Configure Access Point in Sniffer Mode on Catalyst 9800 Wireless Controllers

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Caveats

Configure

- Network Diagram
- Configurations
  - Configure AP in Sniffer Mode via GUI
  - Configure AP in Sniffer Mode via CLI
  - Configure AP to Scan a Channel via GUI
  - Configure AP to Scan a Channel via CLI
  - Configure Wireshark to Collect the Packet Capture

Verify

Troubleshoot

Related Information

Introduction

This document describes how to configure an Access Point (AP) in Sniffer Mode on a Catalyst 9800 Series Wireless Controller (9800 WLC) through the Graphic User Interface (GUI) or Command Line Interface (CLI) and how to collect a Packet Capture (PCAP) Over the Air (OTA) with the sniffer AP in order to troubleshoot and analyze wireless behaviors.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- 9800 WLC configuration
- Basic knowledge in the 802.11 standard

Components Used

The information in this document is based on these software and hardware versions:

- AP 2802
- 9800 WLC Cisco IOS®-XE version 17.3.2a
- Wireshark 3.4.4 or higher

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. If your network is live, ensure that you understand the potential impact of any command.

Caveats

Do not use the Sniffer Mode AP feature if the 9800 is connected to Cisco Application Centric Infrastructure (ACI) with default endpoint learning. The 9800 will transmit its UDP-encapsulated 802.11 captured packets sourced from the 9800's egress IP address, but with the source MAC address being the sniffer AP's radio's MAC, with low-order nibble set to 0x0F. This will cause problems as ACI will see the same IP address sourced from multiple MAC addresses. See Cisco bug ID CSCwa45713.

Configure

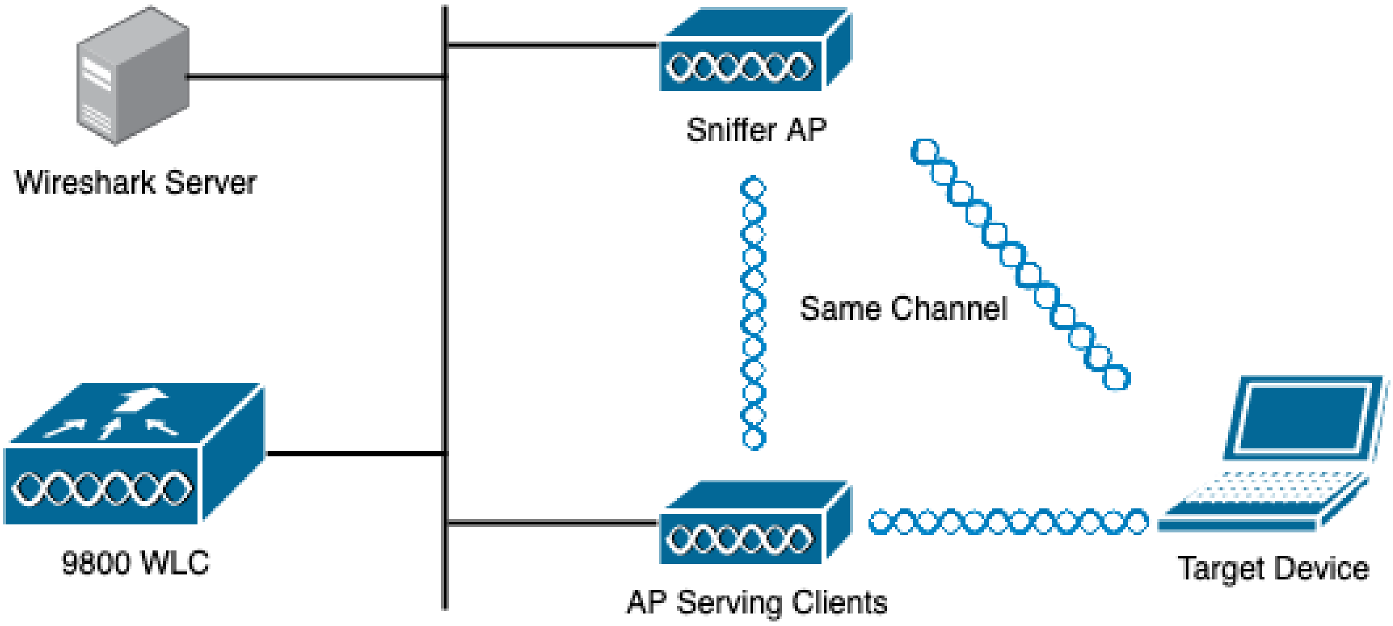
Things to consider:

- It is recommended to have the sniffer AP close to the target device and the AP to which this device is connected.
- Ensure you know which 802.11 Channel and Width, the client device and the AP use.

Note: Sniffer mode is not supported when the controller L3 interface is the Wireless Mangement Interface (WMI).

Note: The AP in sniffer mode is not supported on 9800-CL deployed on a Public Cloud.

