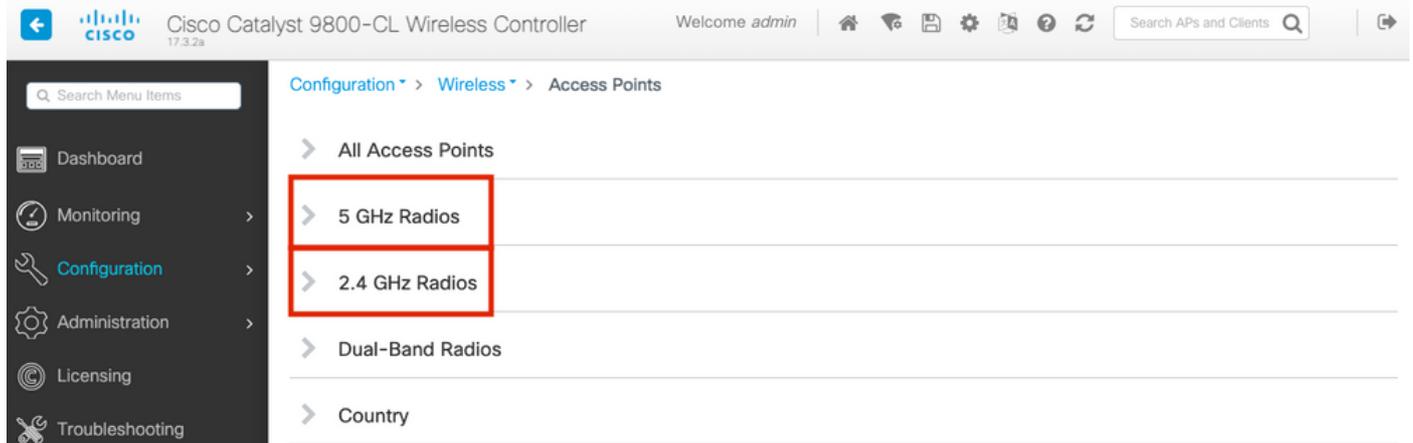
Schritt 3: Konfigurieren Sie den Access Point im Sniffer-Modus.

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

## Konfigurieren des AP zum Scannen eines Kanals über die Benutzeroberfläche

Schritt 1: Navigieren Sie in der Benutzeroberfläche des 9800 WLC zu **Configuration > Wireless > Access Points (Konfiguration > Wireless > Access Points)**.

Schritt 2: Zeigen Sie auf der Seite **Access Points** die Menüliste **5-GHz-Funkmodule** oder **2,4-GHz-Funkmodule an**. Dies hängt vom Kanal ab, der gescannt werden soll, wie im Bild gezeigt.



Schritt 2: Durchsuchen Sie den Access Point. Klicken Sie auf den **Pfeil nach unten**, um das Suchwerkzeug anzuzeigen, wählen Sie **Container** aus der Dropdown-Liste aus, und geben Sie den **AP-Namen ein**, wie im Bild gezeigt.

Cisco Catalyst 9800-CL Wireless Controller | 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

Schritt 3: Wählen Sie den Access Point aus, und aktivieren Sie das Kontrollkästchen **Enable Sniffer** unter **Configure**> Sniffer Channel Assignment (**Sniffer-Zuweisung aktivieren**), wie im Bild gezeigt.

Cisco Catalyst 9800-CL Wireless Controller | Welcome admin

Configuration > Wireless > Edit Radios 5 GHz Band

All Access Points

5 GHz Radios

Number of AP(s): 1

AP Name "Contains"

AP Name: 2802-carcerva-sniffer

Configure Detail

Antenna Mode	Omni
Antenna A	✓
Antenna B	✓
Antenna C	✓
Antenna D	✓
Antenna Gain	10
<b>Sniffer Channel Assignment</b>	
Enable Sniffing	<input checked="" type="checkbox"/>
Sniff Channel	36
Sniffer IP*	172.16.0.190
Sniffer IP Status	Valid

Download [Core Dump](#) to bootflash

Cancel

Schritt 4: Wählen Sie den Kanal aus der Dropdown-Liste "Sniff Channel" aus, und geben Sie die Sniffer-IP-Adresse (Server-IP-Adresse mit Wireshark) ein, wie im Bild gezeigt.

