在Catalyst 9800無線控制器上以監聽器模式設定存取點

目錄

簡介
必要條件
- 需求
- 採用元件

背景資訊
注意事項
設定
- 網路圖表
- 組態
  - 通過GUI在監聽器模式下配置AP
  - 在監聽器模式下通過CLI配置AP
  - 配置AP以通過GUI掃描通道
  - 配置AP以通過CLI掃描通道
  - 配置Wireshark以收集資料包捕獲

驗證
疑難排解
相關資訊

簡介

本文說明如何在Catalyst 9800系列無線控制器(9800 WLC)上以監聽器模式設定存取點(AP)。

必要條件

需求

思科建議您瞭解以下主題：

- 9800 WLC組態
- 802.11標準的基本知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- AP 2802
- 9800 WLC Cisco IOS® XE版本17.3.2a
- Wireshark 3.4.4或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

可通過圖形使用者介面(GUI)或命令列介面(CLI)配置處於監聽器模式的接入點。 本文亦涵蓋如何透過監聽器AP收集空中封包擷取(PCAP)，以便進行無線行為疑難排解和分析。

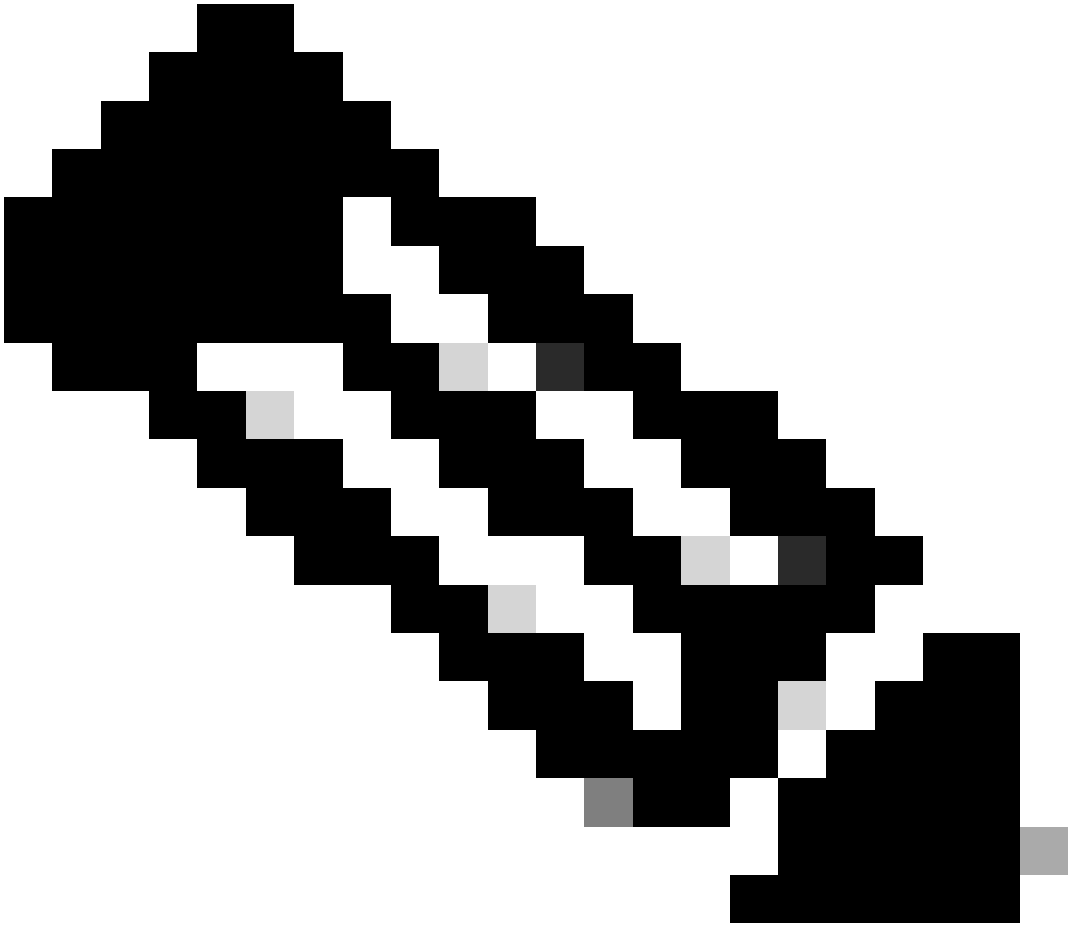
注意事項

如果9800連線到思科以應用為中心的基礎設施(ACI)，且帶有預設終端學習，則不要使用監聽器模式AP功能。 9800會傳輸其UDP封裝的802.11擷取封包，這些封包來源於9800的輸出IP位址，但來源MAC位址是監聽器AP無線電的MAC，且低位半位元組設定為0x0F。 這會導致問題，因為ACI看到來自多個MAC地址的相同IP地址。 請參閱思科錯誤ID CSCwa45713
.

