在Catalyst 9800無線控制器上以監聽器模式設定存取點

目錄

簡介

本文說明如何透過圖形使用者介面(GUI)或指令行介面(CLI)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)，以及如何使用監聽器AP透過空氣收集封包擷取(PCAP)，以便進行無線行為疑難排解和分析。

必要條件

需求

思科建議您瞭解以下主題：

- 9800 WLC組態
- 802.11標準中的基本知識

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.X

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

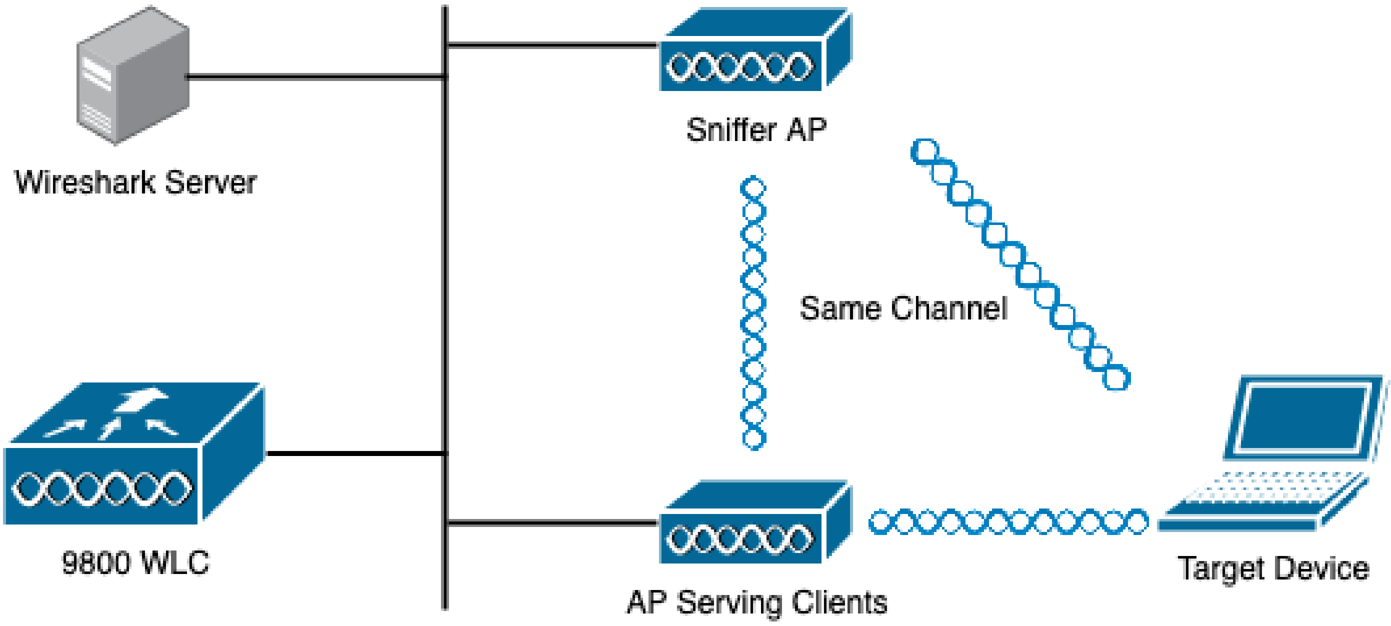
）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