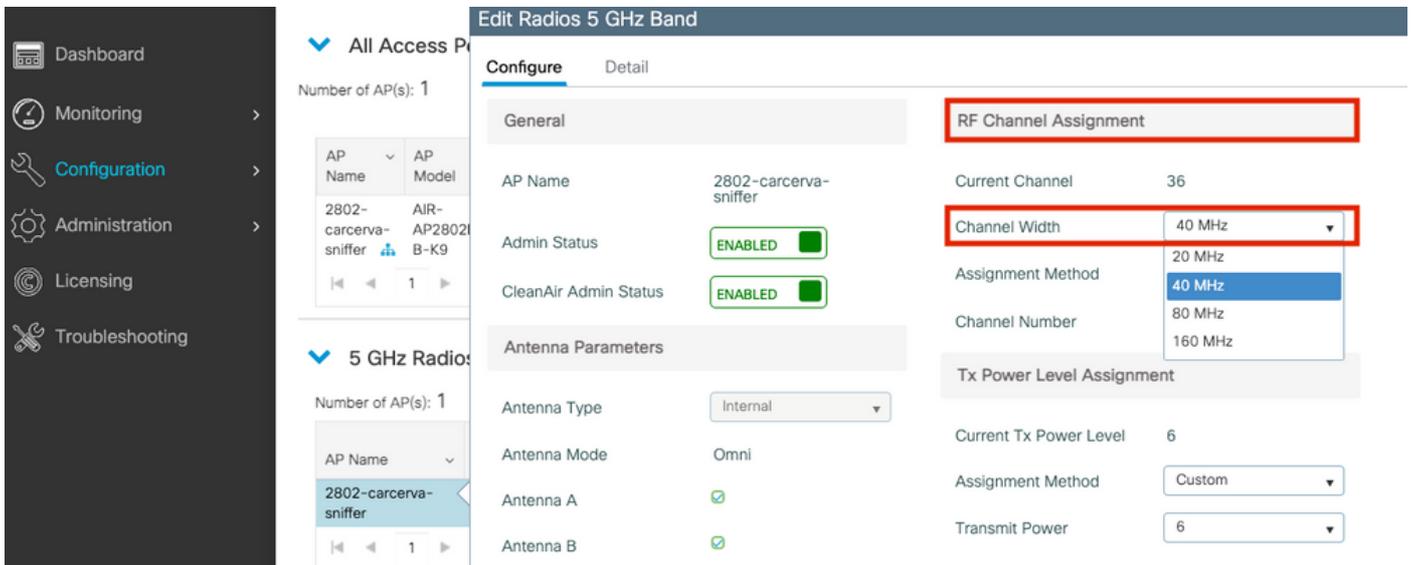
The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration interface. The page title is "Edit Radios 5 GHz Band". The "Configure" tab is selected. The "Sniffer Channel Assignment" section is highlighted, showing the following configuration:

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

The "Sniffer IP Status" is "Valid". There is a "Download Core Dump to bootflash" link. A "Cancel" button is located at the bottom of the configuration area.

Schritt 5: Wählen Sie die Kanalbreite aus, die das Zielgerät und der Access Point beim Anschluss verwenden.

Navigieren Sie zu **Configure > RF Channel Assignment**, um dies zu konfigurieren, wie im Bild gezeigt.



## Konfigurieren des AP zum Scannen eines Kanals über die CLI

Schritt 1: Aktivieren Sie den Kanalschnitt auf dem Access Point. Führen Sie diesen Befehl aus:

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

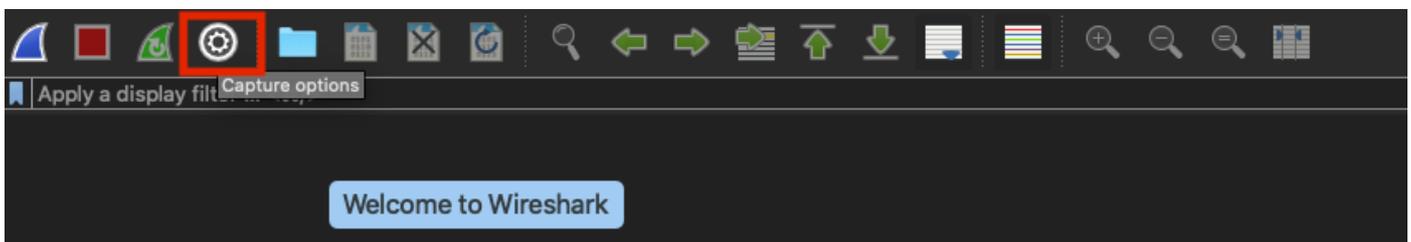
Beispiel:

