Catalyst 9800 Wireless Controller의 스니퍼 모드에서 액세스 포인트 구성

목차

소개

이 문서에서는 Catalyst 9800 Series Wireless Controller(9800 WLC)의 스니퍼 모드에서 AP(Access Point)를 GUI(Graphic User Interface) 또는 CLI(Command Line Interface)를 통해 구성하는 방법과 무선 동작을 트러블슈팅 및 분석하기 위해 AP를 사용하여 PCAP(Packet Capture)를 OTA(Over the Air)를 수집하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 9800 WLC 구성
- 802.11 Standard의 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

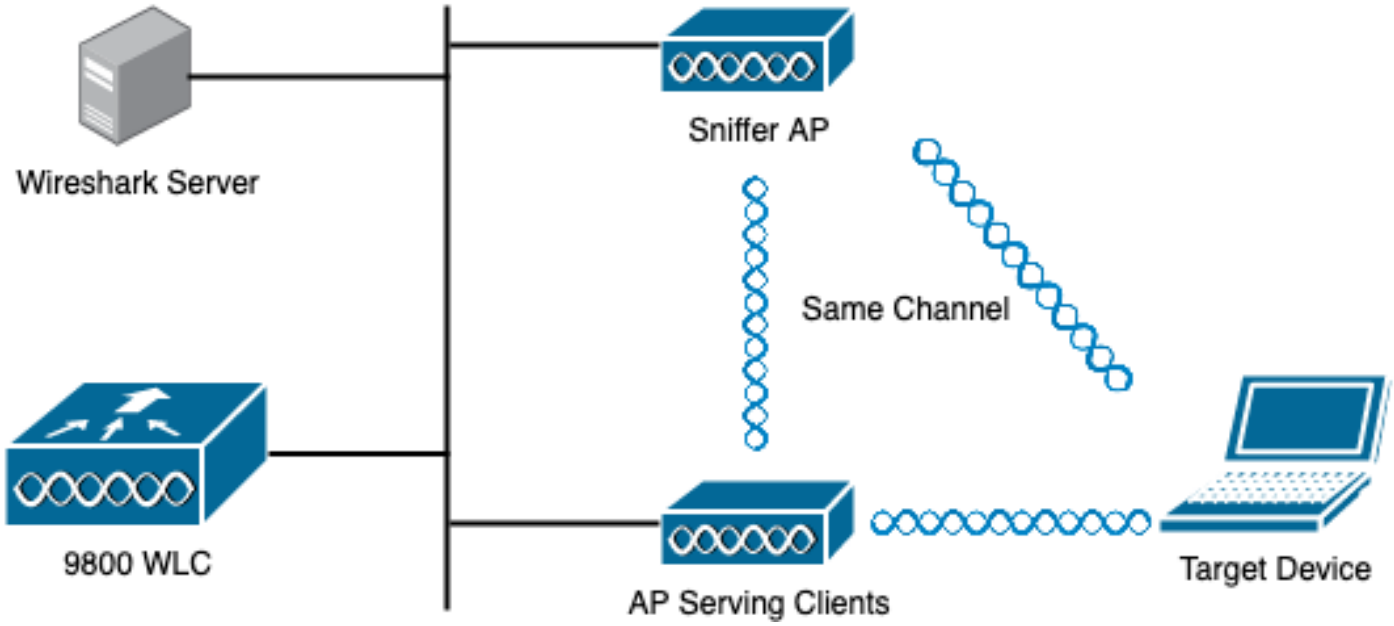
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

고려해야 할 사항:

- 대상 장치와 이 장치가 연결된 AP에 스니퍼 AP를 가깝게 하는 것이 좋습니다.
- 어떤 802.11 채널 및 폭, 클라이언트 디바이스 및 AP가 사용되는지 확인합니다.