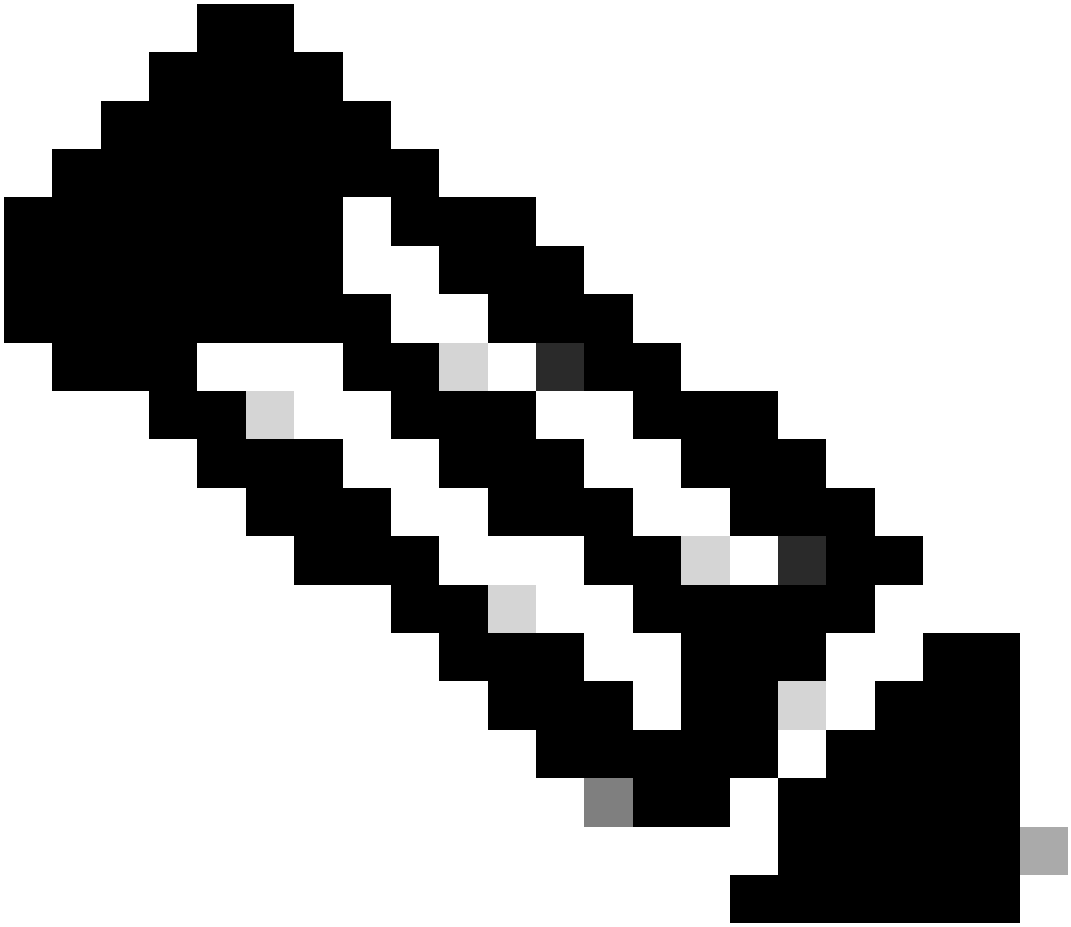
設定

需要考慮的事項：

- 建議讓監聽器AP靠近目標裝置以及此裝置所連線的AP。
- 確保您知道客戶端裝置和AP使用哪個802.11通道和寬度。

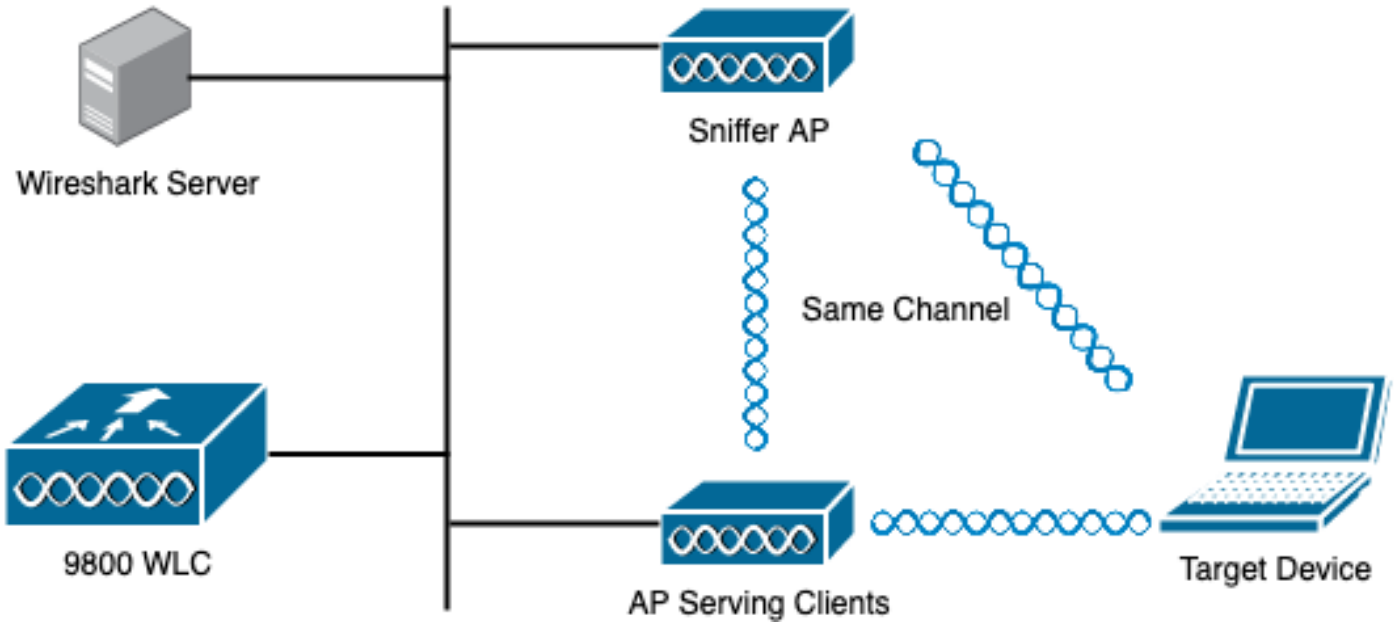


附註：當控制器L3介面是無線管理介面(WMI)時，不支援監聽器模式。



附註：部署在公共雲上的9800-CL不支援處於監聽器模式的AP。

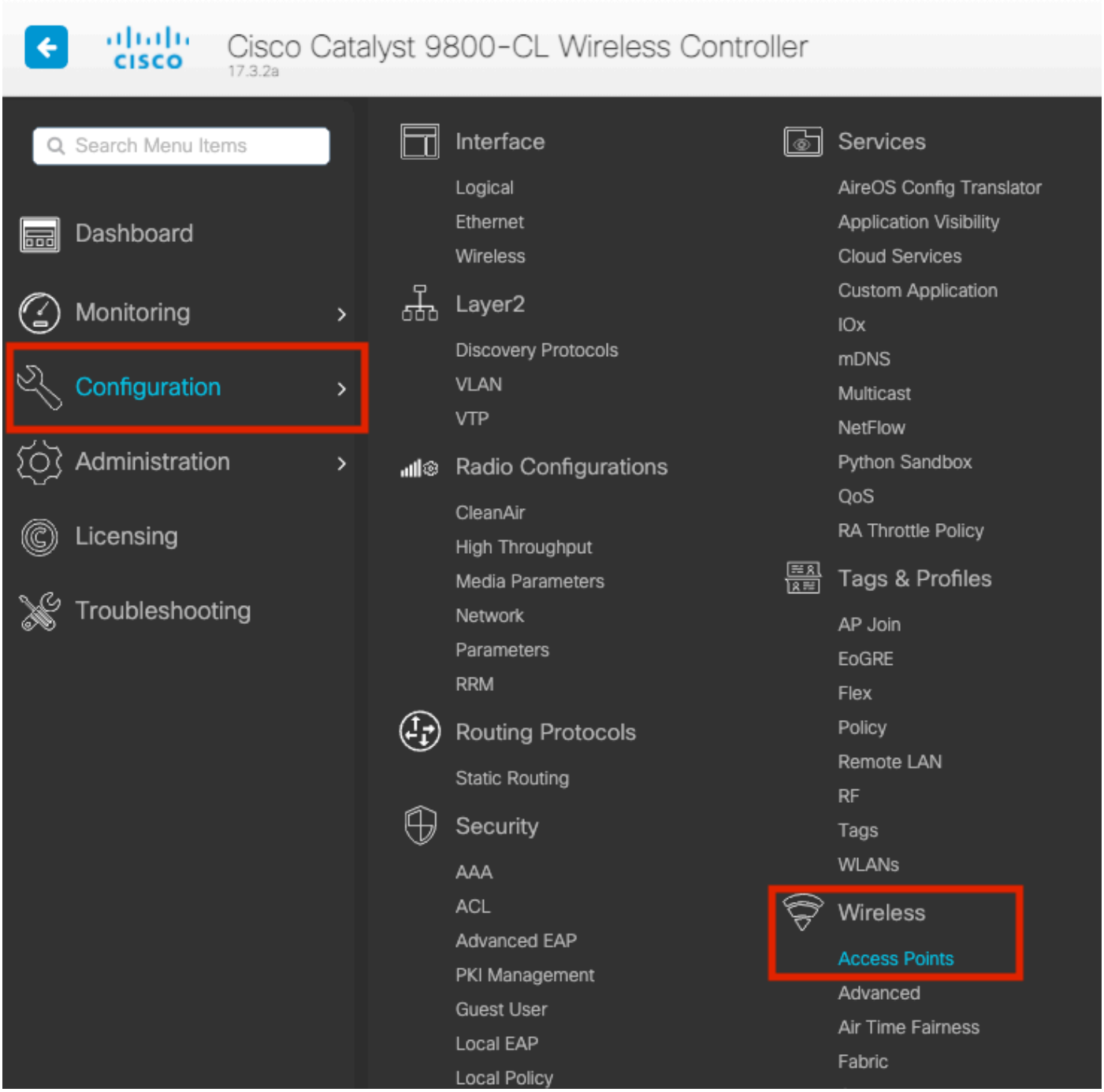
網路圖表



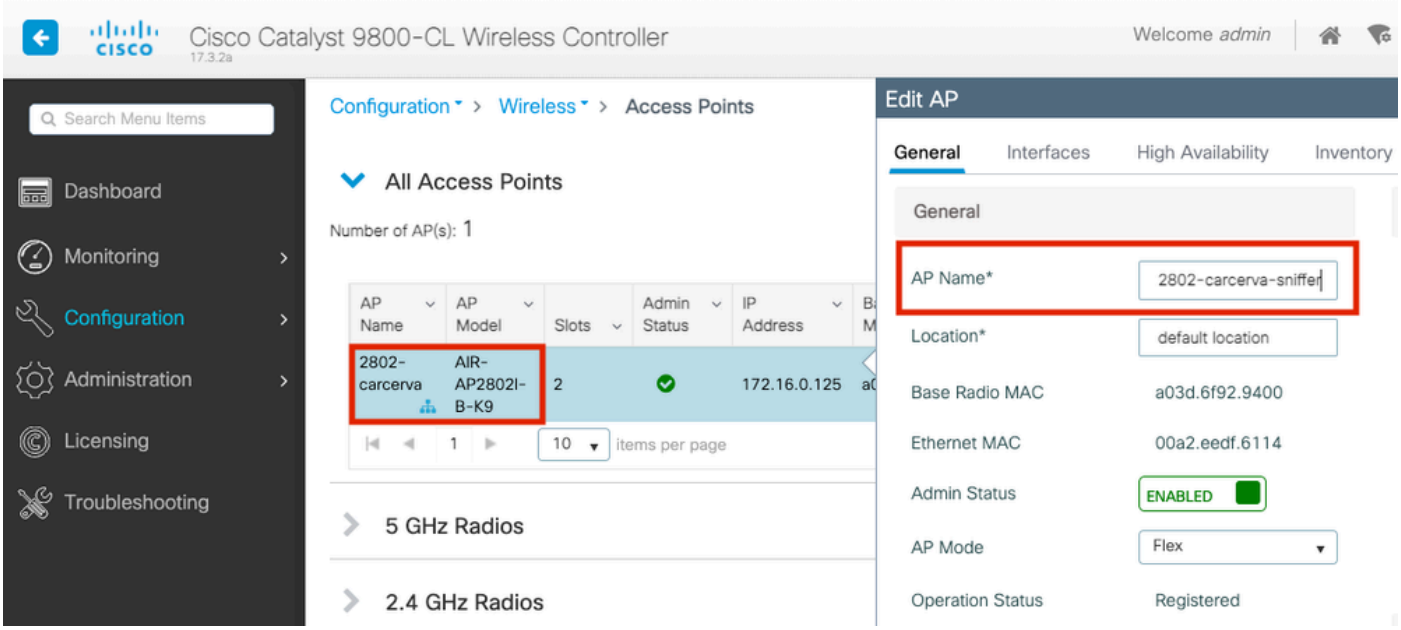