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

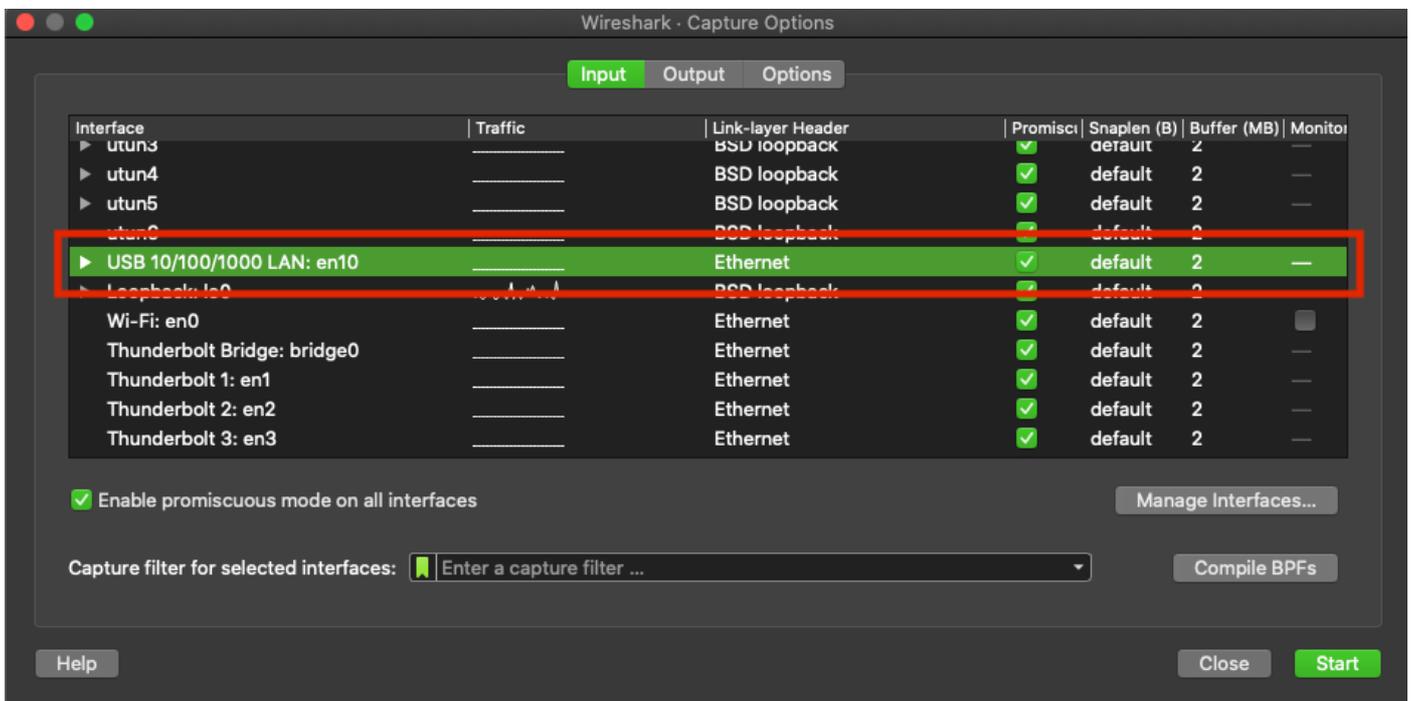
## Konfigurieren von Wireshark zum Erfassen der Paketerfassung

Schritt 1: Starten Sie Wireshark.