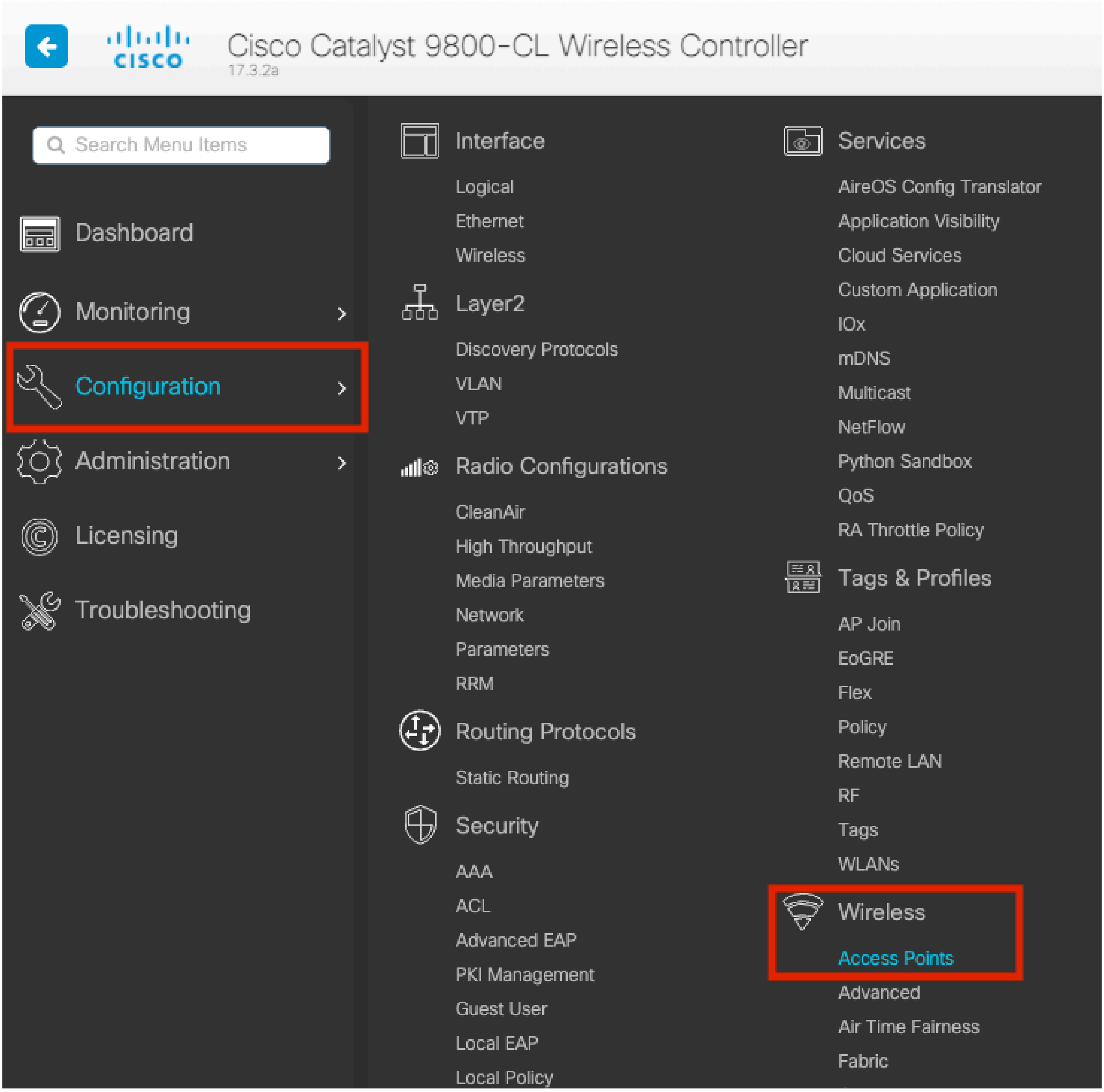
Network Diagram



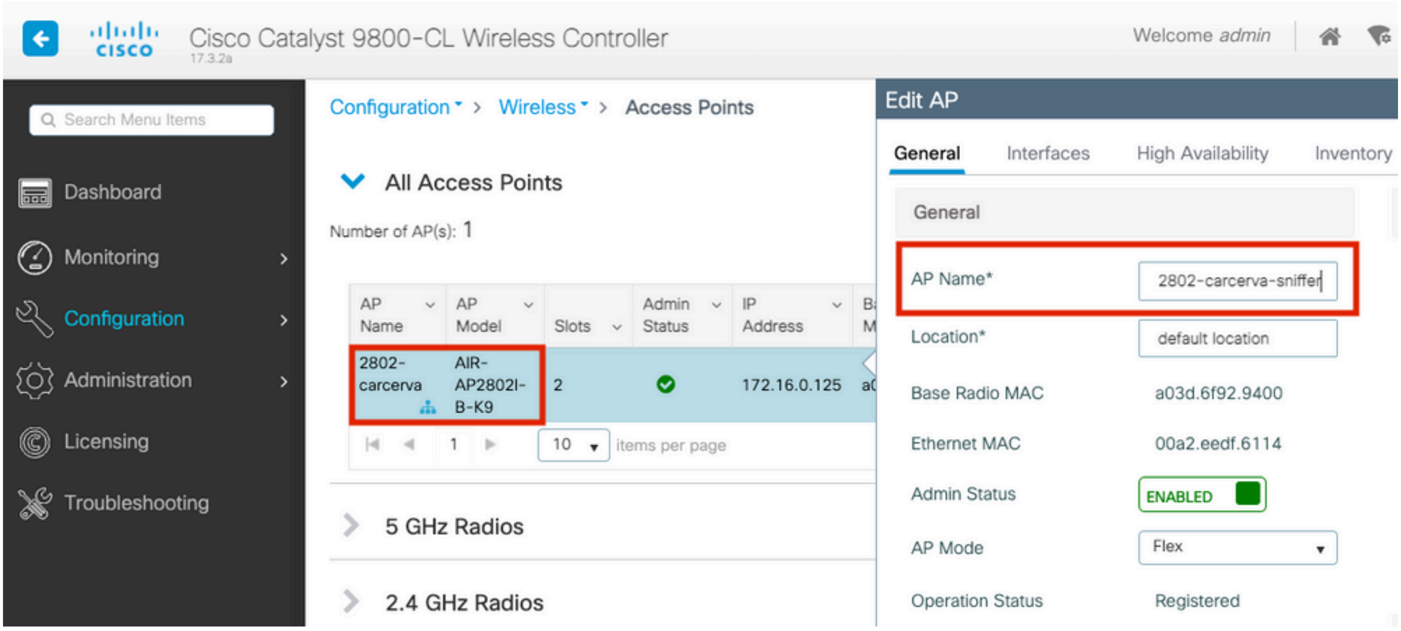
Configurations

Configure AP in Sniffer Mode via GUI

Step 1. On the 9800 WLC GUI, navigate to **Configuration** > **Wireless** > **Acces Points** > **All Acces Points**, as shown in the image.



Step 2. Select the AP that is desired to be used in sniffer mode. On the **General** tab, update the name of the AP, as shown in the image.



Number of AP(s): 1

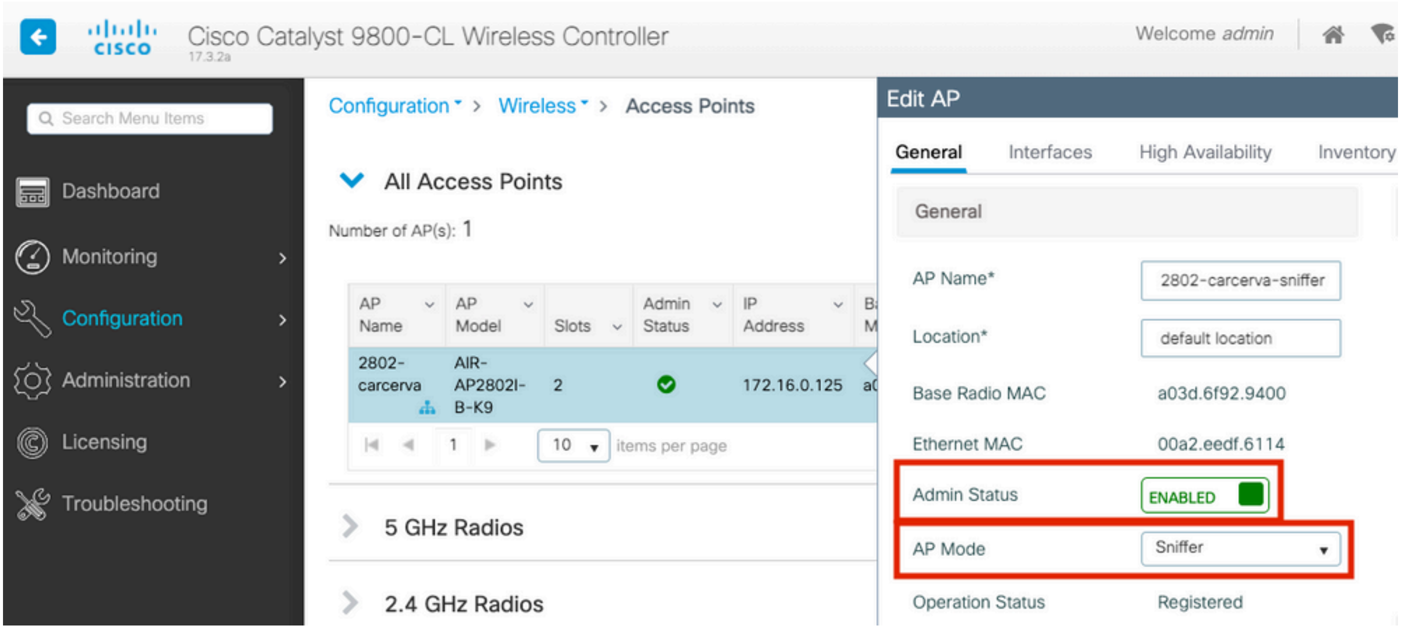
AP Name	AP Model	Slots	Admin Status	IP Address
2802-carcerva	AIR-AP2802I-B-K9	2	✓	172.16.0.125

1 — 10 items per page

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

Step 3. Verify the **Admin Status** is **Enabled** and change the **AP Mode** to **Sniffer**, as shown in the image.



Number of AP(s): 1

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

1 — 10 items per page

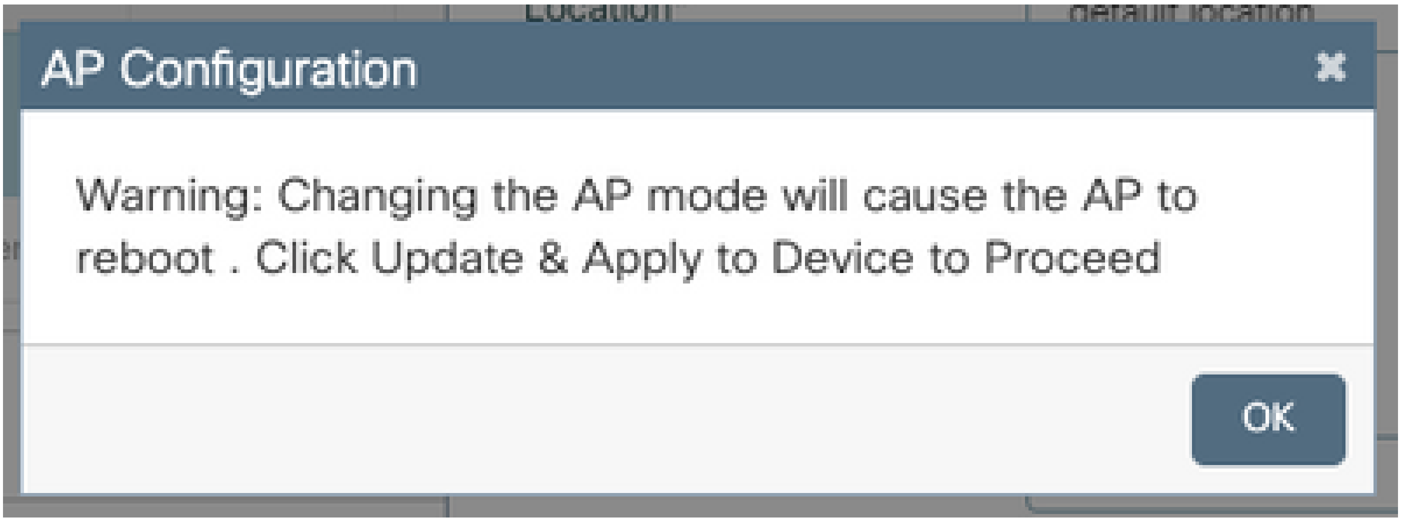
General

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

A pop-up window appears with the next alert:

"Warning: Changing the AP mode will cause the AP to reboot. Click Update & Apply to Device to Proceed"

