

Configurazione di un punto di accesso in modalità sniffer sui controller wireless Catalyst 9800

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione dell'access point in modalità sniffer tramite GUI](#)

[Configurazione dell'access point in modalità sniffer tramite CLI](#)

[Configurazione dell'access point per la scansione di un canale tramite GUI](#)

[Configurazione dell'access point per la scansione di un canale tramite CLI](#)

[Configurazione di Wireshark per la raccolta dell'acquisizione del pacchetto](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare un Access Point (AP) in modalità sniffer su un Catalyst serie 9800 Wireless Controller (9800 WLC) tramite l'interfaccia grafica utente (GUI) o l'interfaccia della riga di comando (CLI) e come raccogliere un Packet Capture (PCAP) over the Air (OTA) con lo sniffer AP per risolvere i problemi e analizzare i comportamenti wireless.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione 9800 WLC
- Conoscenze base dello standard 802.11

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

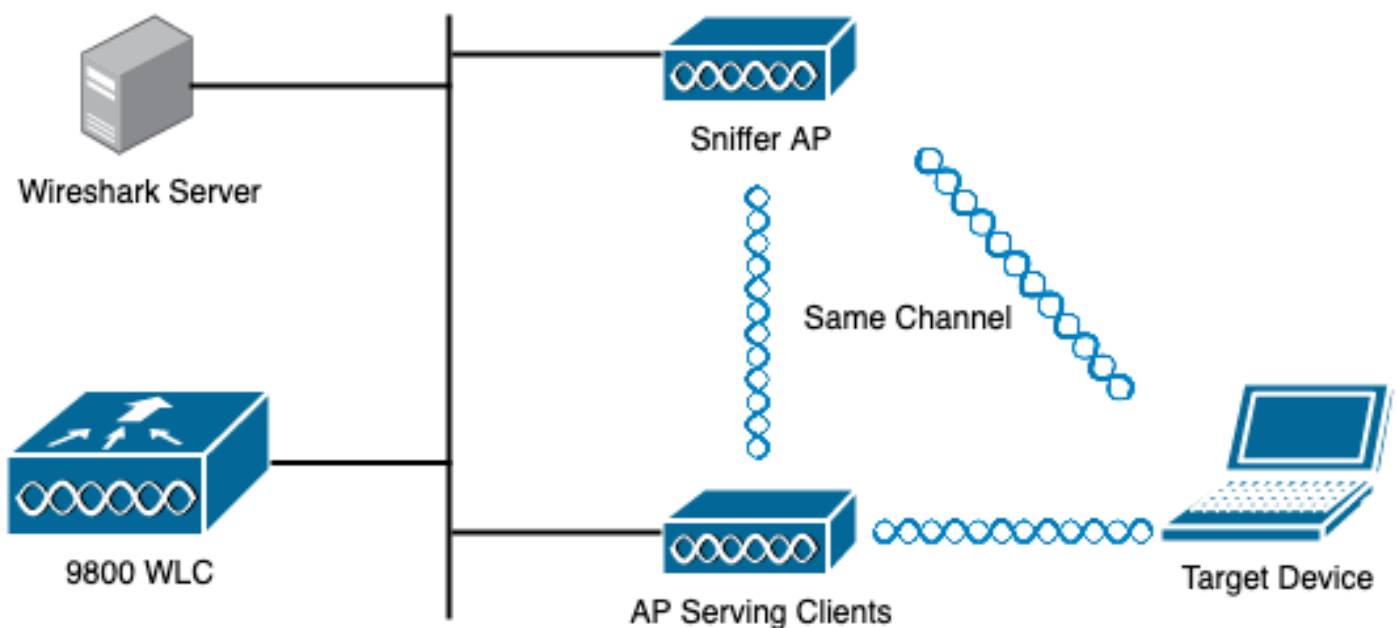
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Elementi da considerare:

- Si consiglia di avvicinare l'access point sniffer al dispositivo di destinazione e all'access point a cui è connesso il dispositivo.
- Accertarsi di conoscere il canale e la larghezza 802.11 utilizzati dal dispositivo client e dall'access point.

