在Catalyst 9800 WC上以嗅探器模式配置AP

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

注意事项

设计注意事项

配置

- 通过GUI在嗅探器模式下配置AP
  - 通过CLI在嗅探器模式下配置AP
- 配置AP以通过GUI扫描所需信道
- 配置AP以通过CLI扫描通道
- 配置Wireshark以收集数据包捕获
- 备用分路点 — 嗅探器AP交换机端口
- 备用分路点 — 9800中的EPC

验证

故障排除

相关信息

简介

本文档介绍如何在Catalyst 9800系列无线控制器(9800 WLC)上以嗅探器模式配置接入点(AP)。

先决条件

要求

Cisco 建议您了解以下主题：

- 9800 WLC配置
- 802.11标准的基本知识

使用的组件

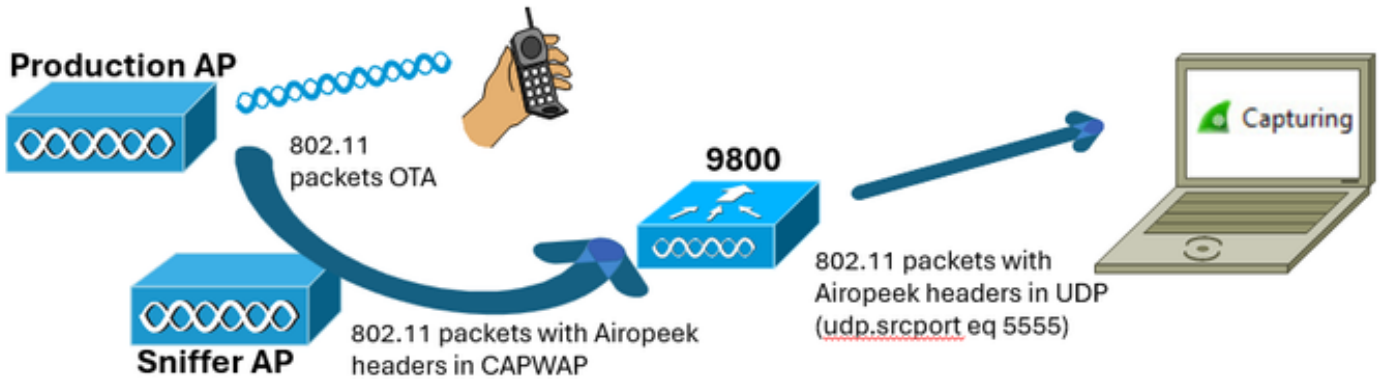
本文档中的信息基于以下软件和硬件版本：

- AP2802、C9130AXI AP
- Wireshark 3.4.4或更高版本
- 9800 WLC Cisco IOS® XE版本17.3.2a和26.1.1

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。

背景信息

嗅探器模式AP是加入到Catalyst 9800控制器的接入点，该控制器的无线电专用于在给定信道上接收所有802.11数据包，并将带有AiroPeek报头的数据包以CAPWAP形式传输到9800。9800会将UDP（源端口5555，目标端口500）中这些被嗅探的数据包转发到IPv4嗅探器目标设备，例如以混杂模式运行Wireshark的计算机。然后可以脱机分析这些数据包。



嗅探器模式下的接入点可通过图形用户界面(GUI)或命令行界面(CLI)进行配置。 本文档还介绍如何使用嗅探器AP收集空中数据包捕获(PCAP)以排除故障和分析无线行为。

注意事项

如果Catalyst 9800通过默认终端学习连接到思科以应用为中心的基础设施(ACI)，请勿使用嗅探器模式AP功能。9800传输其UDP封装的802.11捕获的数据包源自9800s出口IP地址，但源MAC地址设

置为嗅探器AP无线电的MAC，低位半字节设置为0xF。这会导致问题，因为ACI看到来自多个MAC地址的相同IP地址；请参阅Cisco Bug ID CSCwa45713。

设计注意事项

注意事项:

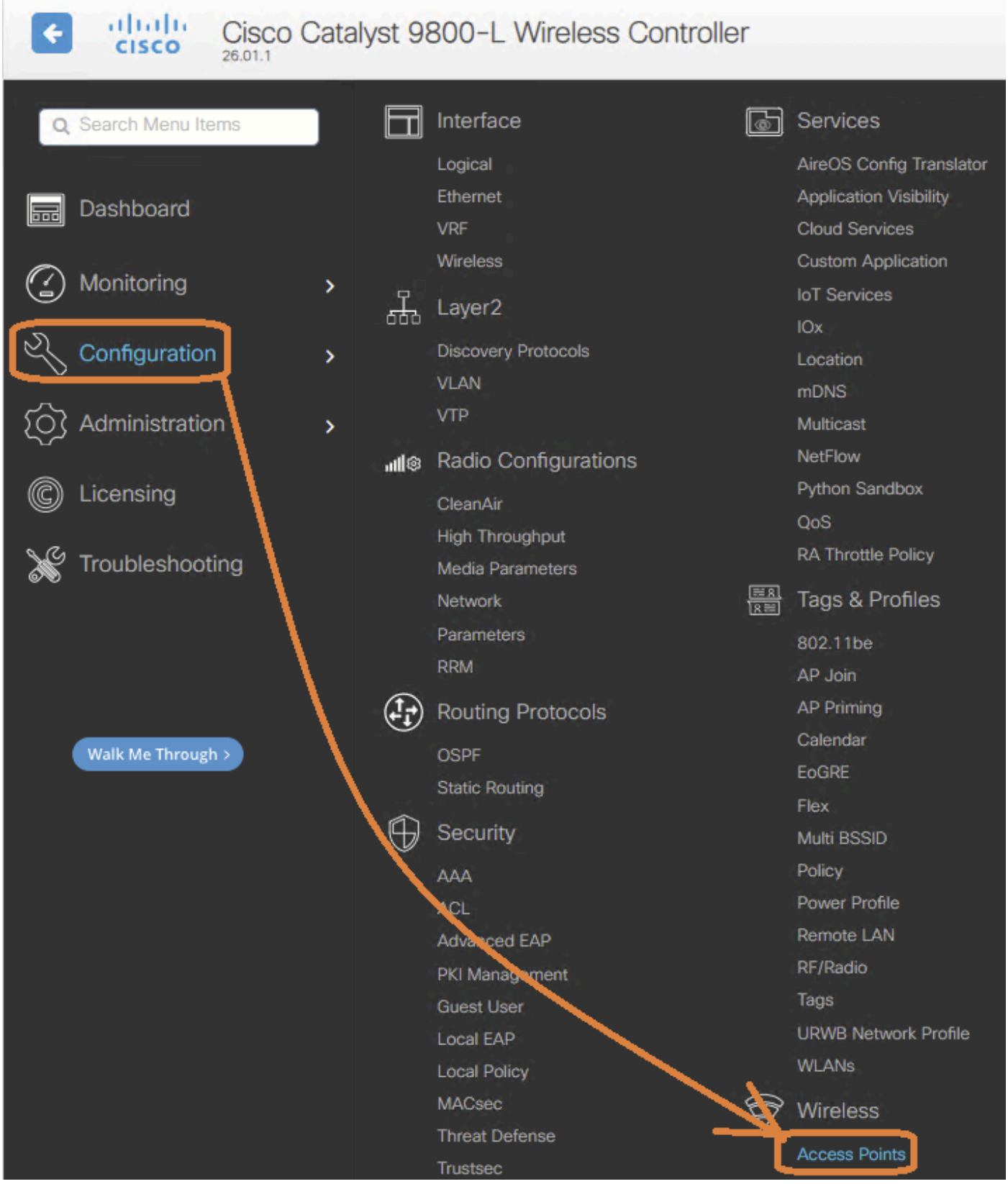
- 建议让嗅探器AP靠近目标设备和连接该设备的AP。如果嗅探器AP远离发射器，则它无法解调大多数数据帧。
- 嗅探器AP可以支持被测试的发射设备和接收设备使用的调制集。例如，如果受测试设备使用802.11ax，则使用802.11ax或802.11be AP进行嗅探，而不使用802.11ac AP，如AP2802。

