在Catalyst 9800无线控制器上以嗅探器模式配置接入点

目录

简介

本文档介绍如何通过图形用户界面(GUI)或命令行界面(CLI)在Catalyst 9800系列无线控制器(9800 WLC)的嗅探器模式下配置接入点(AP)，以及如何通过空中(OTA)收集数据包捕获(PCAP))，以便对无线行为进行故障排除和分析。

先决条件

要求

Cisco 建议您了解以下主题：

- 9800 WLC配置
- 802.11标准中的基本知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

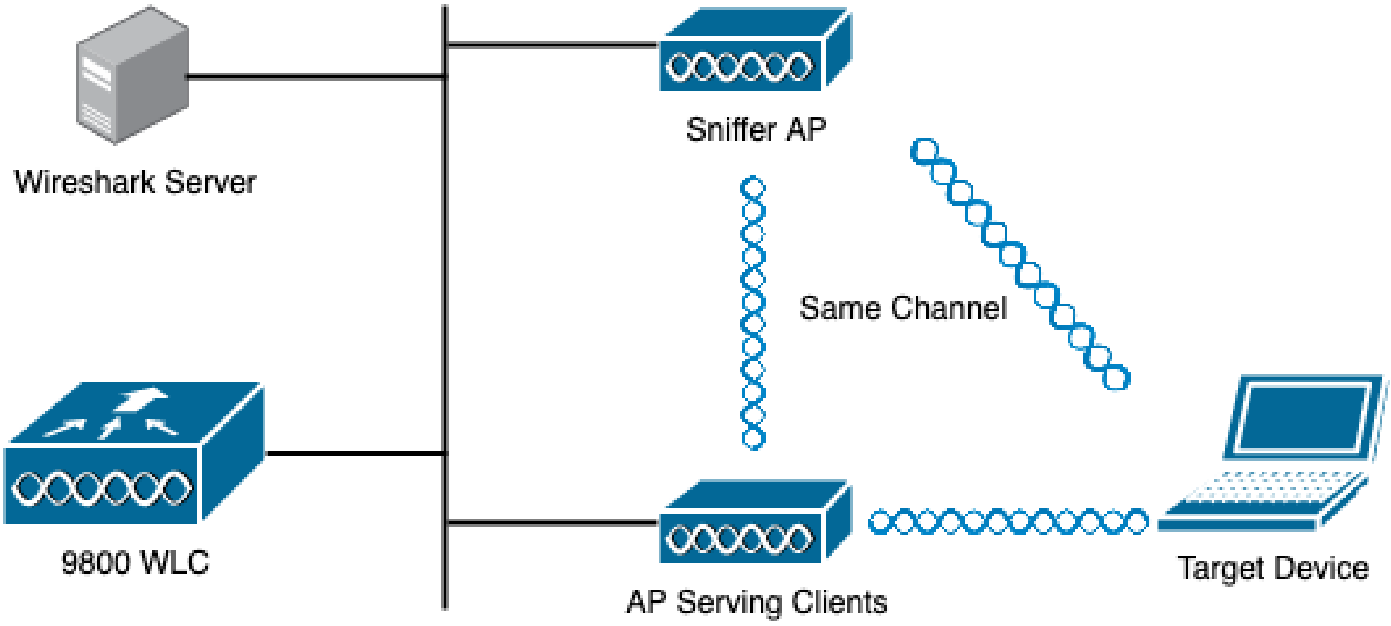
始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

注意事项:

- 建议使嗅探器AP靠近目标设备和此设备所连接的AP。
- 确保您知道客户端设备和AP使用哪个802.11通道和宽度。

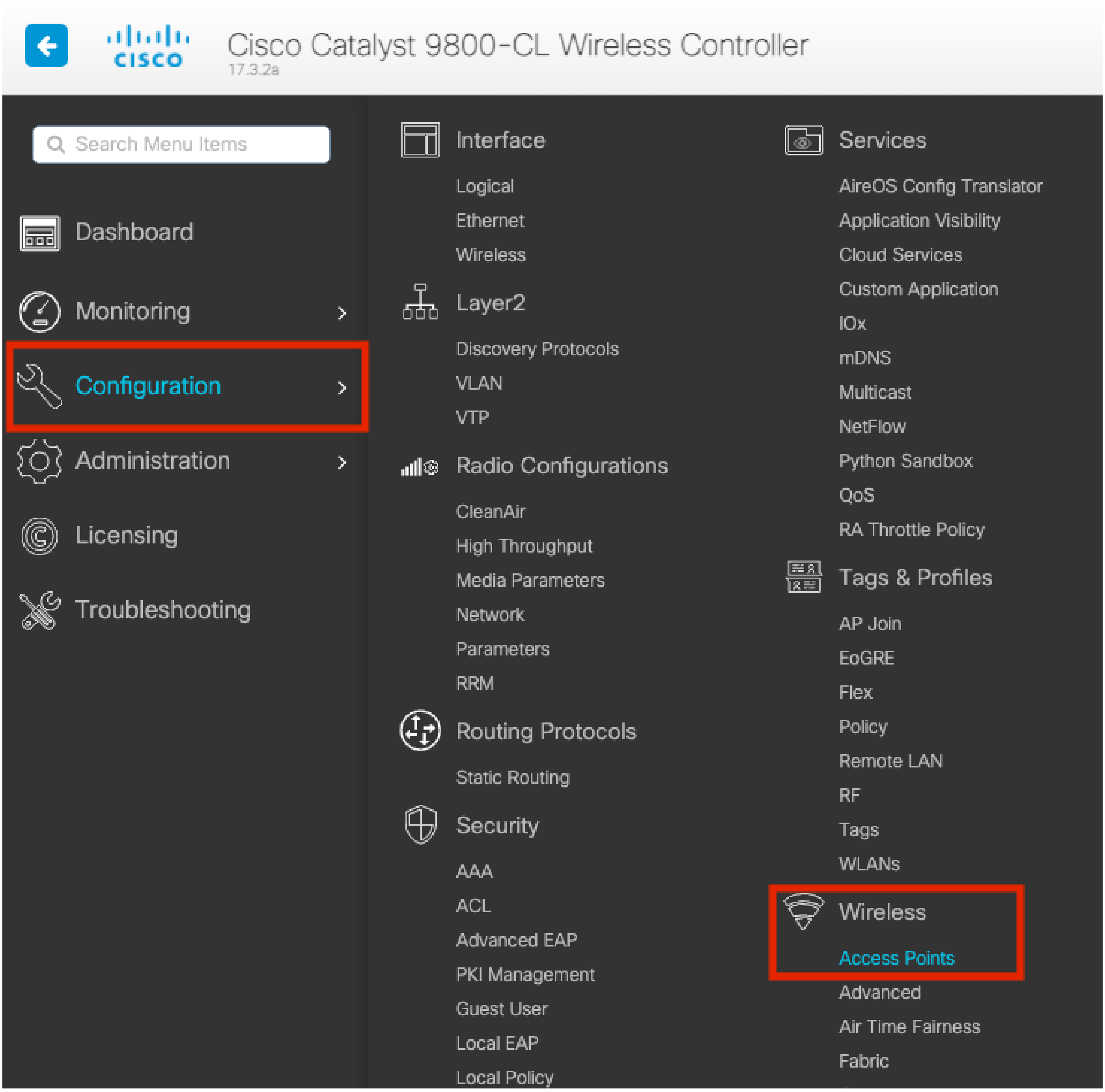
网络图



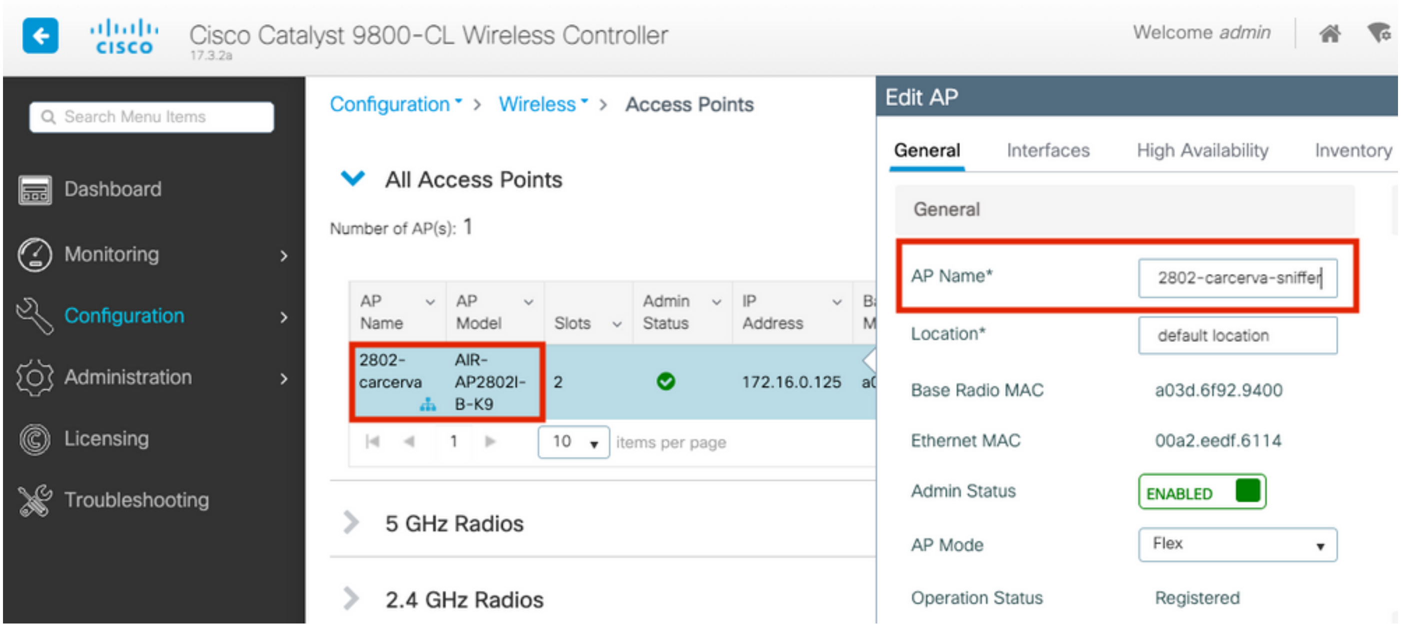
配置

通过GUI在嗅探器模式下配置AP

步骤1.在9800 WLC GUI上，导航至**Configuration > Wireless > Acces Points > All Acces Points**，如图所示。



步骤2.选择希望在嗅探器模式下使用的AP。在**General**选项卡上，更新AP的名称，如图所示。



All Access Points

Number of AP(s): 1

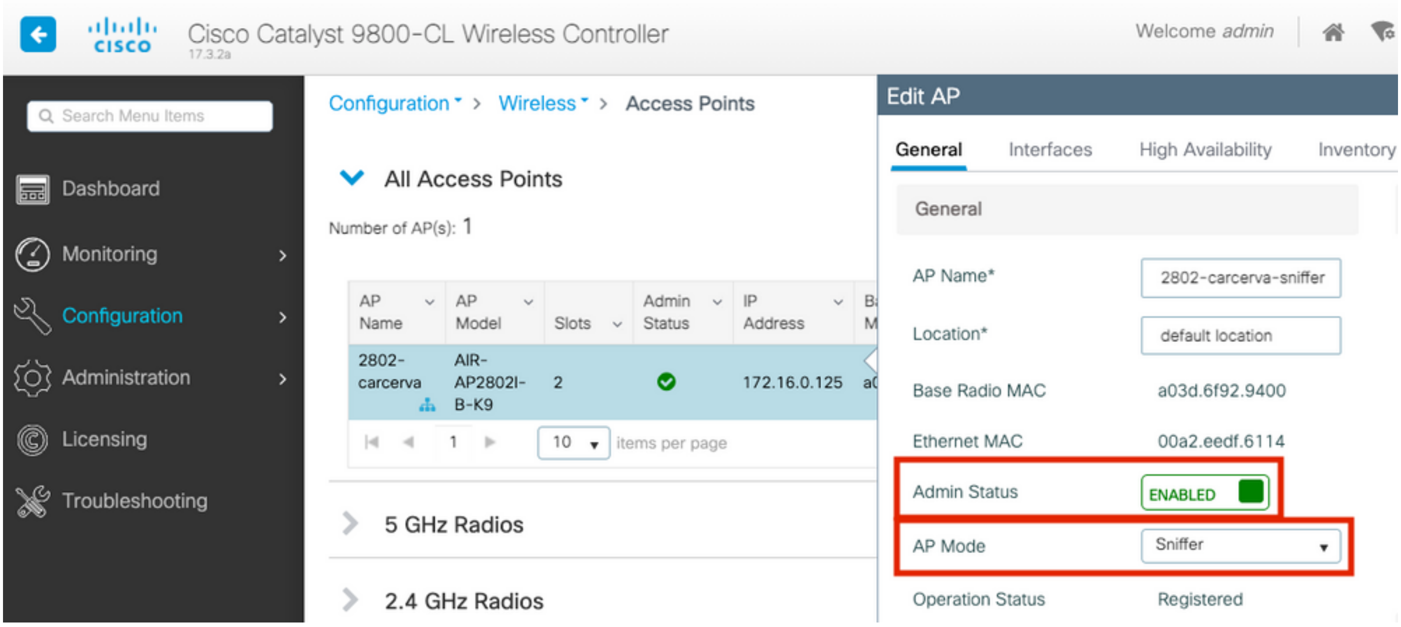
AP Name	AP Model	Slots	Admin Status	IP Address	Ba M
2802-carcerva	AIR-AP2802I-B-K9	2	✓	172.16.0.125	a0

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

步骤3.验证**Admin Status**是否**已启**用，并将**AP Mode**更改为**Sniffer**，如图所示。



All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Ba M
2802-carcerva	AIR-AP2802I-B-K9	2	✓	172.16.0.125	a0

10 items per page

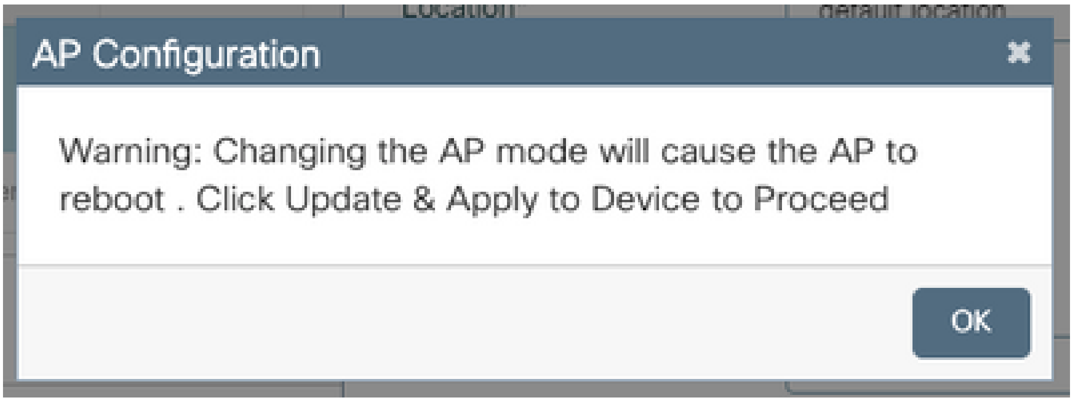
General

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

系统将显示一个弹出窗口，其中包含下一个注释：

"警告：更改AP模式将导致AP重新启动。点击更新并应用到设备以继续”