組態

通過GUI在監聽器模式下配置AP

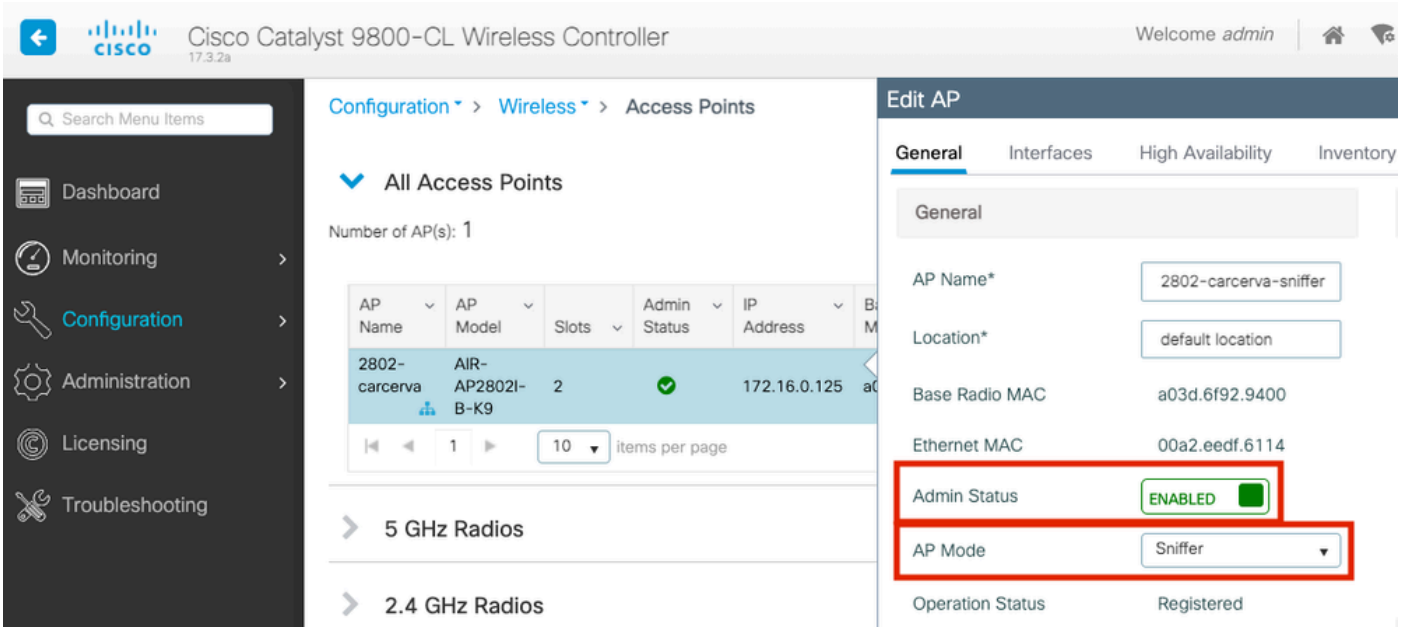
步驟1。在9800 WLC GUI上，導覽至Configuration > Wireless > Access Points >All Access Points，如下圖所示。



步驟2.選擇希望在監聽器模式下使用的AP。在General索引標籤上，更新AP的名稱，如下圖所示。



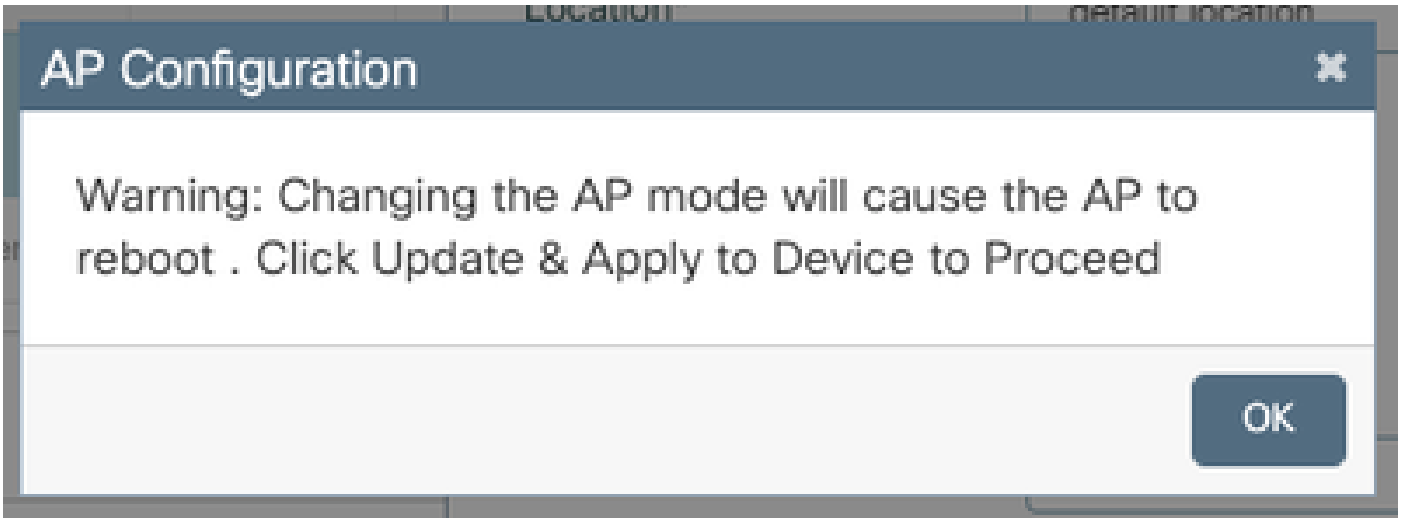
步驟3.確認Admin Status為Enabled，並將AP Mode變更為Sniffer，如下圖所示。