注意：部署在公共云上的9800-CL不支持嗅探器模式下的AP。

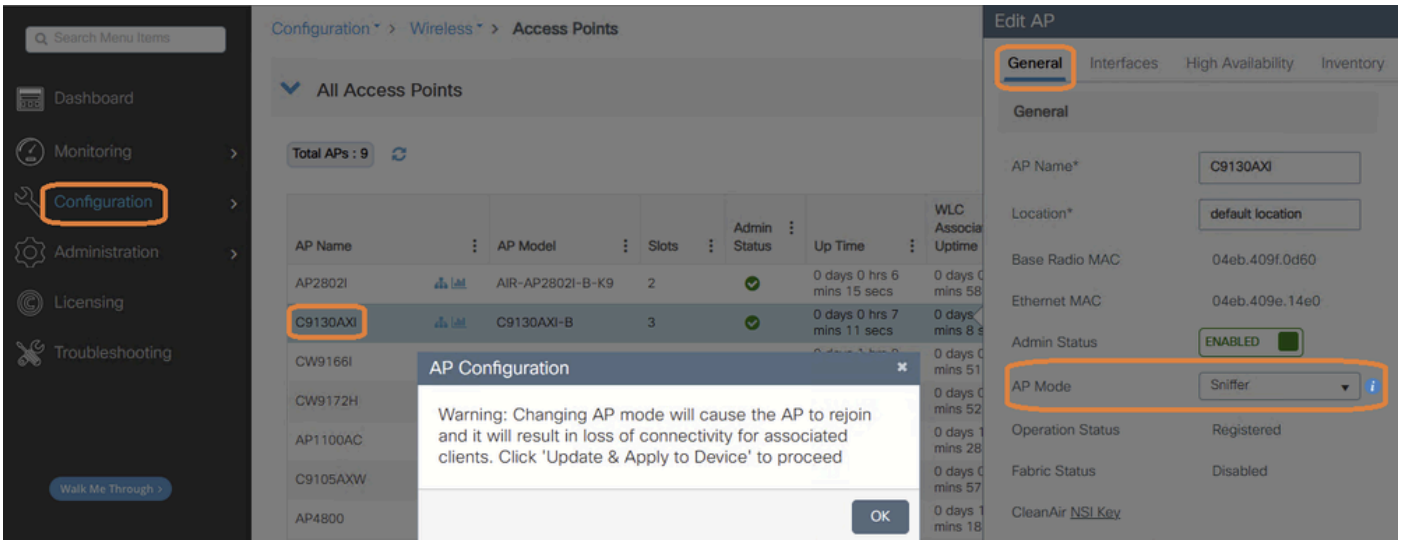
配置

通过GUI在嗅探器模式下配置AP

1.在9800 WLC GUI上，导航到Configuration > Wireless > Access Points > All Access Points，如图所示：



2.选择要用于嗅探器模式的AP。在General选项卡中，确保Admin Status为ENABLED，并将AP Mode设置为Sniffer。在弹出警告中点击OK，然后点击Update & Apply to the device。