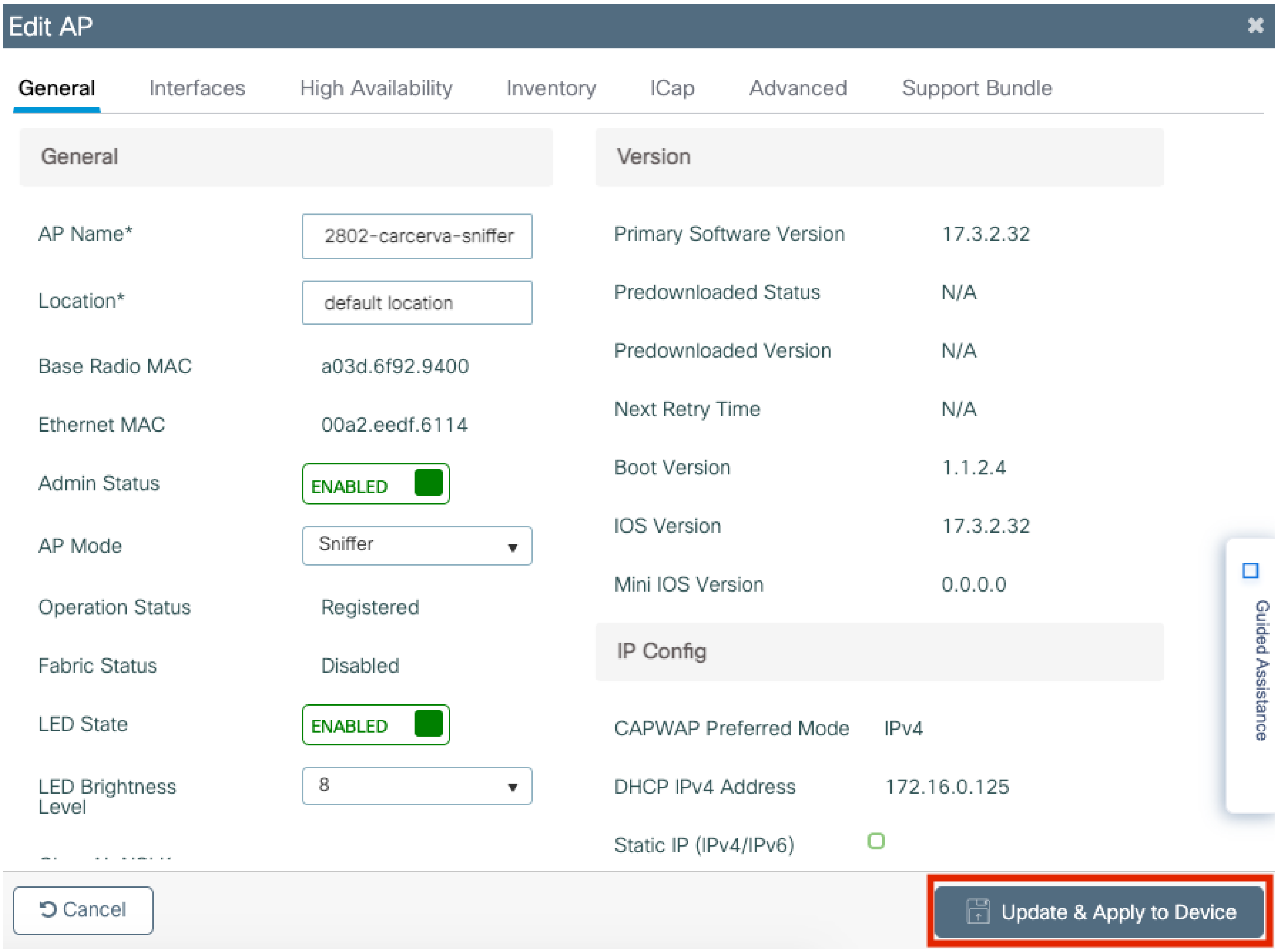
选择**OK**，如图所示。



AP Configuration

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

步骤4.单击“**更新并应用到设备**”，如图所示。



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

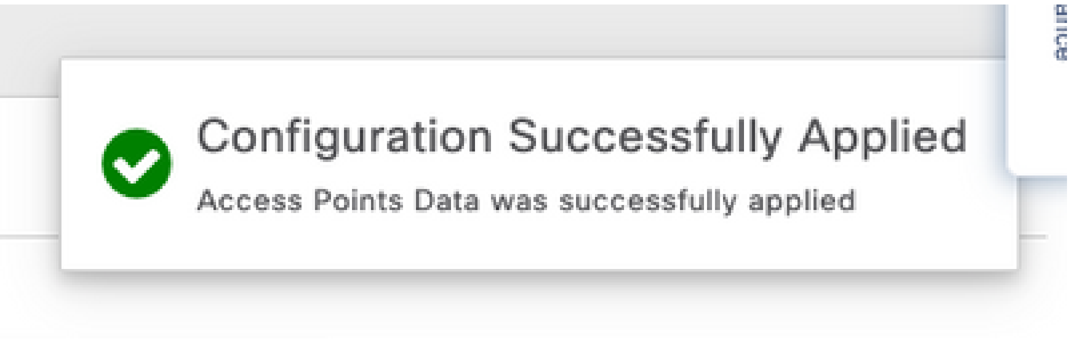
Version

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)	□

系统将显示一个弹出窗口，确认更改和AP退回，如图所示。



Configuration Successfully Applied

Access Points Data was successfully applied

通过CLI在嗅探器模式下配置AP

步骤1.确定希望用作嗅探器模式的AP并获取AP名称。

步骤2.修改AP名称。

此命令修改AP名称。其中，<AP-name>是AP的当前名称。

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

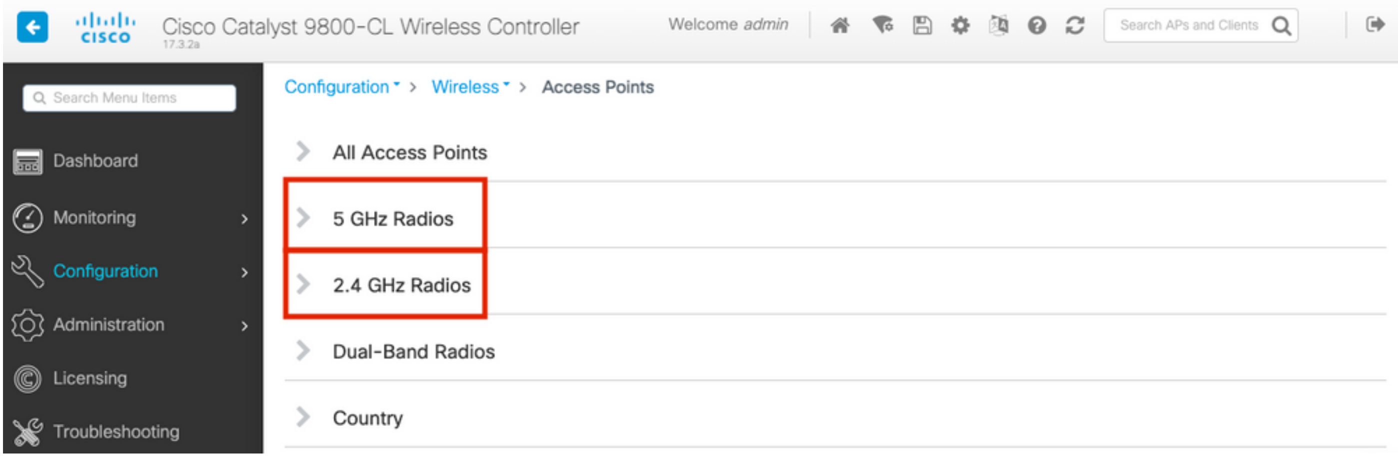
步骤3.在嗅探器模式下配置AP。

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

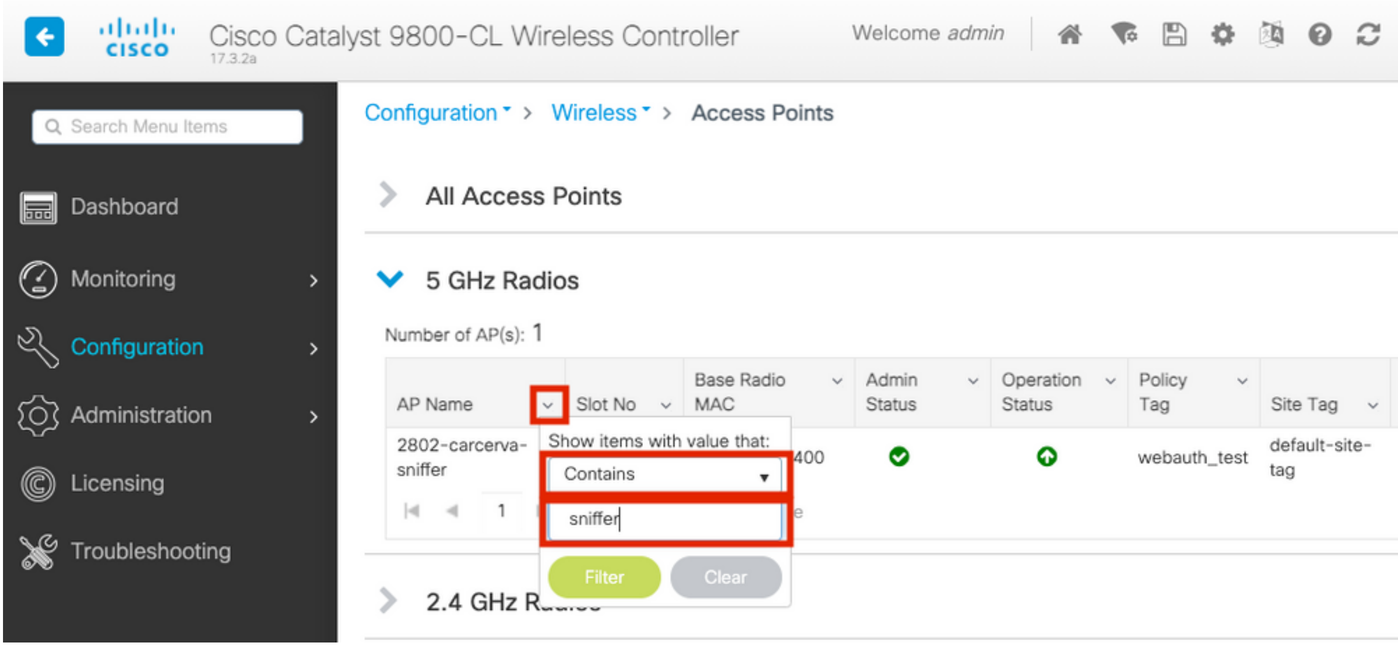
配置AP以通过GUI扫描通道

步骤1.在9800 WLC GUI中，导航至**Configuration > Wireless > Acces Points**。