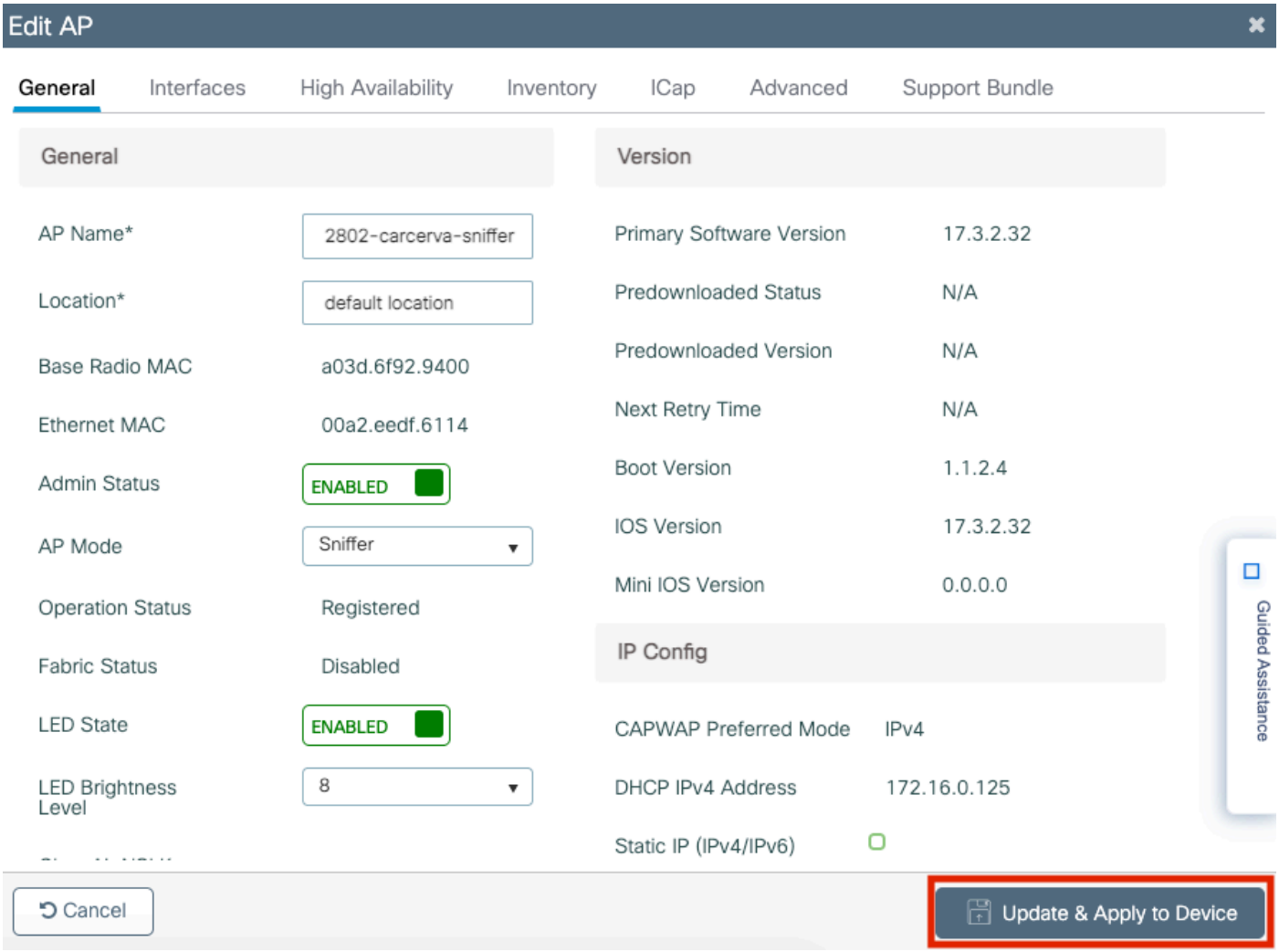
系統將顯示一個彈出視窗，其中包含下一個警報：

"警告:更改AP模式將導致AP重新啟動。按一下「更新並應用到裝置」以繼續。

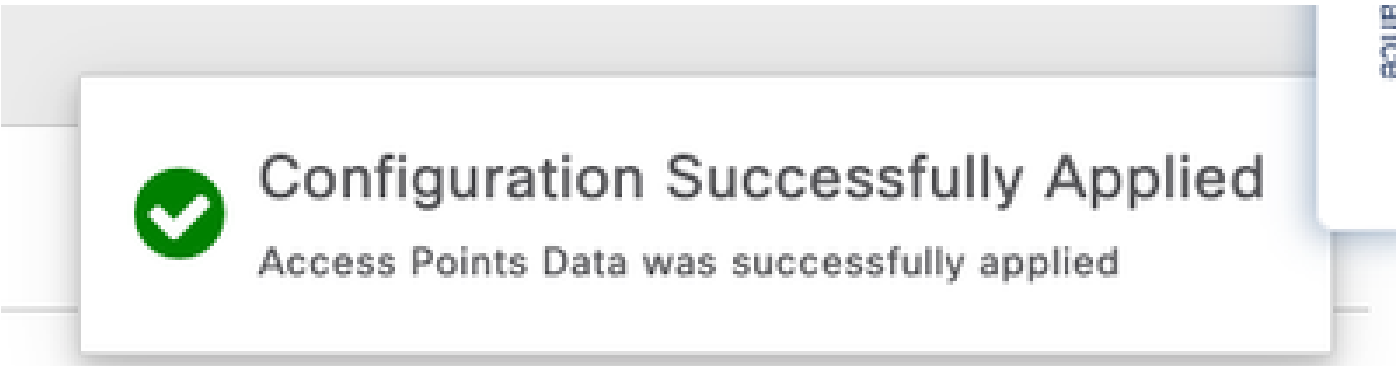
選擇OK，如下圖所示。



步驟4.按一下Update & Apply to Device，如下圖所示。



系統將顯示一個彈出視窗，以確認更改和AP彈出，如下圖所示。



在監聽器模式下通過CLI配置AP

步驟1.確定需要用作監聽器模式的AP，並獲取AP名稱。

步驟2.修改AP名稱。

此命令將修改AP名稱。其中<AP-name>是AP的當前名稱。

<#root>

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

步驟3.在監聽器模式下配置AP。

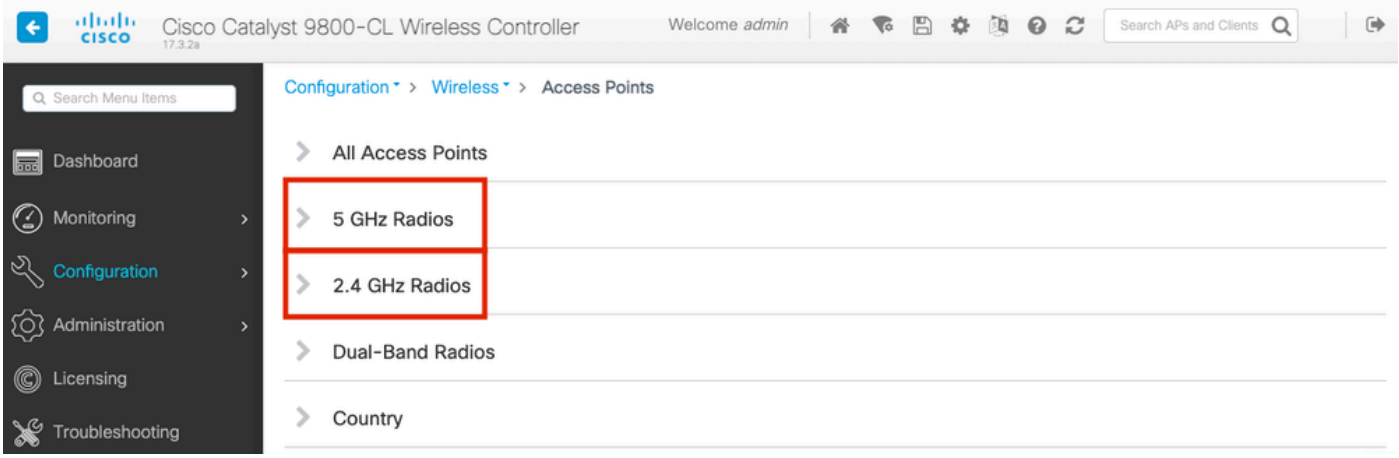
<#root>

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

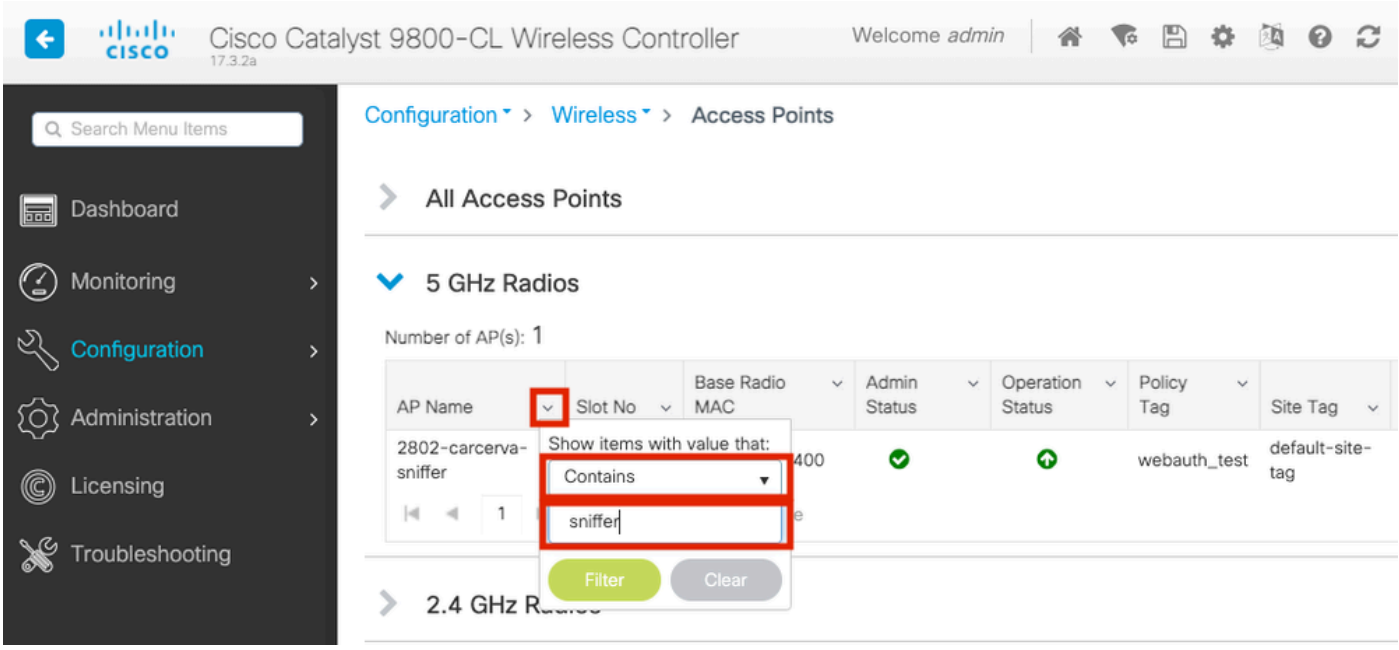
配置AP以通過GUI掃描通道

步驟1。在9800 WLC GUI中，導覽至Configuration > Wireless > Access Points。

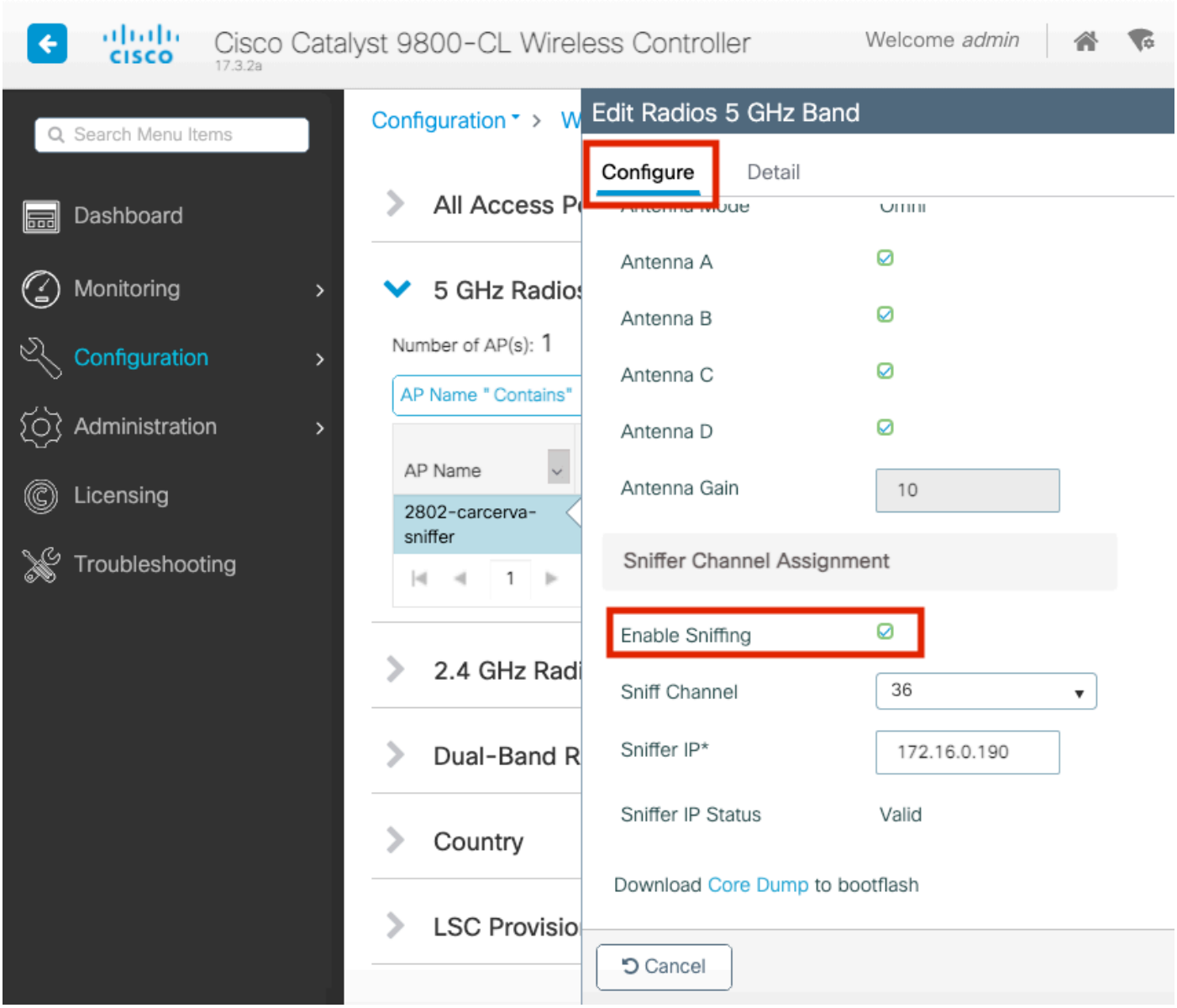
步驟2.在Access Points頁面上，顯示5 GHz Radio或2.4 GHz Radio選單清單。這取決於要掃描的通道，如圖所示。