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。

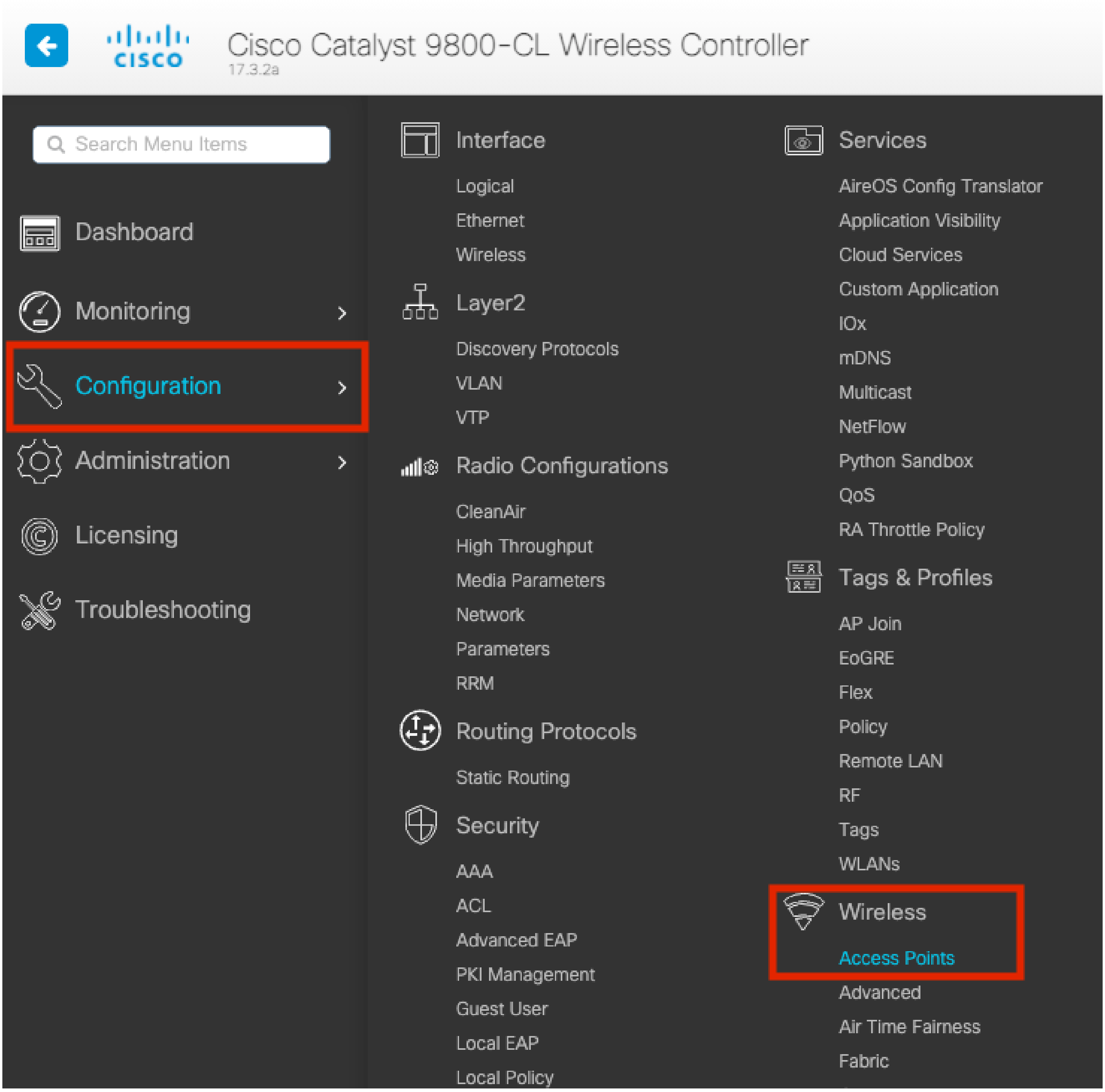
網路圖表



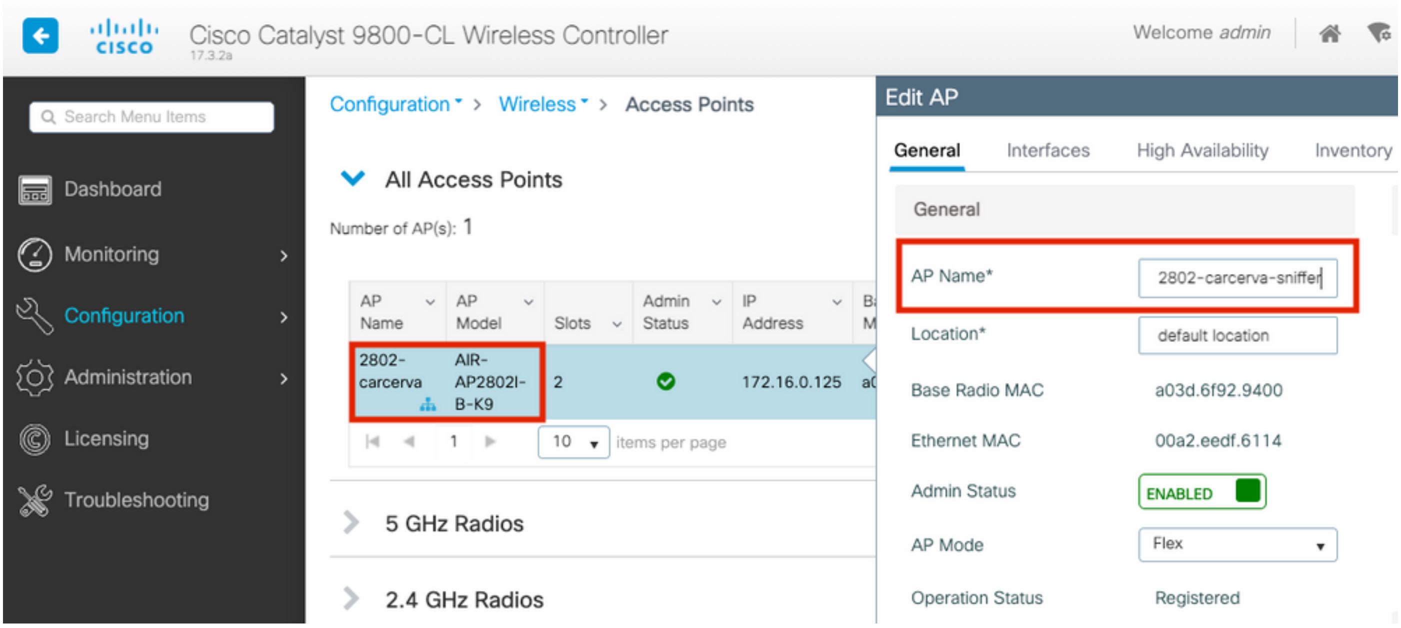
組態

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.選擇在監聽器模式下希望使用的AP。在**General**索引標籤上，更新AP的名稱，如下圖所示。



Number of AP(s): 1

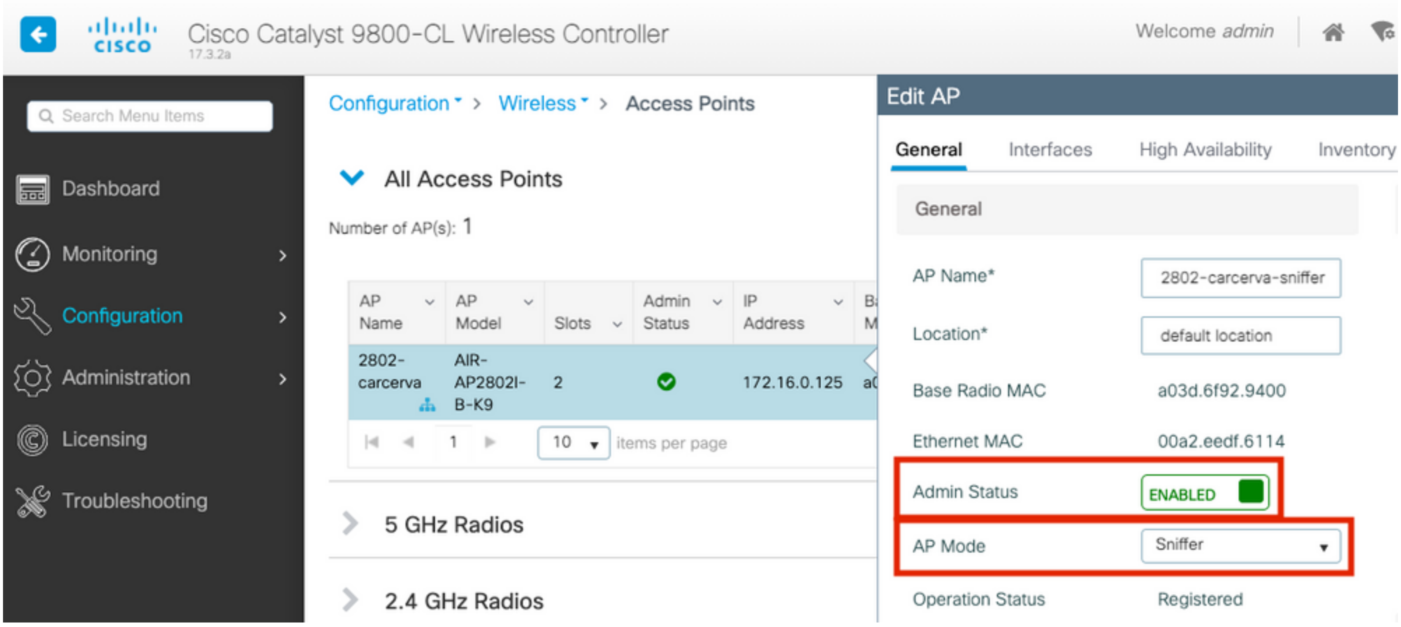
AP Name	AP Model	Slots	Admin Status	IP Address	Ba M
2802-carcerva	AIR-AP2802I-B-K9	2	✓	172.16.0.125	a0