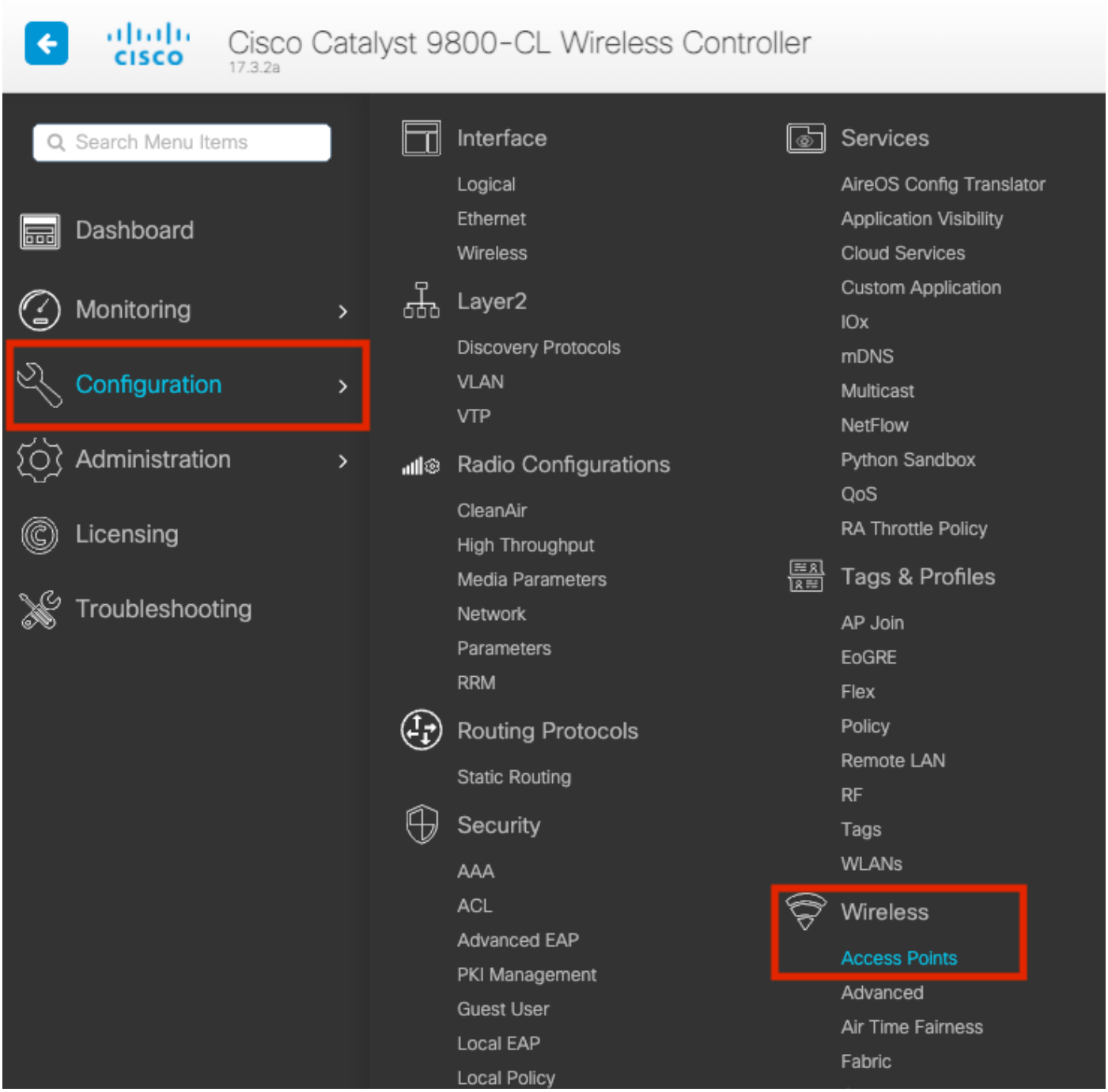
네트워크 다이어그램



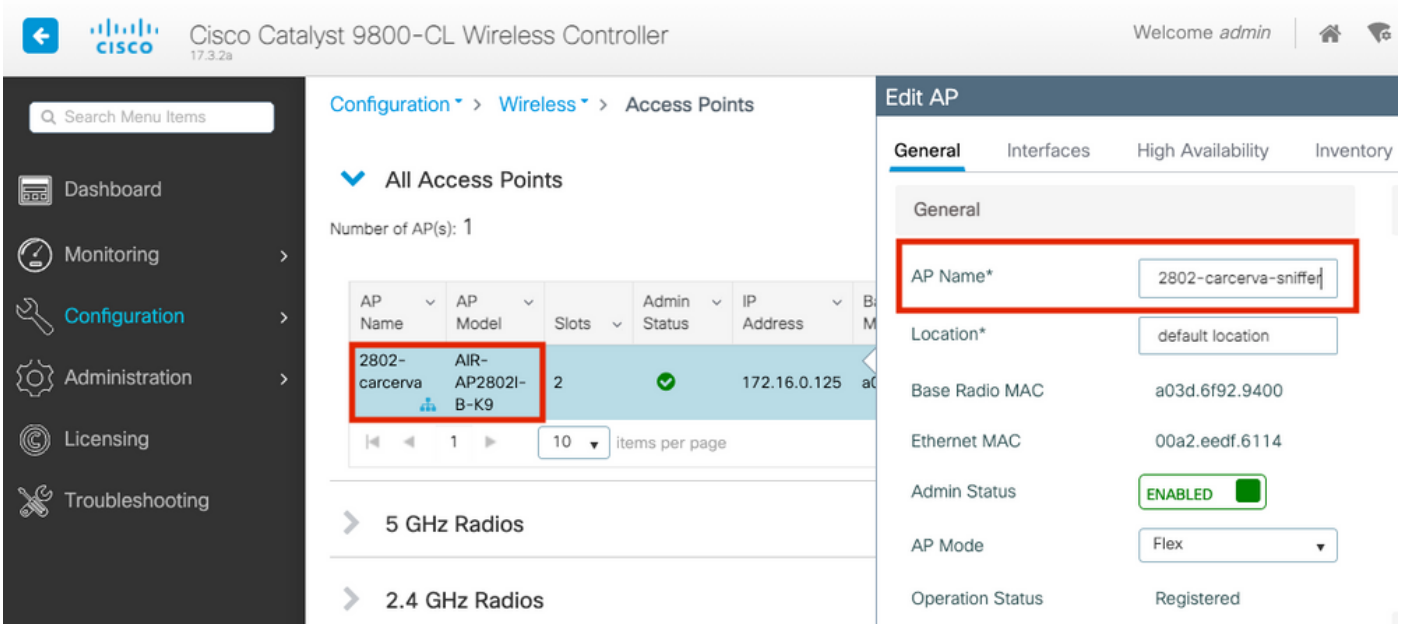
구성

GUI를 통해 스니퍼 모드에서 AP 구성

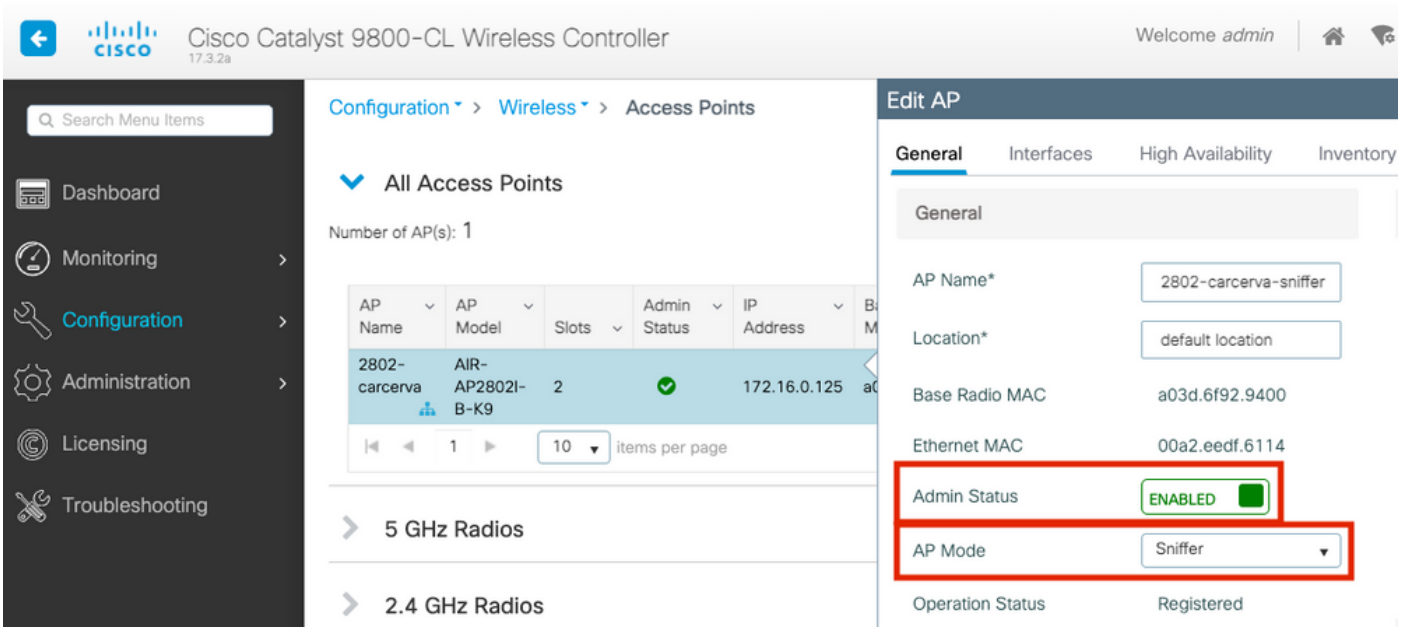
1단계. 9800 WLC GUI에서 이미지에 표시된 대로 **Configuration(구성) > Wireless(무선) > Access Points(액세스 포인트)** > All Access Points(모든 액세스 포인트)로 이동합니다.



2단계. 스니퍼 모드에서 사용할 AP를 선택합니다.General(**일반**) 탭에서 이미지에 표시된 대로 AP의 이름을 업데이트합니다.



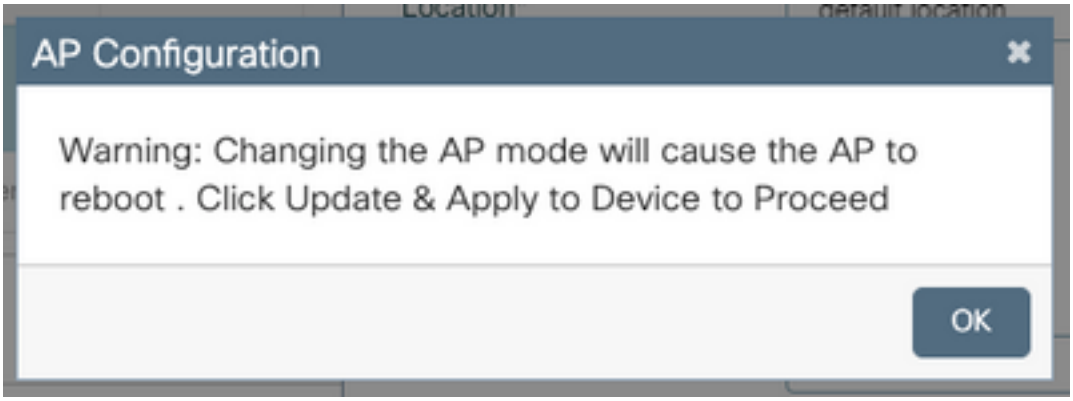
3단계. **Admin Status(관리 상태)**가 **Enabled(활성화됨)**인지 확인하고 이미지에 표시된 대로 **AP Mode(AP 모드)**를 **Sniffer(스니퍼)**로 변경합니다.