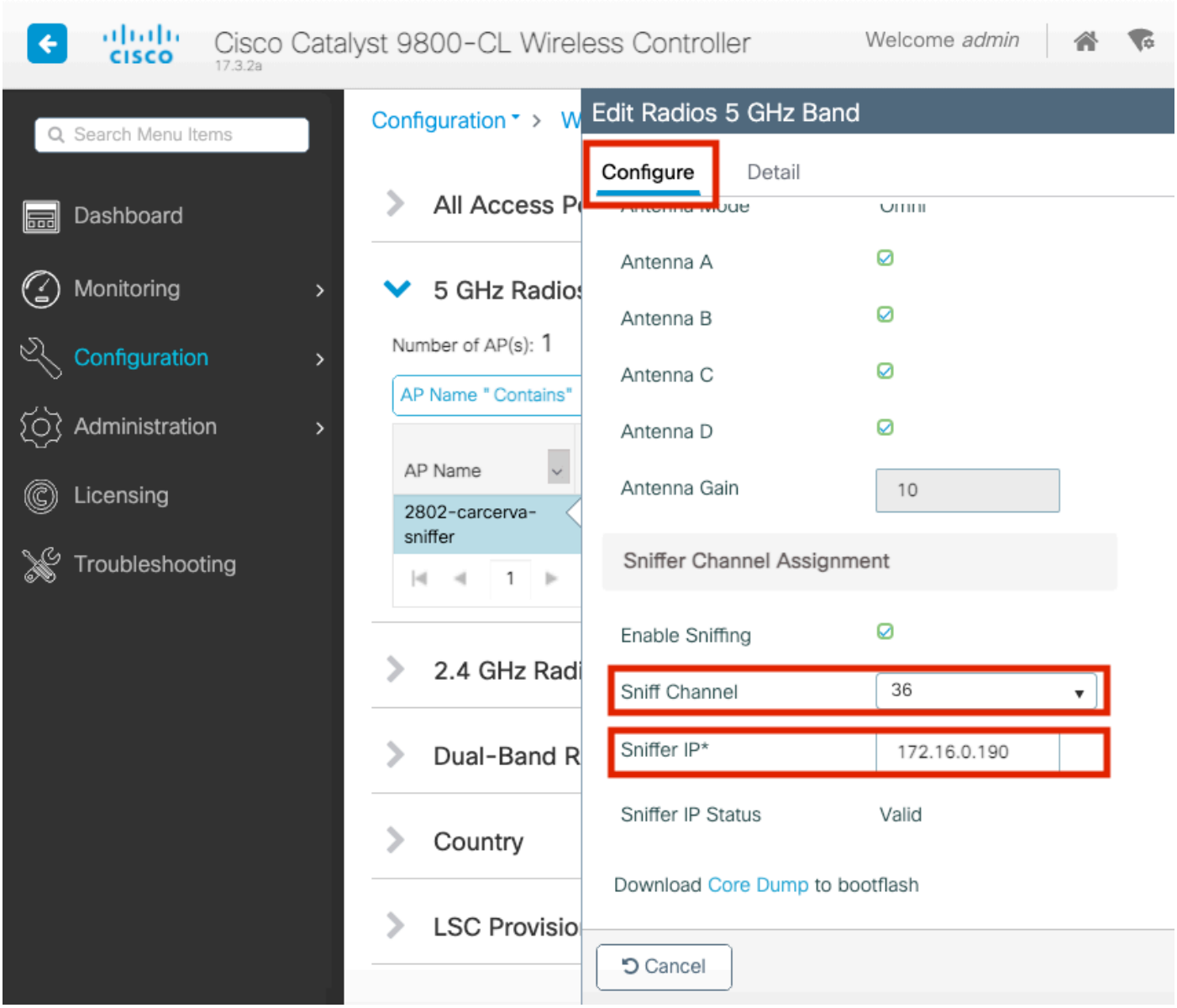
步驟2.搜尋AP。按一下向下箭頭按鈕以顯示搜尋工具，從下拉選單中選擇Contains，然後鍵入AP名稱，如下圖所示。



步驟3.選擇AP，並勾選Configure > Sniffer Channel Assignment底下的Enable Sniffer覈取方塊，如下圖所示。

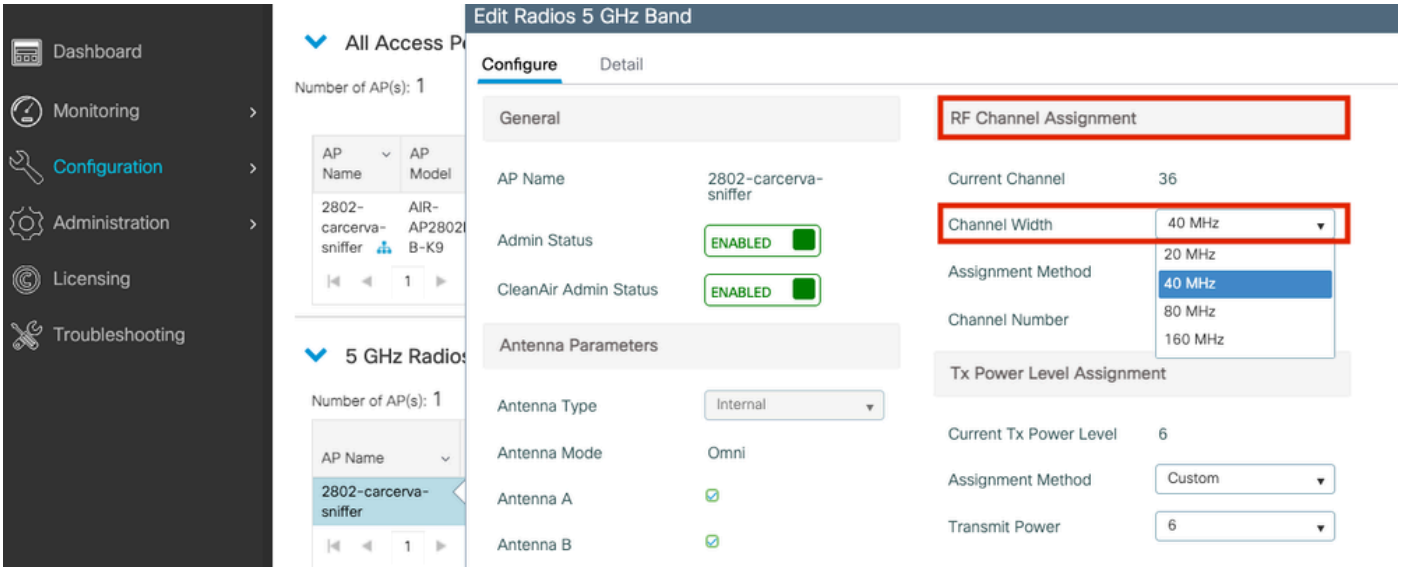


步驟4.從Sniff Channel下拉選單中選擇Channel，然後鍵入Sniffer IP address（使用Wireshark的伺服器IP地址），如下圖所示。