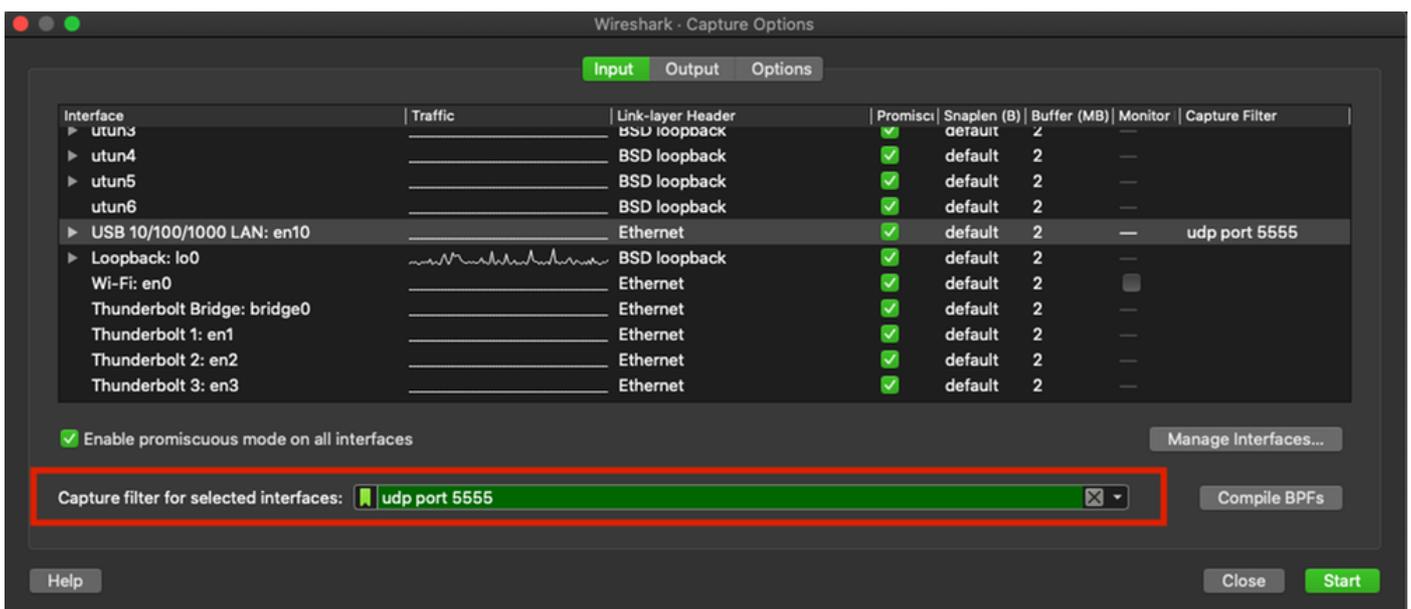
Schritt 2: Wählen Sie das Menüsymbol Capture options aus Wireshark, wie im Bild gezeigt.