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

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



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

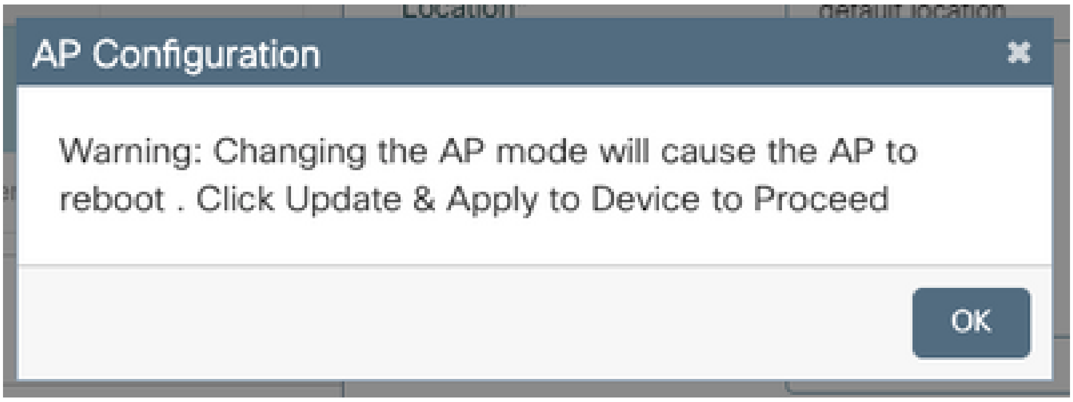
General

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

系統會顯示一個彈出視窗，其中包含下一個附註：

"警告:更改AP模式將導致AP重新啟動。點選更新並應用到裝置以繼續」

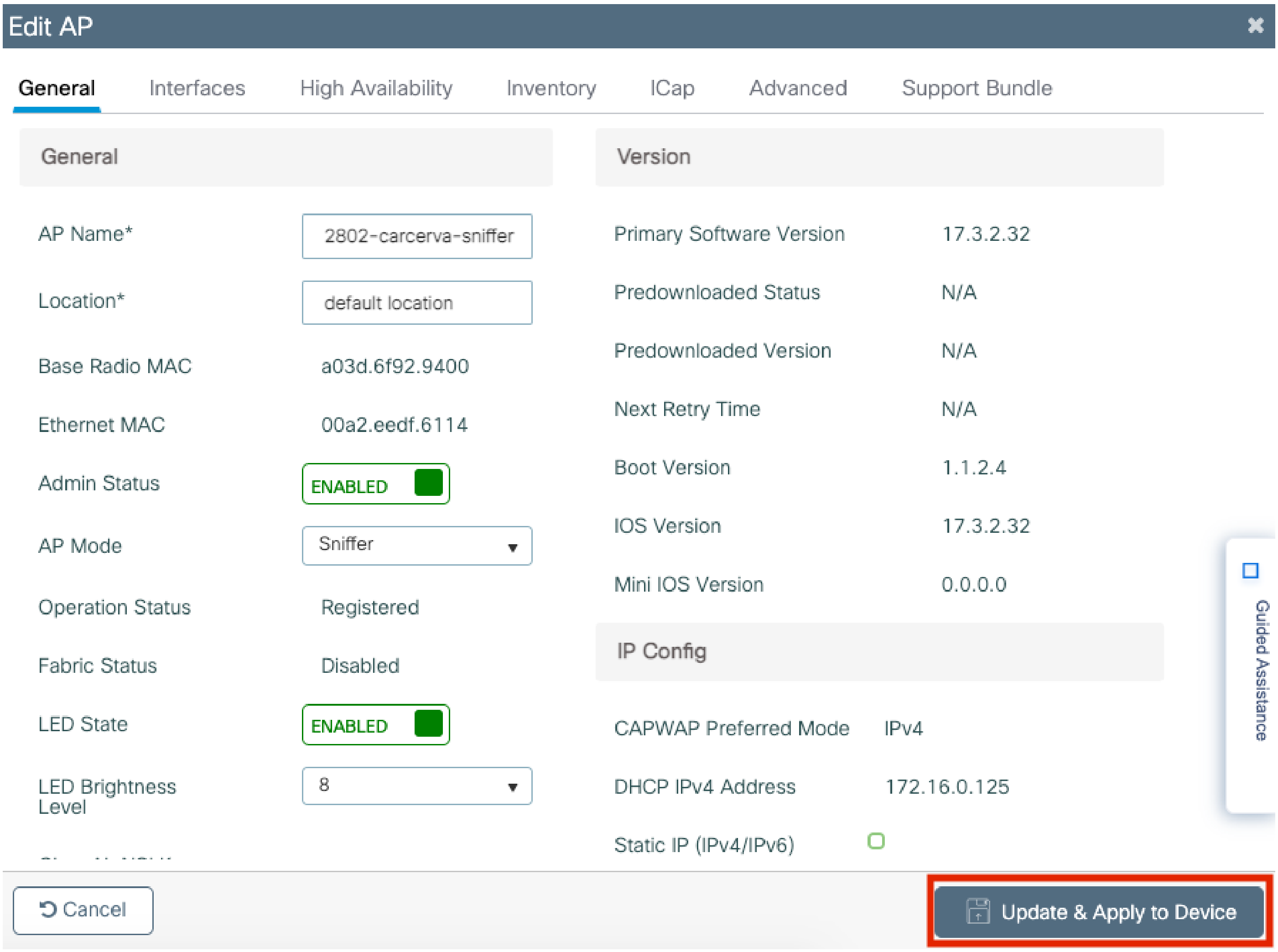
選擇**OK**，如下圖所示。



AP Configuration

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

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



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

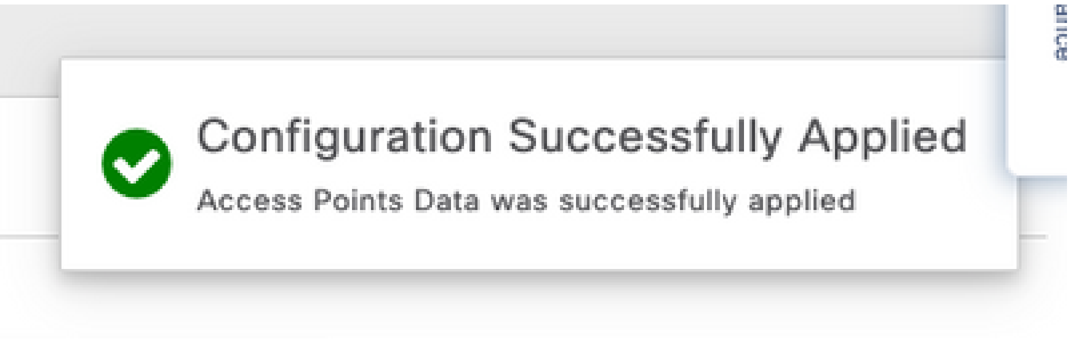
IP Config

CAPWAP Preferred Mode IPv4