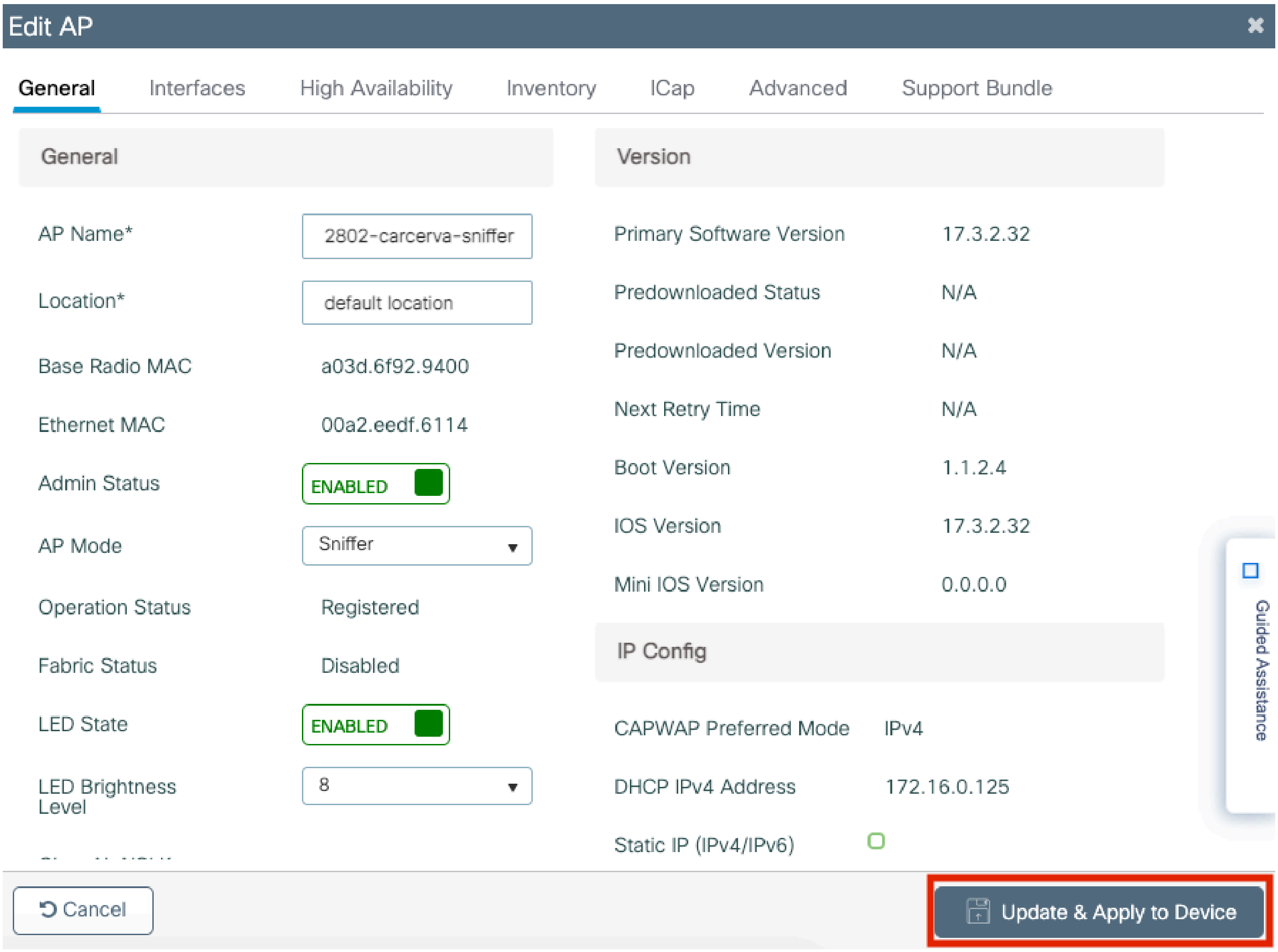
Select **OK**, as shown in the image.



AP Configuration

Warning: Changing the AP mode will cause the AP to reboot . Click Update & Apply to Device to Proceed

Step 4. Click on **Update & Apply to Device**, as shown in the image.



Edit AP

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
Fabric Status	Disabled
LED State	ENABLED
LED Brightness Level	8

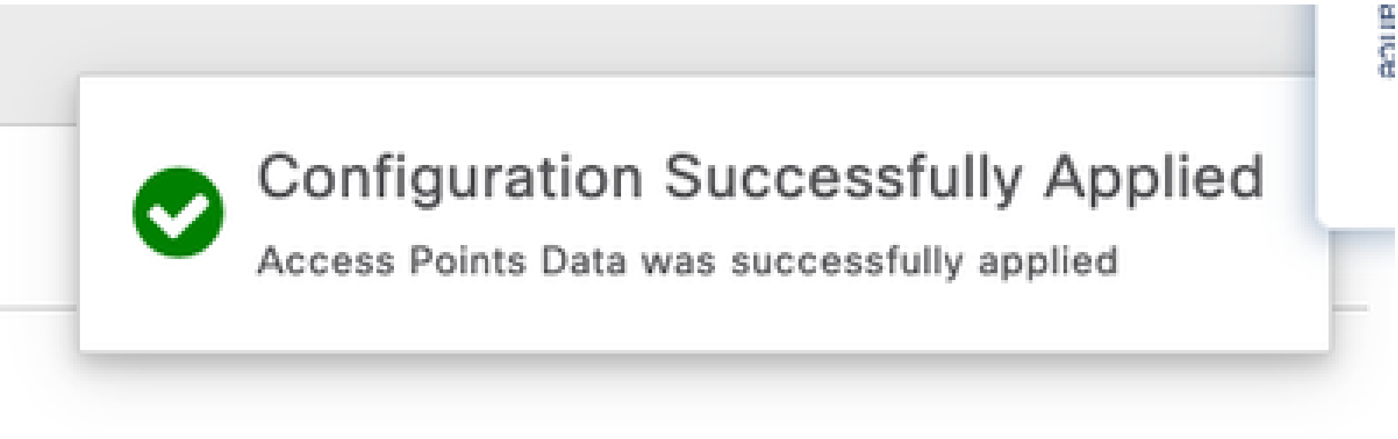
Version

Primary Software Version	17.3.2.32
Predownloaded Status	N/A
Predownloaded Version	N/A
Next Retry Time	N/A
Boot Version	1.1.2.4
IOS Version	17.3.2.32
Mini IOS Version	0.0.0.0

IP Config

CAPWAP Preferred Mode	IPv4
DHCP IPv4 Address	172.16.0.125
Static IP (IPv4/IPv6)	□

A pop-up appears to confirm the changes and the AP bounces, as shown in the image.



Configuration Successfully Applied

Access Points Data was successfully applied

Configure AP in Sniffer Mode via CLI

Step 1. Determine the AP that is desired to be used as Sniffer Mode and grab the AP Name.

Step 2. Modify the AP name.

This command modifies the AP name. Where <AP-name> is the current name of the AP.

<#root>

```
carcerva-9k-upg#

ap name

<AP-name>

 name 2802-carcerva-sniffer
```

Step 3. Configure the AP in Sniffer mode.

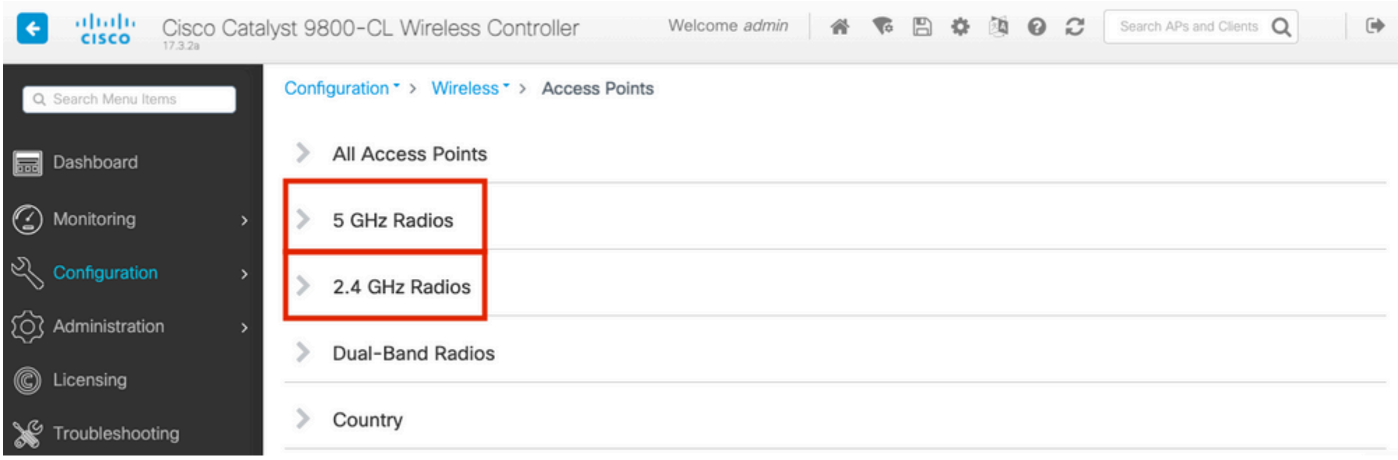
<#root>

```
carcerva-9k-upg#

ap name 2802-carcerva-sniffer mode sniffer
```

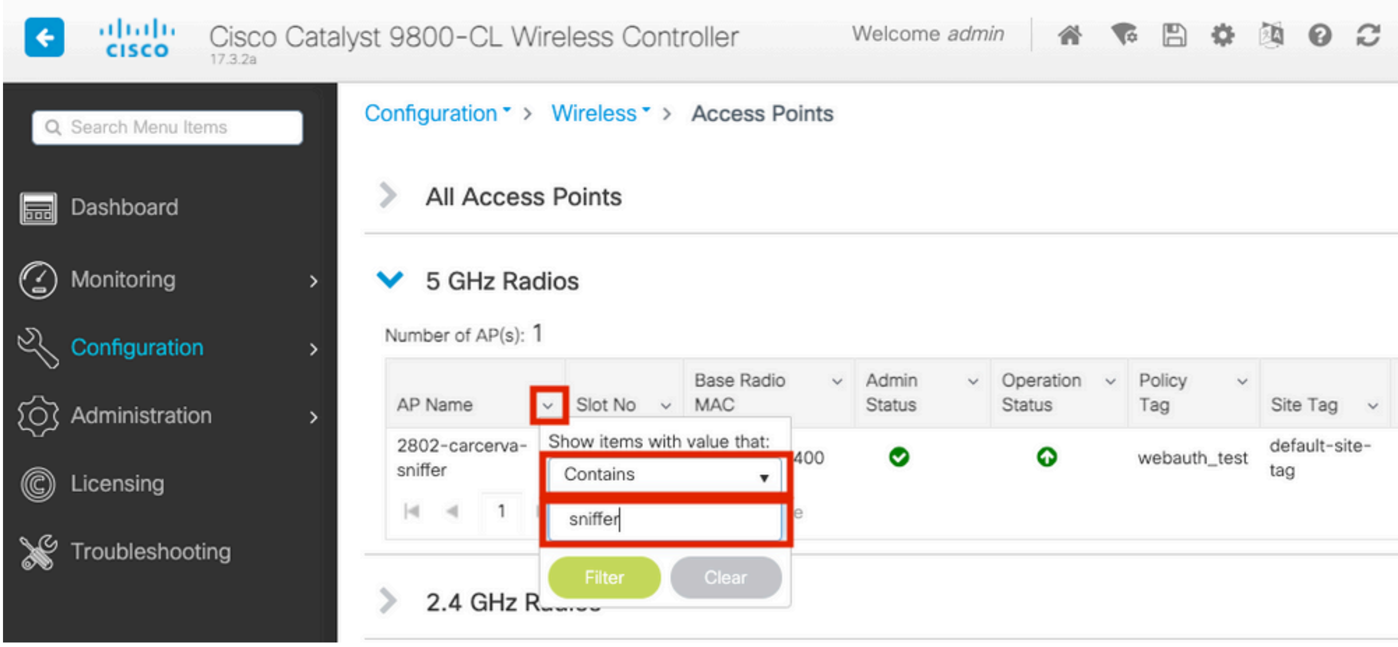
Configure AP to Scan a Channel via GUI

Step 1. In the 9800 WLC GUI, navigate to **Configuration > Wireless > Acces Points**.