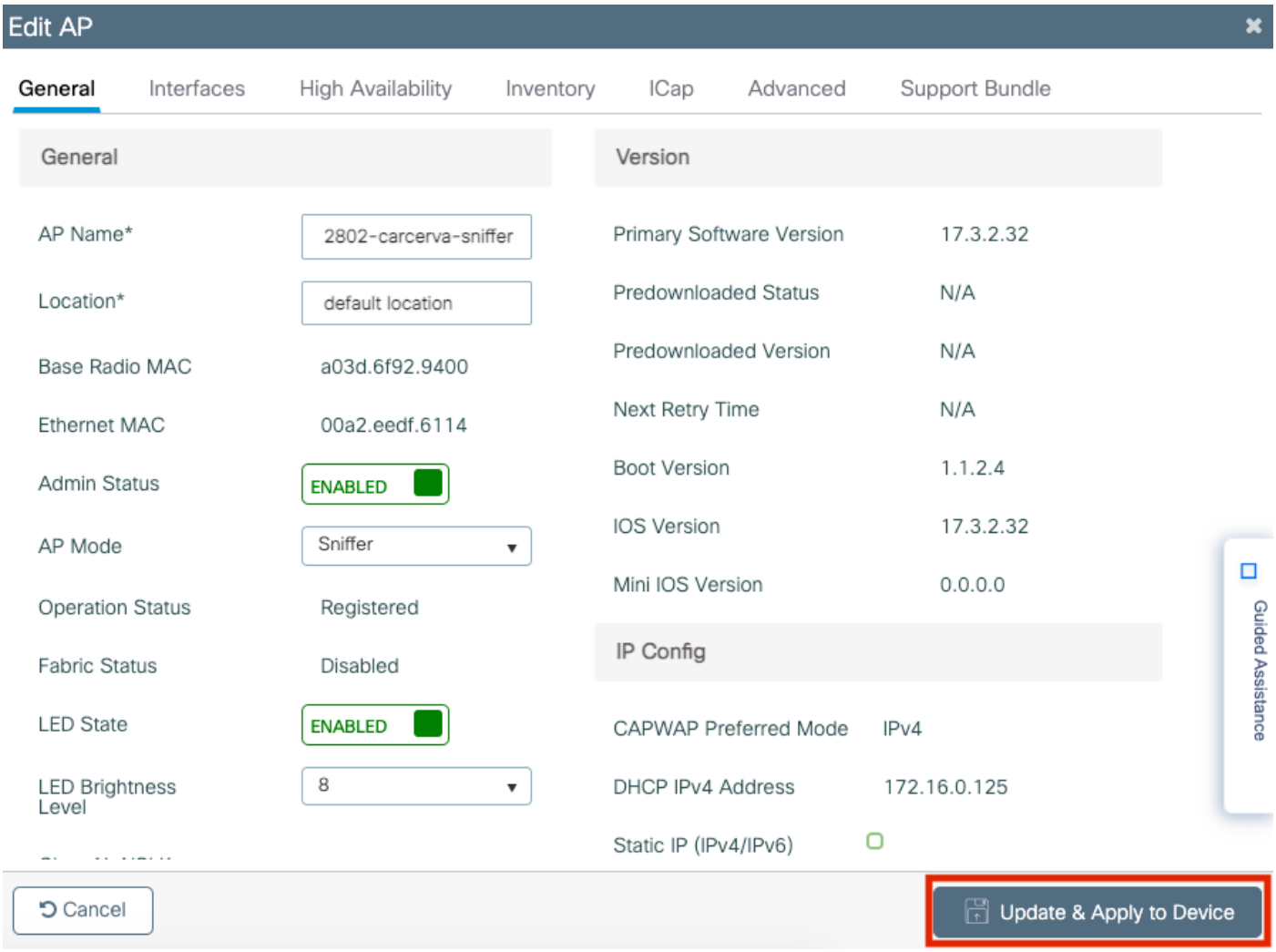
다음 메모와 함께 팝업이 나타납니다.

"경고:AP 모드를 변경하면 AP가 재부팅됩니다.계속하려면 Update & Apply to Device(업데이트 및 디바이스에 적용)를 클릭합니다."

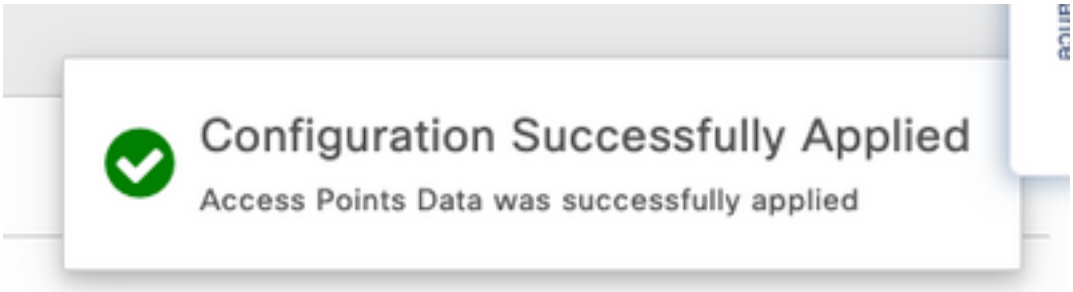
이미지에 표시된 대로 확인을 선택합니다.



4단계. 이미지에 표시된 대로 **Update & Apply to Device(업데이트 및** 장치에 적용)를 클릭합니다.



이미지에 표시된 대로 변경 사항 및 AP 바운스를 확인하는 팝업이 나타납니다.



CLI를 통해 스니퍼 모드에서 AP 구성

1단계. 스니퍼 모드로 사용할 AP를 확인하고 AP 이름을 선택합니다.

2단계. AP 이름을 수정합니다.

이 명령은 AP 이름을 수정합니다.여기서 <AP-name>은 AP의 현재 이름입니다.

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

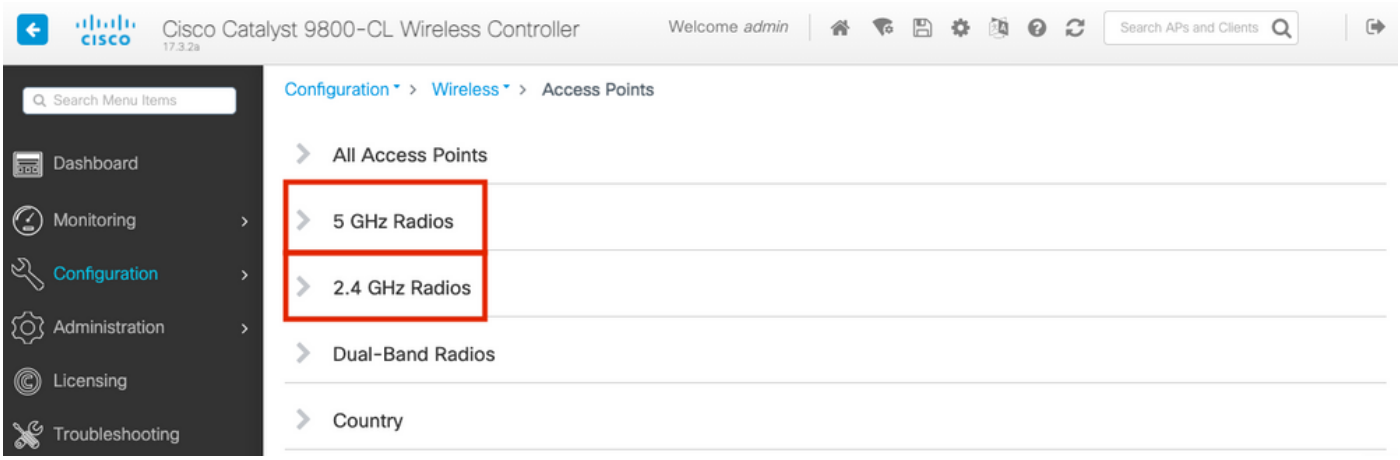
3단계. 스니퍼 모드에서 AP를 구성합니다.

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

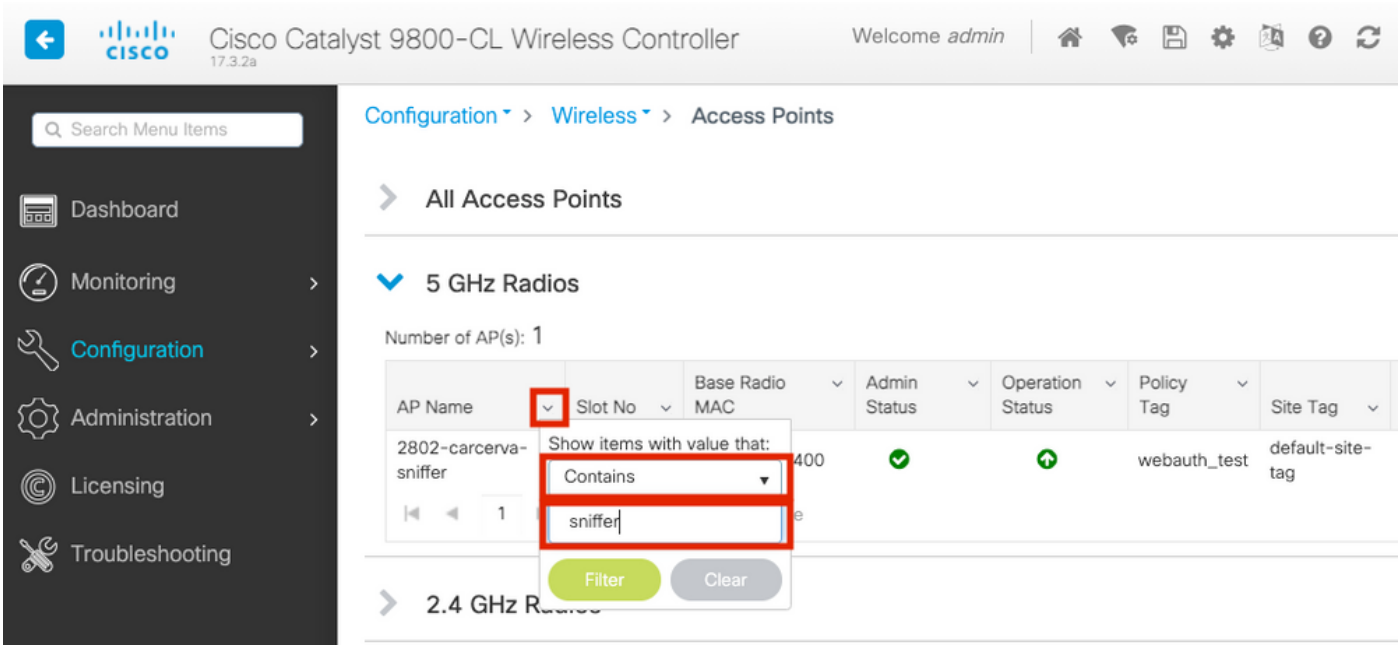
GUI를 통해 채널을 스캔하도록 AP 구성

1단계. 9800 WLC GUI에서 Configuration(구성) **> Wireless(무선) > Access Points(액세스 포인트)로 이동합니다**.