Esempio di rete



Configurazioni

Configurazione dell'access point in modalità sniffer tramite GUI

Passaggio 1. Sull'interfaccia utente del WLC 9800, selezionare **Configuration > Wireless > Access Point > All Access Point**, come mostrato nell'immagine.



Q Search Menu Items

- Dashboard
- Monitoring >
- Configuration** >
- Administration >
- Licensing
- Troubleshooting

- Interface
 - Logical
 - Ethernet
 - Wireless
- Layer2
 - Discovery Protocols
 - VLAN
 - VTP
- Radio Configurations
 - CleanAir
 - High Throughput
 - Media Parameters
 - Network
 - Parameters
 - RRM
- Routing Protocols
 - Static Routing
- Security
 - AAA
 - ACL
 - Advanced EAP
 - PKI Management
 - Guest User
 - Local EAP
 - Local Policy

- Services
 - AireOS Config Translator
 - Application Visibility
 - Cloud Services
 - Custom Application
 - IOx
 - mDNS
 - Multicast
 - NetFlow
 - Python Sandbox
 - QoS
 - RA Throttle Policy
- Tags & Profiles
 - AP Join
 - EoGRE
 - Flex
 - Policy
 - Remote LAN
 - RF
 - Tags
 - WLANs
- Wireless**
 - Access Points**
 - Advanced
 - Air Time Fairness
 - Fabric

Passaggio 2. Selezionare l'access point che si desidera utilizzare in modalità sniffer. Nella scheda **Generale**, aggiornare il nome dell'access point, come mostrato nell'immagine.

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

| AP Name | AP Model | Slots | Admin Status | IP Address | Bl | M |
|---------------|------------------|-------|--------------|--------------|----|---|
| 2802-carcerva | AIR-AP2802I-B-K9 | 2 | ✓ | 172.16.0.125 | ac | |

5 GHz Radios

2.4 GHz Radios

Edit AP

General Interfaces High Availability Inventory

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

Passaggio 3. Verificare che **Admin Status** sia **Enabled** (Stato amministratore) e modificare **AP Mode** (Modalità punto di accesso) in **Sniffer**, come mostrato nell'immagine.

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

| AP Name | AP Model | Slots | Admin Status | IP Address | Bl | M |
|---------------|------------------|-------|--------------|--------------|----|---|
| 2802-carcerva | AIR-AP2802I-B-K9 | 2 | ✓ | 172.16.0.125 | ac | |