Step 2. On the **Access Points** page, display the **5 GHz Radios** or **2.4 GHz Radios** menu list. This depends on the channel that is desired to scan, as shown in the image.



Step 2. Search the AP. Click on the **arrow down** button to display the search tool, select **Contains** from the dropdown list, and type the **AP name**, as shown in the image.

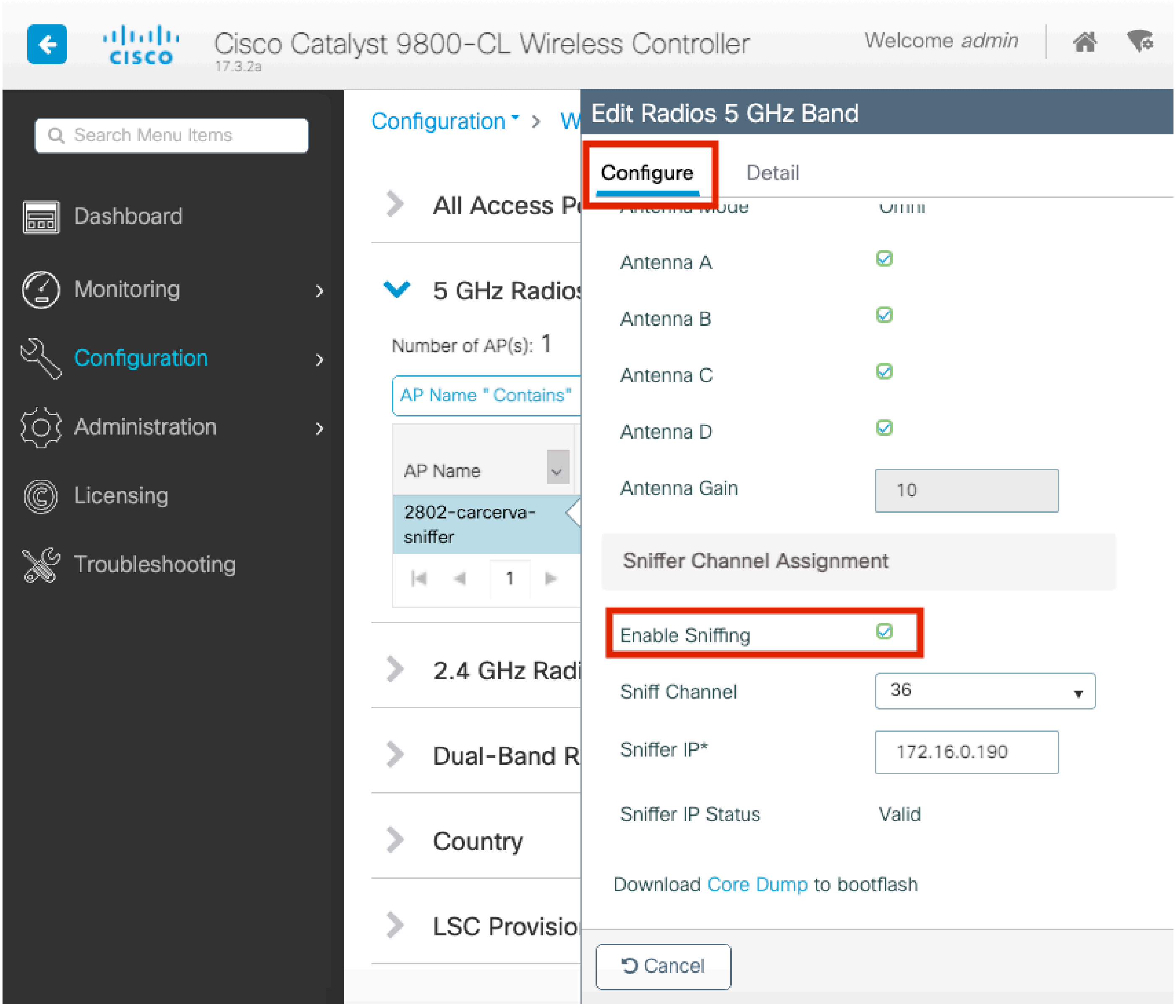


Number of AP(s): 1

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

Step 3. Select the AP and tick the **Enable Sniffer** checkbox under the **Configure** > **Sniffer Channel Assignment**, as shown in the image.



Antenna A ☑

Antenna B ☑

Antenna C ☑

Antenna D ☑

Antenna Gain 10

Sniffer Channel Assignment

Enable Sniffing ☑

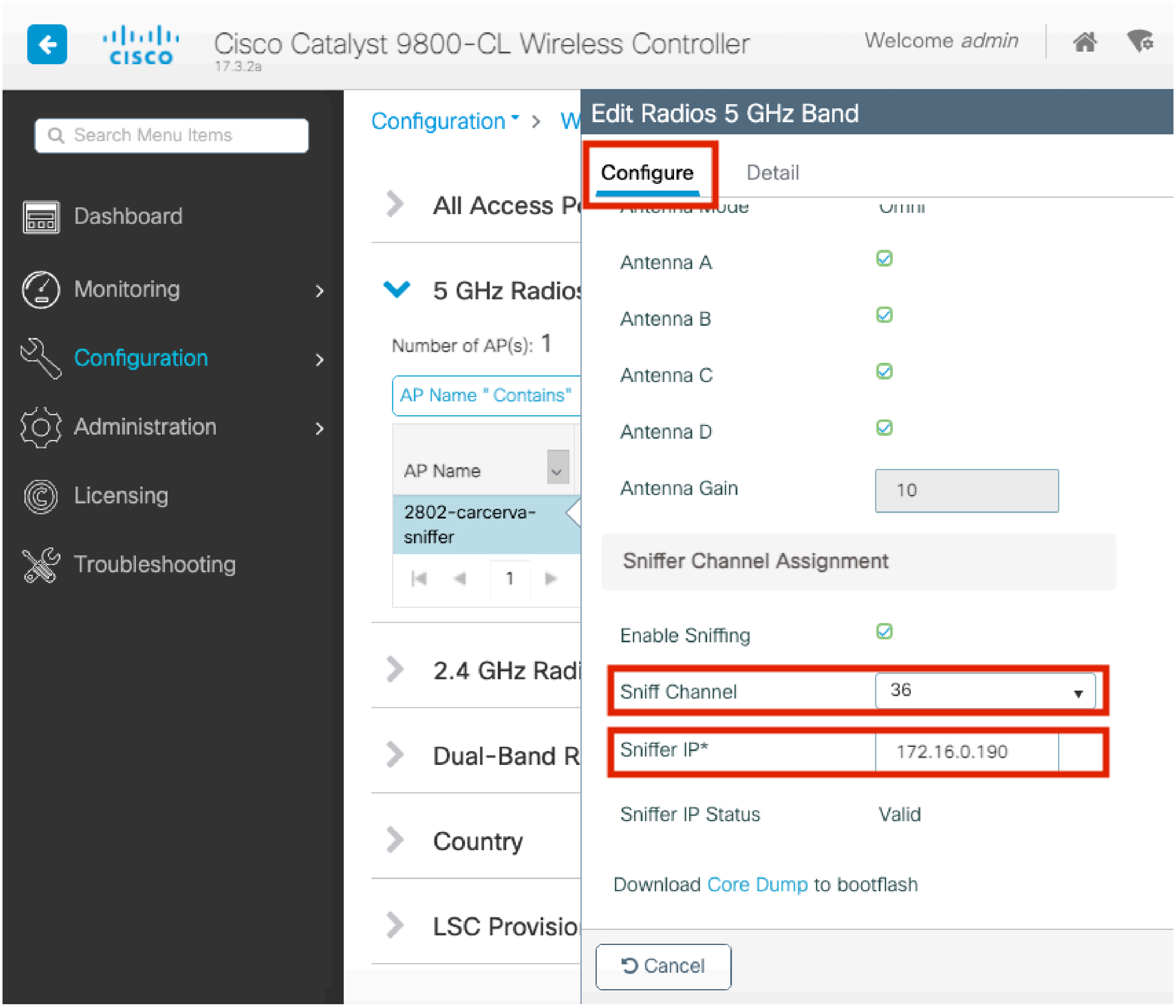
Sniff Channel 36

Sniffer IP* 172.16.0.190

Sniffer IP Status Valid

Download Core Dump to bootflash

Step 4. Select the Channel from the **Sniff Channel** dropdown list and type the **Sniffer IP address** (Server IP address with Wireshark), as shown in the image.