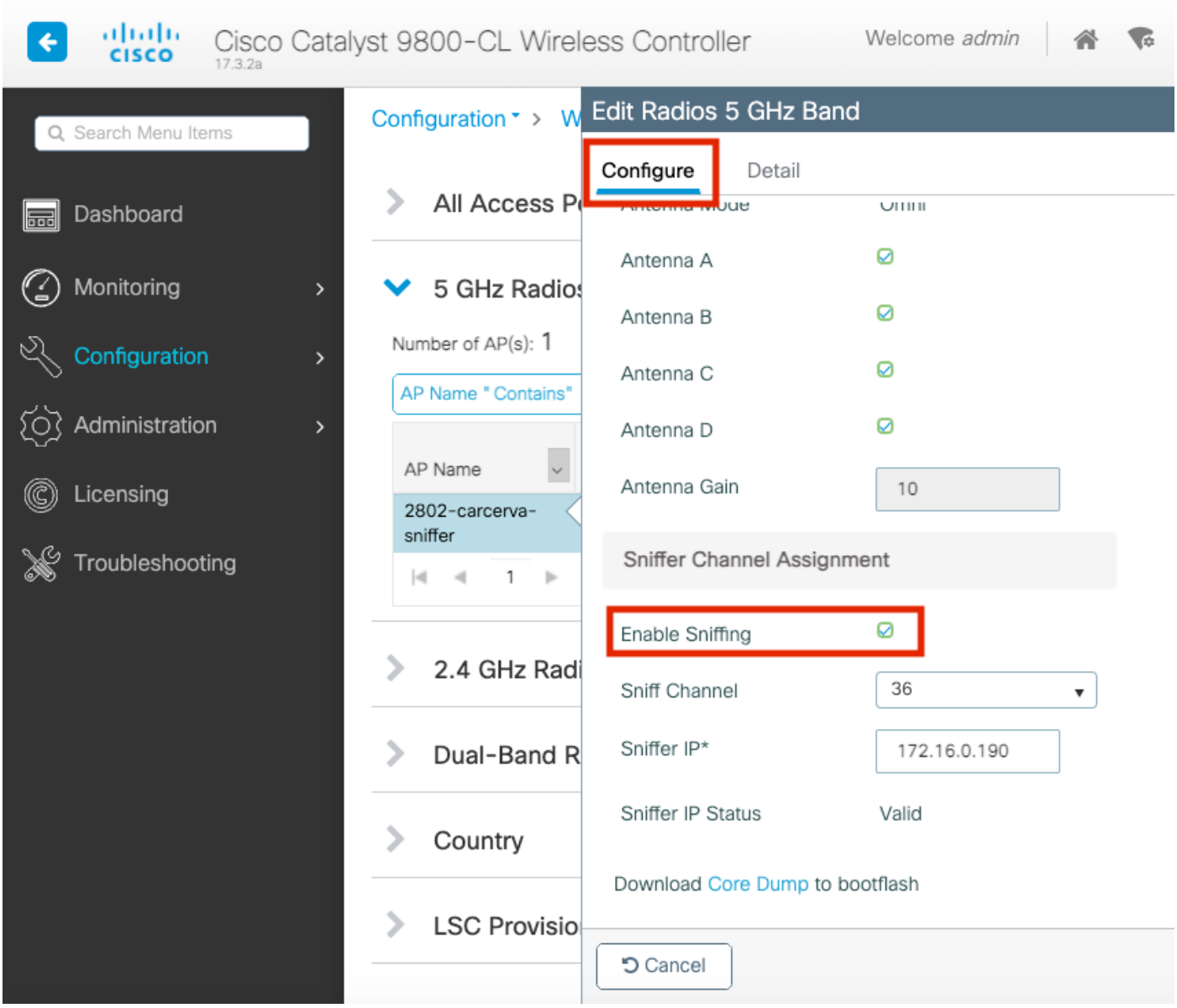
2단계. **액세스 포인트** 페이지에서 **5GHz Radio** 또는 **2.4GHz Radio** 메뉴 목록을 표시합니다.이는 이미지에 표시된 대로 스캔할 채널에 따라 달라집니다.



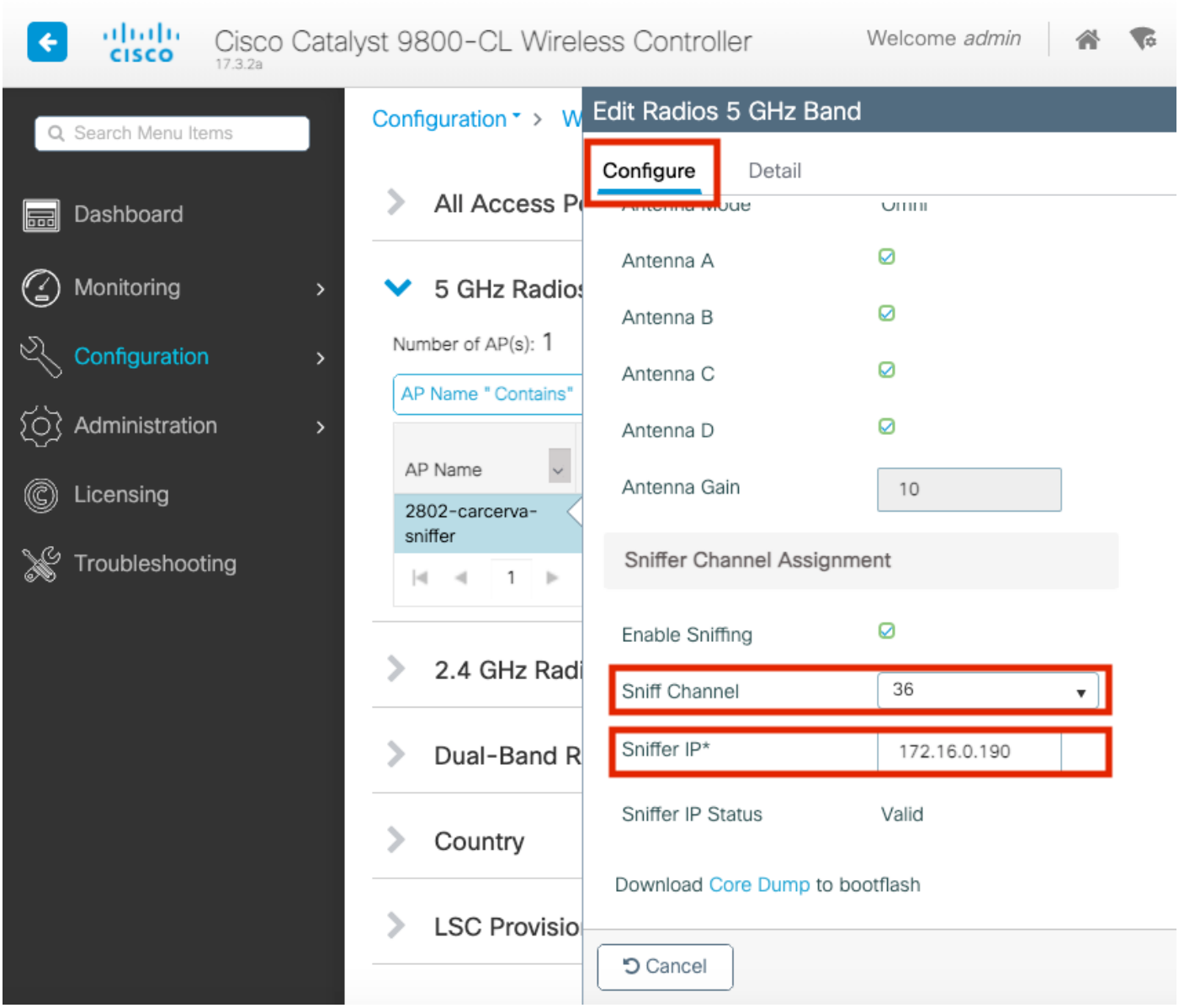
2단계. AP를 검색합니다.**화살표 아래쪽** 버튼을 클릭하여 검색 툴을 표시하고 드롭다운 목록에서 **Contains**(포함)를 선택하고 이미지에 표시된 대로 **AP 이름**을 입력합니다.