步骤2.在“接**入点**”页面上，显**示5 GHz**无线电**或2.4 GHz无线电菜**单列表。这取决于要扫描的通道，如图所示。



步骤2.搜索AP。单击向下**箭头**按钮以显示搜索工具，从下拉列表中选**择**“包含”，然后键入**AP名**称，如图所示。



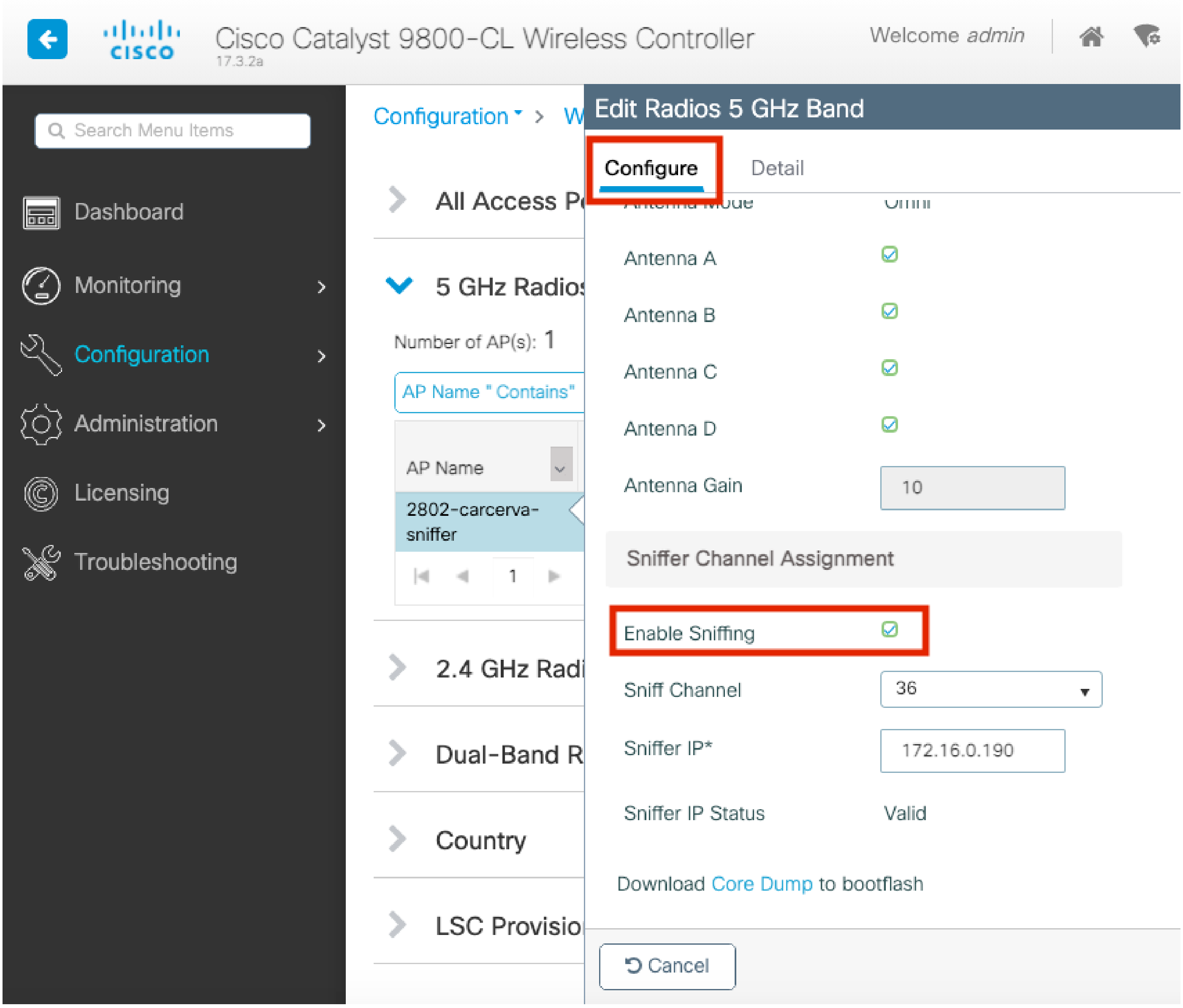
Number of AP(s): 1

Show items with value that: Contains

sniffer

AP Name	Slot No	Base Radio MAC	Admin Status	Operation Status	Policy Tag	Site Tag
2802-carcerva-sniffer		…400	✓	●	webauth_test	default-site-tag

步骤3.选择AP并勾选Configure > Sniffer Channel Assignment**下的Enable Sniffer**复选框，如图所示。



Number of AP(s): 1

2802-carcerva-sniffer

Antenna Mode: Omni

Antenna A ☑

Antenna B ☑

Antenna C ☑

Antenna D ☑

Antenna Gain: 10

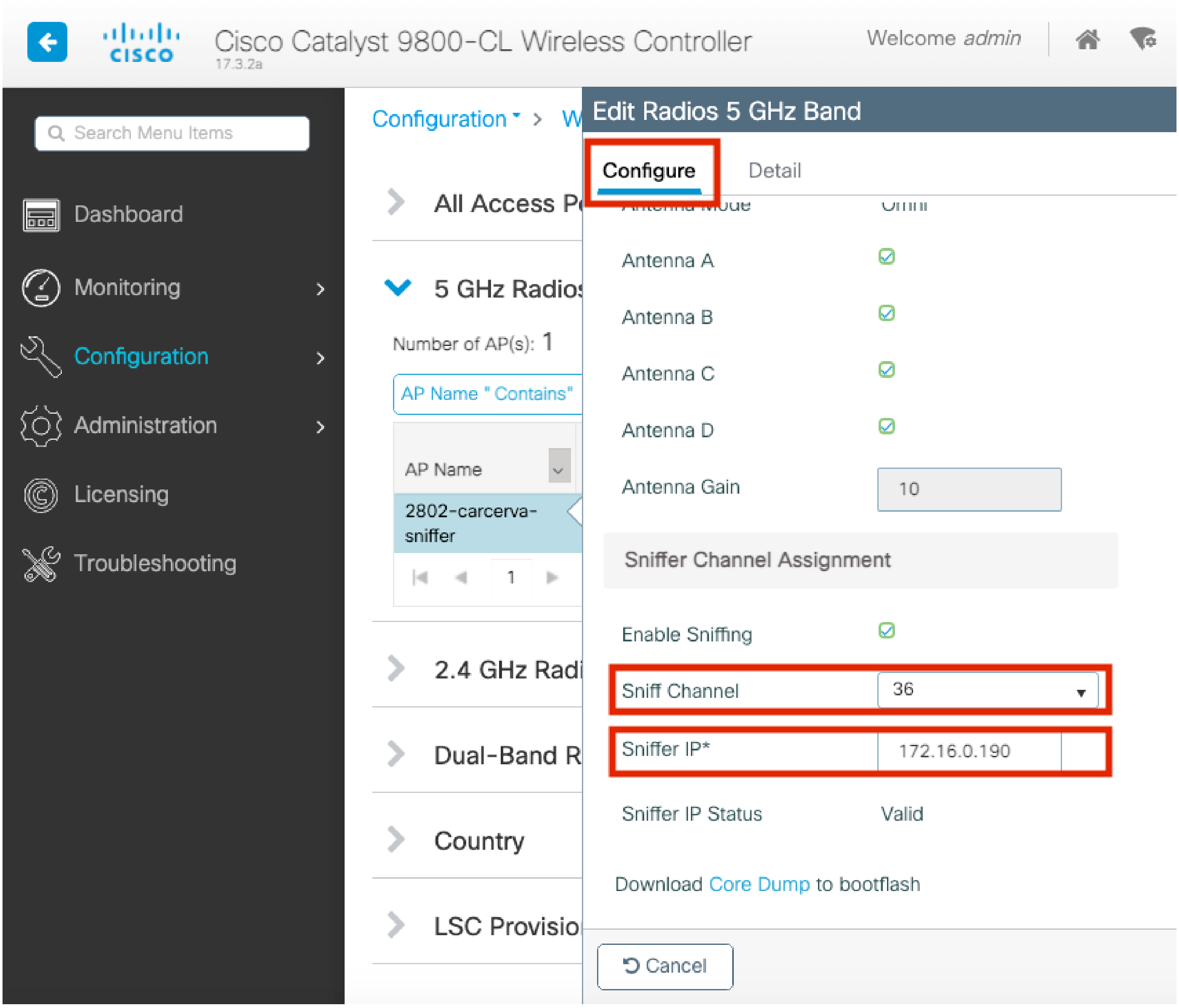
Enable Sniffing ☑

Sniff Channel: 36

Sniffer IP*: 172.16.0.190

Sniffer IP Status: Valid

步骤4.从Sniff Channel下拉列表中**选择Channel**，然后键入**Sniffer IP address**(Server IP address with Wireshark)，如图所示。