Edit Radios 5 GHz Band

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

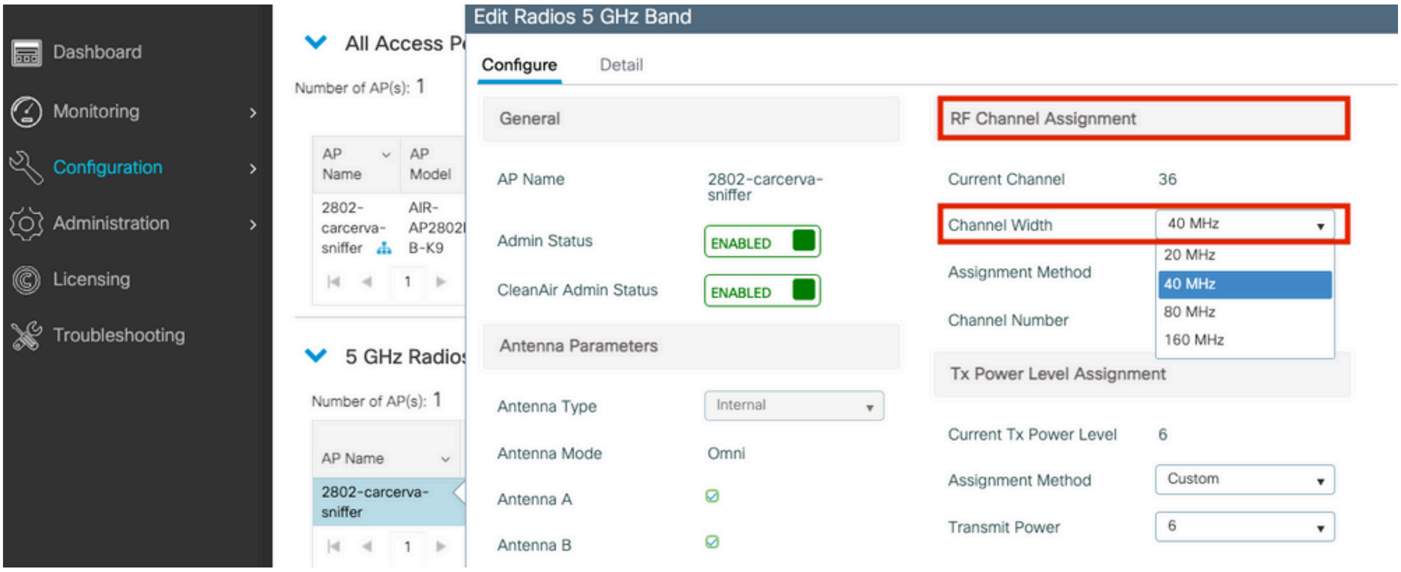
Sniffer IP Status Valid

Download Core Dump to bootflash

AP Name: 2802-carcerva-sniffer

Step 5. Select the **Channel width** that the target device and the AP use when connected.

Navigate to **Configure > RF Channel Assignment** in order to configure this, as shown in the image.



Edit Radios 5 GHz Band

AP Name	AP Model
2802-carcerva-sniffer	AIR-AP2802I-B-K9

General

AP Name 2802-carcerva-sniffer

Admin Status ENABLED

CleanAir Admin Status ENABLED

Antenna Parameters

Antenna Type Internal

Antenna Mode Omni

Antenna A ☑

Antenna B ☑

RF Channel Assignment

Current Channel 36

Channel Width 40 MHz

Assignment Method

Channel Number

Tx Power Level Assignment

Current Tx Power Level 6

Assignment Method Custom

Transmit Power 6

Configure AP to Scan a Channel via CLI

Step 1. Enable the channel sniff on the AP. Run this command:

```
<#root>

carcerva-9k-upg#

ap name

 <ap-name>

sniff

{dot11a for 5GHz | dot11bfor 2.4GHz | dual-band}

 <channel> <Wireshark-server-ip-address>
```

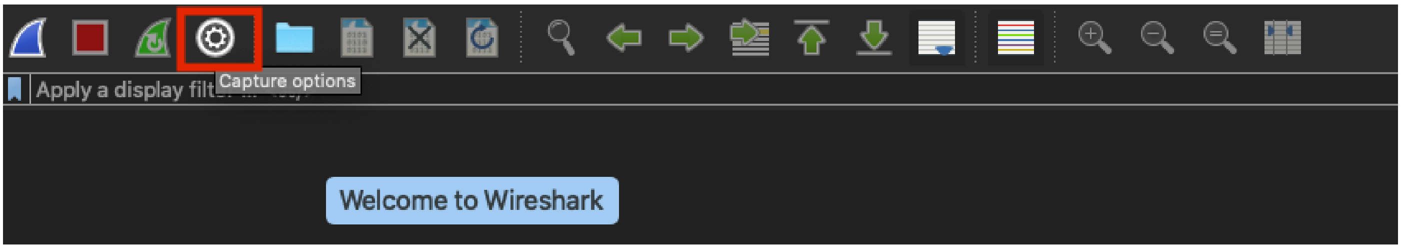
Example:

```
<#root>

carcerva-9k-upg#

ap name 2802-carcerva-sniffer sniff dot11a 36 172.16.0.190
```

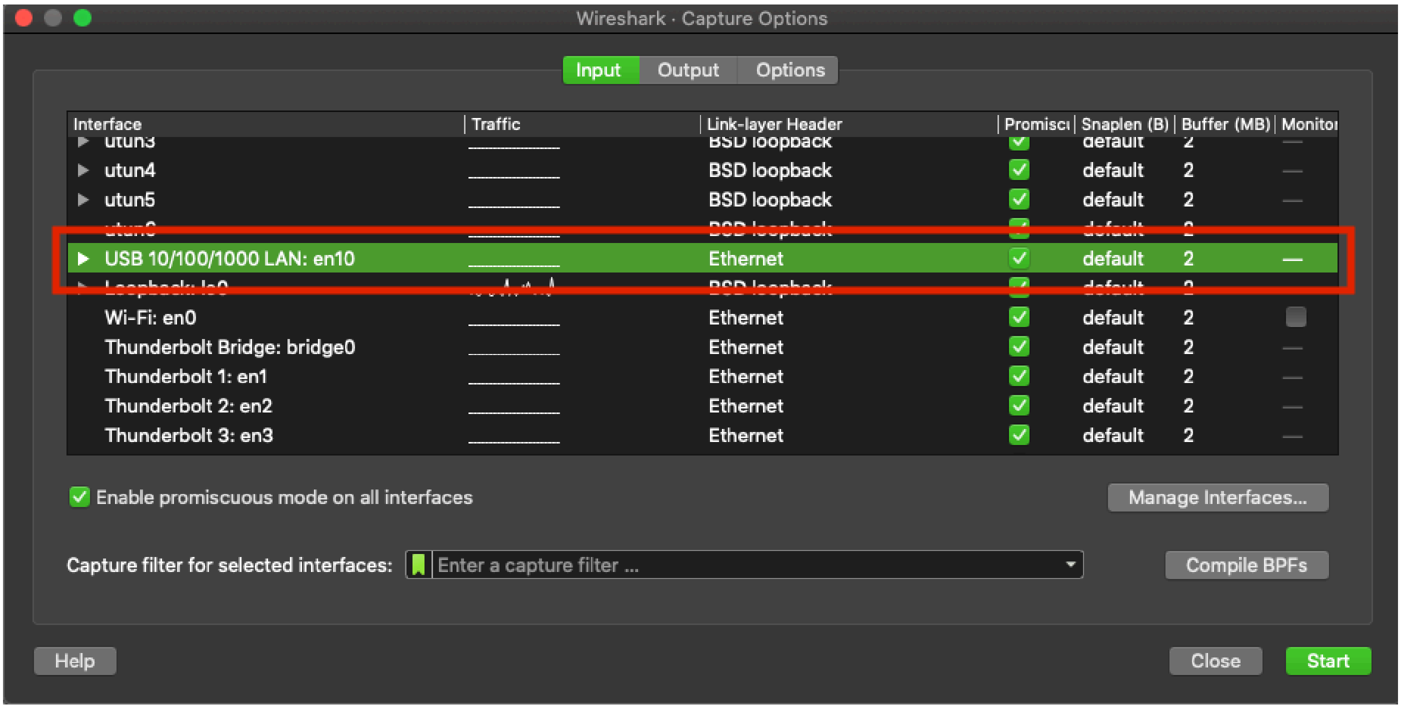
Configure Wireshark to Collect the Packet Capture

Step 1. Launch Wireshark.

Step 2. Select the **Capture options** menu icon from Wireshark, as shown in the image.



Step 3. This action displays a pop-up window. Select the Wired Interface from the list as the source of the capture, as shown in the image.