3단계. AP를 선택하고 이미지에 표시된 대로 Configure(구성)**> Sniffer Channel Assignment(스니퍼 채널 할당)** 아래에서 Enable Sniffer(스니퍼 활성화) 확인란을 선택합니다.

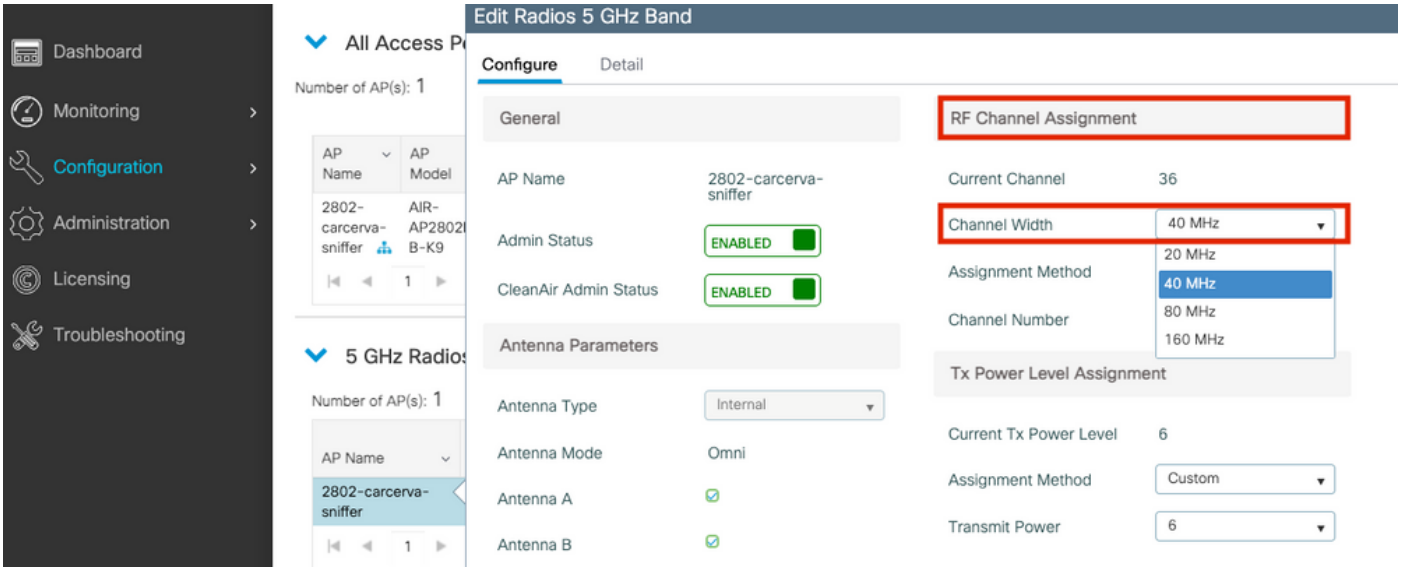


4단계. Sniff **Channel** 드롭다운 목록에서 Channel을 선택하고 이미지에 표시된 대로 Sniffer **IP 주소**(Wireshark가 있는 서버 IP 주소)를 입력합니다.



5단계. 대상 장치 및 AP가 연결할 때 사용하는 **채널 너비**를 선택합니다.

Configure(구성)> RF **Channel Assignment(RF 채널 할당)**로 이동하여 이미지에 표시된 대로 구성합니다.



CLI를 통해 채널을 스캔하도록 AP 구성

1단계. AP에서 채널 스니프를 활성화합니다.다음 명령을 실행합니다.

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

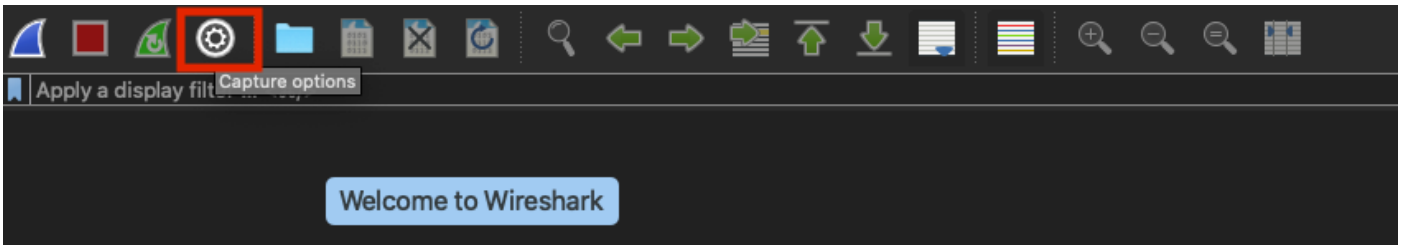
예:

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

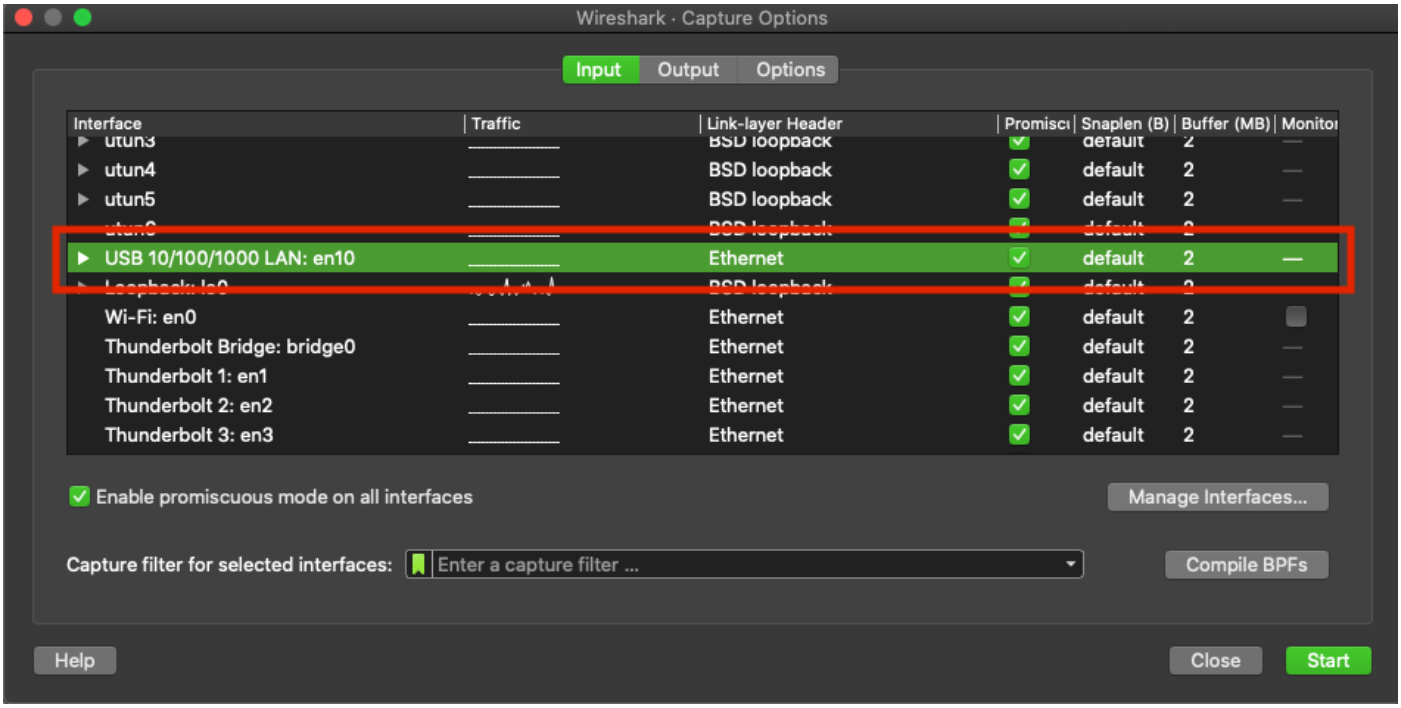
패킷 캡처를 수집하도록 Wireshark 구성

1단계. Wireshark를 실행합니다.