Edit Radios 5 GHz Band

Configure | Detail

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

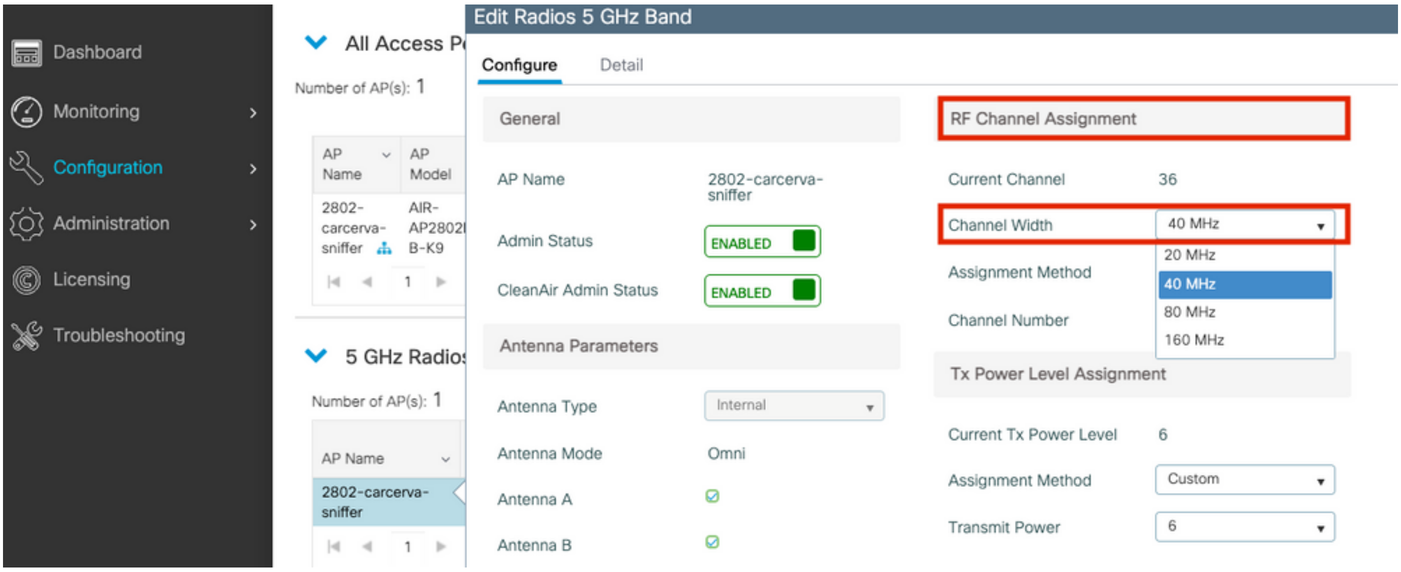
Sniffer IP Status Valid

Download Core Dump to bootflash

Cancel

步骤5.选择目标设备和AP在连接时使用的通道宽度。

导航至**Configure > RF Channel Assignment以配置此配置，如图所示。**



Edit Radios 5 GHz Band

Configure | Detail

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

20 MHz
40 MHz
80 MHz
160 MHz

Assignment Method

Channel Number

Tx Power Level Assignment

Current Tx Power Level 6

Assignment Method Custom

Transmit Power 6

配置AP以通过CLI扫描通道

步骤1.在AP上启用信道嗅探。运行此指令：

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

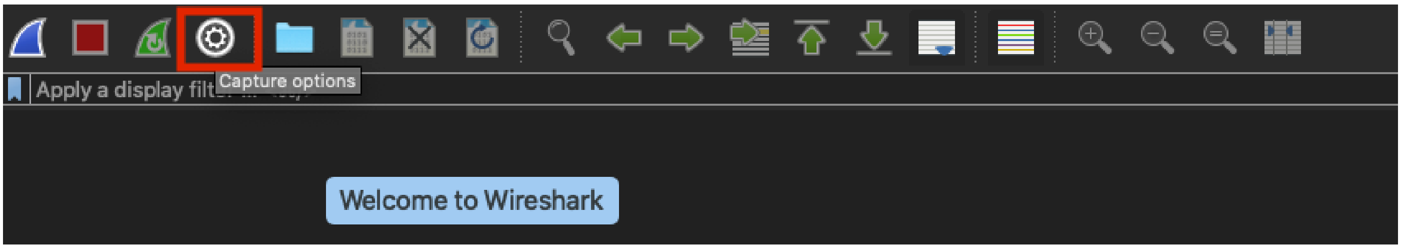
示例：

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

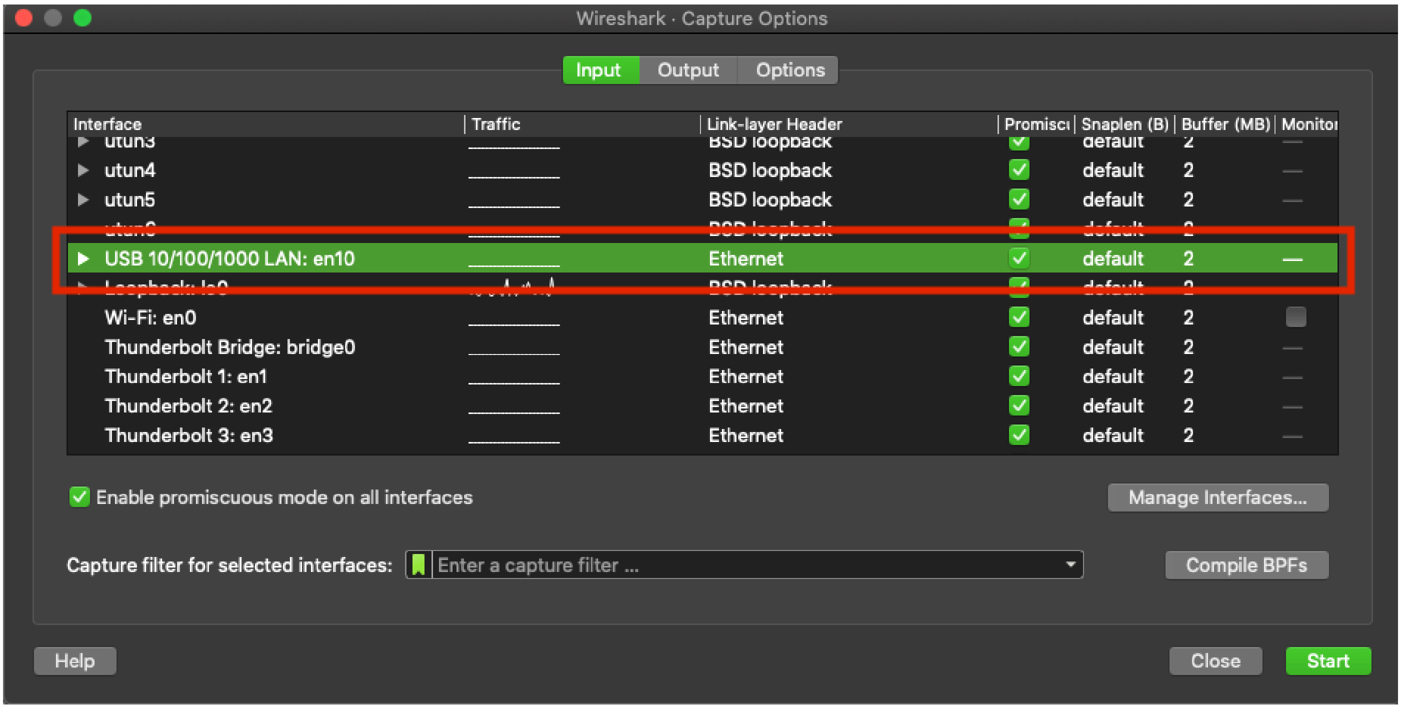
配置Wireshark以收集数据包捕获

步骤1.启动Wireshark。

步骤2.从Wireshark中选择**“捕**获选项”菜单图标，如图所示。



步骤3.此操作将显示弹出窗口。从列表中选择有线接口作为捕获的源，如图所示。

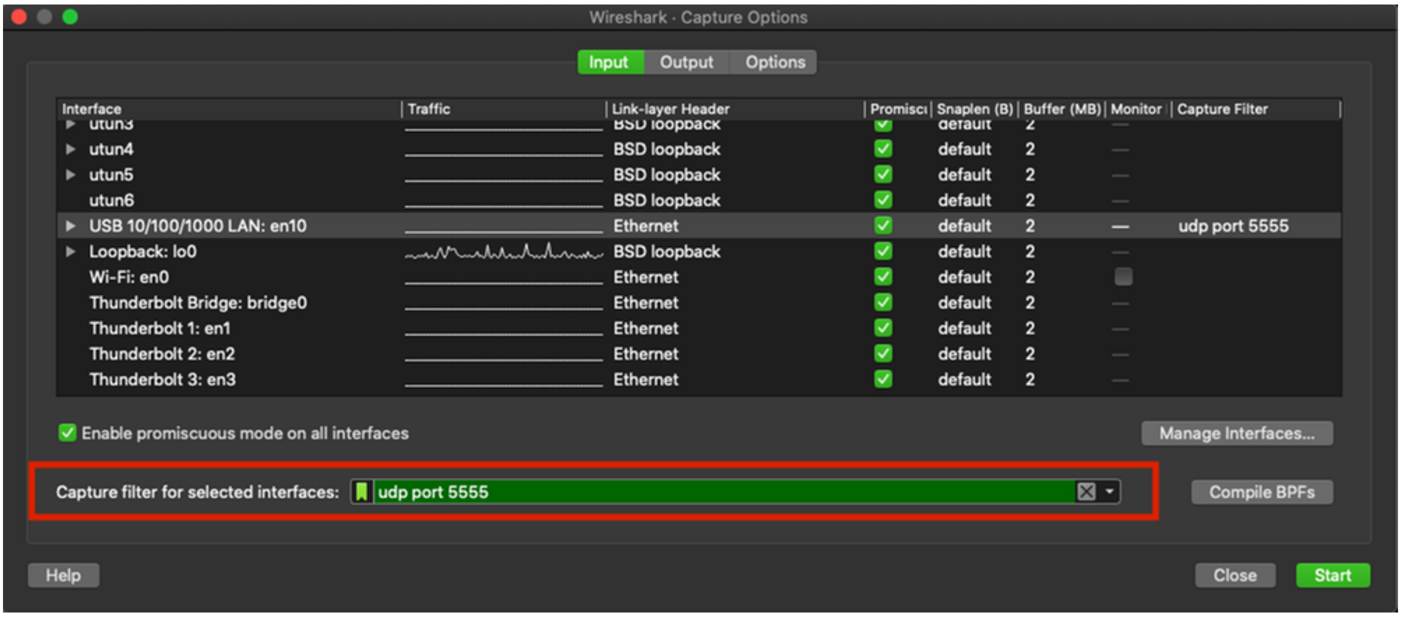


Interface	Traffic	Link-layer Header	Promiscu	Snaplen (B)	Buffer (MB)	Monitor
▶ utun3		BSD loopback	✓	default	2	—
▶ utun4		BSD loopback	✓	default	2	—