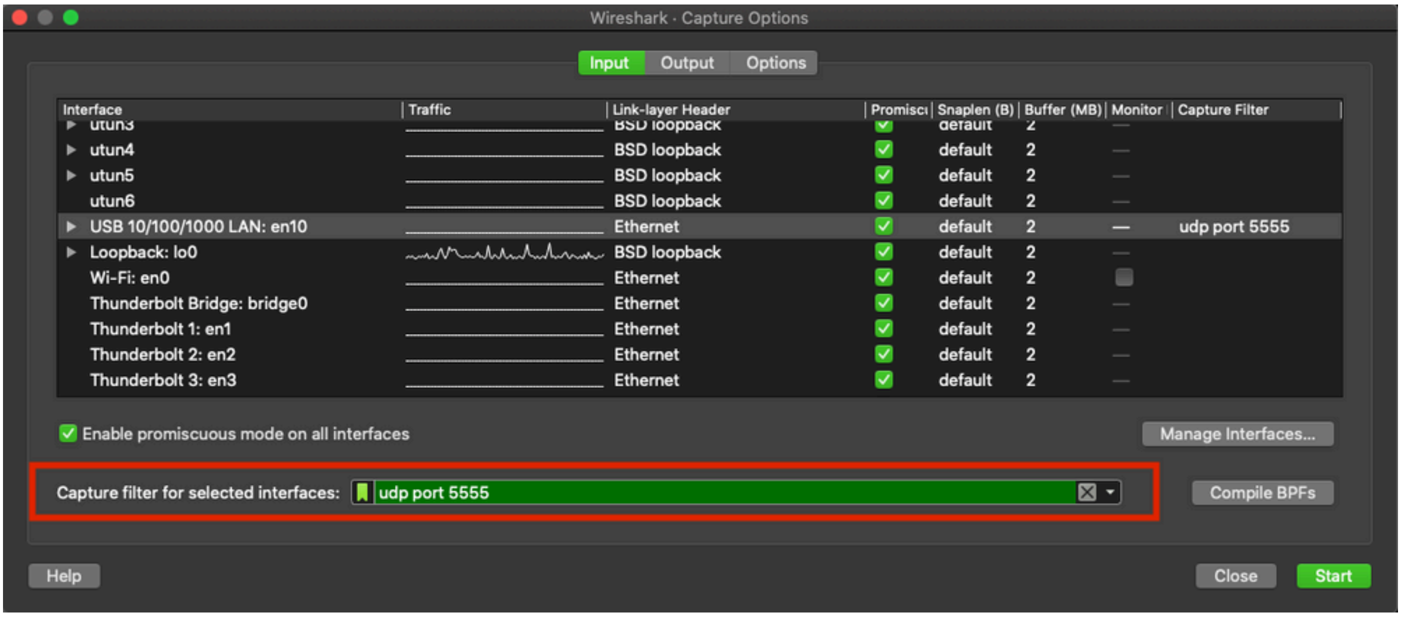


Interface	Traffic	Link-layer Header	Promiscı	Snaplen (B)	Buffer (MB)	Monitor
▶ utun3		BSD loopback	✓	default	2	—
▶ utun4		BSD loopback	✓	default	2	—
▶ utun5		BSD loopback	✓	default	2	—
utun6		BSD loopback	✓	default	2	
▶ USB 10/100/1000 LAN: en10		Ethernet	✓	default	2	—
▶ Loopback: lo0		BSD loopback	✓	default	2	
Wi-Fi: en0		Ethernet	✓	default	2	☐
Thunderbolt Bridge: bridge0		Ethernet	✓	default	2	—
Thunderbolt 1: en1		Ethernet	✓	default	2	—
Thunderbolt 2: en2		Ethernet	✓	default	2	—
Thunderbolt 3: en3		Ethernet	✓	default	2	—

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Step 4. Under the **Capture filter for selected interfaces:** field box, type **udp port 5555**, as shown in the image.

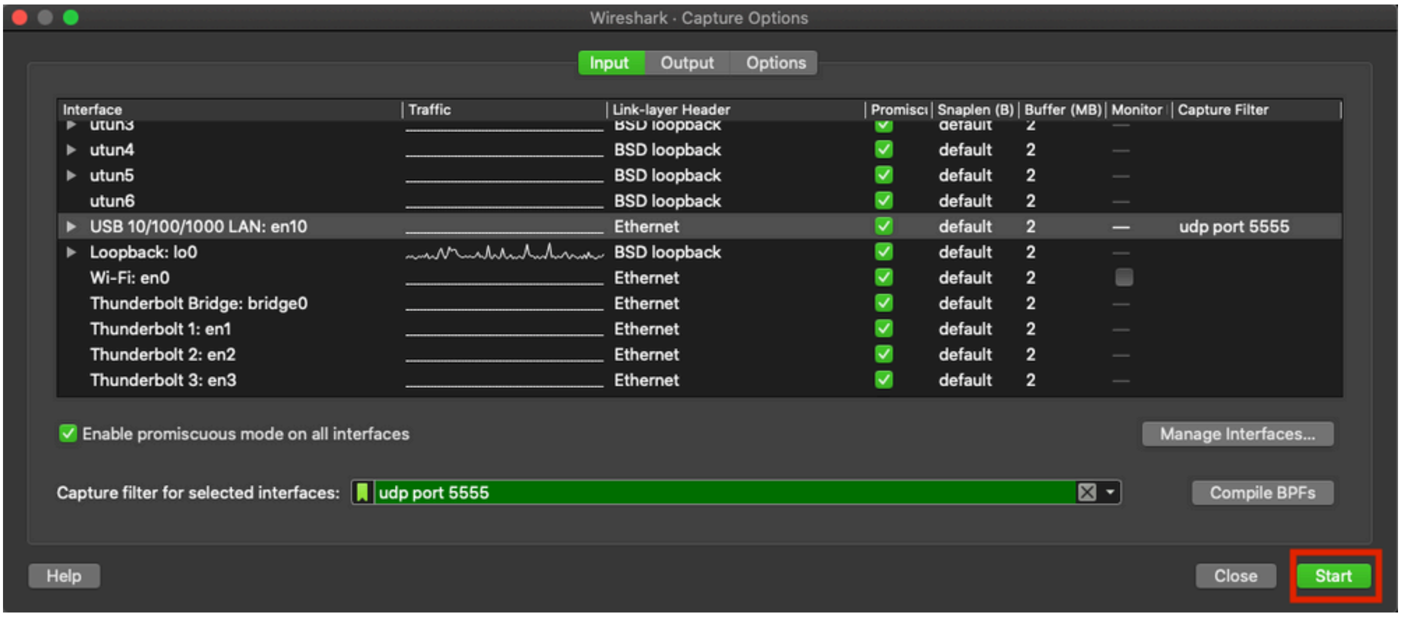


Interface	Traffic	Link-layer Header	Promiscı	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
▶ utun3		BSD loopback	✓	default	2	—	
▶ utun4		BSD loopback	✓	default	2	—	
▶ utun5		BSD loopback	✓	default	2	—	
utun6		BSD loopback	✓	default	2	—	
▶ USB 10/100/1000 LAN: en10		Ethernet	✓	default	2	—	udp port 5555
▶ Loopback: lo0		BSD loopback	✓	default	2	—	
Wi-Fi: en0		Ethernet	✓	default	2	☐	
Thunderbolt Bridge: bridge0		Ethernet	✓	default	2	—	
Thunderbolt 1: en1		Ethernet	✓	default	2	—	
Thunderbolt 2: en2		Ethernet	✓	default	2	—	
Thunderbolt 3: en3		Ethernet	✓	default	2	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: udp port 5555

Step 5. Click **Start**, as shown in the image.

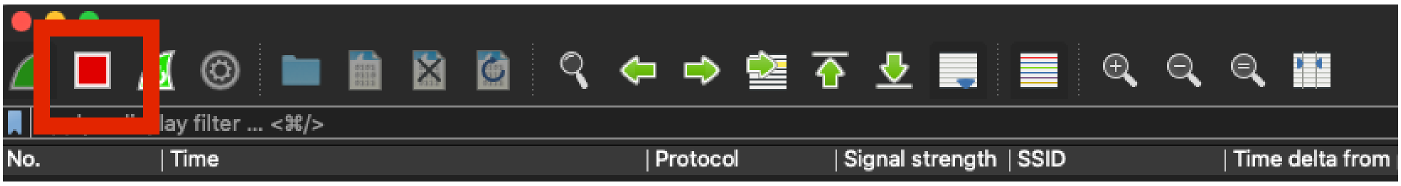


Interface	Traffic	Link-layer Header	Promisc	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
utun3		BSD loopback	✓	default	2	—	
utun4		BSD loopback	✓	default	2	—	
utun5		BSD loopback	✓	default	2	—	
utun6		BSD loopback	✓	default	2	—	
USB 10/100/1000 LAN: en10		Ethernet	✓	default	2	—	udp port 5555
Loopback: lo0		BSD loopback	✓	default	2	—	
Wi-Fi: en0		Ethernet	✓	default	2	□	
Thunderbolt Bridge: bridge0		Ethernet	✓	default	2	—	
Thunderbolt 1: en1		Ethernet	✓	default	2	—	
Thunderbolt 2: en2		Ethernet	✓	default	2	—	
Thunderbolt 3: en3		Ethernet	✓	default	2	—	