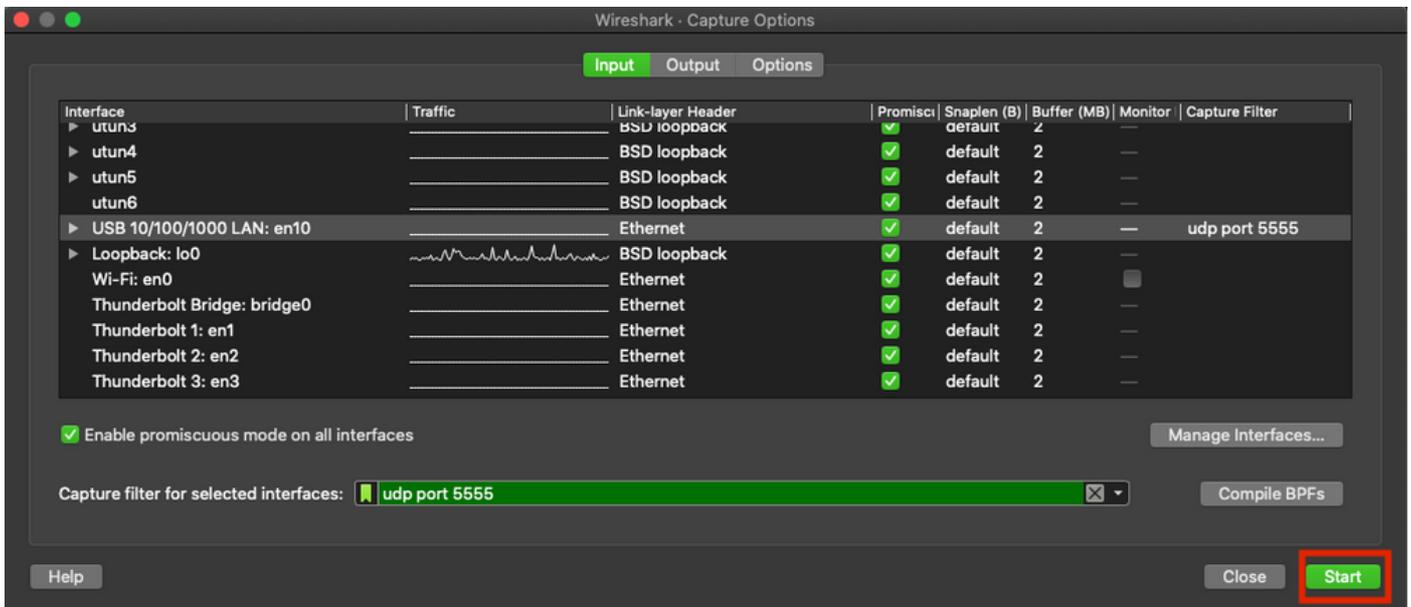
Schritt 3: Bei dieser Aktion wird ein Popup-Fenster angezeigt. Wählen Sie die Kabelschnittstelle aus der Liste als Quelle der Erfassung aus, wie im Bild gezeigt.



Schritt 4: Unter dem Erfassungsfiler für ausgewählte Schnittstellen: Geben Sie udp port 5555 ein, wie im Bild gezeigt.



Schritt 5: Klicken Sie auf **Start**, wie im Bild gezeigt.