---

3. AP解除，几分钟后重新加入。

通过CLI在嗅探器模式下配置AP

1.标识要用作嗅探器模式的AP。

2.将AP配置为嗅探器模式。

<#root>

9800-L#

ap name C9130AXI mode sniffer

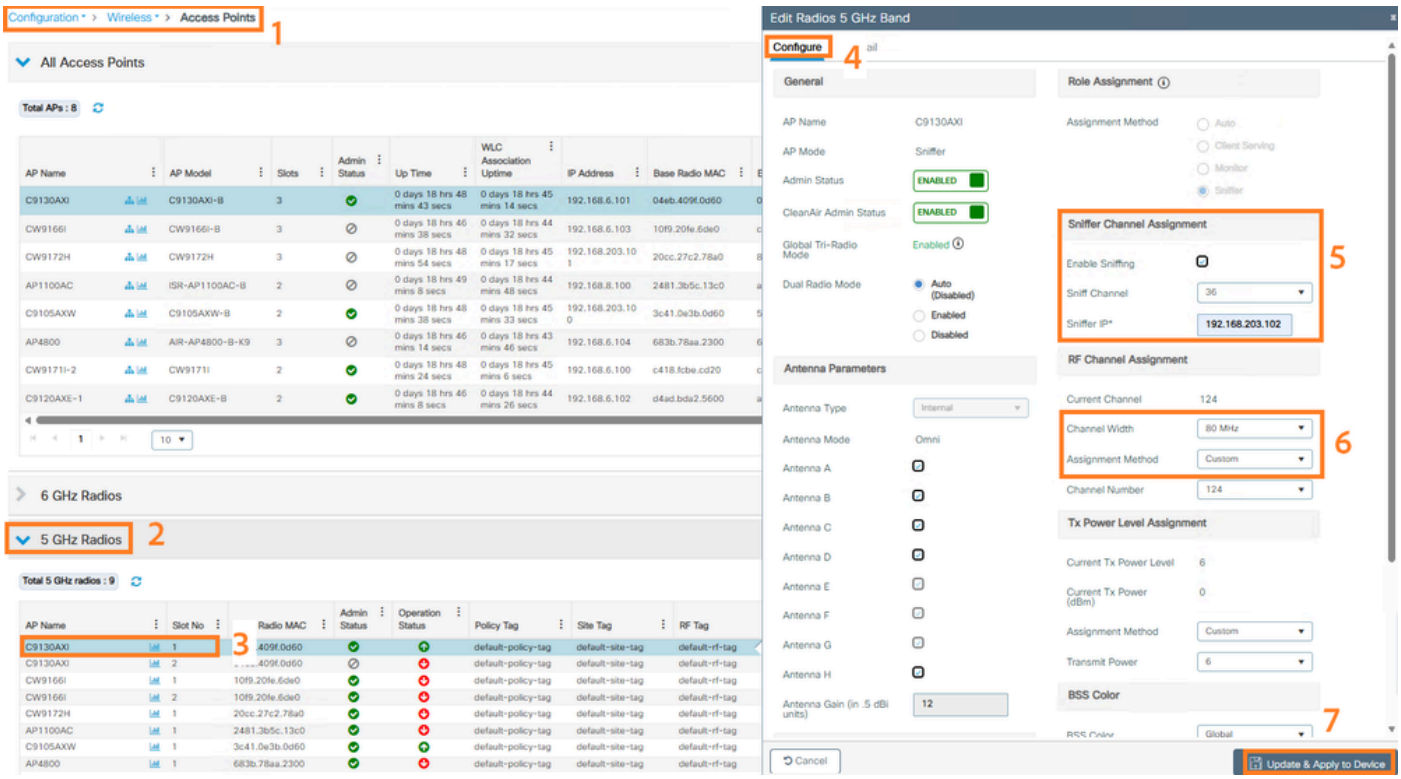
---

3. AP解除，几分钟后重新加入。

配置AP以通过GUI扫描所需信道

1.在Configuration > Wireless > Access Points(1)中，向下滚动以查找所需频段的嗅探器AP无线电。在本示例中，在5 GHz无线电(2)下，AP C9130AXI的Slot 1无线电(3)。 配置该无线电(4)以启用嗅探(5)，将所需信道分配给嗅探，并输入嗅探设备的IP地址。

2.在“RF信道分配”(6)下，将分配方法设置为自定义，然后在下拉列表中设置所需的信道宽度。单击更新和应用于设备(7)。



配置AP以通过CLI扫描通道

1.将信道配置为在AP上嗅探并执行以下命令：

<#root>

9800-L#

ap name

<ap-name>

dot11 sniff

{24ghz | 5ghz | 6ghz}

slot

示例：

<#root>

9800-L#

ap name C9130AXI dot11 5ghz slot 1 sniff 36 192.168.203.102

2.配置信道宽度：

<#root>

9800-L#

ap name

<ap-name>

dot11

{24ghz | 5ghz | 6ghz}

slot

channel width

示例：

<#root>

9800-L#

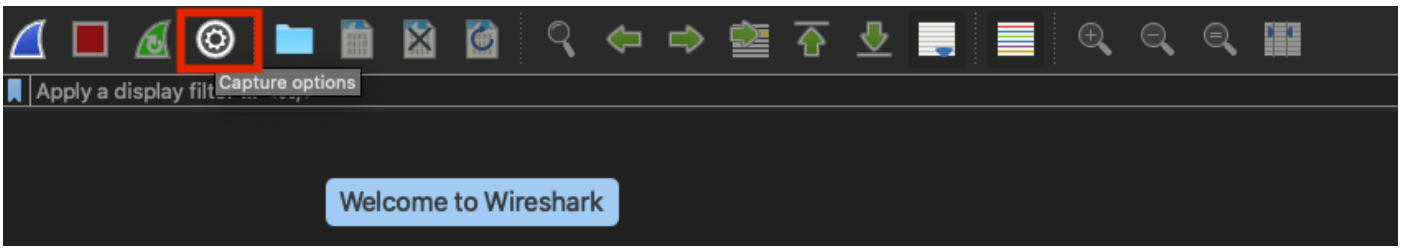
ap name C9130AXI dot11 5ghz slot 1 channel width 40