☑ Enable promiscuous mode on all interfaces

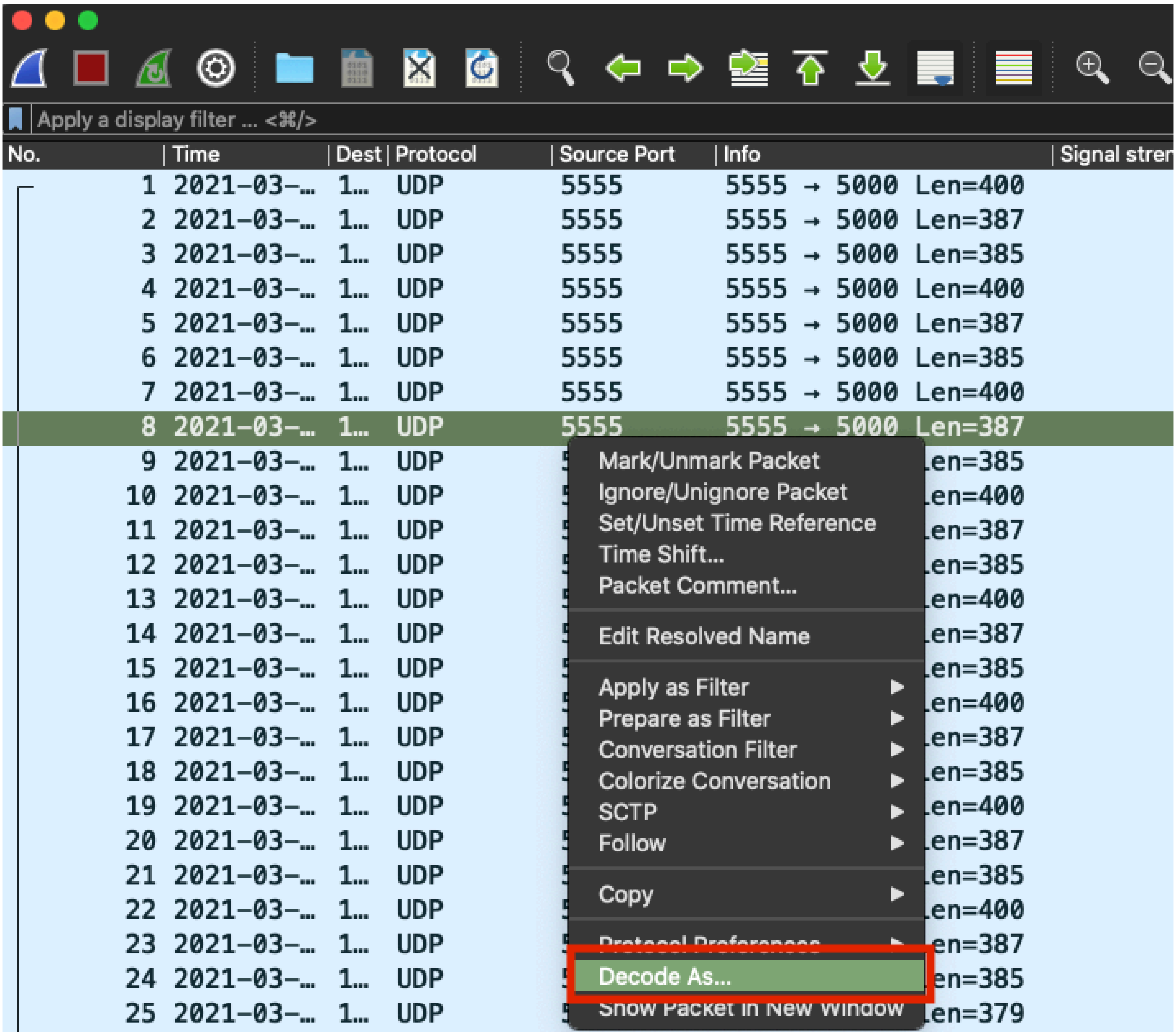
Capture filter for selected interfaces: udp port 5555

Step 6. Wait for Wireshark to collect the information required and select the **Stop** button from Wireshark, as shown in the image.



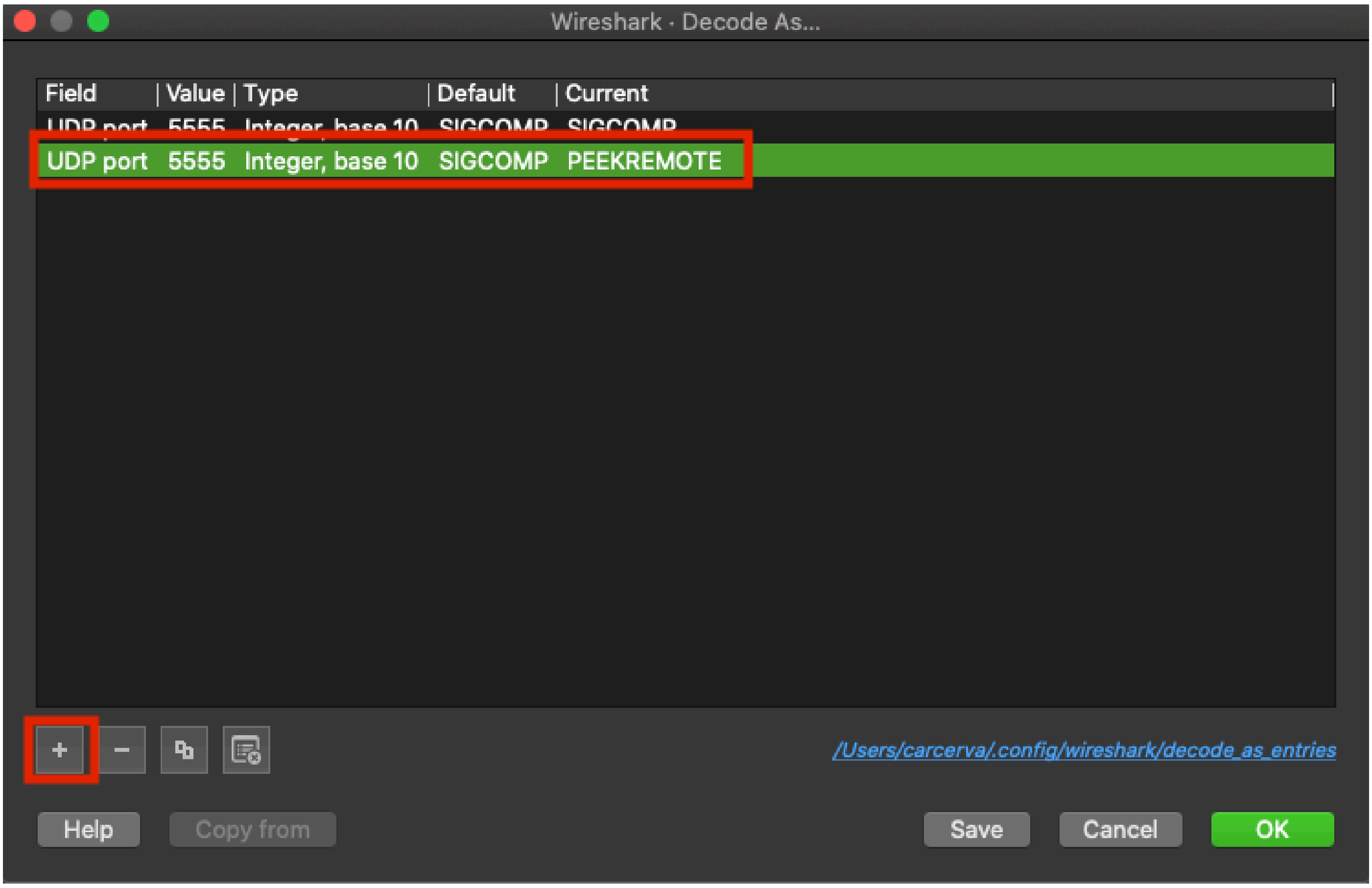
Tip: If the WLAN uses encryption such as Pre-shared Key (PSK), ensure the capture catches the four-way handshake between the AP and the desired client. This can be done if the OTA PCAP starts before the device is associated with the WLAN or if the client is deauthenticated and reauthenticated while the capture runs.

Step 7. Wireshark does not decode the packets automatically. In order to decode the packets select a line from the capture, use the right-click to display the options, and select **Decode As...**, as shown in the image.



No.	Time	Dest	Protocol	Source Port	Info	Signal stren
1	2021-03-…	1…	UDP	5555	5555 → 5000 Len=400	
2	2021-03-…	1…	UDP	5555	5555 → 5000 Len=387	
3	2021-03-…	1…	UDP	5555	5555 → 5000 Len=385	
4	2021-03-…	1…	UDP	5555	5555 → 5000 Len=400	
5	2021-03-…	1…	UDP	5555	5555 → 5000 Len=387	
6	2021-03-…	1…	UDP	5555	5555 → 5000 Len=385	
7	2021-03-…	1…	UDP	5555	5555 → 5000 Len=400	
8	2021-03-…	1…	UDP	5555	5555 → 5000 Len=387	
9	2021-03-…	1…	UDP	5	en=385	
10	2021-03-…	1…	UDP	5	en=400	
11	2021-03-…	1…	UDP	5	en=387	
12	2021-03-…	1…	UDP	5	en=385	
13	2021-03-…	1…	UDP	5	en=400	
14	2021-03-…	1…	UDP	5	en=387	
15	2021-03-…	1…	UDP	5	en=385	
16	2021-03-…	1…	UDP	5	en=400	
17	2021-03-…	1…	UDP	5	en=387	
18	2021-03-…	1…	UDP	5	en=385	
19	2021-03-…	1…	UDP	5	en=400	
20	2021-03-…	1…	UDP	5	en=387	
21	2021-03-…	1…	UDP	5	en=385	
22	2021-03-…	1…	UDP	5	en=400	
23	2021-03-…	1…	UDP	5	en=387	
24	2021-03-…	1…	UDP	5	en=385	
25	2021-03-…	1…	UDP	5	en=379	

Step 8. A pop-up window appears. Select the add button and add a new entry, select these options: **UDP port** from **Field, 5555** from **Value**, **SIGCOMP** from **Default**, and **PEEKREMOTE** from **Current**, as shown in the image.



Field	Value	Type	Default	Current
UDP port	5555	Integer, base 10	SIGCOMP	SIGCOMP
UDP port	5555	Integer, base 10	SIGCOMP	PEEKREMOTE

Step 9. Click **OK**. The packets are decoded and ready to start the analysis.