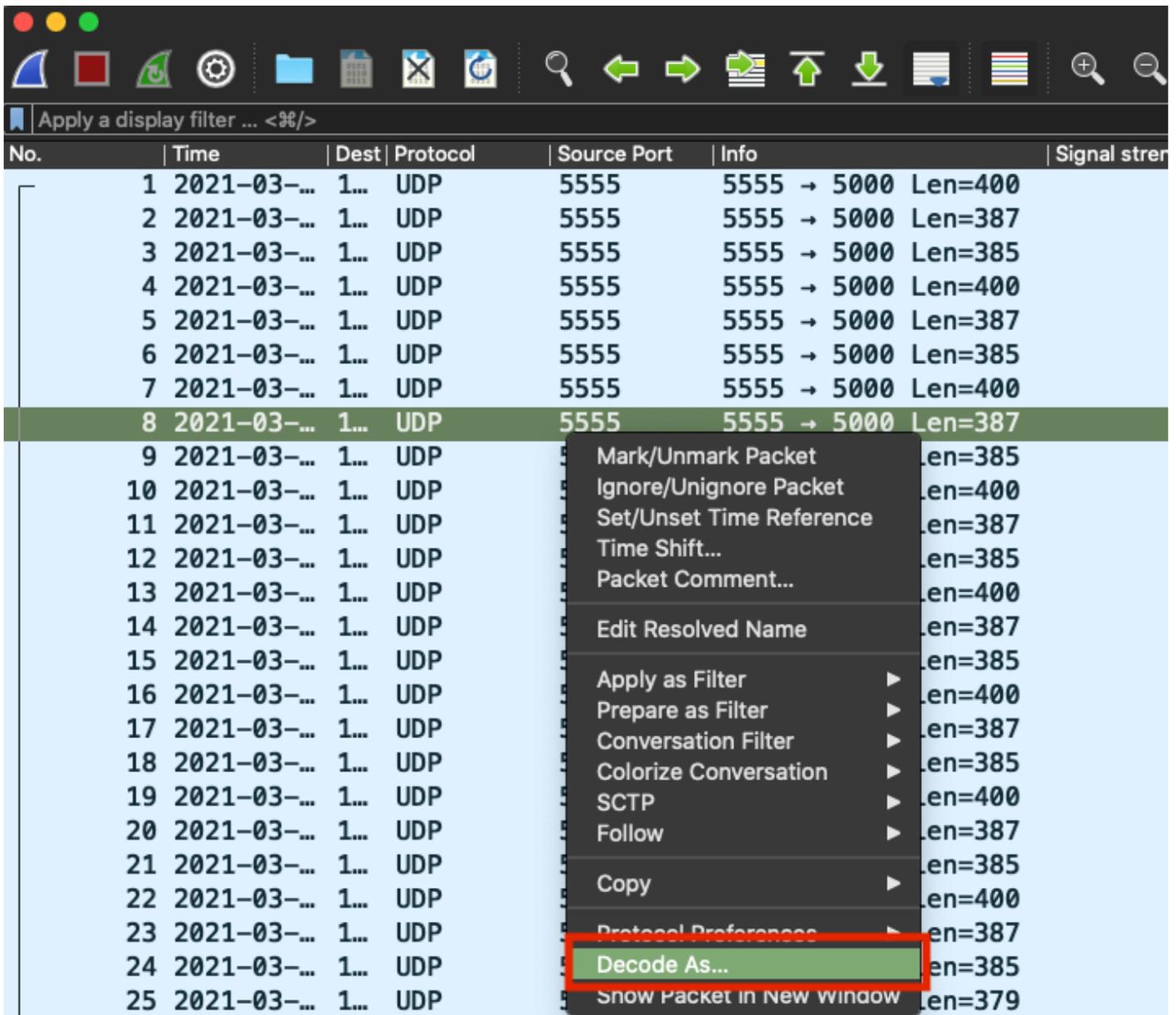


Schritt 6: Warten Sie, bis Wireshark die erforderlichen Informationen erfasst hat, und wählen Sie die **Stopp**-Schaltfläche aus Wireshark aus, wie im Bild gezeigt.