▶ utun5		BSD loopback	✓	default	2	—
utun6		BSD loopback	✓	default	2	
▶ USB 10/100/1000 LAN: en10		Ethernet	✓	default	2	—
▶ Loopback: lo0		BSD loopback	✓	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 ...

步骤4.在Capture（捕获）**过滤器下，选择的接口：** 字段框，键**入udp端口5555**，如图所示。

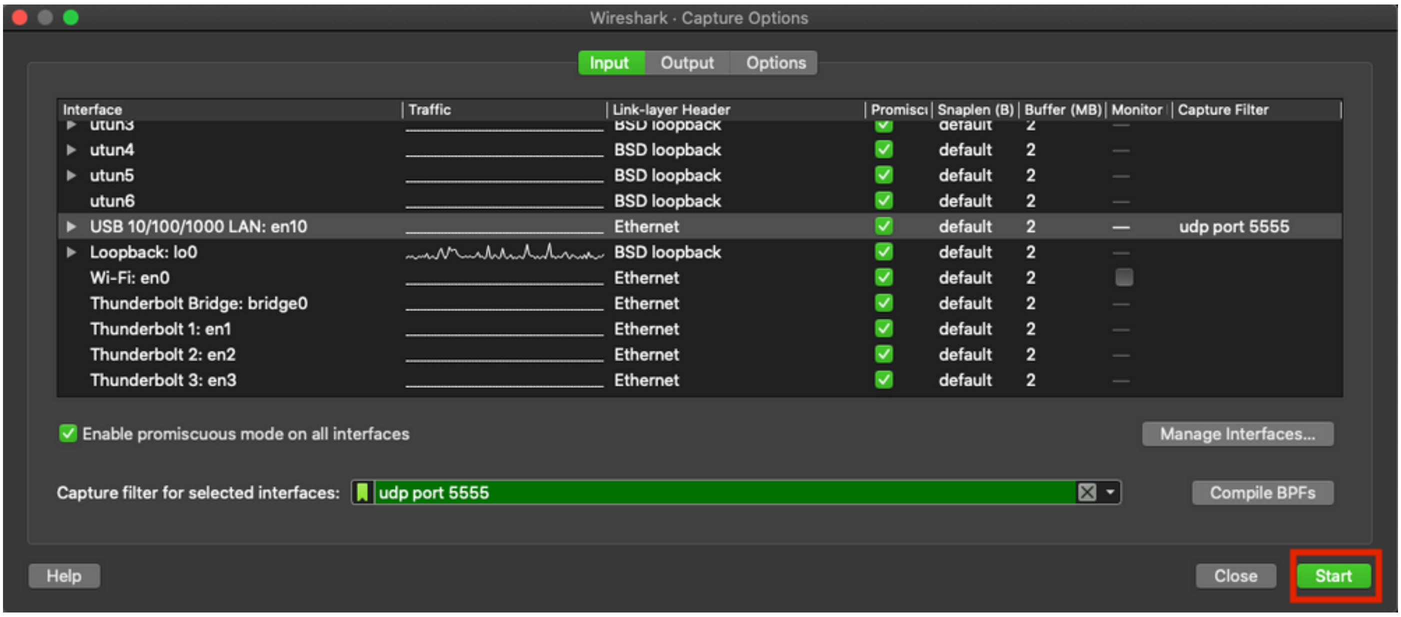


Interface	Traffic	Link-layer Header	Promisci	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
▸ utun3		BSD loopback	✓	default	2		
▸ utun4		BSD loopback	✓	default	2	—	
▸ utun5		BSD loopback	✓	default	2	—	
utun6		BSD loopback	✓	default	2	—	
▸ USB 10/100/1000 LAN: en10		Ethernet	✓	default	2	—	udp port 5555
▸ 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

步骤5.单击“**开始**”，如图所示。

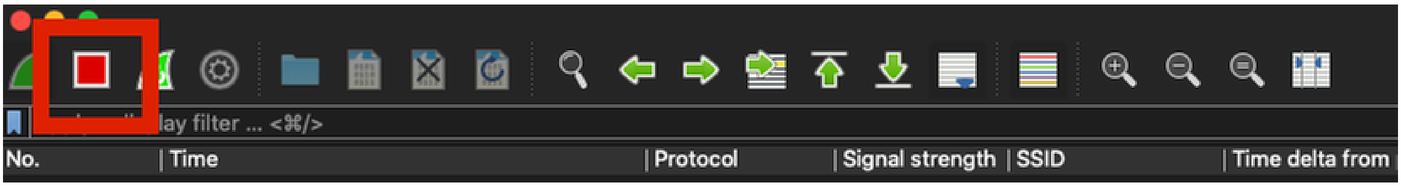


Interface	Traffic	Link-layer Header	Promisci	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
▸ utun3		BSD loopback	✓	default	2		
▸ utun4		BSD loopback	✓	default	2	—	
▸ utun5		BSD loopback	✓	default	2	—	
utun6		BSD loopback	✓	default	2	—	
▸ USB 10/100/1000 LAN: en10		Ethernet	✓	default	2	—	udp port 5555
▸ 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