此时，嗅探器AP正在通过空中数据包进行捕获，并将它们以CAPWAP形式发送到9800。然后，9800将嗅探到的数据包转发到捕获设备。

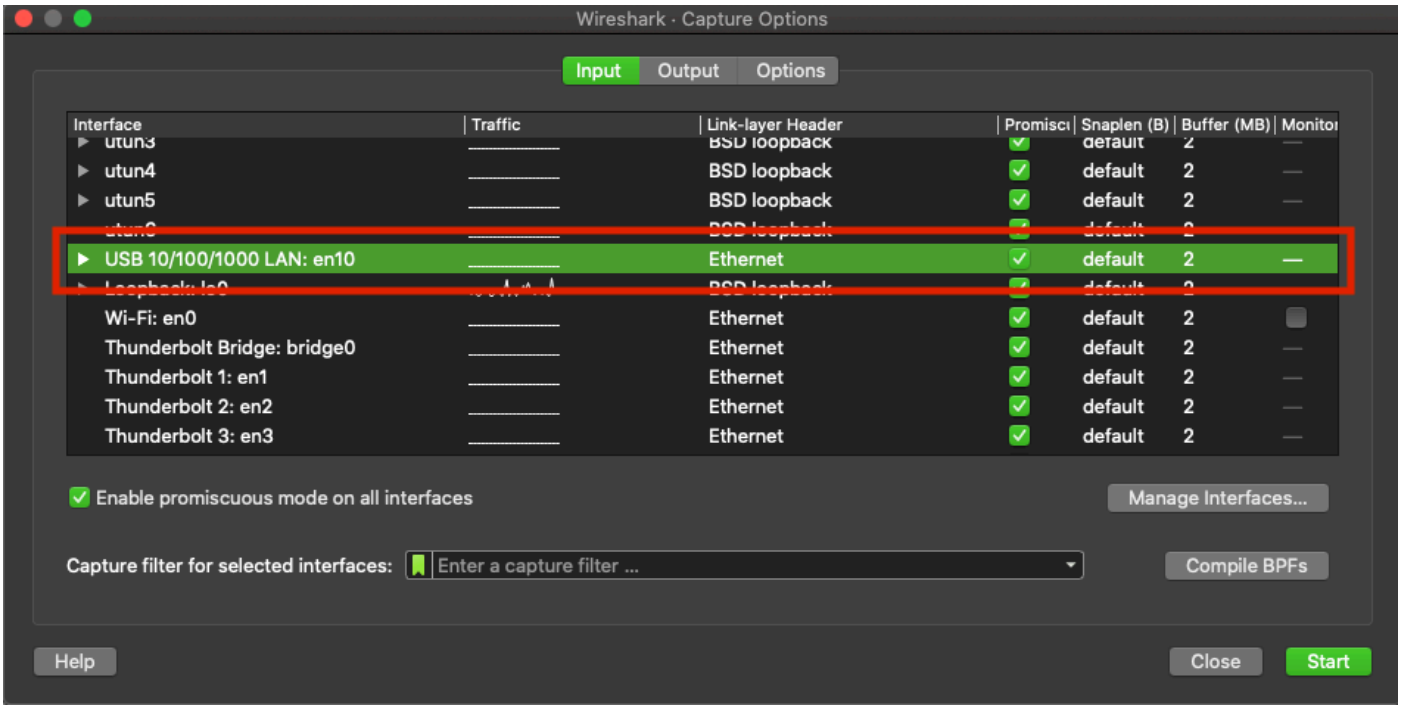
配置Wireshark以收集数据包捕获

1.启动Wireshark。

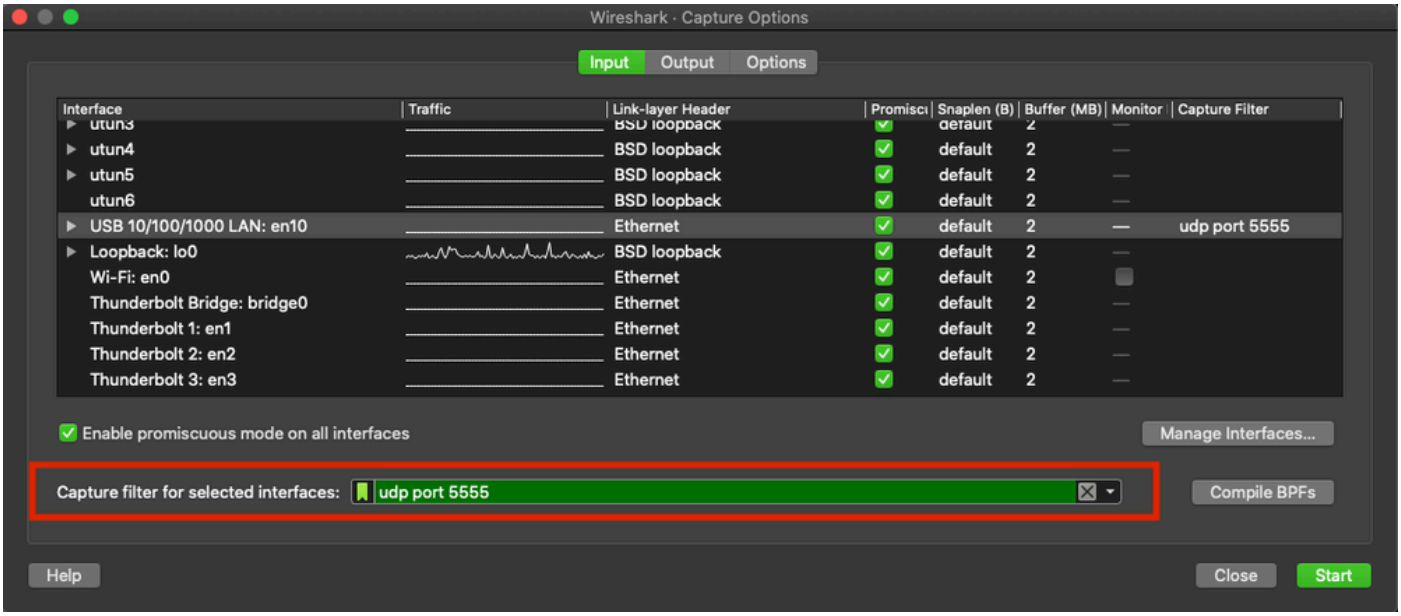
2.从Wireshark中选择“捕获”选项菜单图标：



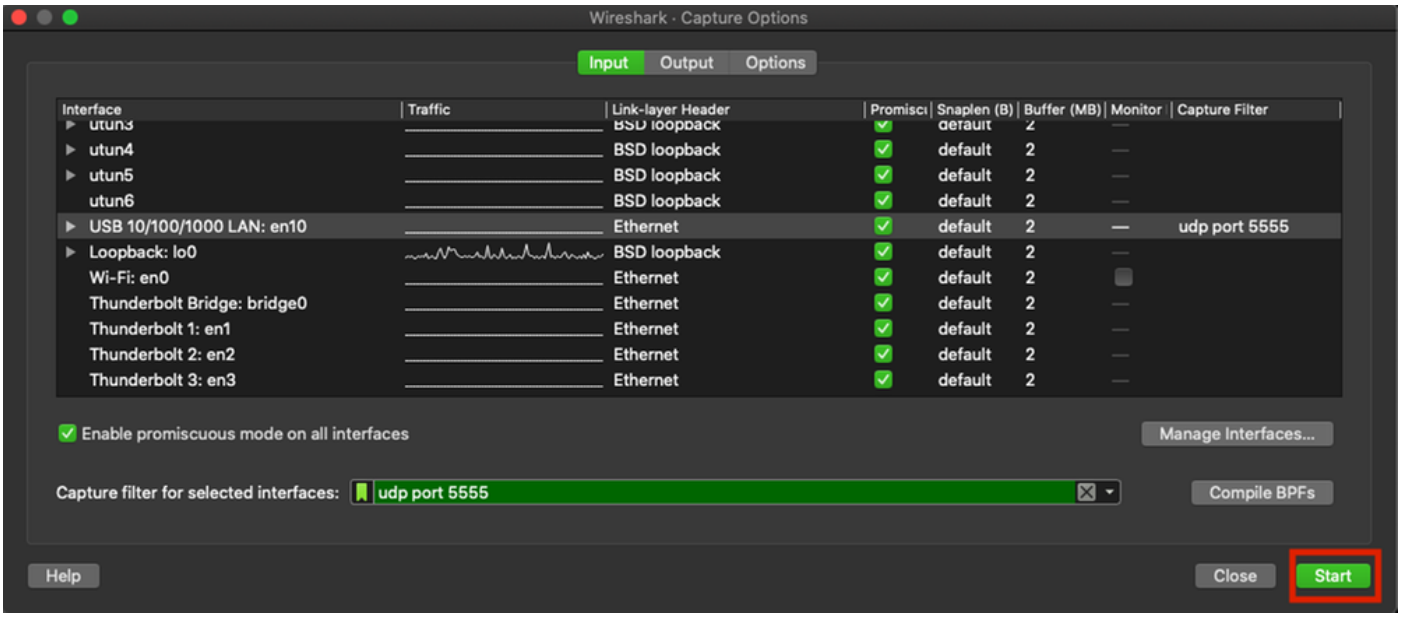
3.此操作会显示一个弹出窗口。从列表中选择Wired Interface作为捕获源。确保选中Promiscuous选项。