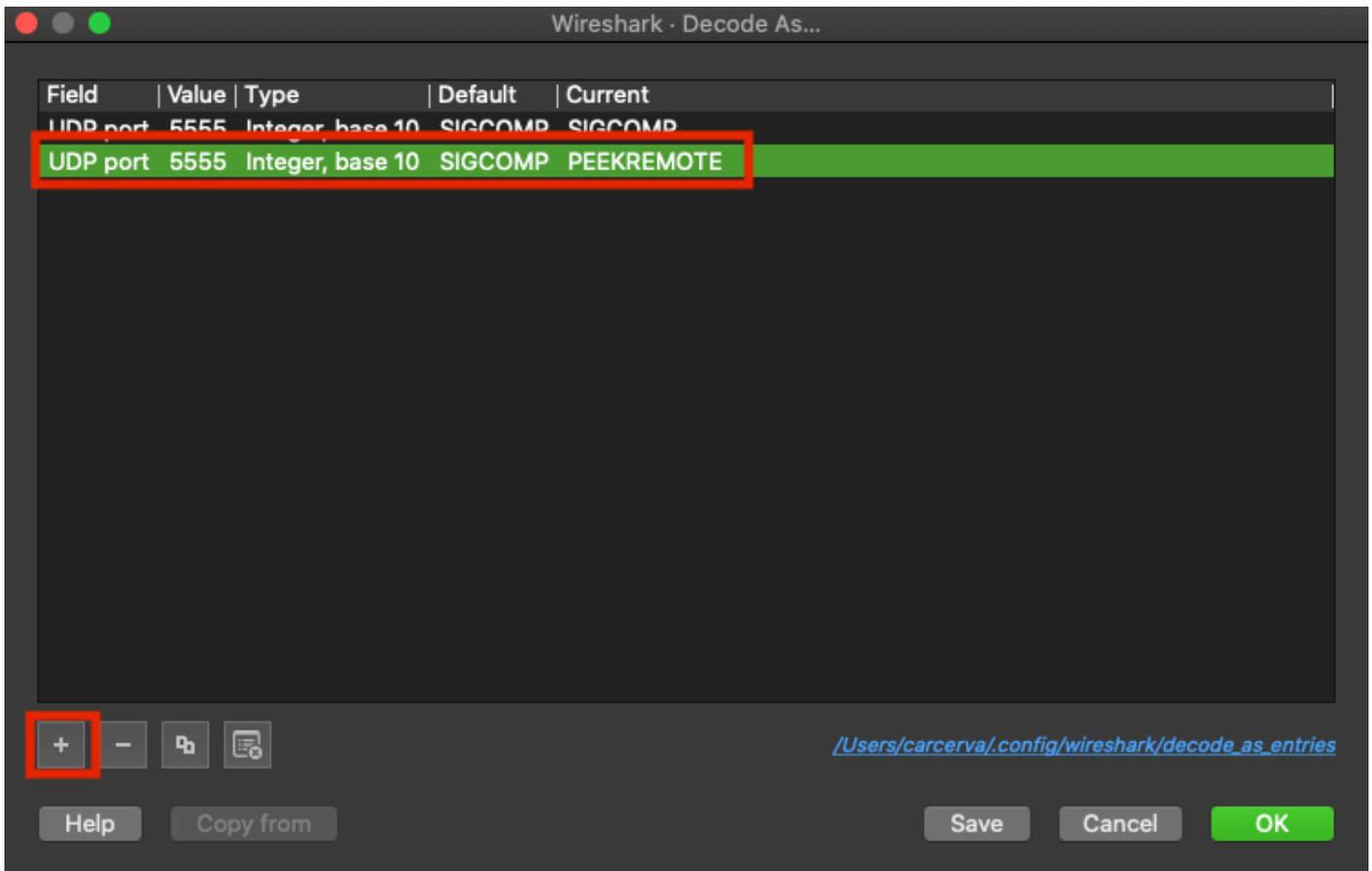


**Tip:** Wenn das WLAN Verschlüsselung wie Pre-shared Key (PSK) verwendet, stellen Sie sicher, dass die Erfassung den 4-Wege-Handshake zwischen dem Access Point und dem gewünschten Client abfängt. Dies kann erfolgen, wenn der OTA-PCAP startet, bevor das Gerät dem WLAN zugeordnet wird, oder wenn der Client deauthentifiziert und erneut authentifiziert wird, während die Erfassung ausgeführt wird.

Schritt 7: Wireshark decodiert die Pakete nicht automatisch. Um die Pakete zu dekodieren, wählen Sie eine Zeile aus der Erfassung aus, klicken Sie mit der rechten Maustaste, um die Optionen anzuzeigen, und wählen Sie **Decode As...**, wie im Bild gezeigt.



Schritt 8: Ein Popup-Fenster wird angezeigt. Wählen Sie die Schaltfläche Hinzufügen aus, und fügen Sie einen neuen Eintrag hinzu. Wählen Sie die folgenden Optionen aus: **UDP-Port** von **Field**, **555** von **Value**, **SIGCOMP** von **Default** und **PEEKREMOTE** von **Current**, wie im Bild gezeigt.



Schritt 9: Klicken Sie auf **OK**. Die Pakete werden dekodiert und sind bereit, die Analyse zu starten.

## Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

So überprüfen Sie, ob sich der Access Point über die Benutzeroberfläche des 9800 im Sniffer-Modus befindet:

Schritt 1: Navigieren Sie auf der Benutzeroberfläche des 9800 WLC zu **Configuration > Wireless > Access Points > All Access Points** (**Konfiguration > Wireless > Access Points > Zugangspunkte**).

Schritt 2: Durchsuchen Sie den Access Point. Klicken Sie auf den Pfeil nach unten, um das Suchtool anzuzeigen, wählen Sie aus der Dropdown-Liste **Contains** aus, und geben Sie den AP-Namen ein, wie im Bild gezeigt.

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	✓	172.16.0.125	a03d.6f92.9400	Sniffer	Registered	Healthy	webauth_test	default-site-tag

5 GHz Radios

Schritt 3: Stellen Sie sicher, dass der **Admin-Status** mit dem Häkchen in grün und der **AP-Modus Sniffer** lautet, wie im Bild gezeigt.