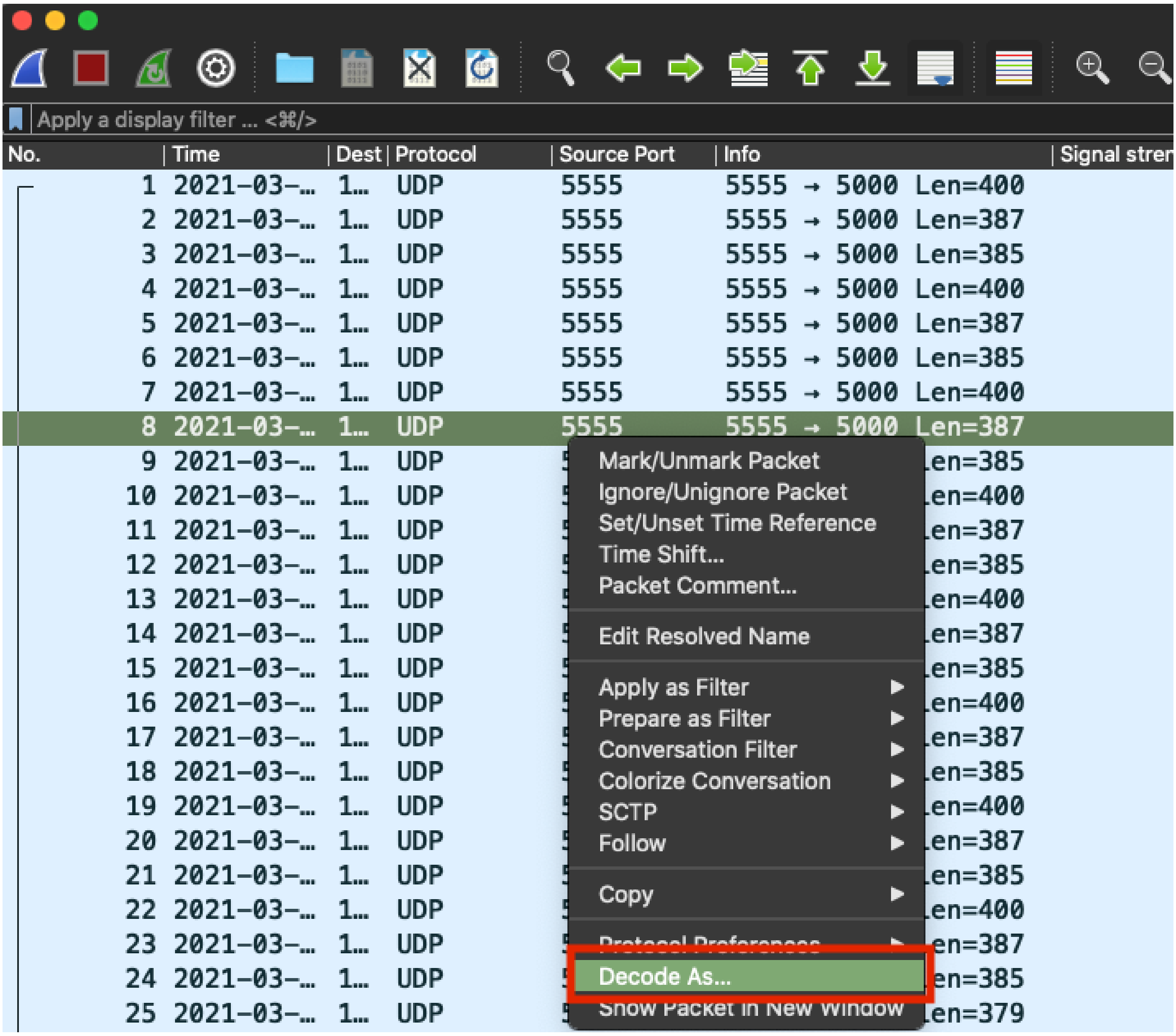
Capture filter for selected interfaces: udp port 5555

步骤6.等待Wireshark收集所需信息，然后从Wireshark中选择“停止”按钮，如图所示。



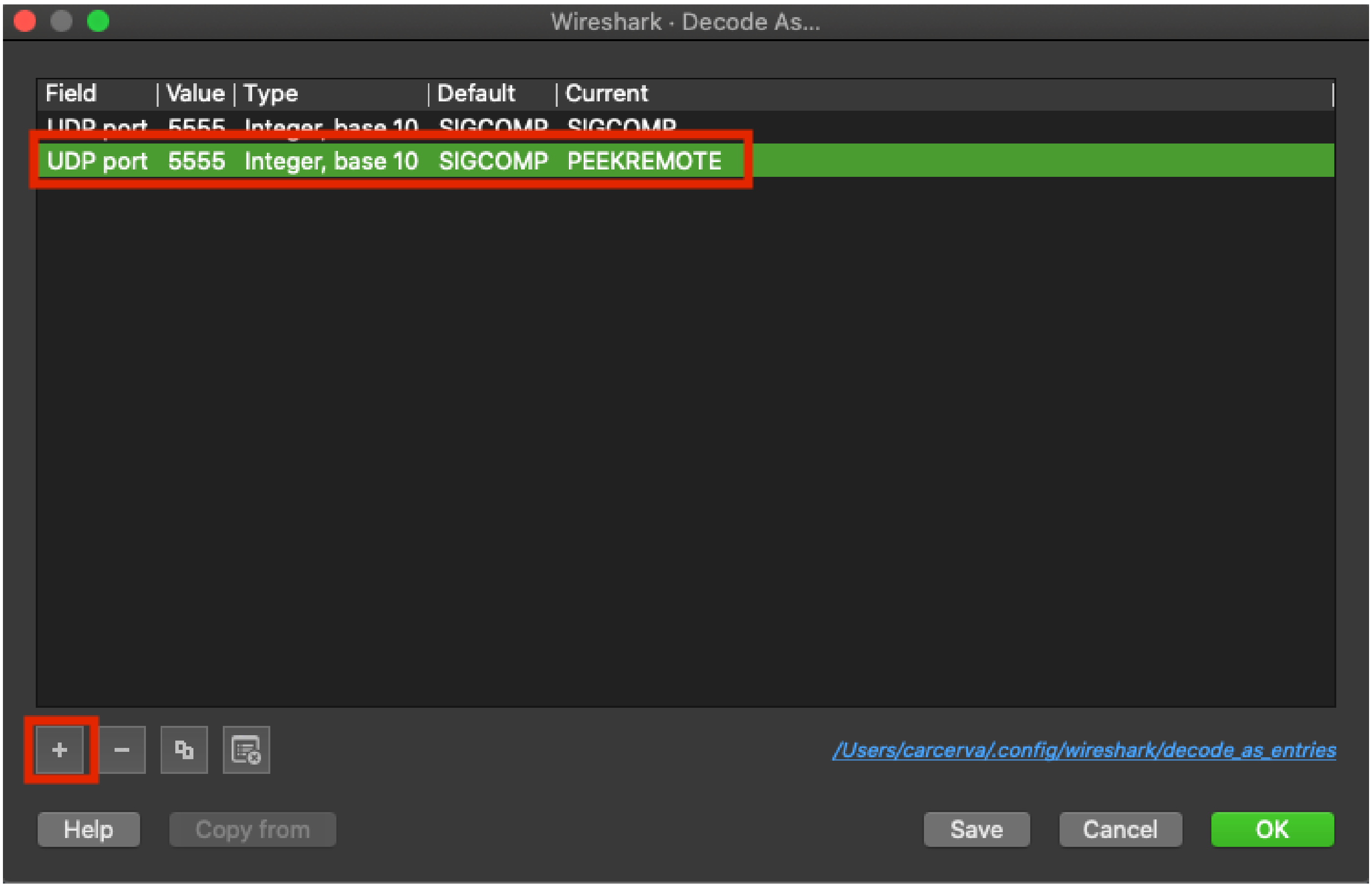
提示：如果WLAN使用加密(如预共享密钥(PSK))，请确保捕获捕获AP与所需客户端之间的四次握手。如果OTA PCAP在设备与WLAN关联之前启动，或者如果客户端在捕获运行期间取消身份验证并重新进行身份验证，则可以执行此操作。

步骤7. Wireshark不会自动解码数据包。要对数据包进行解码，请从捕获中选择一行，使用右键单击显示选项，然后选择**解码为……**，如图所示。



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	

步骤8.系统将显示弹出窗口。选择添加按钮并添加新条目，选择以下选项：**来自字段的UDP端口、来自值的5555、来自默认的SIGCOMP和来自当前的PEEKREMOTE，如图所示。**