4.在Capture filter for selected interfaces字段框下，键入udp port 5555，如图所示：



5.单击开始。

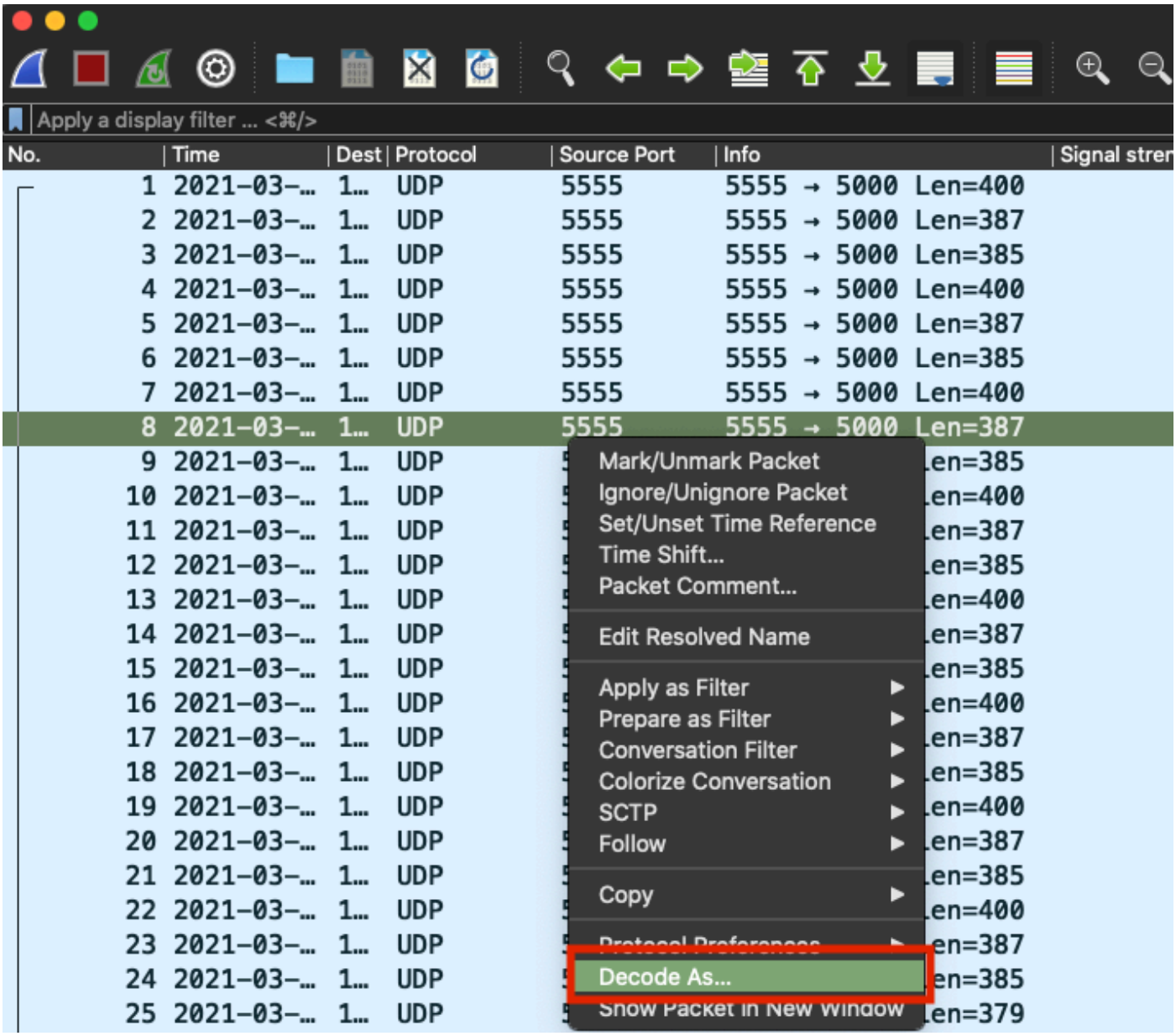


6.等待Wireshark收集所需信息，然后从Wireshark中选择Stop按钮。

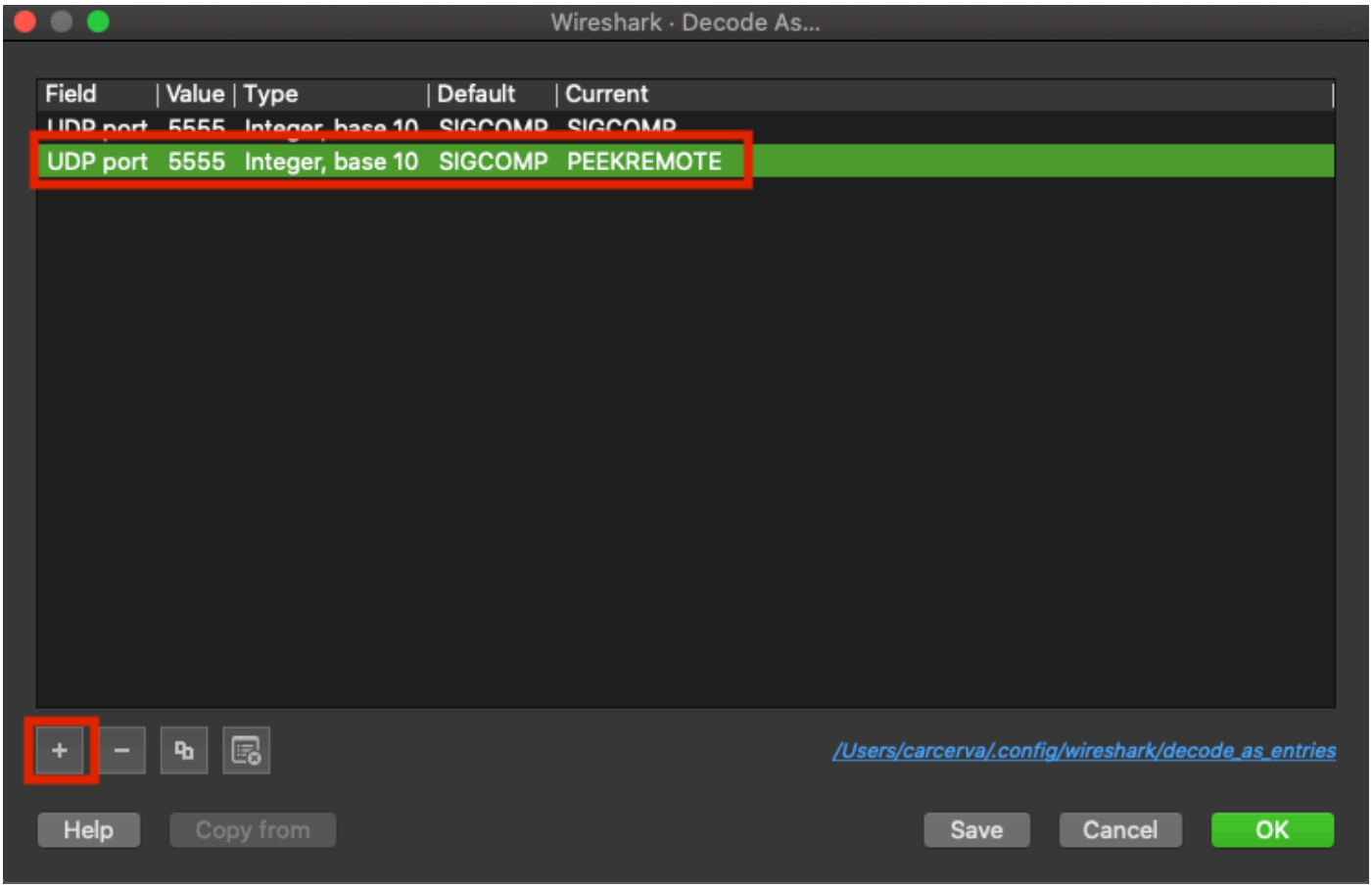


提示：如果WLAN使用加密(如预共享密钥(PSK))，请确保捕获捕获捕获在AP和所需客户端之间的四次握手。如果OTA PCAP在设备与WLAN关联之前启动，或者如果客户端在捕获运行时取消身份验证并重新进行身份验证，则可以完成此操作。

7. Wireshark不会自动解码数据包。要解码数据包，请从捕获中选择line，然后右键单击以显示选项，然后选择Decode As...



8.系统将显示一个弹出窗口，单击+符号选择添加按钮并添加新条目。选择以下选项：UDP端口来自Field、5555来自Value、SIGCOMP来自Default和PEEKREMOTE来自Current。