DHCP IPv4 Address 172.16.0.125

Static IP (IPv4/IPv6) □

系統將顯示一個彈出視窗，以確認更改和AP彈出，如下圖所示。



Configuration Successfully Applied

Access Points Data was successfully applied

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。

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

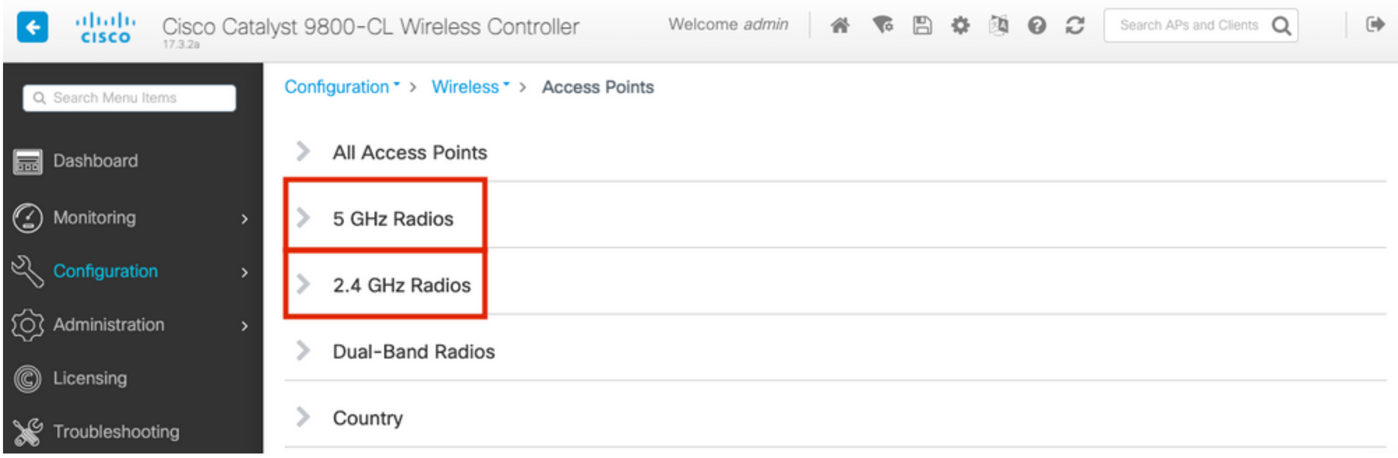
步驟3.在監聽器模式下配置AP。

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

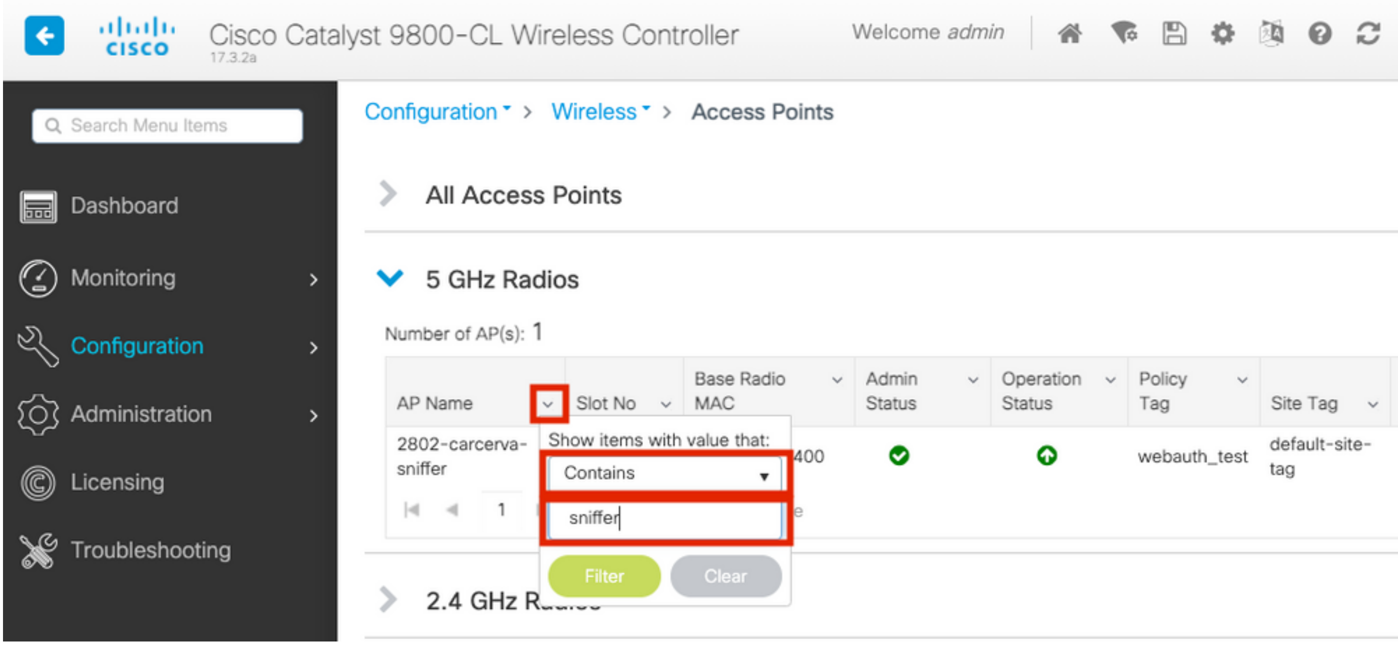
配置AP以通過GUI掃描通道

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

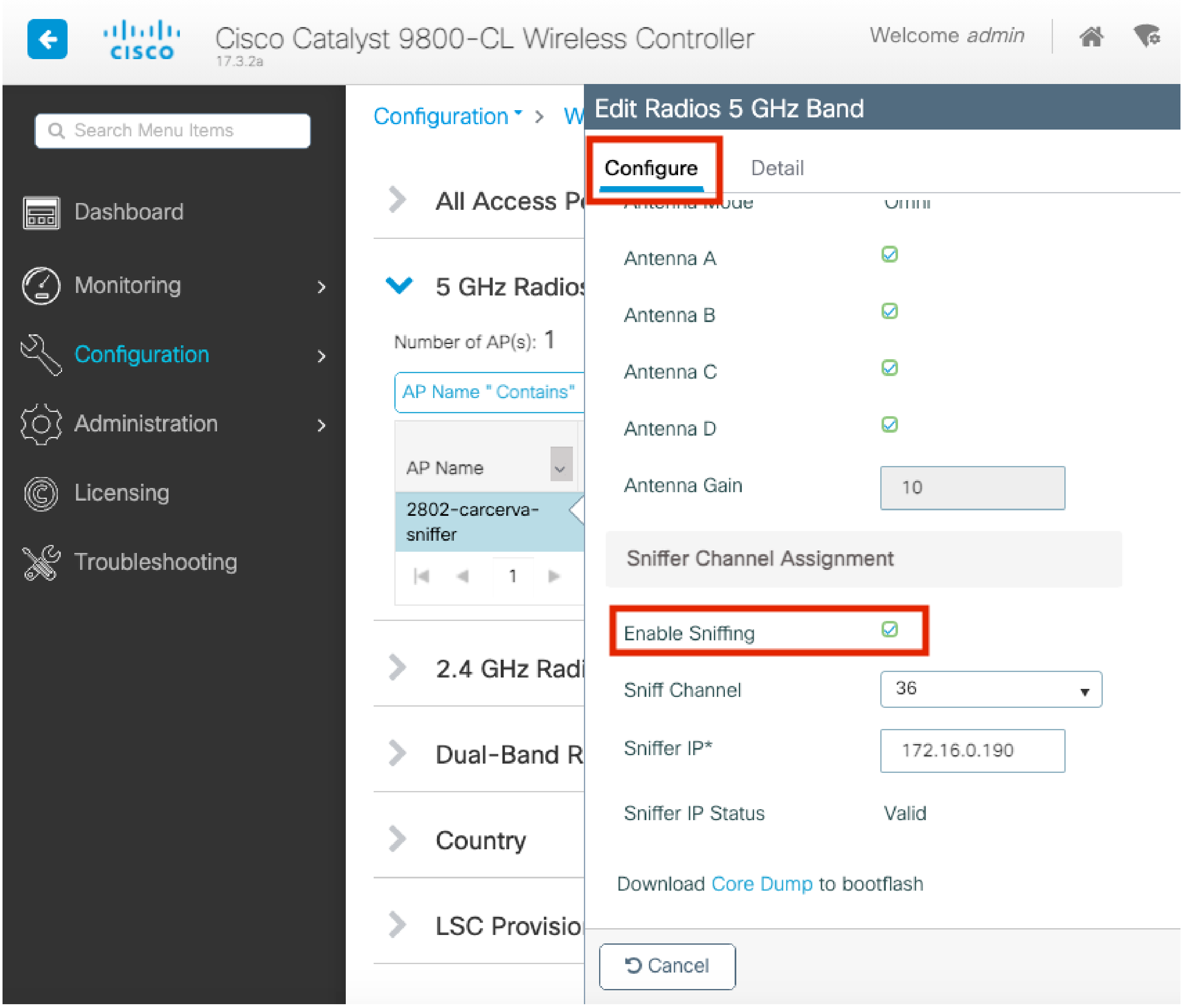
步驟2.在**Access Points**頁面上，顯示**5 GHz Radio**或**2.4 GHz Radio**選單清單。這取決於掃描所需的通道，如圖所示。