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

步骤9.单击**OK**。数据包已解码并准备开始分析。

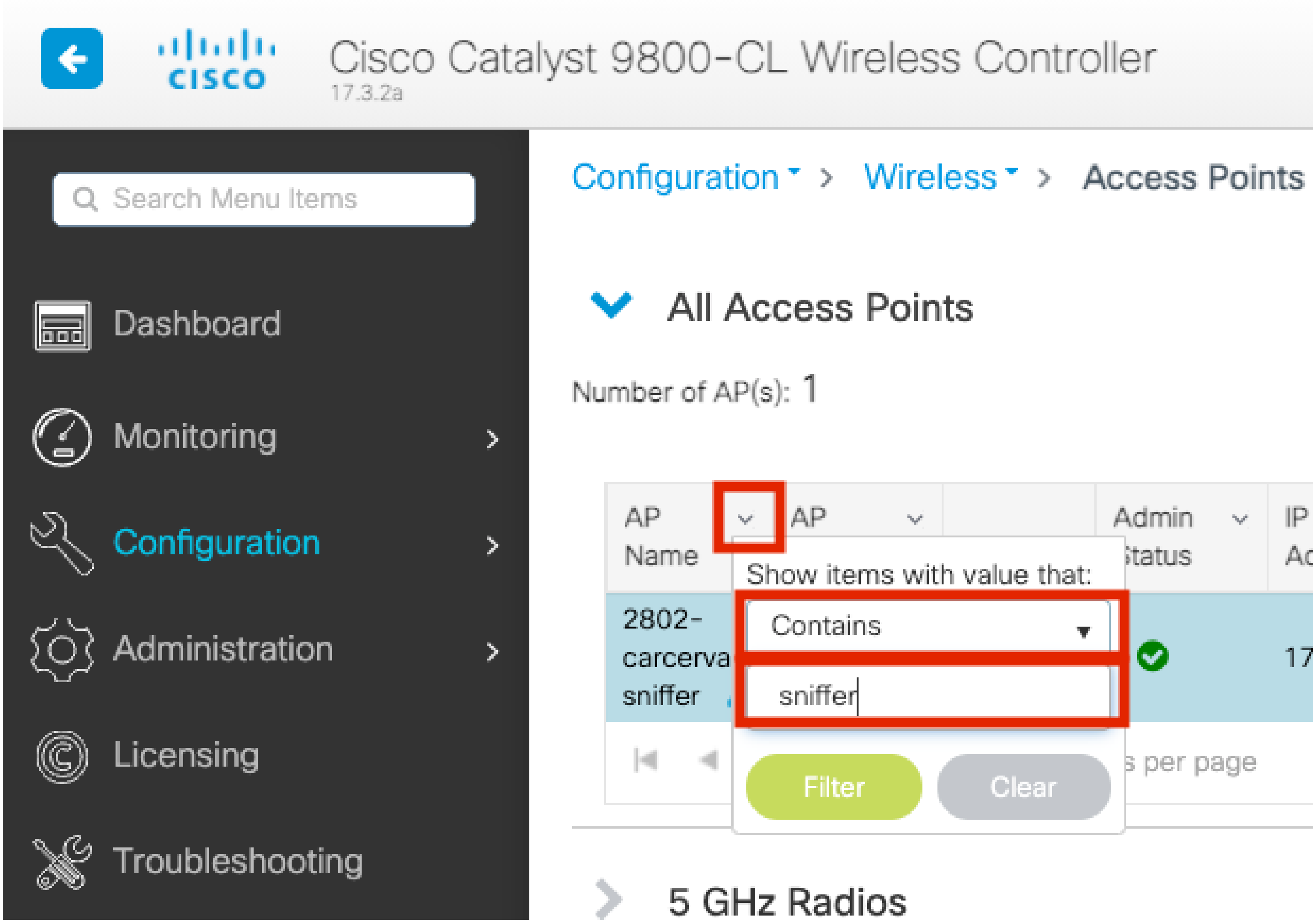
验证

使用本部分可确认配置能否正常运行。

要从9800 GUI确认AP处于嗅探器模式：

步骤1.在9800 WLC GUI上，导航至**Configuration > Wireless > Acces Points > All Acces Points**。

步骤2.搜索AP。单击向下箭头按钮显示搜索工具，从下拉列表中选择**Contains**，然后键入AP名称，如图所示。

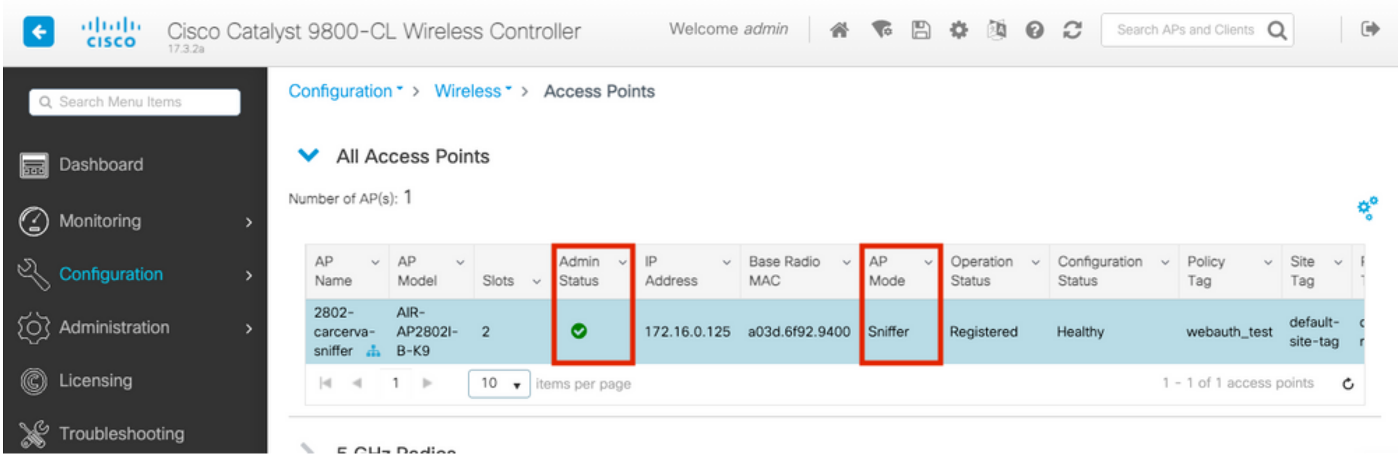


Show items with value that:

Contains

sniffer

步骤3.如图所示，**验**证Admin Status为**绿色,AP Mode** 为**Sniffer**。



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

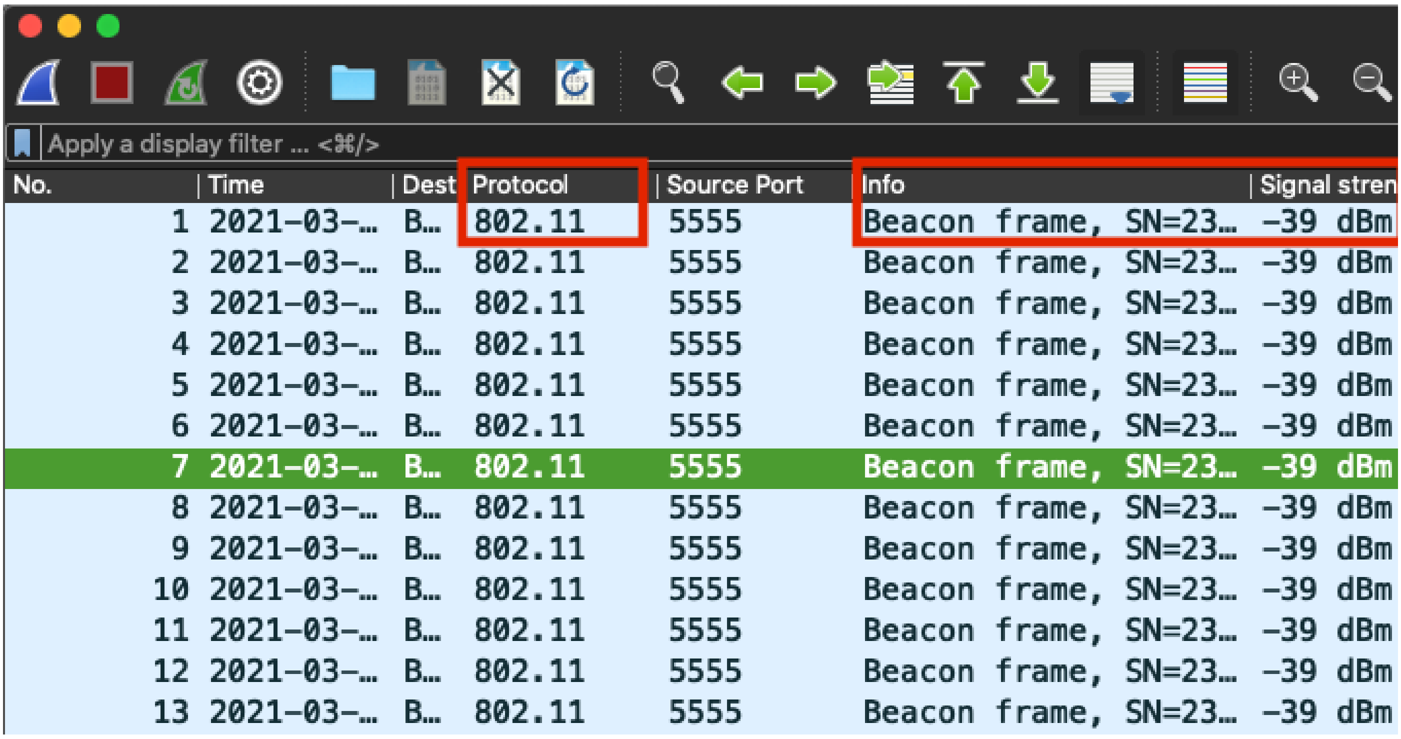
为了从9800 CLI确认AP处于嗅探器模式。运行以下命令：

```
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
```

为了确认数据包在Wireshark上已解码。协议从**UDP更改为802.11**，并且**出现Beacon帧**，如图所示。



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

故障排除

本部分提供了可用于对配置进行故障排除的信息。

问题：Wireshark不从AP接收任何数据。

解决方案：Wireshark服务器必须可通过无线管理接口(WMI)访问。 请确认Wireshark服务器与WLC中的WMI之间的可达性。

相关信息

- Cisco Catalyst 9800系列无线控制器软件配置指南，Cisco IOS XE Amsterdam 17.3.x — 第章：嗅探器模式
- 802.11无线嗅探的基础
- 技术支持和文档 - Cisco Systems