5 GHz Radios

2.4 GHz Radios

Edit AP

General Interfaces High Availability Inventory

General

AP Name* 2802-carcerva-sniffer

Location* default location

Base Radio MAC a03d.6f92.9400

Ethernet MAC 00a2.eedf.6114

Admin Status ENABLED

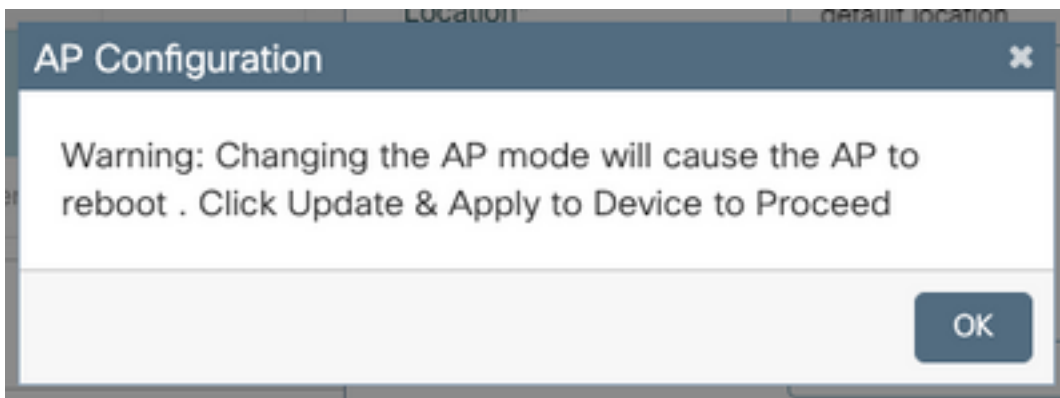
AP Mode Sniffer

Operation Status Registered

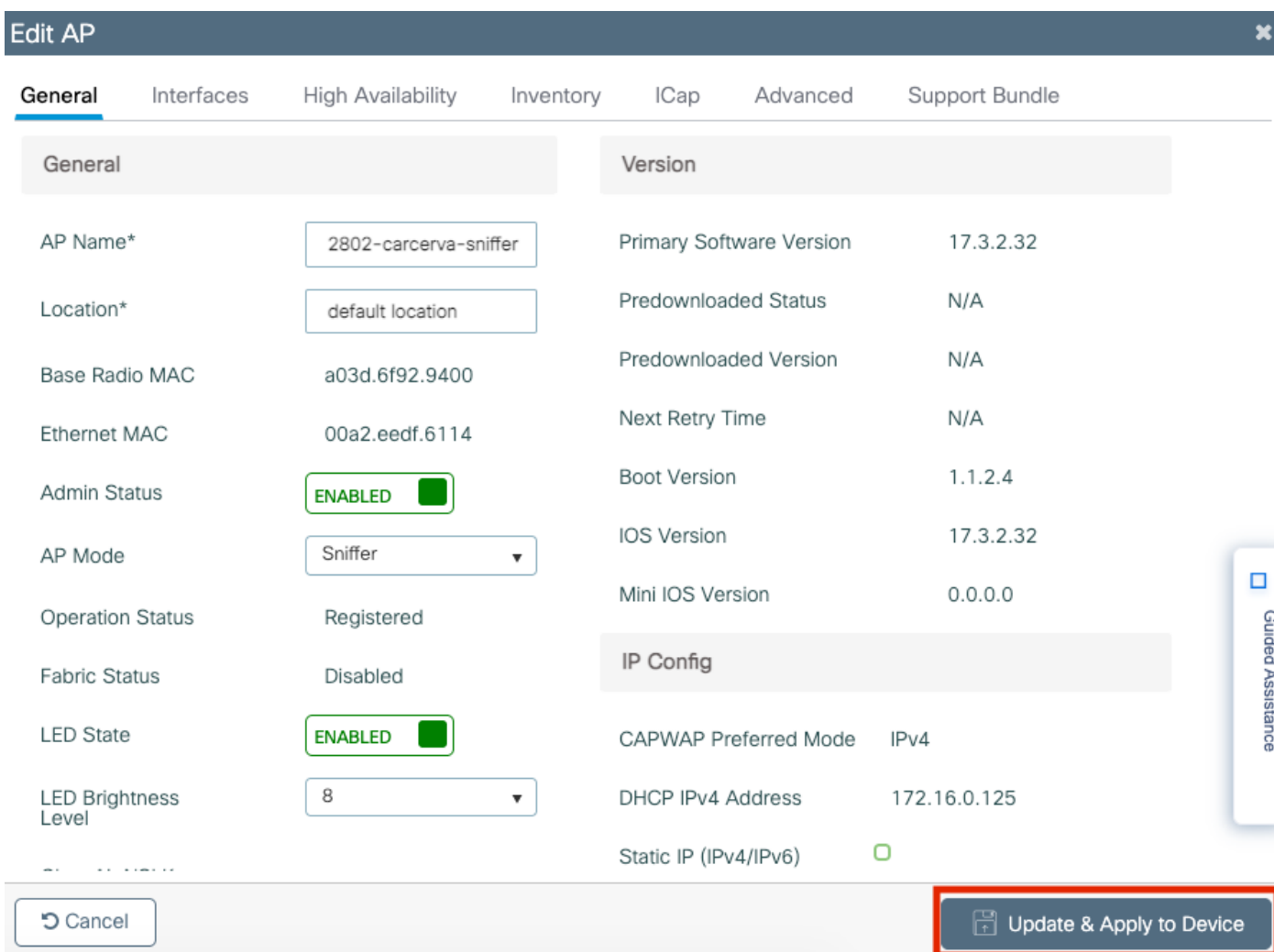
Viene visualizzato un popup con la nota successiva:

"Avviso: Se si modifica la modalità, l'access point verrà riavviato. Fare clic su Aggiorna e applica al dispositivo per continuare"

Selezionate **OK**, come mostrato nell'immagine.