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。



Antenna Mode: Omni

Antenna A ☑

Antenna B ☑

Antenna C ☑

Antenna D ☑

Antenna Gain: 10

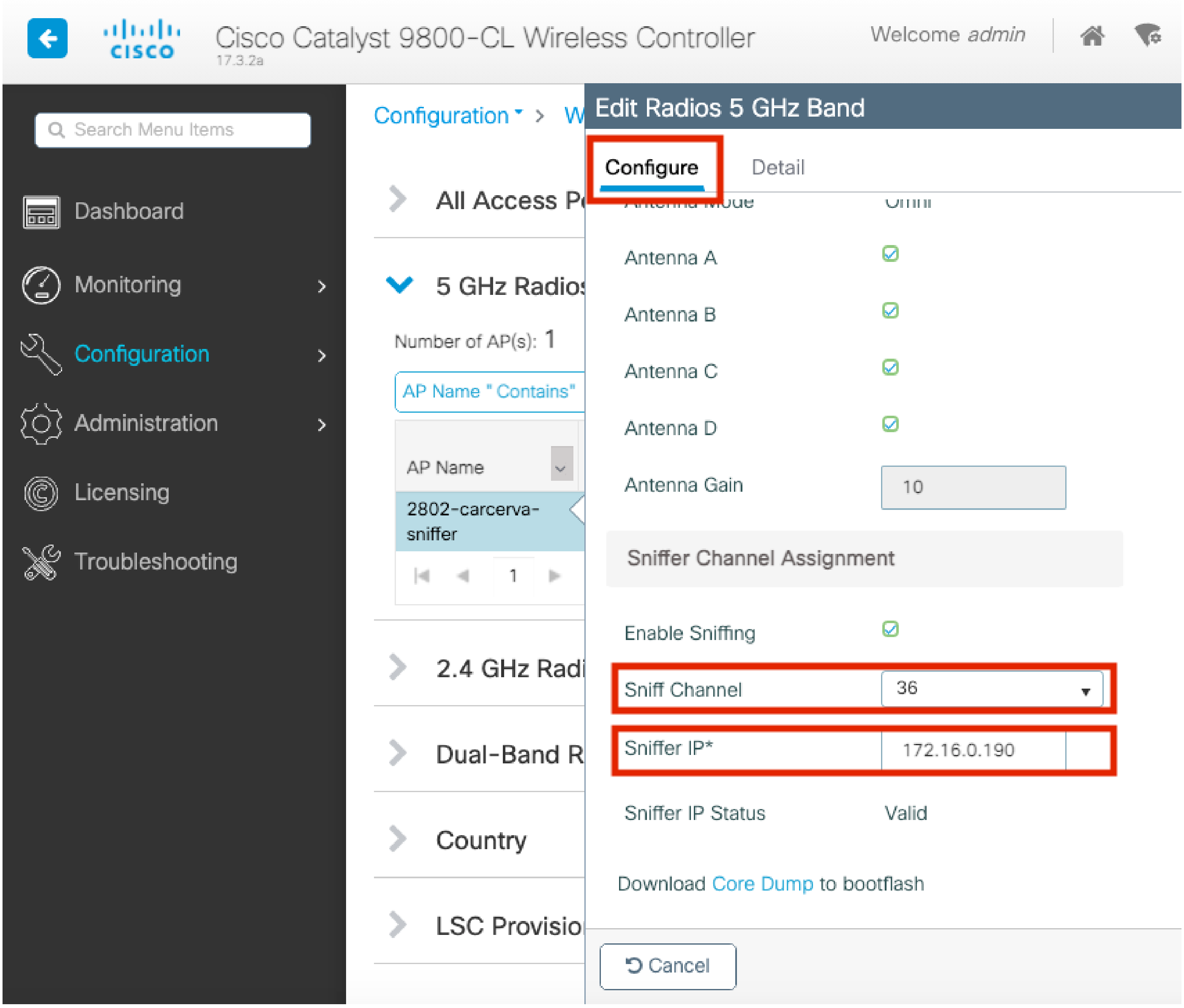
Enable Sniffing ☑

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。



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

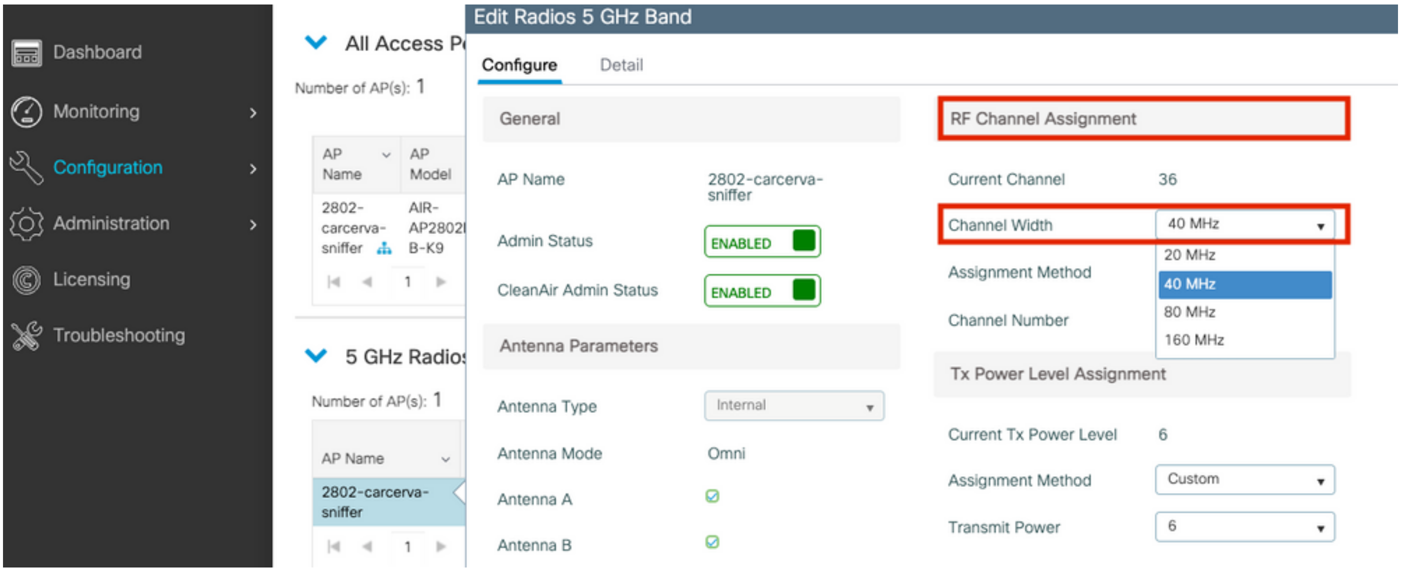
Sniffer IP* 172.16.0.190

Sniffer IP Status Valid

Download Core Dump to bootflash

步驟5.選擇目標裝置和AP在連線時使用的**通道寬度**。

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



Edit Radios 5 GHz Band

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

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：

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

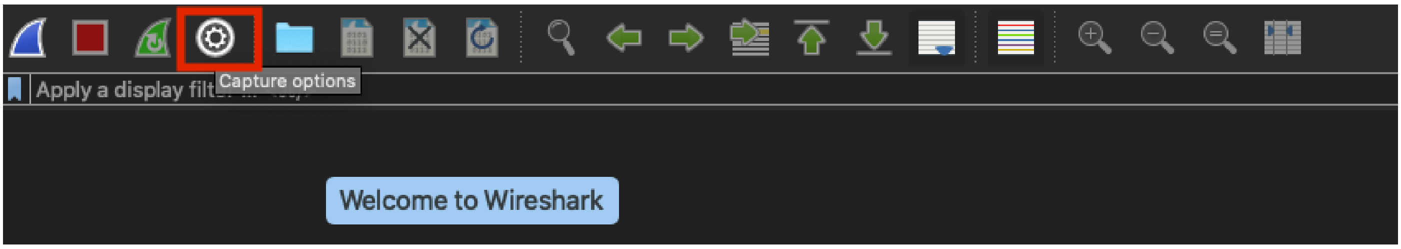
範例：

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

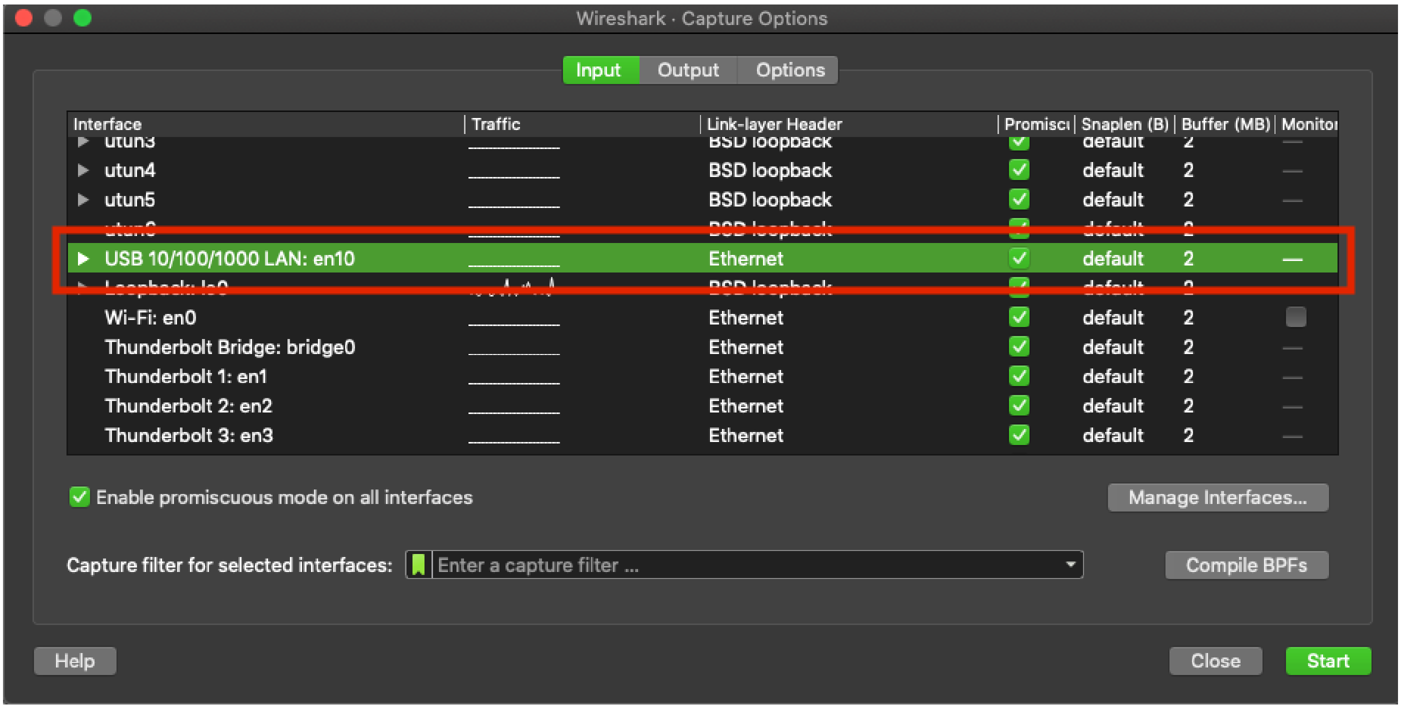
配置Wireshark以收集資料包捕獲

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。從清單中選擇有線介面作為捕獲源，如下圖所示。

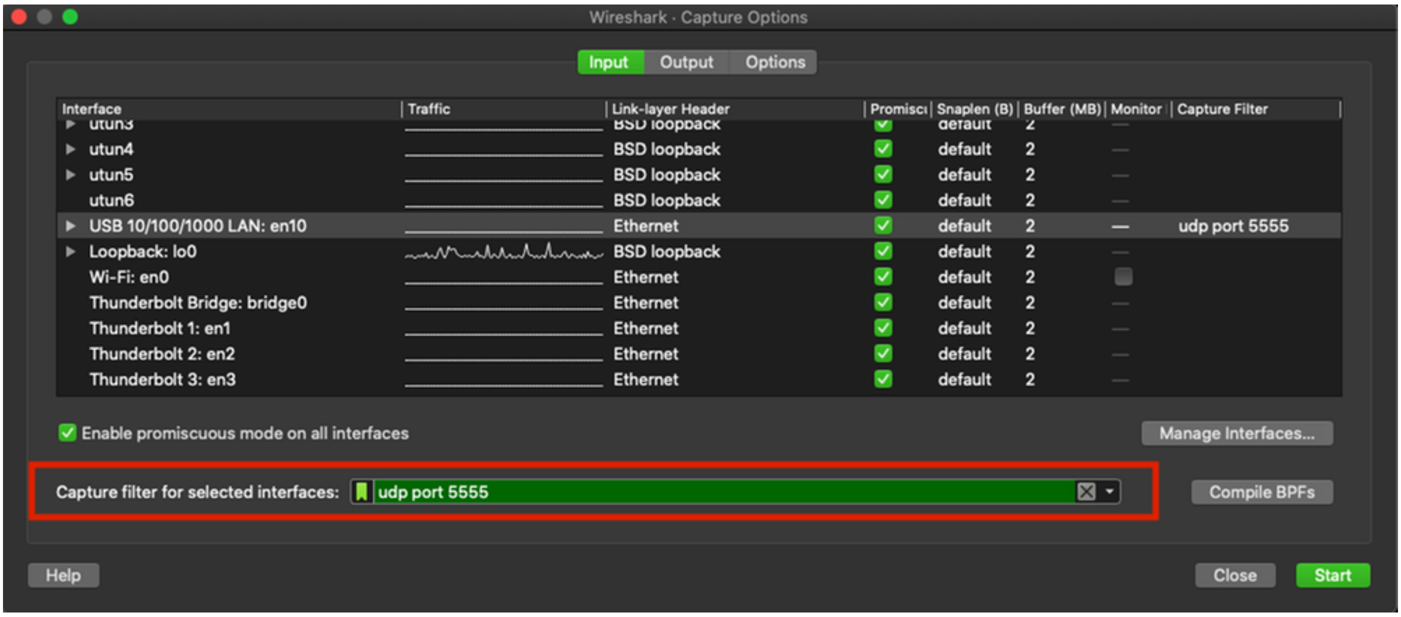


Interface	Traffic	Link-layer Header	Promiscu	Snaplen (B)	Buffer (MB)	Monitor
▶ utun3		BSD loopback	✓	default	2	—