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	✓	172.16.0.125	a03d.6f92.9400	Sniffer	Registered	Healthy	webauth_test	default-site-tag

5 GHz Radios

Um zu überprüfen, ob sich der Access Point in der CLI 9800 im Sniffer-Modus befindet. Führen Sie folgende Befehle aus:

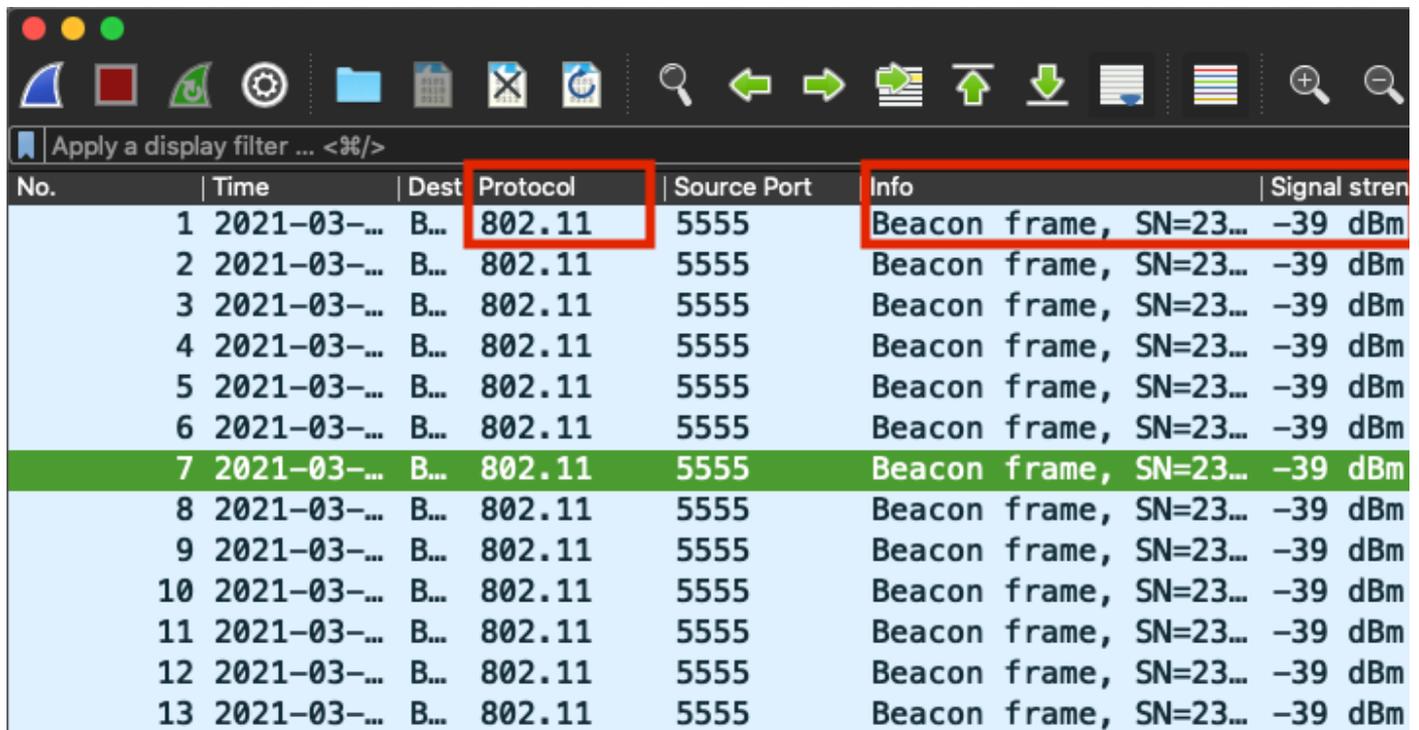
```
carcerva-9k-upg#show ap name 2802-carcerva-sniffer config general | i Administrative
Administrative State : Enabled
```

```
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

Um zu bestätigen, dass die Pakete auf Wireshark dekodiert werden. Das Protokoll wechselt von UDP zu 802.11 und es werden **Beacon-Frames** angezeigt, wie im Bild gezeigt.



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

## Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Problem: Wireshark empfängt keine Daten vom Access Point.

Lösung: Der Wireshark-Server muss über die Wireless Management Interface (WMI) erreichbar sein. Bestätigen Sie die Erreichbarkeit zwischen dem Wireshark-Server und der WMI vom WLC.

## Zugehörige Informationen

- [Cisco Catalyst Wireless Controller Software Configuration Guide 9800, Cisco IOS XE Amsterdam 17.3.x - Kapitel: Sniffer-Modus](#)
- [Grundlagen von 802.11 Wireless Sniffing](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)