9.单击确定。数据包已解码并准备好开始分析。

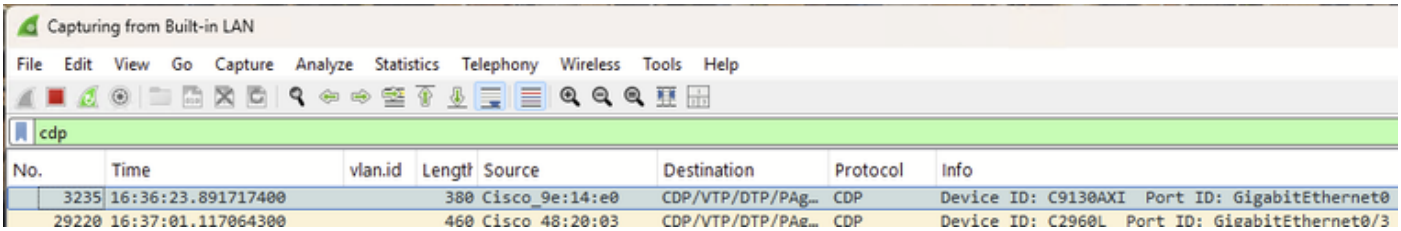
备用分路点 — 嗅探器AP交换机端口

作为捕获源自控制器的嗅探数据包的替代方案，您可以将嗅探器AP交换机端口跨接到有线嗅探器。这捕获封装在CAPWAP中的Airopeek格式化的802.11数据包。如果从AP到9800的链路CAPWAP链路有损失，则有避免损失的好处。

在9800上，您可以运行show ap name <APNAME> cdp neighbors命令来查找AP的交换机名称、IP地址和交换机端口。将LAN嗅探器（例如PC或具有LAN接口的MacBook）连接到AP交换机上的空闲交换机端口。运行Wireshark并将其设置为混杂模式，以捕获从交换机端口接收的所有数据包（如上所述）。在交换机上，运行如下命令以跨AP:

```
switch(config)#monitor session 1 source interface Gi0/3
switch(config)#monitor session 1 destination interface Gi0/19
```