步驟5.選擇目標裝置和AP在連線時使用的Channel width。

導覽至Configure > RF Channel Assignment以設定此設定，如下圖所示。



配置AP以通過CLI掃描通道

步驟1.在AP上啟用通道嗅探。運行此命令：

<#root>

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

範例：

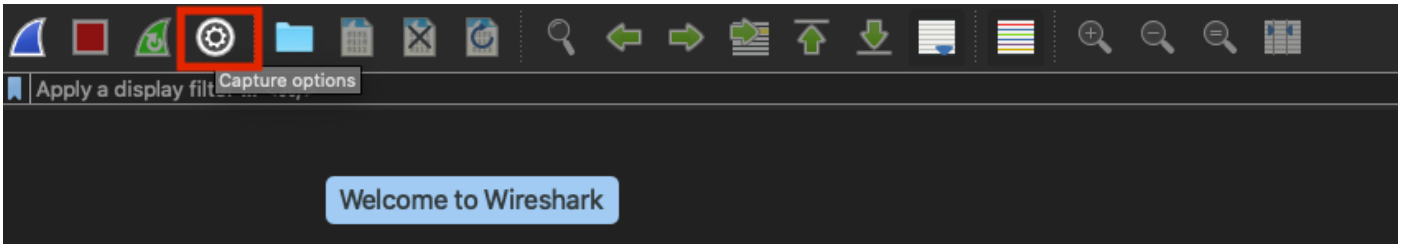
<#root>

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

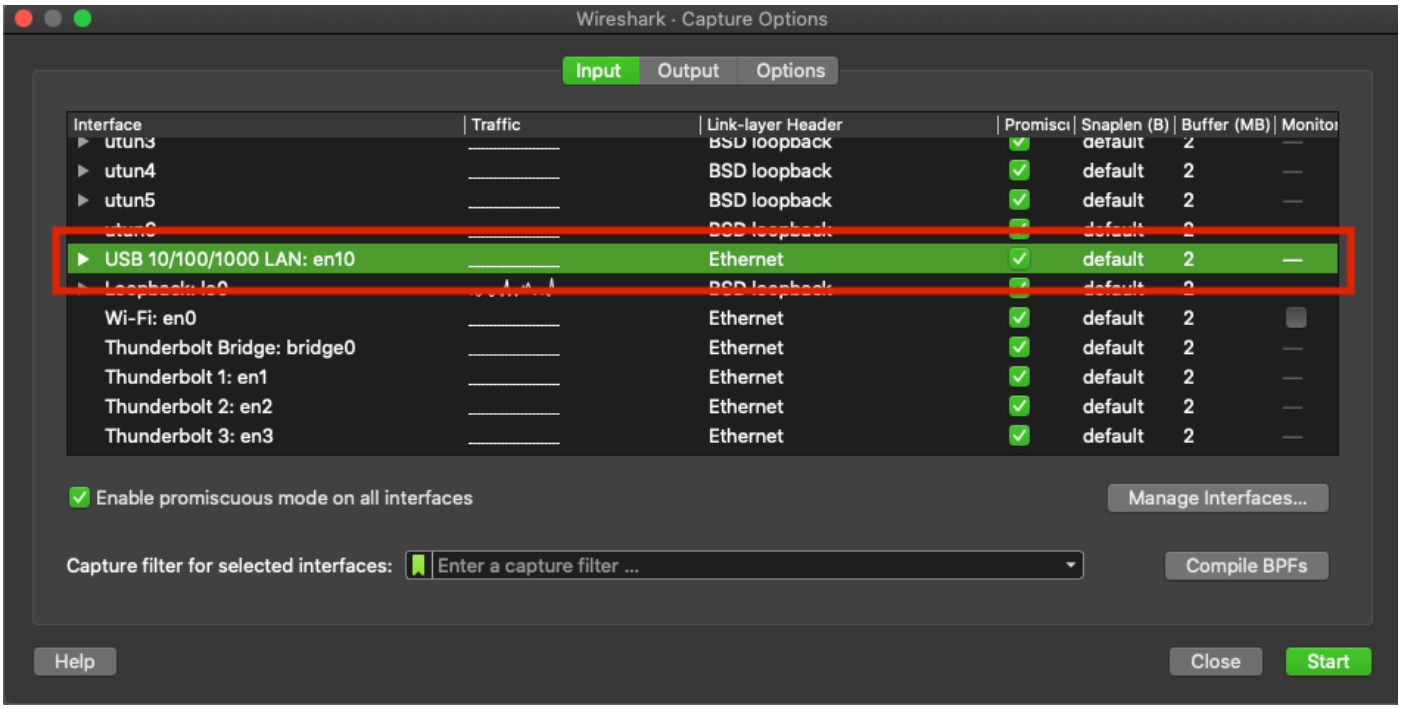
配置Wireshark以收集資料包捕獲

步驟1.啟動Wireshark。

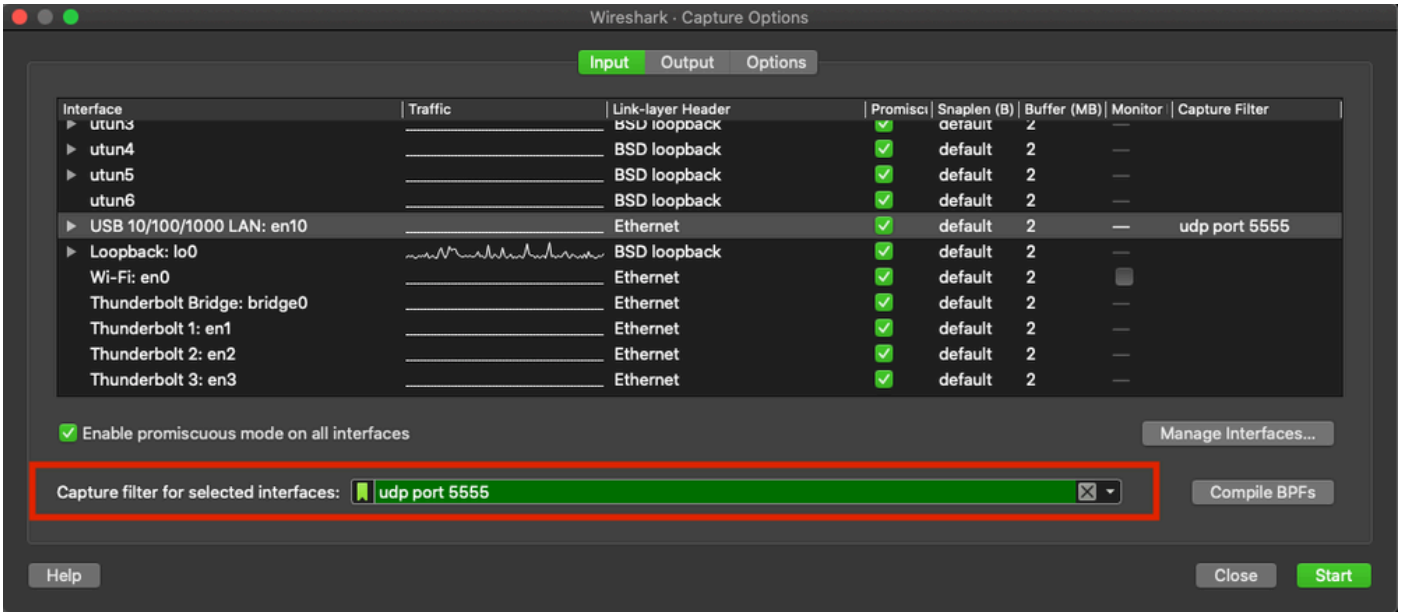
步驟2.從Wireshark中選擇Capture options選單圖示，如下圖所示。



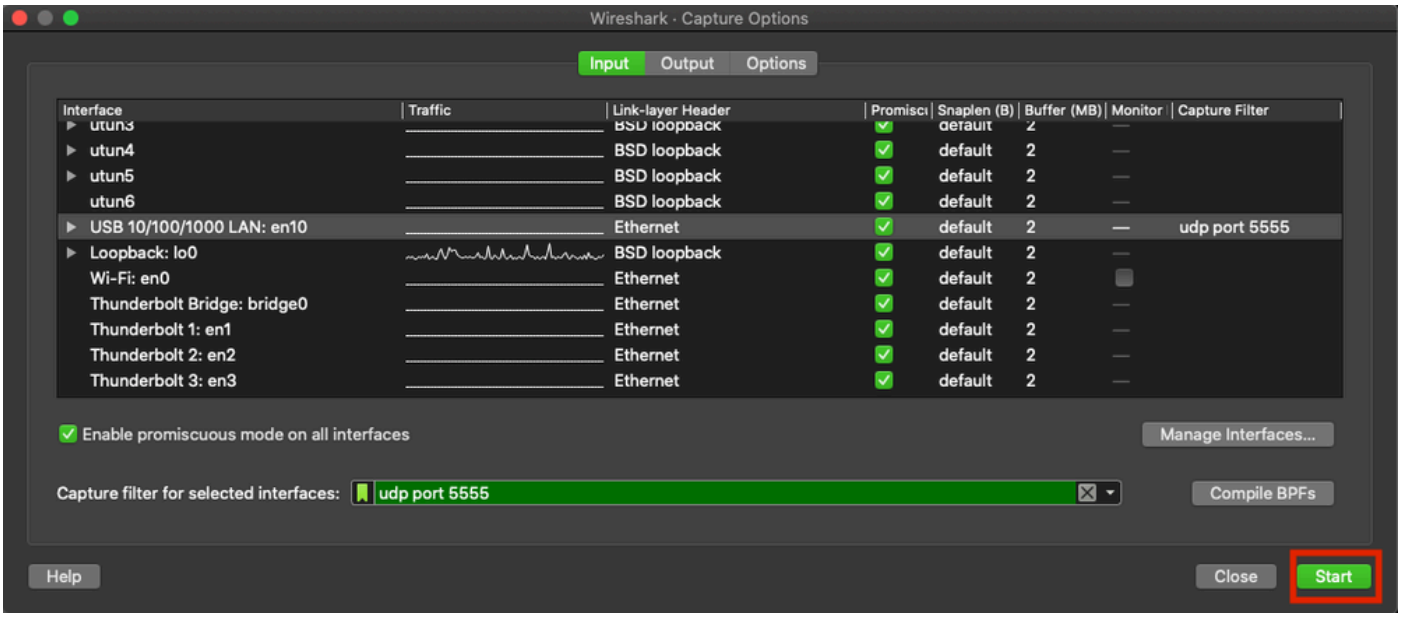
步驟3.此操作將顯示一個彈出視窗。從清單中選擇WiredInterface作為捕獲源，如下圖所示。