▶ utun4		BSD loopback	✓	default	2	—
▶ utun5		BSD loopback	✓	default	2	—
utun6		BSD loopback	✓	default	2	
▶ USB 10/100/1000 LAN: en10		Ethernet	✓	default	2	—
▶ Loopback: lo0		BSD loopback	✓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

步驟4.在**Capture filter for selected interfaces**下： 欄位框中，鍵入**udp port 5555**，如下圖所示。

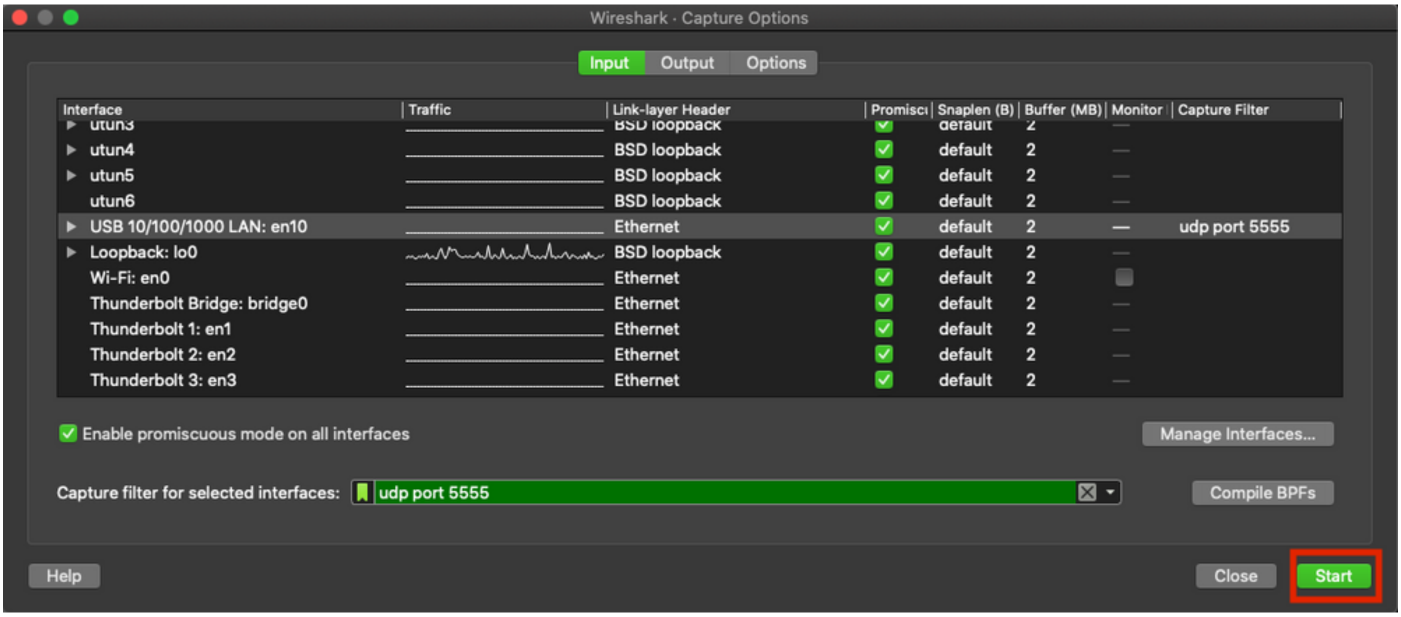


Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
▸ utun3		BSD loopback	✓	default	2		
▸ utun4		BSD loopback	✓	default	2	—	
▸ utun5		BSD loopback	✓	default	2	—	
utun6		BSD loopback	✓	default	2	—	
▸ USB 10/100/1000 LAN: en10		Ethernet	✓	default	2	—	udp port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

步驟5.按一下**Start**，如下圖所示。

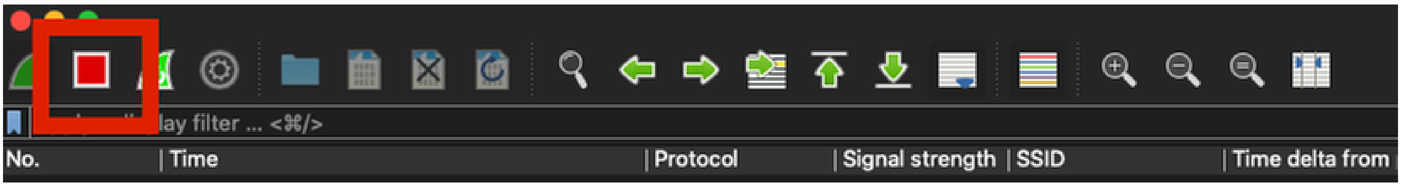


Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (B)	Buffer (MB)	Monitor	Capture Filter
▸ utun3		BSD loopback	✓	default	2		
▸ utun4		BSD loopback	✓	default	2	—	
▸ utun5		BSD loopback	✓	default	2	—	
utun6		BSD loopback	✓	default	2	—	
▸ USB 10/100/1000 LAN: en10		Ethernet	✓	default	2	—	udp port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