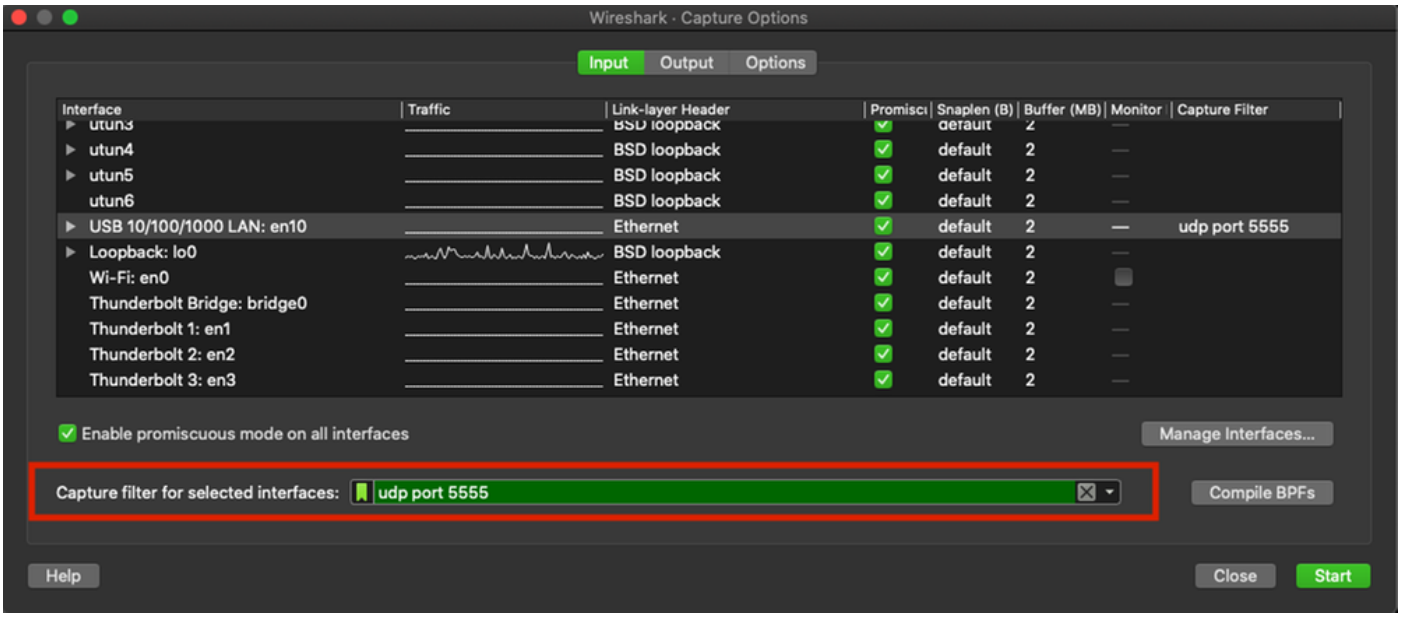
2단계. Wireshark에서 이미지에 표시된 대로 **Capture options** 메뉴 아이콘을 선택합니다.



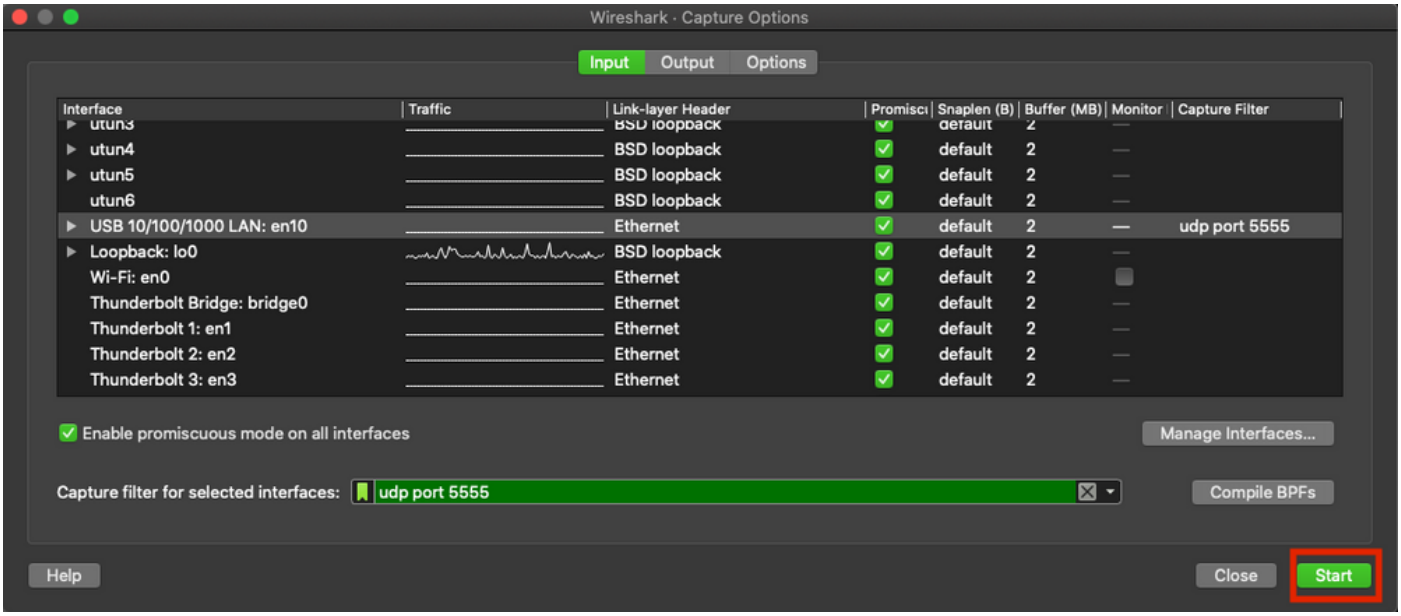
3단계. 이 작업은 팝업 창을 표시합니다.이미지에 표시된 대로 목록에서 Wired Interface를 캡처의 소스로 선택합니다.



4단계. **선택한 인터페이스**의 **Capture(캡처) 필터 아래에서** 필드 상자에 **udp port 5555**를 입력합니다(이미지에 표시됨).



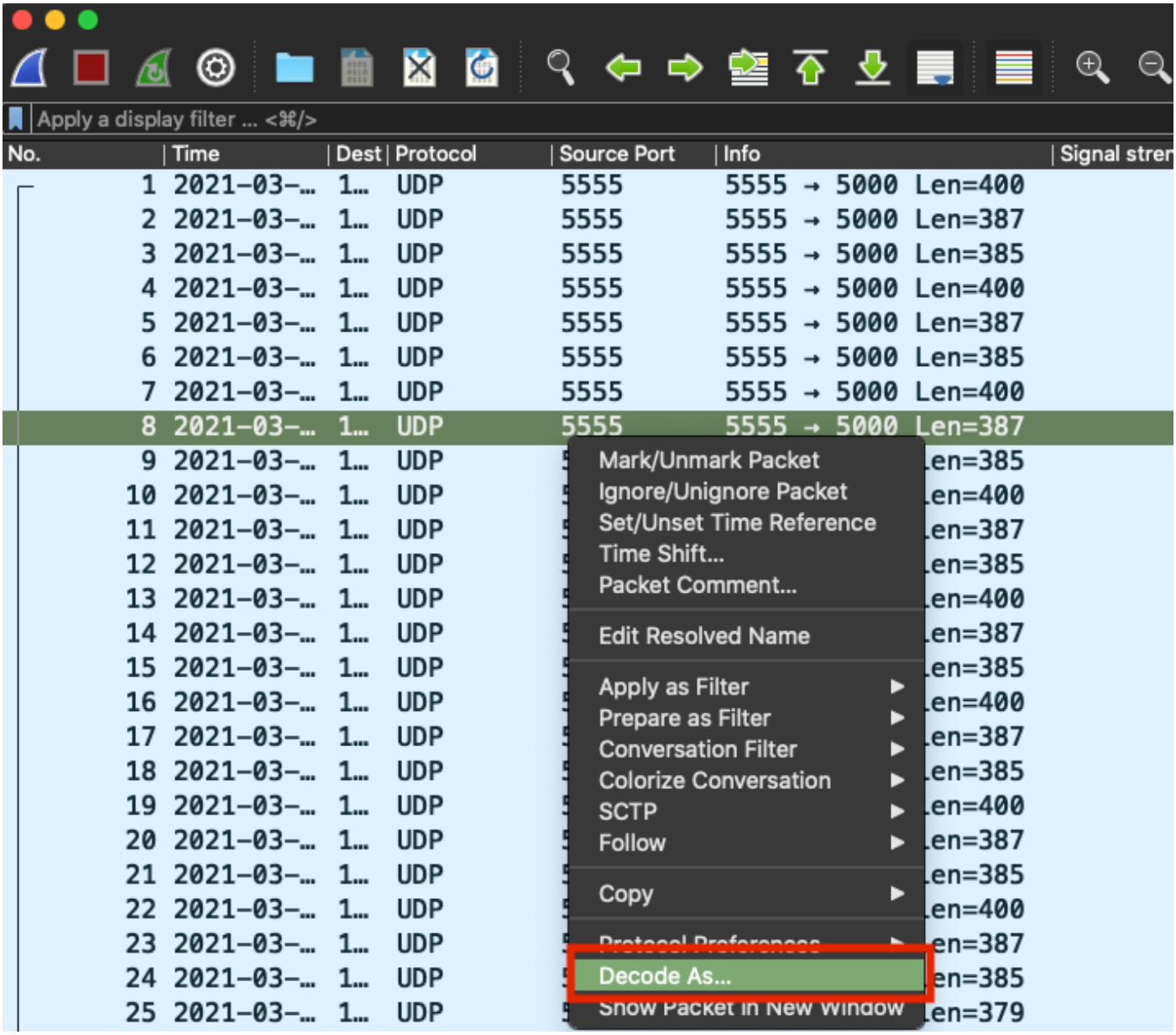
5단계. 이미지에 표시된 대로 **시작**을 클릭합니다.