Passaggio 4. Fare clic su **Update & Apply to Device** (Aggiorna e applica al dispositivo), come mostrato nell'immagine.



Viene visualizzato un popup per confermare le modifiche e i rimbalzi dell'access point, come mostrato nell'immagine.



Configuration Successfully Applied

Access Points Data was successfully applied

2018

Configurazione dell'access point in modalità sniffer tramite CLI

Passaggio 1. Determinare l'access point che si desidera utilizzare come modalità Sniffer e selezionare il nome dell'access point.

Passaggio 2. Modificare il nome dell'access point.

Questo comando modifica il nome dell'access point. Dove <AP-name> è il nome corrente del punto di accesso.

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

Passaggio 3. Configurare l'access point in modalità Sniffer.

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

Configurazione dell'access point per la scansione di un canale tramite GUI

Passaggio 1. Nell'interfaccia utente di 9800 WLC, selezionare **Configuration > Wireless > Access Point** (Configurazione > Wireless > Punti di accesso).

Passaggio 2. Nella pagina **Access Point**, visualizzare l'elenco dei menu delle **radio da 5 GHz** o da **2,4 GHz**. Dipende dal canale che si desidera digitalizzare, come mostrato nell'immagine.

The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller GUI. The breadcrumb navigation is 'Configuration > Wireless > Access Points'. The main content area lists several radio configuration options: 'All Access Points', '5 GHz Radios', '2.4 GHz Radios', 'Dual-Band Radios', and 'Country'. The '5 GHz Radios' and '2.4 GHz Radios' options are highlighted with a red box.

Passaggio 2. Cercare nell'access point. Fare clic sul pulsante **freccia giù** per visualizzare lo strumento di ricerca, selezionare **Contiene** dall'elenco a discesa e digitare il **nome** dell'access point, come mostrato nell'immagine.

Cisco Catalyst 9800-CL Wireless Controller 17.3.2a

Welcome admin

Configuration > Wireless > Access Points

All Access Points

5 GHz Radios

Number of AP(s): 1

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

Show items with value that:
 Contains
 sniffer

Filter Clear

2.4 GHz Radios

Passaggio 3. Selezionare l'access point e selezionare la casella di controllo **Abilita sniffer** in **Configurazione > Assegnazione canale sniffer**, come mostrato nell'immagine.

Cisco Catalyst 9800-CL Wireless Controller 17.3.2a

Welcome admin

Configuration > Wireless > Edit Radios 5 GHz Band

All Access Points

5 GHz Radios

Number of AP(s): 1

AP Name "Contains"

AP Name
2802-carcerva-sniffer

2.4 GHz Radios

Dual-Band Radios

Country

LSC Provisioning

Configure Detail

Antenna Mode

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

Passaggio 4. Selezionare il canale dall'elenco a discesa **Canale sniffer** e digitare l'**indirizzo IP dello sniffer** (indirizzo IP del server con Wireshark), come mostrato nell'immagine.