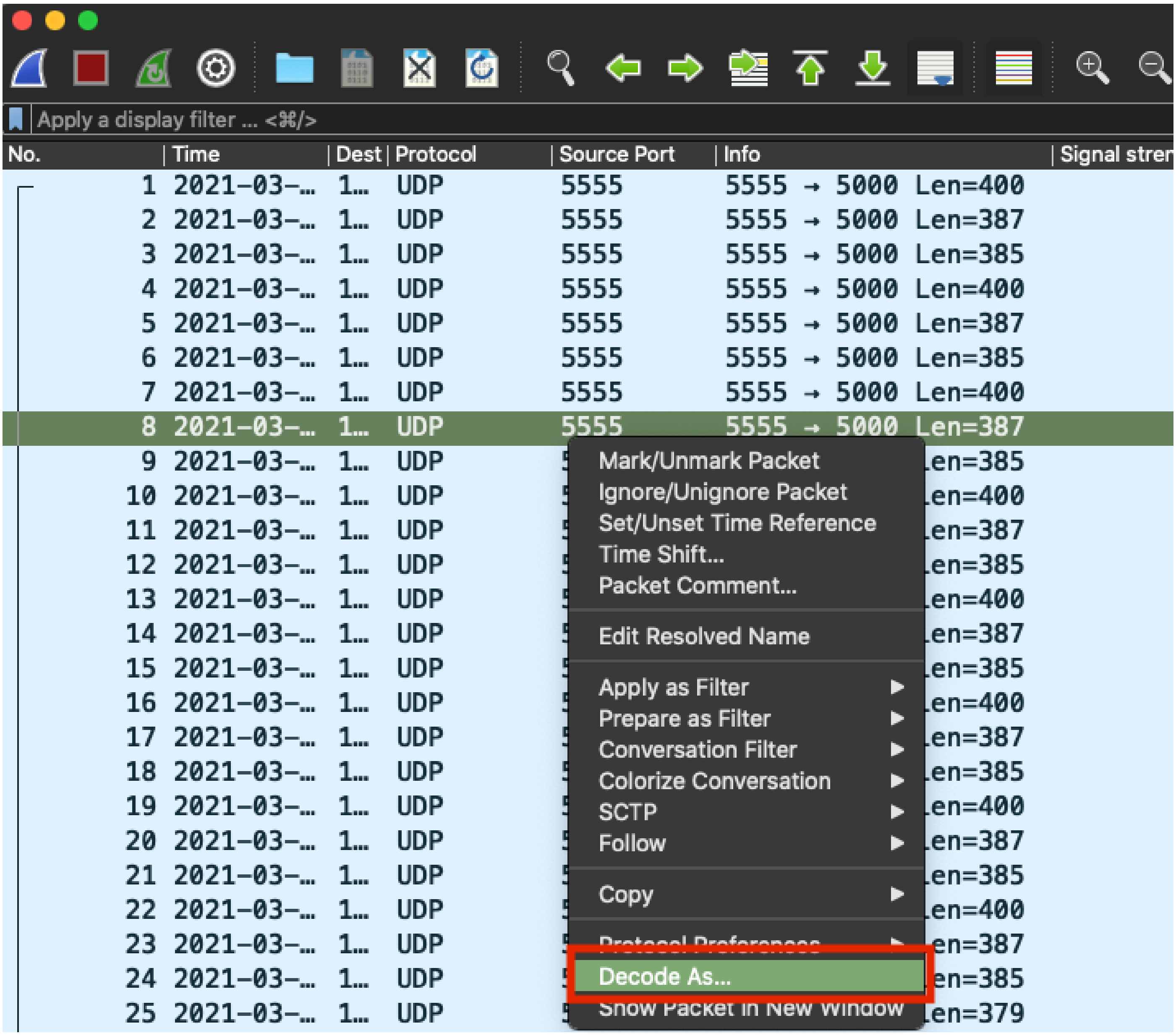
步驟6.等待Wireshark收集所需資訊，然後從Wireshark中選擇**停止**按鈕，如下圖所示。



No. | Time | Protocol | Signal strength | SSID | Time delta from

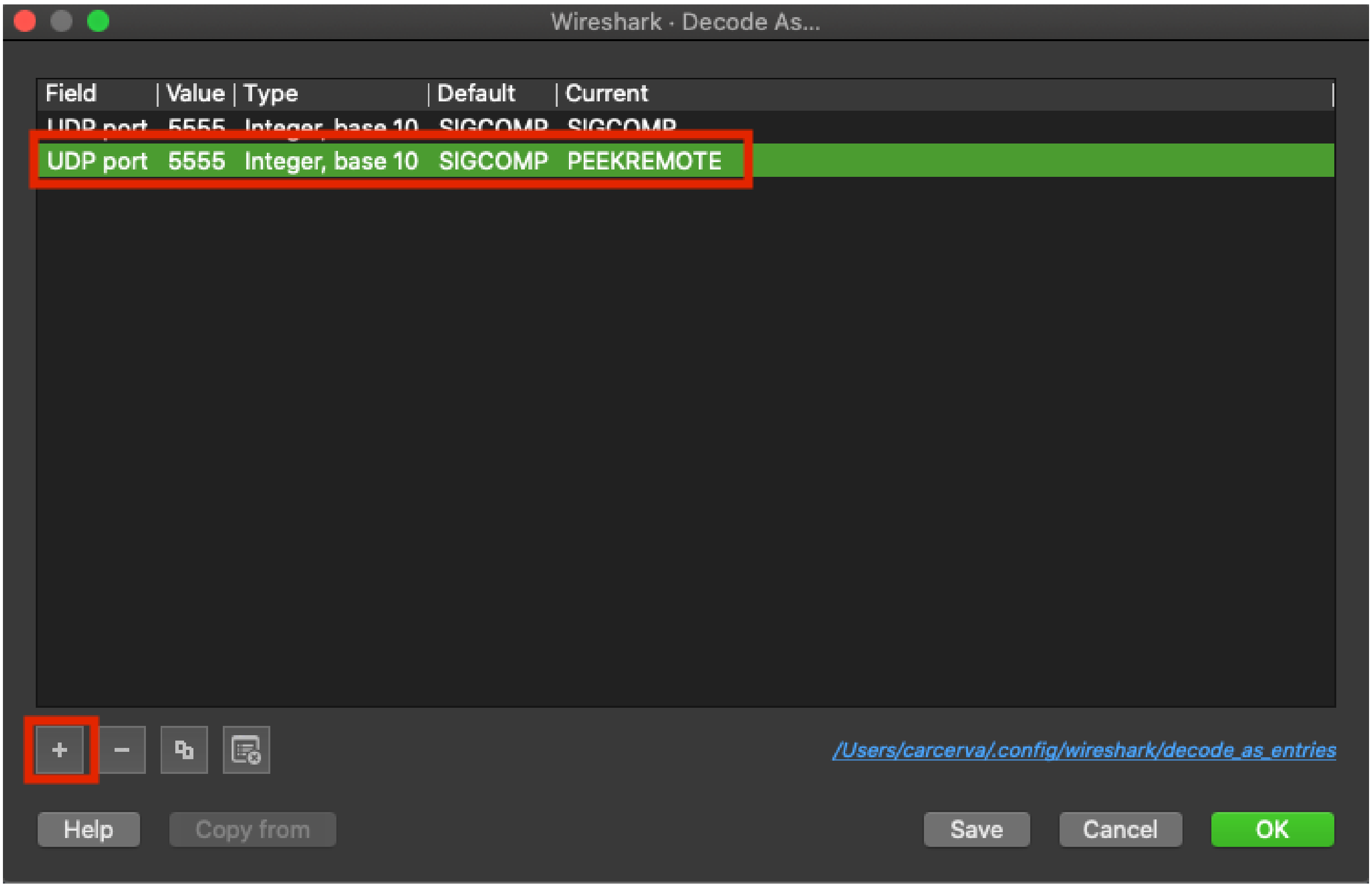
提示：如果WLAN使用加密(例如預共用金鑰(PSK))，請確保擷取會擷取AP和所需使用者端之間的四次握手。如果OTA PCAP在裝置與WLAN關聯之前啟動，或者如果客戶端在捕獲運行時被取消身份驗證並重新身份驗證，則可以完成此操作。

步驟7. Wireshark不會自動解碼資料包。要對資料包進行解碼，請從捕獲中選擇一行，使用按一下右鍵以顯示選項，然後選擇**解碼為……**（如圖所示）。



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	

步驟8.出現一個彈出視窗。選擇新增按鈕並新增新條目，選擇以下選項：**UDP連線埠從欄位、5555 from Value、SIGCOMP from Default和PEEKREMOTE** from Current，如下圖所示。