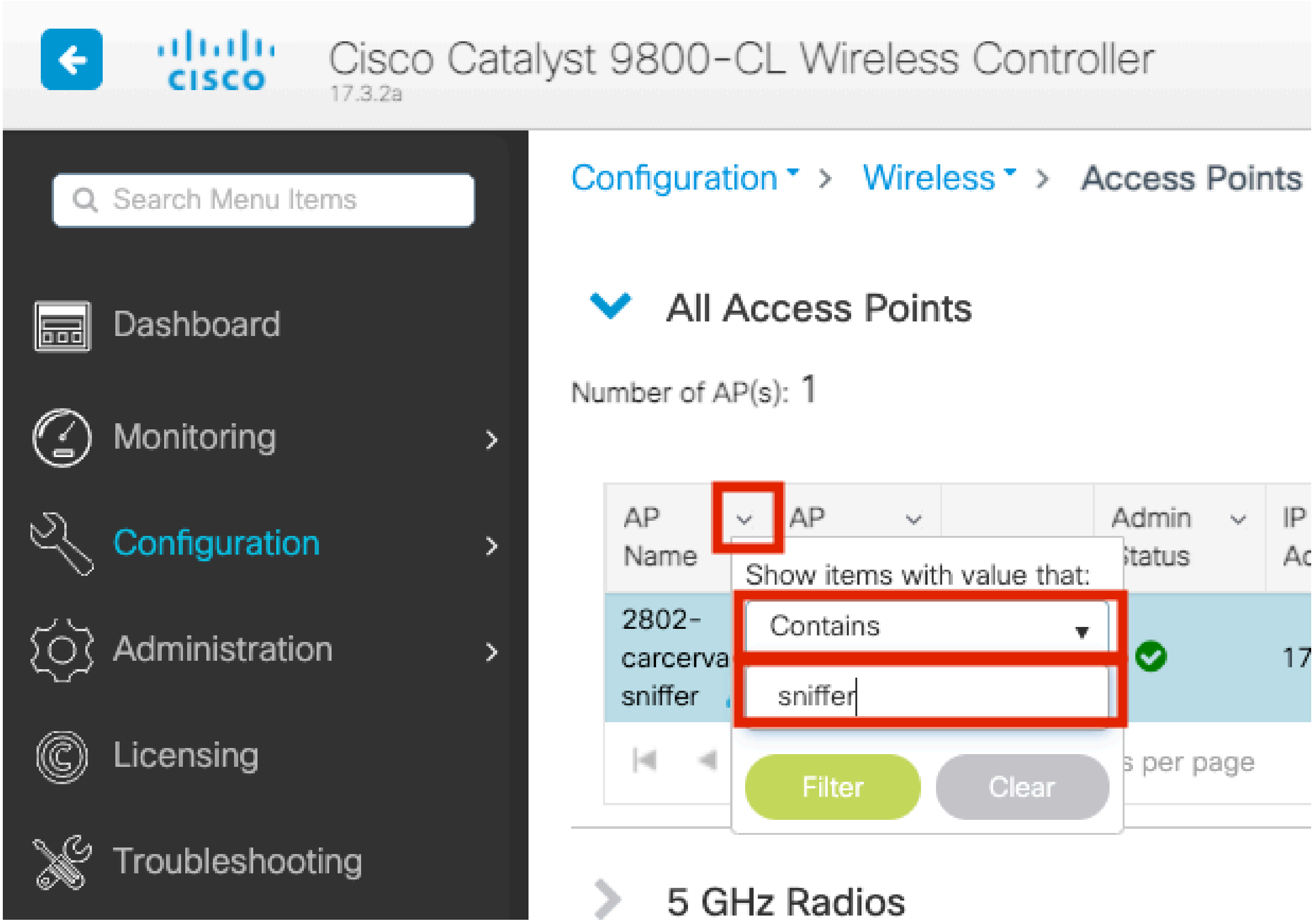
Verify

Use this section in order to confirm that your configuration works properly.

In order to confirm the AP is in Sniffer mode from the 9800 GUI:

Step 1. On the 9800 WLC GUI Navigate to **Configuration** > **Wireless** > **Acces Points** > **All Acces Points**.

Step 2. Search the AP. Click on the arrow down button to display the search tool, select **Contains** from the dropdown list, and type the AP name, as shown in the image.



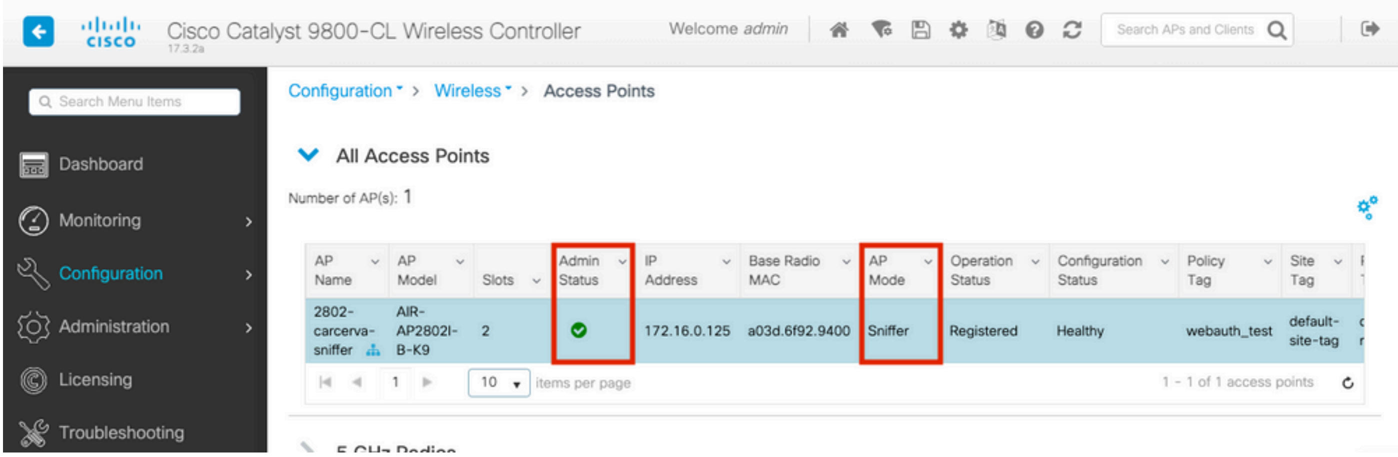
Number of AP(s): 1

Show items with value that:

Contains

sniffer

Step 3. Verify the **Admin Status** is with the **checkmark in green** and the **AP Mode** is **Sniffer**, as shown in the image.



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

1 · 10 items per page · 1 - 1 of 1 access points

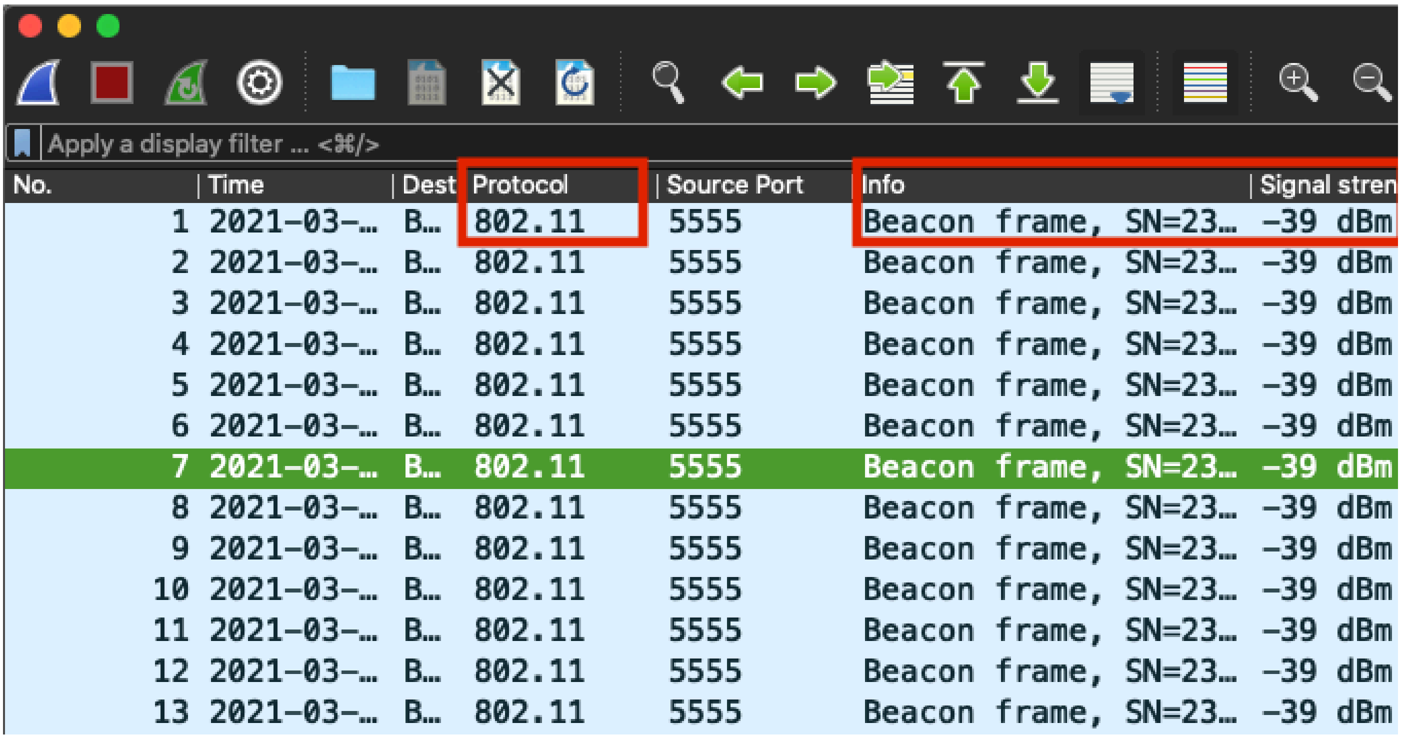
In order to confirm the AP is in Sniffer mode from the 9800 CLI. Run these commands:

<#root>

```
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
```

In order to confirm the packets are decoded on Wireshark. The Protocol changes from **UDP** to **802.11** and there are seen **Beacon frames**, as shown in the 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

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Problem: Wireshark does not receive any data from the AP.

Solution: The Wireshark server must be reachable by the Wireless Management Interface (WMI). Confirm the reachability between the Wireshark server and the WMI from the WLC.

Related Information

- Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Amsterdam 17.3.x - Chapter: Sniffer Mode

- Fundamentals of 802.11 Wireless Sniffing
- Technical Support & Documentation - Cisco Systems