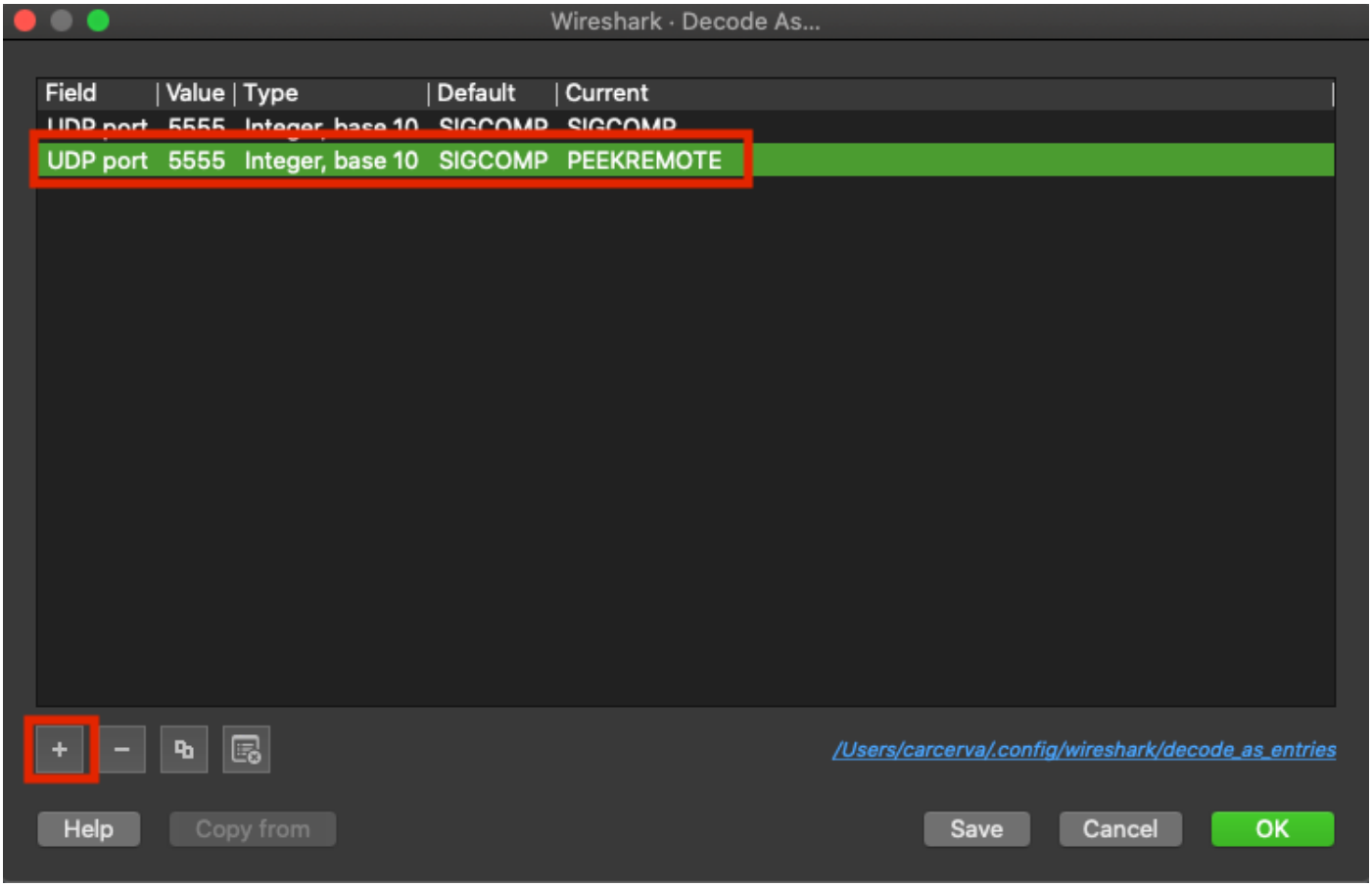
6단계. Wireshark가 필요한 정보를 수집할 때까지 기다렸다가 이미지에 표시된 대로 Wireshark에서 **Stop** 버튼을 선택합니다.

> **팁:**WLAN에서 PSK(Pre-shared Key)와 같은 암호화를 사용하는 경우 캡처가 AP와 원하는 클라이언트 간에 4방향 핸드셰이크를 catch하는지 확인합니다.디바이스가 WLAN에 연결되기 전에 OTA PCAP가 시작되거나 캡처가 실행되는 동안 클라이언트가 인증되지 않고 재인증된 경우 이 작업을 수행할 수 있습니다.

7단계. Wireshark는 패킷을 자동으로 디코딩하지 않습니다.패킷을 디코딩하려면 캡처에서 행을 선택하고 마우스 오른쪽 버튼을 클릭하여 옵션을 표시하고 이미지에 표시된 대로 **Decode As...**를 선택합니다.



8단계. 팝업 창이 나타납니다.추가 단추를 선택하고 새 항목을 추가하려면 다음 옵션을 선택합니다 .**UDP 포트** from **Field, 555** from **Value**, **SIGCOMP** from **Default** 및 PEEKREMOTE from Current(이미지에 표시된 대로)입니다.



9단계. **확인**을 클릭합니다.패킷이 디코딩되고 분석을 시작할 준비가 됩니다.

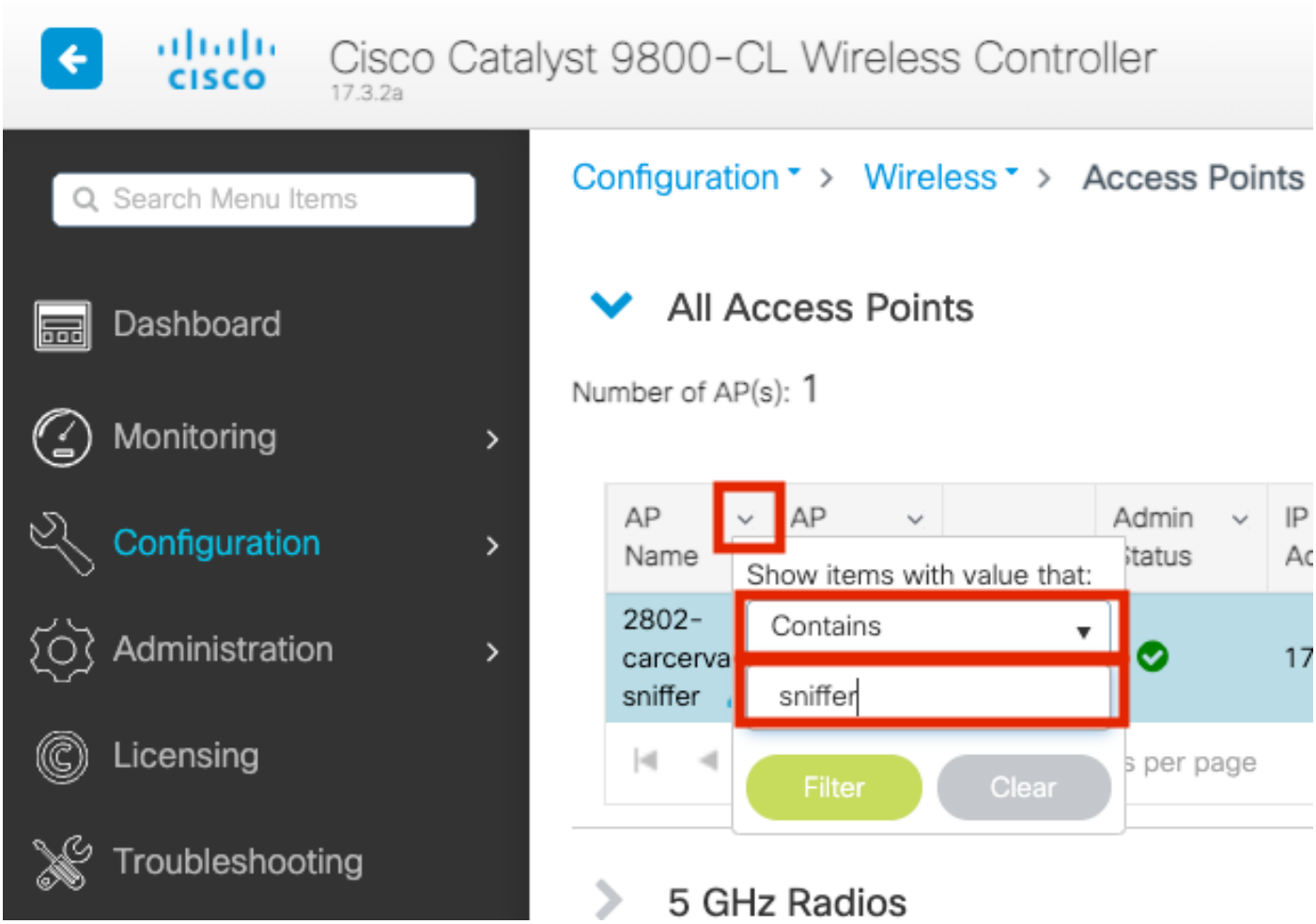
다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