其中Gi0/3是嗅探器AP的交换机端口，GI0/19是LAN嗅探器被点击的交换机端口。要在LAN嗅探器上验证它是否成功地从AP交换机端口收集了范围，可以在cdp上过滤捕获的数据包：



备用分路点 — 9800中的EPC

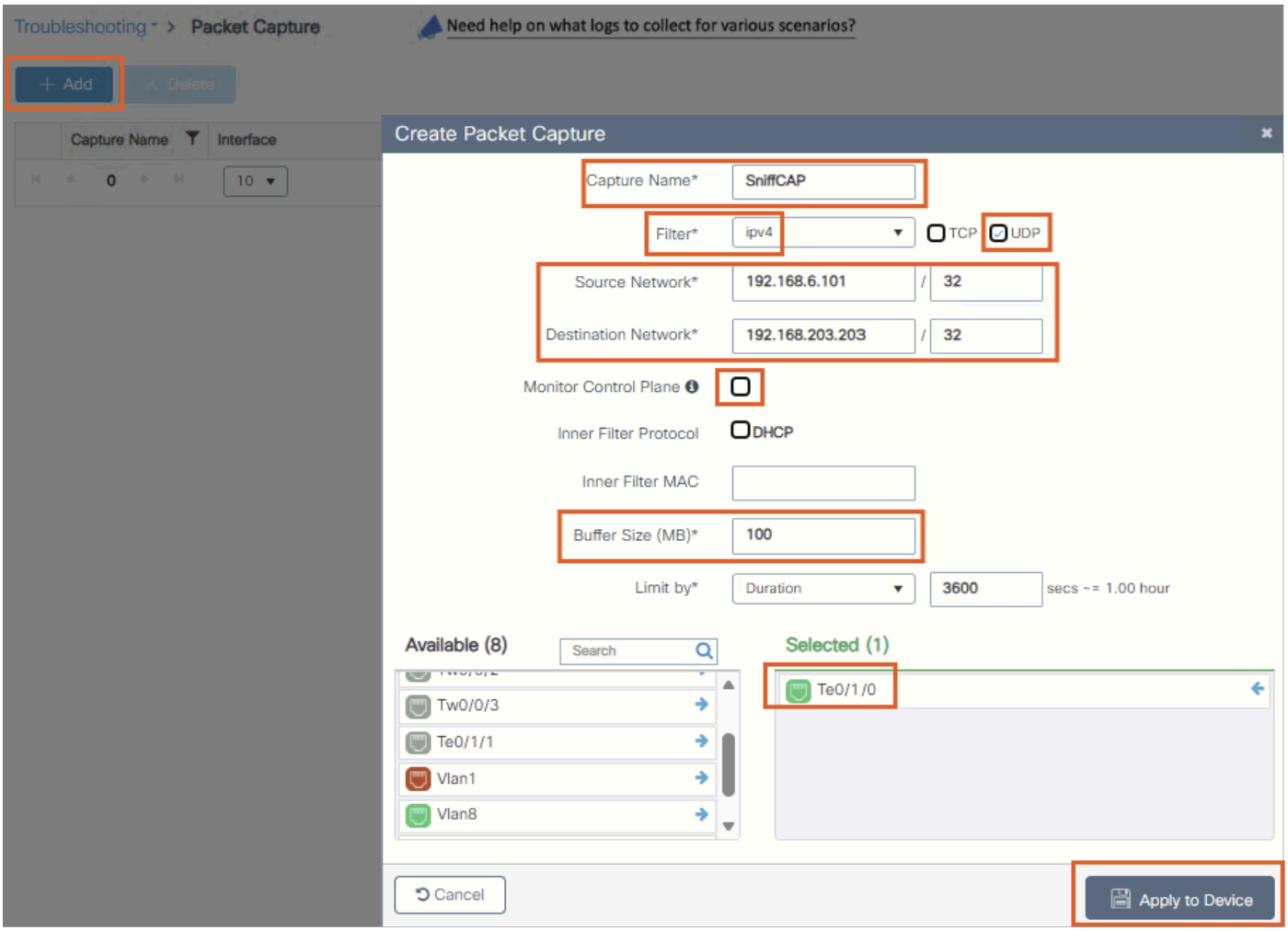
另一个选项是通过9800中的嵌入式数据包捕获(EPC)捕获嗅探的数据包。这非常方便，因为它不需要额外的嗅探器设备进行捕获。

1.在GUI中，导航到故障排除>数据包捕获。

2.通过为捕获点指定捕获名称来添加该捕获点。

3.配置IPv4过滤器，在UDP上将AP的IP地址与源地址匹配，并将9800s WMI地址与目标地址匹配。取消选中Monitor Control Plane。

4.将缓冲区大小增加到最大值(100 MB)，选择WMI接口，然后单击Apple to Device。



5.然后，在Capture Name列表中，为刚创建的捕获点单击Start。捕获感兴趣的事件后，单击Stop，然后单击Export。

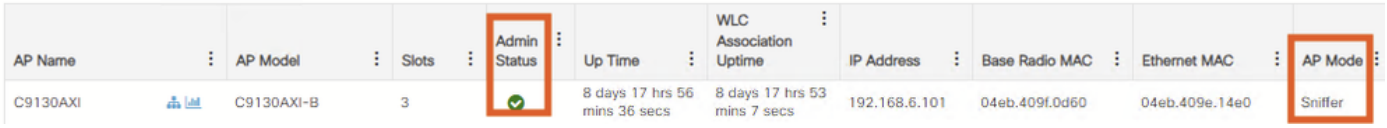
6.您可以导出到桌面，然后在Wireshark中打开文件。与上面的AP交换机端口span方法一样，捕获在CAPWAP中包含UDP（源端口5555）中Aeropeek格式的802.11帧。