步驟4.在Capture filter for selected interfaces下： 欄位方塊，輸入udp port 5555，如下圖所示。



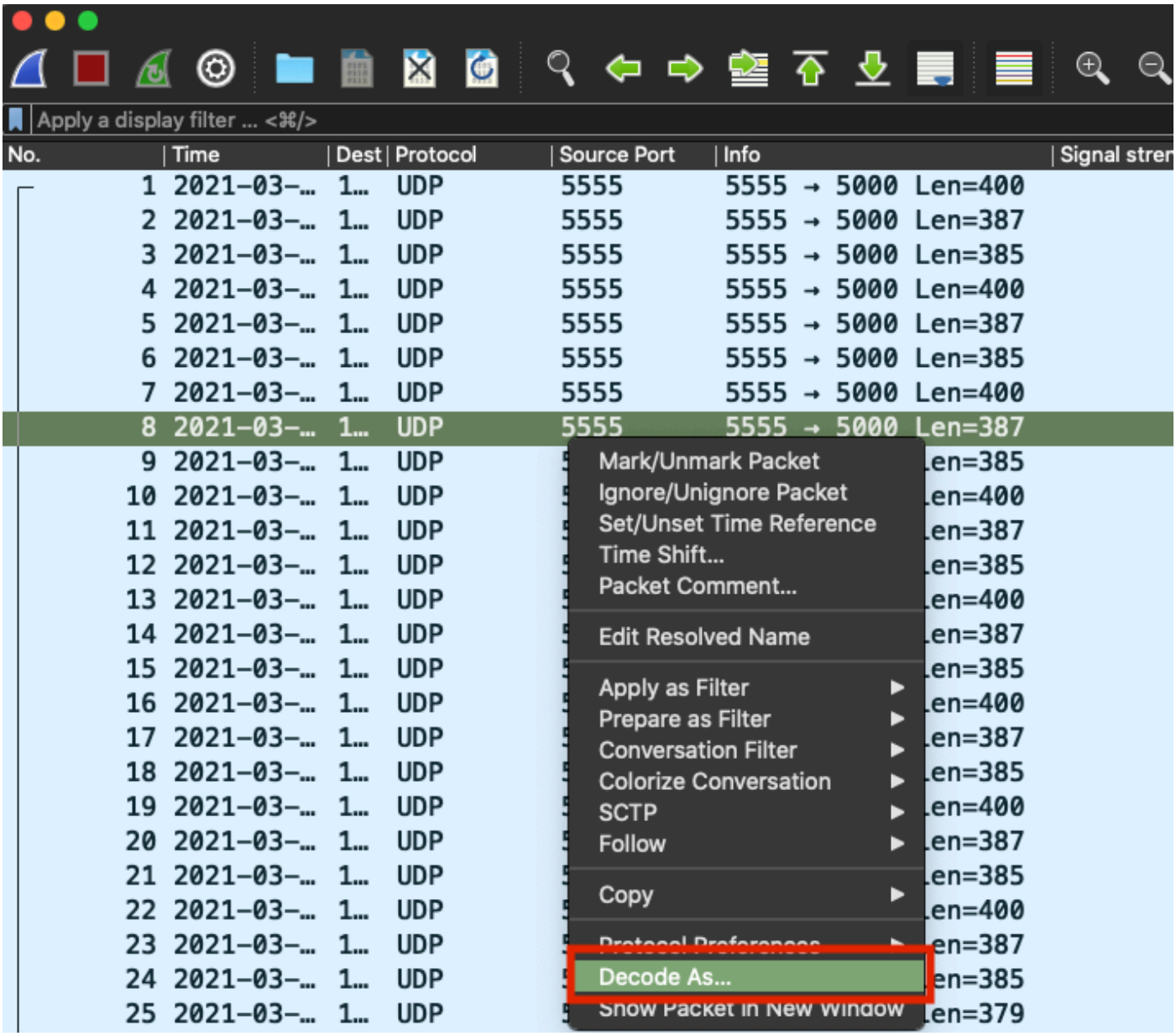
步驟5.按一下Start，如下圖所示。



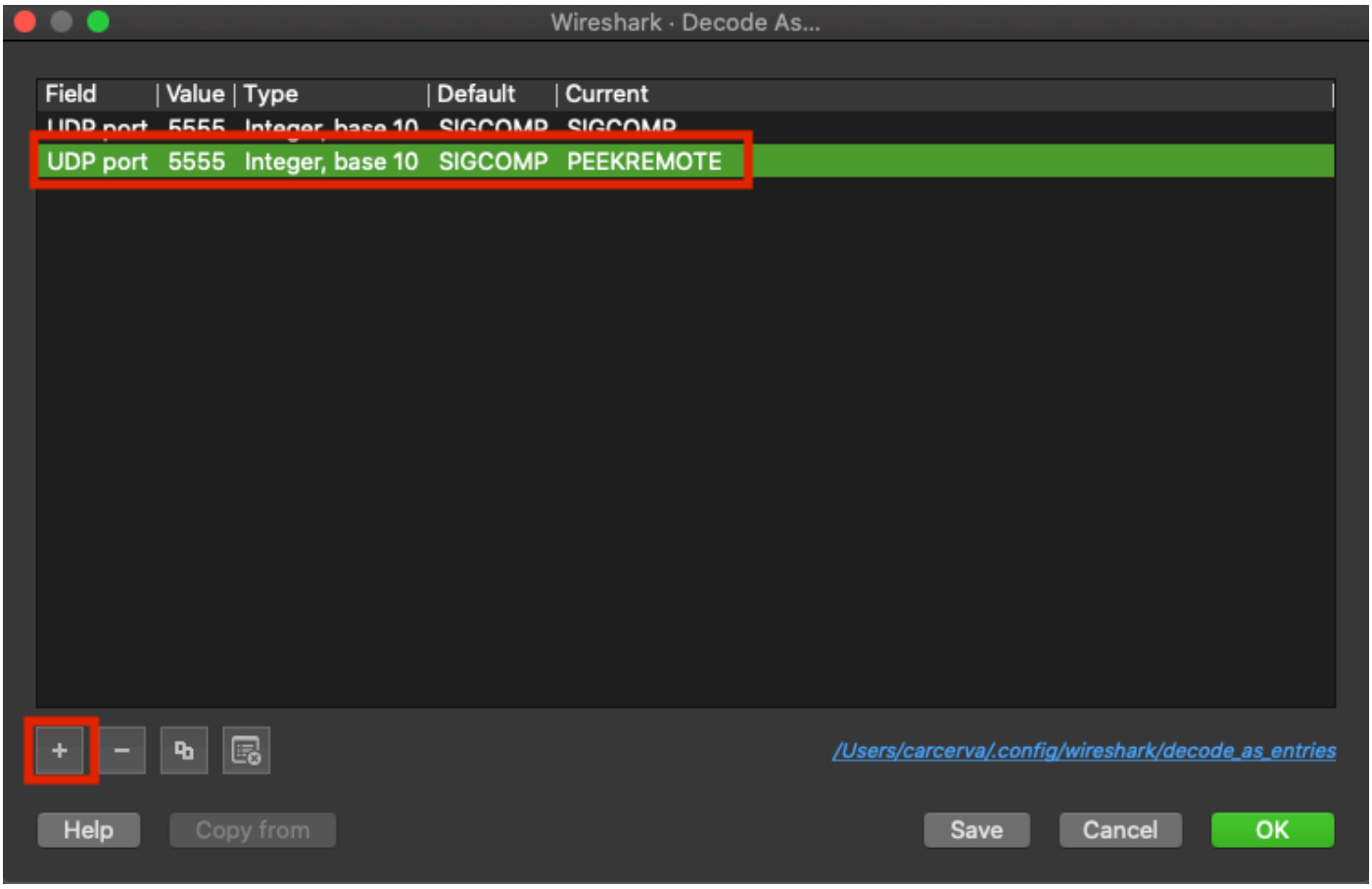
步驟6.等待Wireshark收集所需資訊，然後從Wireshark中選擇停止按鈕，如下圖所示。

提示：如果WLAN使用加密(例如預共用金鑰(PSK))，請確保擷取會擷取AP和所需使用者端之間的四次握手。如果OTA PCAP在裝置與WLAN關聯之前啟動，或者如果客戶端在捕獲運行時被取消身份驗證並重新身份驗證，則可以完成此操作。

步驟7. Wireshark不會自動解碼資料包。若要解碼封包，請從擷取中選擇line，使用按一下右鍵顯示選項，然後選擇Decode As...，如下圖所示。



步驟8.出現一個彈出視窗。選擇add按鈕並新增新的條目。選擇以下選項：UDP連線埠從Field、555 from Value、SIGCOMP from Default和PEEKREMOTE from Current，如下圖所示。