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

步驟9.按一下**OK**。封包已解碼並準備開始分析。

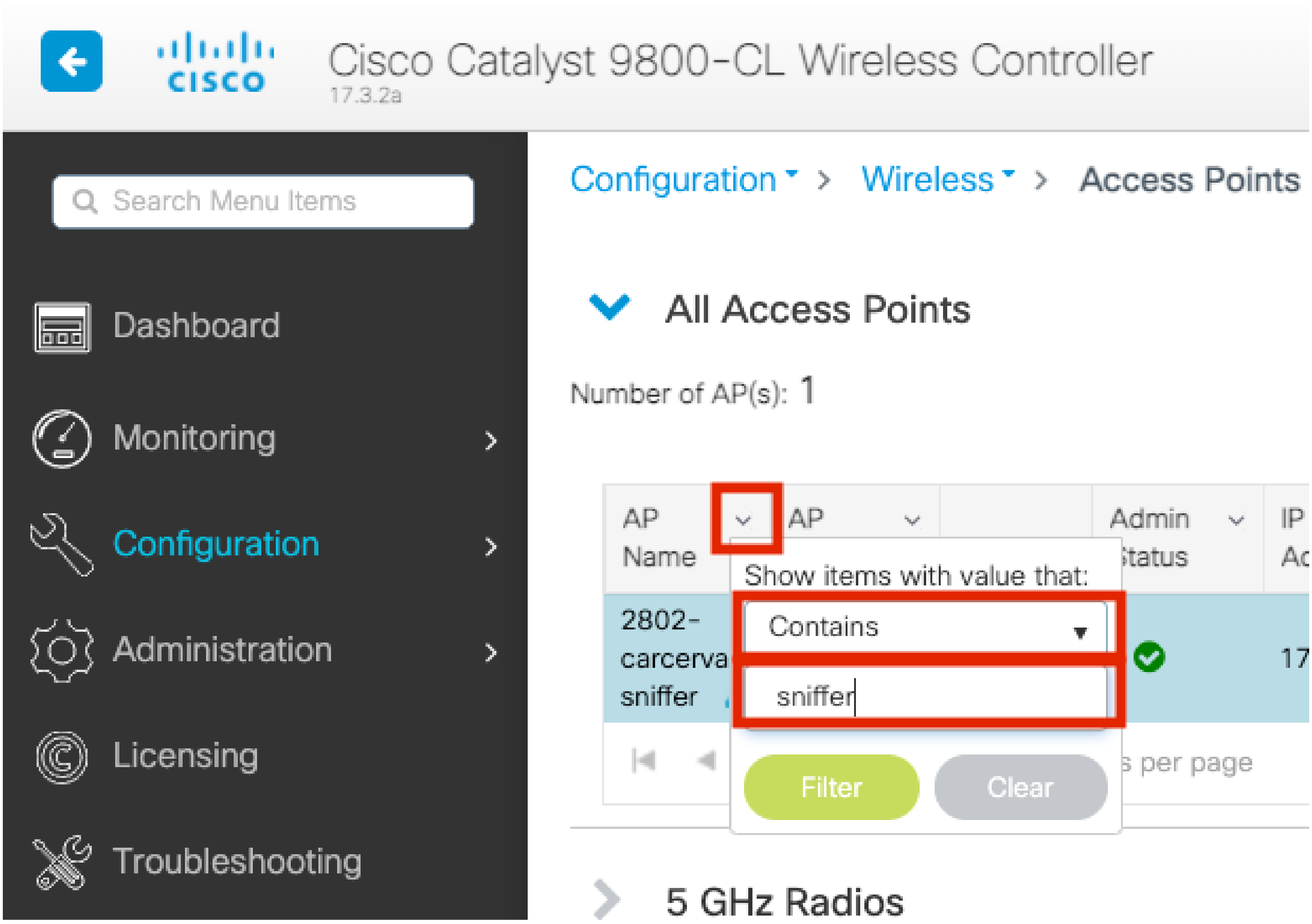
驗證

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，如圖所示。



Number of AP(s): 1

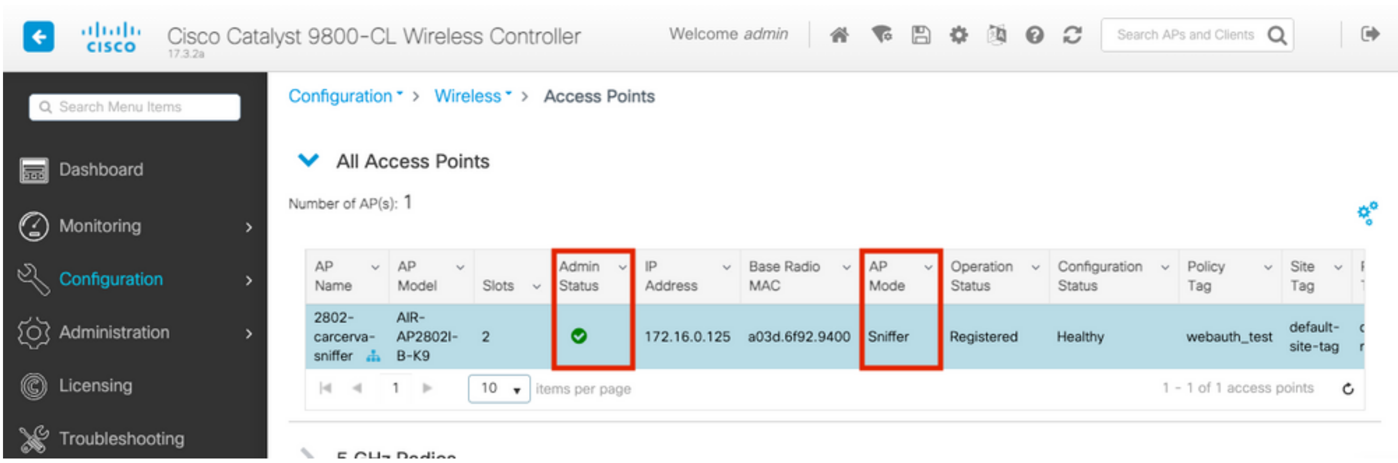
Show items with value that:

Contains

sniffer

AP Name	AP	Admin Status	IP Ac
2802-carcerva-sniffer		✓	17

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。



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

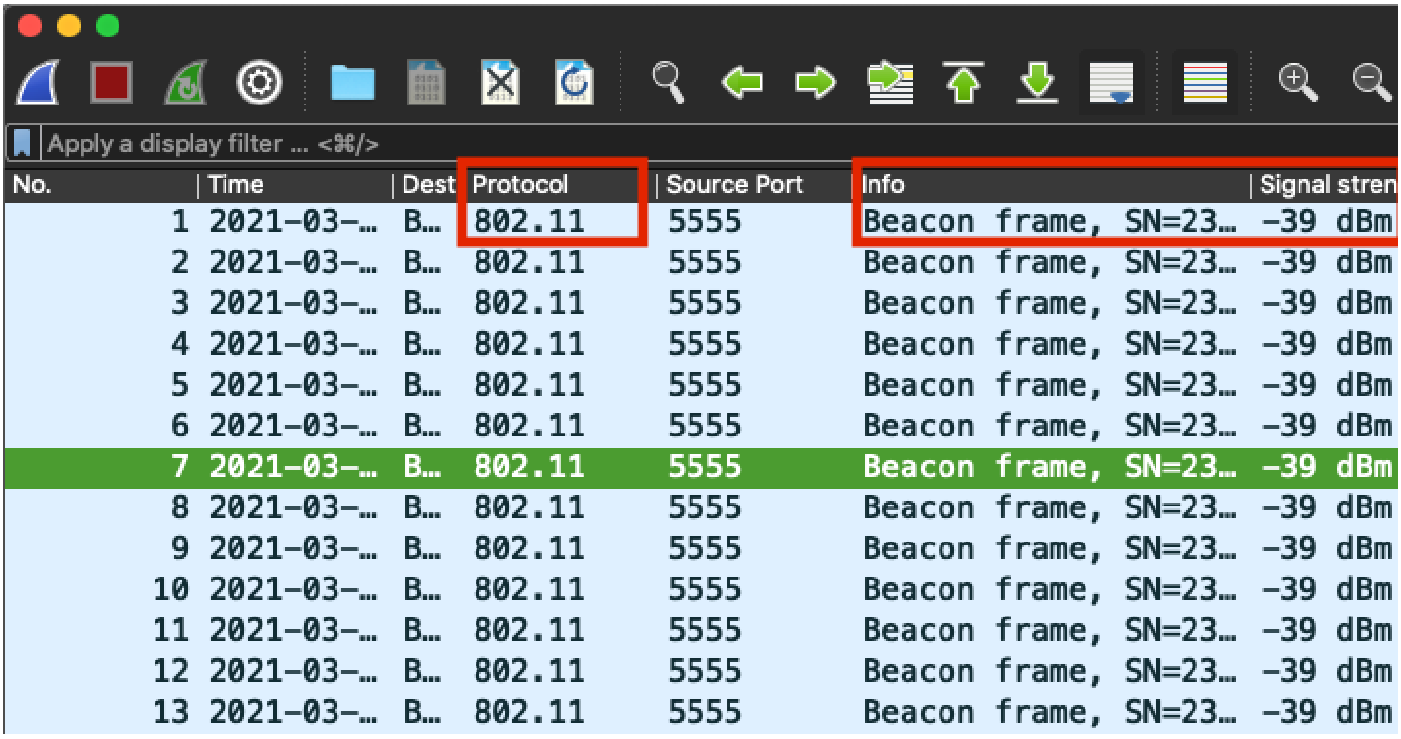
以便從9800 CLI確認AP是否處於監聽器模式。運行以下命令：

```
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
```

為了確認封包已在Wireshark上解碼。通訊協定從UDP變更為802.11，且已看到Beacon frames，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。 請確認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