验证

使用此部分可确认您的配置正常工作。要从9800 GUI确认AP处于嗅探器模式：

1.在9800 WLC GUI中，导航到配置>无线>接入点>所有接入点。

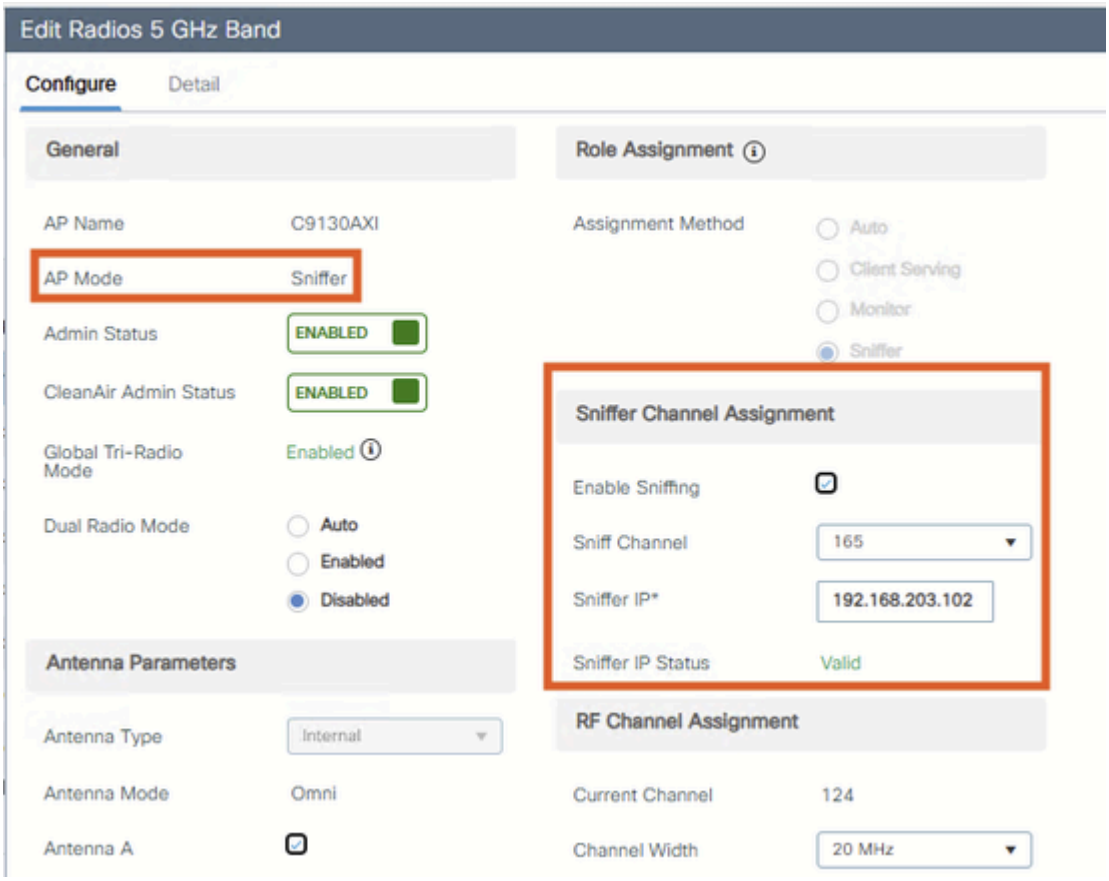
2.查找嗅探器AP;验证Admin Status为绿色，并且AP Mode显示Sniffer。



AP Name	AP Model	Slots	Admin Status	Up Time	WLC Association Uptime	IP Address	Base Radio MAC	Ethernet MAC	AP Mode
C9130AXI	C9130AXI-B	3		8 days 17 hrs 56 mins 36 secs	8 days 17 hrs 53 mins 7 secs	192.168.6.101	04eb.409f.0d60	04eb.409e.14e0	Sniffer

---

3.查找嗅探器APs无线电。验证sniffing是否已启用，并根据需要设置信道分配。检查嗅探器IP状态是否准确，这表示9800与其具有IP连接。



4.要确认AP在9800 CLI中处于嗅探器模式，请运行以下命令：

<#root>

9800-L#

show ap name C9130AXI config general | include Administrative

Administrative State : Enabled

9800-L#

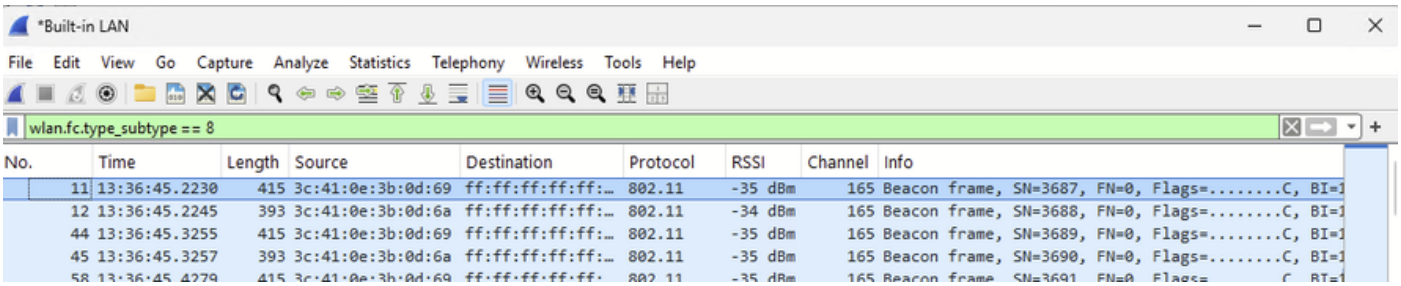
```
show ap name C9130AXI config general | include Sniff
```

```
AP Mode : Sniffer
```

9800-L#

```
show ap name C9130AXI config dot11 5Ghz | include Sniff
AP Mode : Sniffer
Sniffing : Enabled
Sniff Channel : 165
Sniffer IP : 192.168.203.102
Sniffer IP Status : Valid
Radio Mode : Sniffer
Radio Role : Sniffer
```

5.为了确认Wireshark正确解码802.11帧，并且嗅探器AP已定位在靠近所需设备的位置，请对802.11信标(wlan.fc.type_subtype == 和显示RSSI(wlan_radio.signal_dbm):



故障排除

问题：Wireshark不会从AP接收任何数据。

解决方案：必须从无线管理接口(WMI)访问Wireshark服务器。 确认Wireshark服务器与WLC中的WMI之间的连通性。

相关信息

- 802.11 无线嗅探分析和故障排除
- 技术支持和文档 - Cisco Systems

- Cisco Catalyst 9800系列无线控制器软件配置指南，Cisco IOS XE Amsterdam 17.18.x — 章节：嗅探器模式

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。