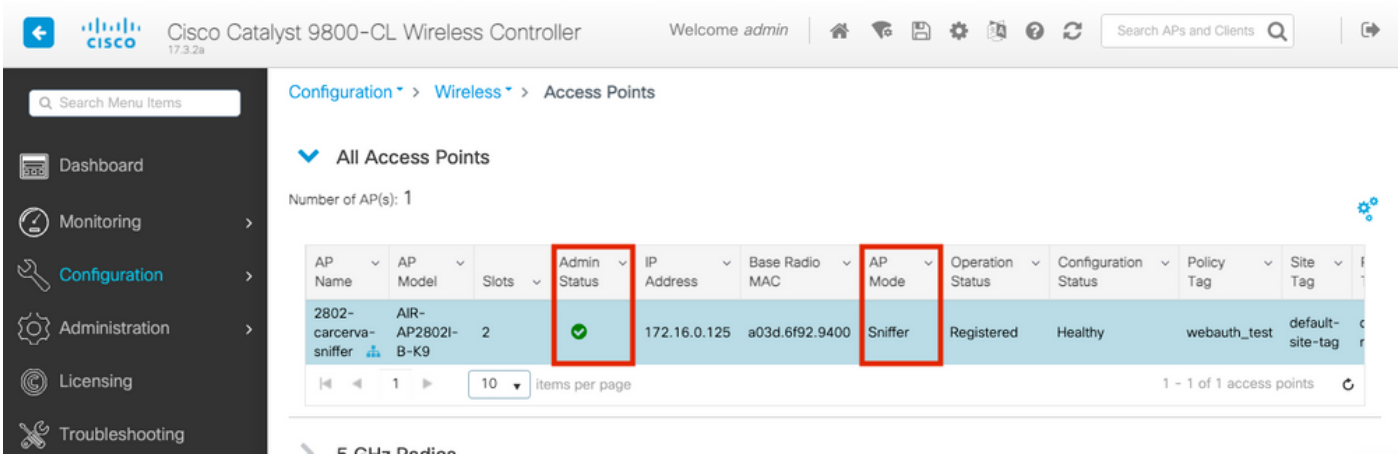
AP가 9800 GUI에서 스니퍼 모드에 있는지 확인하려면 다음을 수행합니다.

1단계. 9800 WLC GUI에서 Configuration(구성) > **Wireless(무선) > Access Points(액세스 포인트) > All Access Points(모든 액세스 포인트)로 이동합니다**.

2단계. AP를 검색합니다.아래쪽 화살표 단추를 클릭하여 검색 도구를 표시하고 드롭다운 목록에서 Contains를 선택한 다음 이미지에 표시된 대로 AP 이름을 입력합니다.



3단계. **관리 상태**가 **녹색 확인 표시**와 **AP 모드**가 **스니퍼**인지 확인합니다(이미지에 표시됨).



AP가 9800 CLI에서 스니퍼 모드에 있는지 확인하기 위해다음 명령을 실행합니다.

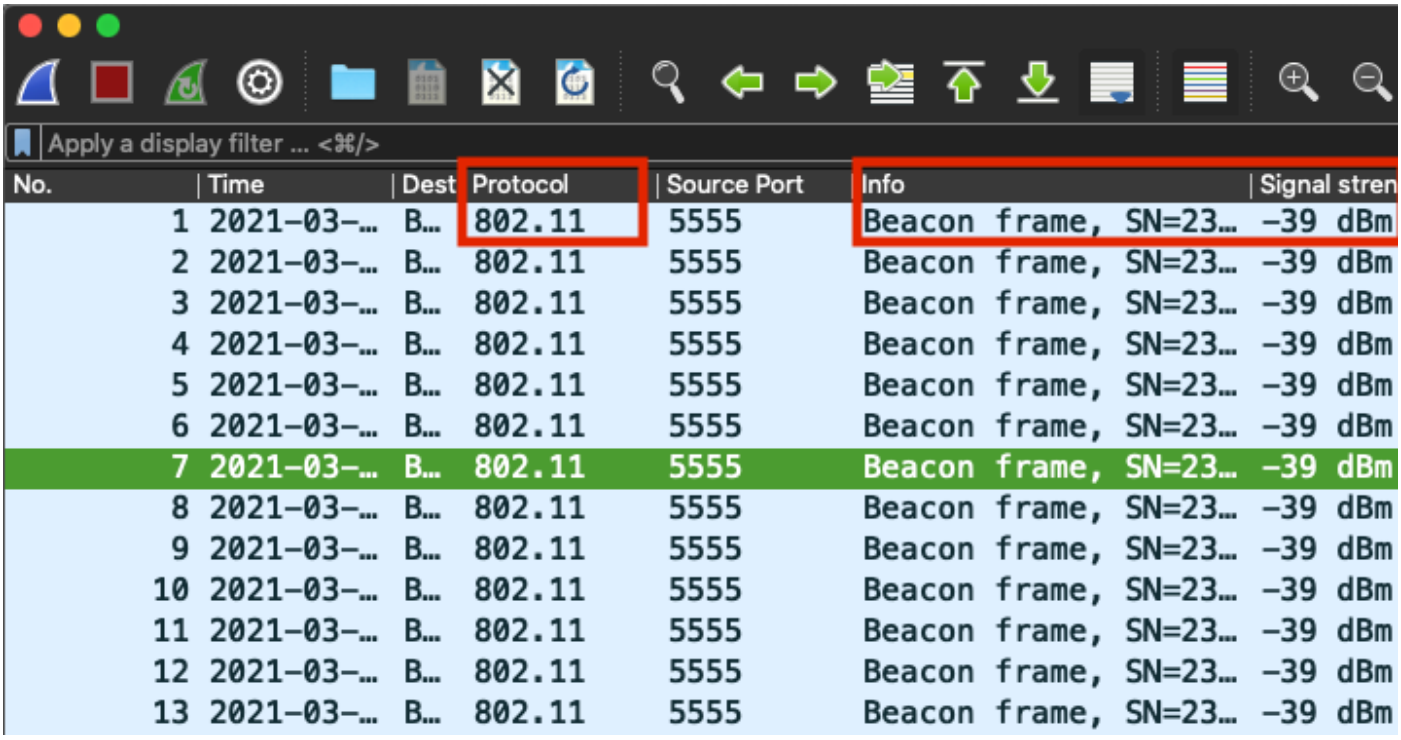
```
carcerva-9k-upg#show ap name 2802-carcerva-sniffer config general | i Administrative
Administrative State : Enabled

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
```

패킷이 Wireshark에서 디코딩되었는지 확인하기 위해프로토콜은 **UDP**에서 **802.11**으로 변경되며 이미지에 표시된 대로 비컨 프레임이 표시됩니다.



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제/장애:Wireshark는 AP에서 데이터를 수신하지 않습니다.

해결책:WMI(Wireless Management Interface)에서 Wireshark 서버에 연결할 수 있어야 합니다. WLC에서 Wireshark 서버와 WMI 간의 연결성을 확인하십시오.

관련 정보

- Cisco Catalyst 9800 Series Wireless Controller 소프트웨어 구성 가이드, Cisco IOS XE Amsterdam 17.3.x - 장:스니퍼 모드
- 802.11 Wireless Sniffing의 기본 사항
- 기술 지원 및 문서 – Cisco Systems