步驟9.按一下OK。封包已解碼並準備開始分析。

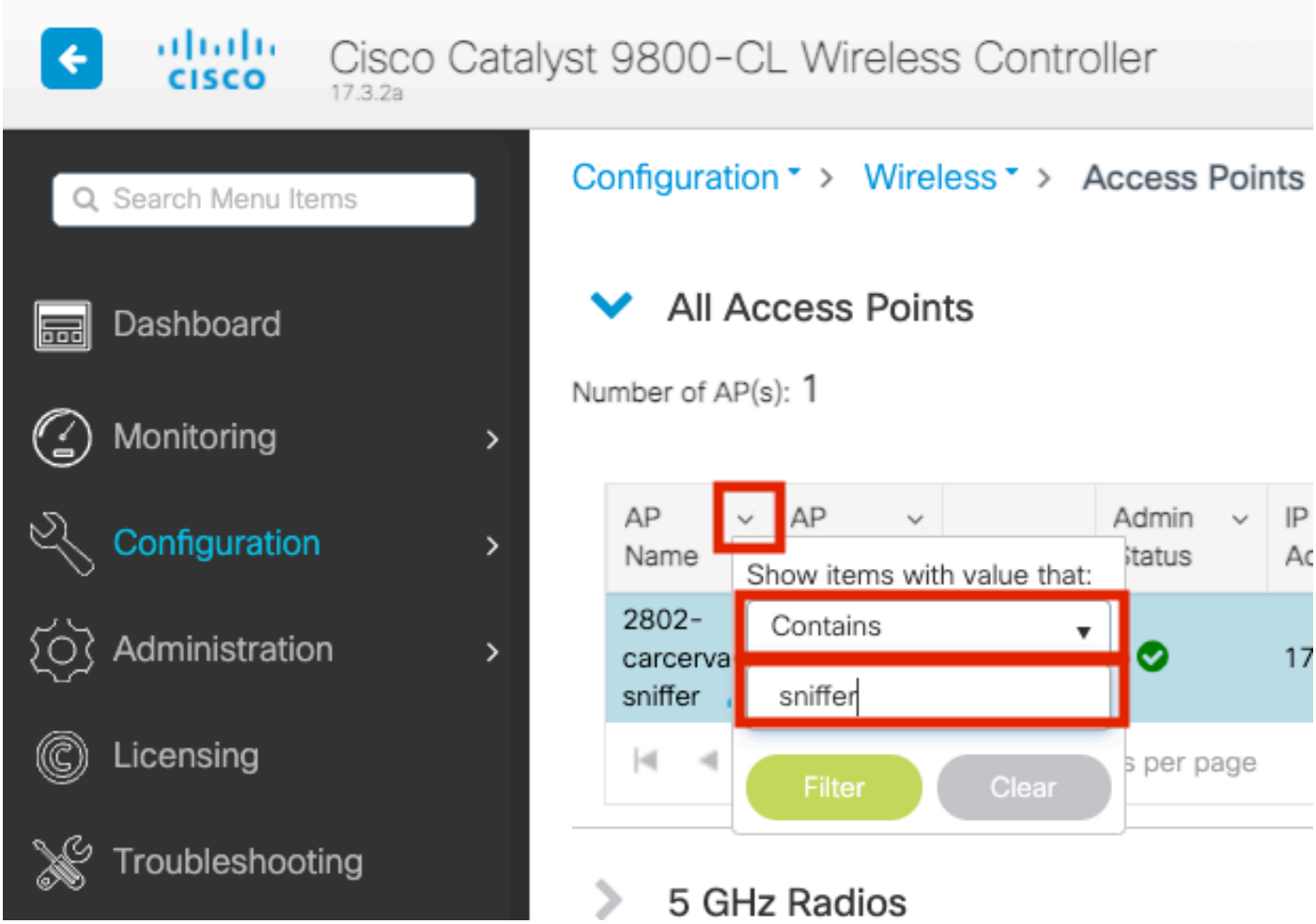
驗證

使用本節內容，確認您的組態是否正常運作。

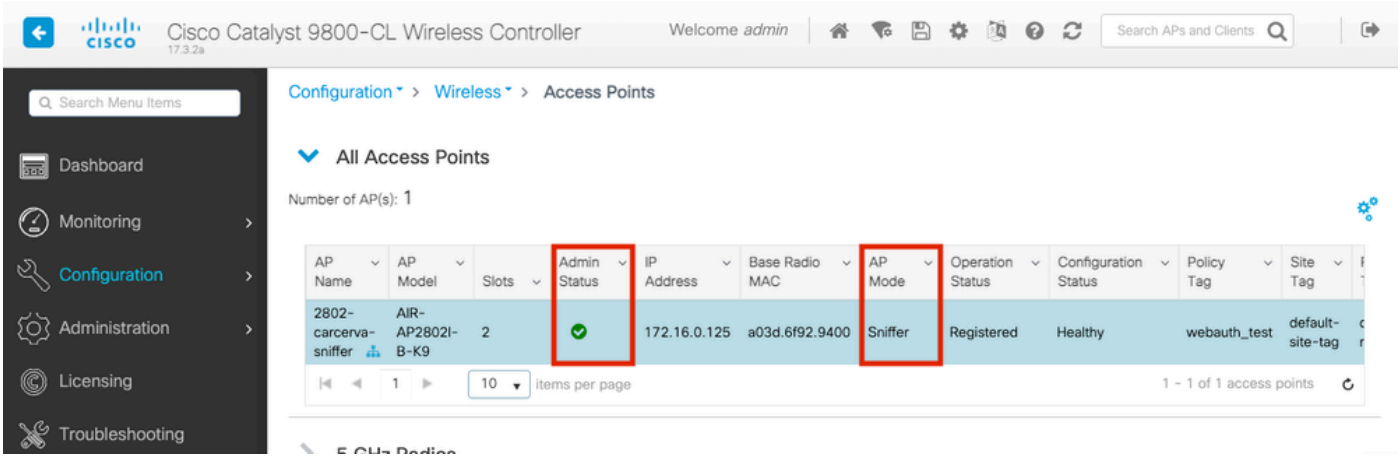
若要確認存取點是否在9800 GUI上處於監聽器模式：

步驟1。在9800 WLC GUI上，導覽至Configuration > Wireless > Access Points >All Access Points。

步驟2.搜尋AP。按一下「arrow down」按鈕以顯示搜尋工具。從下拉選單中選擇Contains，然後鍵入AP名稱，如下圖所示。



步驟3.驗證Admin Status是否具有綠色複選標籤，以及AP Mode是否為Sniffer，如下圖所示。



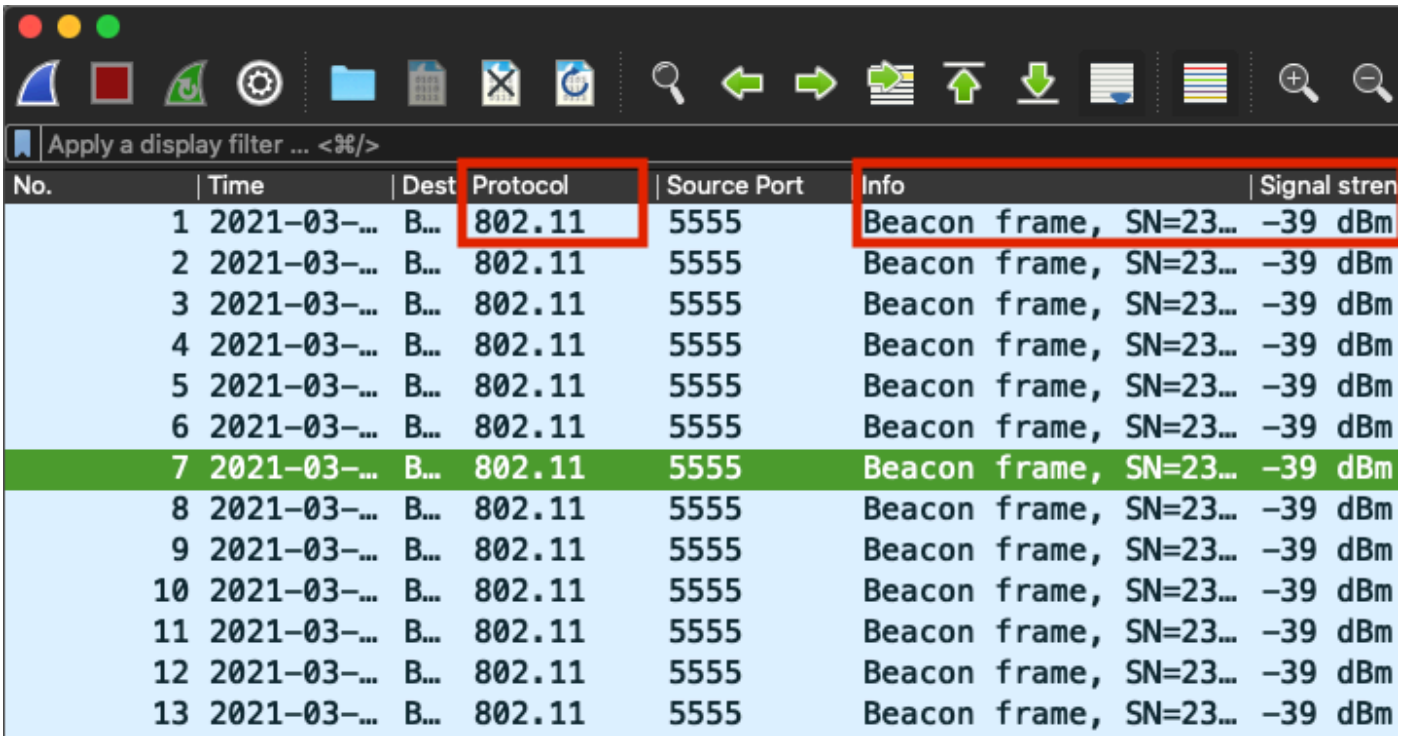
若要確認存取點是否從9800 CLI處於監聽器模式，請執行以下命令：

<#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
```

為了確認資料包在Wireshark上解碼，協定從UDP更改為802.11，並顯示Beacon幀，如下圖所示。



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

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

問題:Wireshark不會從AP接收任何資料。

解決方案：無線管理介面(WMI)必須能夠訪問Wireshark伺服器。 確認Wireshark伺服器與WLC中的WMI之間的連通性。

相關資訊

- Cisco Catalyst 9800系列無線控制器軟體配置指南，Cisco IOS XE Amsterdam 17.3.x — 章節：監聽器模式
- 802.11 無線監聽的基礎知識
- 技術支援與文件 - Cisco Systems

關於此翻譯
思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。