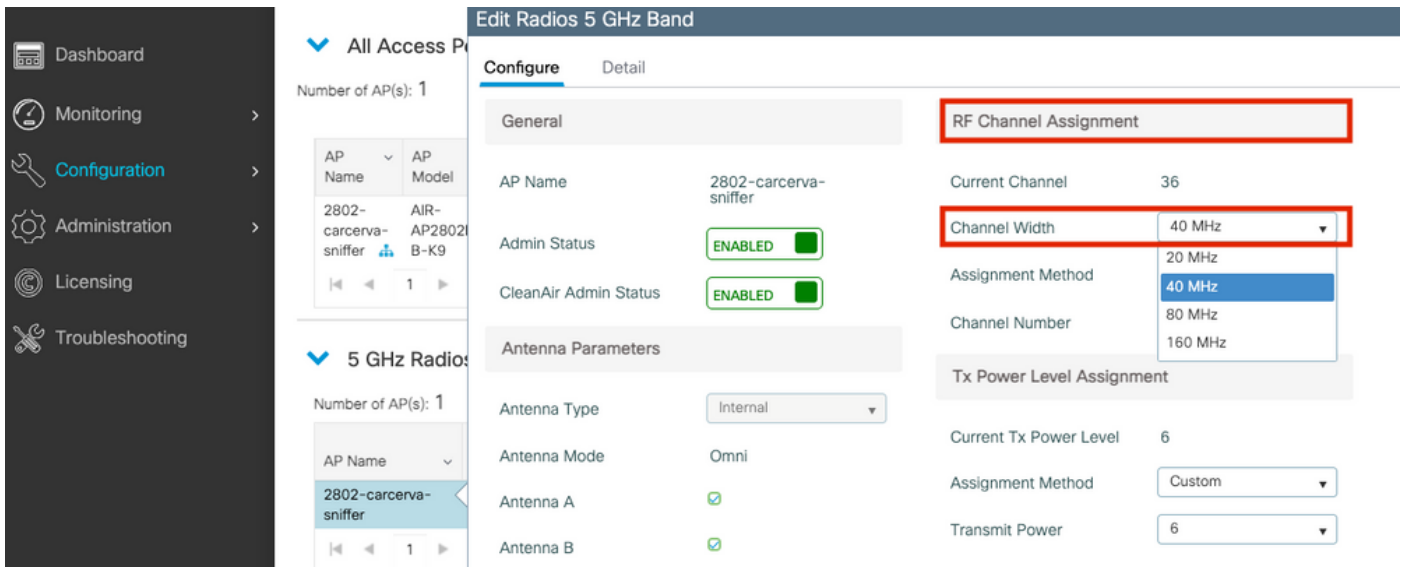
The screenshot shows the Cisco Catalyst 9800-CL Wireless Controller configuration interface. The page title is "Edit Radios 5 GHz Band". The "Configure" tab is selected. The "Sniffer Channel Assignment" section is visible, showing the following configuration:

| Parameter | Value |
|-------------------|-------------------------------------|
| Enable Sniffing | <input checked="" type="checkbox"/> |
| Sniff Channel | 36 |
| Sniffer IP* | 172.16.0.190 |
| Sniffer IP Status | Valid |

The "Sniffer Channel" and "Sniffer IP*" fields are highlighted with red boxes. A "Cancel" button is located at the bottom of the configuration area.

Passaggio 5. Selezionare la **larghezza del canale** utilizzata dal dispositivo di destinazione e dall'access point quando collegato.

Per configurare questa funzione, selezionare **Configure > RF Channel Assignment**, come mostrato nell'immagine.



Configurazione dell'access point per la scansione di un canale tramite CLI

Passaggio 1. Abilitare la funzione di sniffing del canale sull'access point. Eseguire questo comando:

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

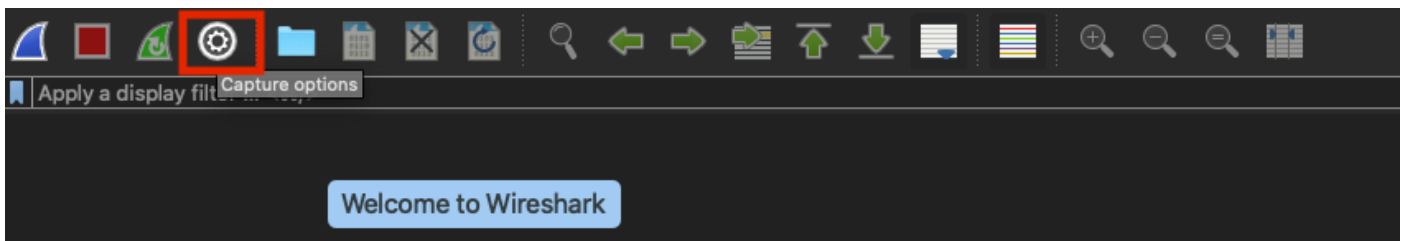
Esempio:

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

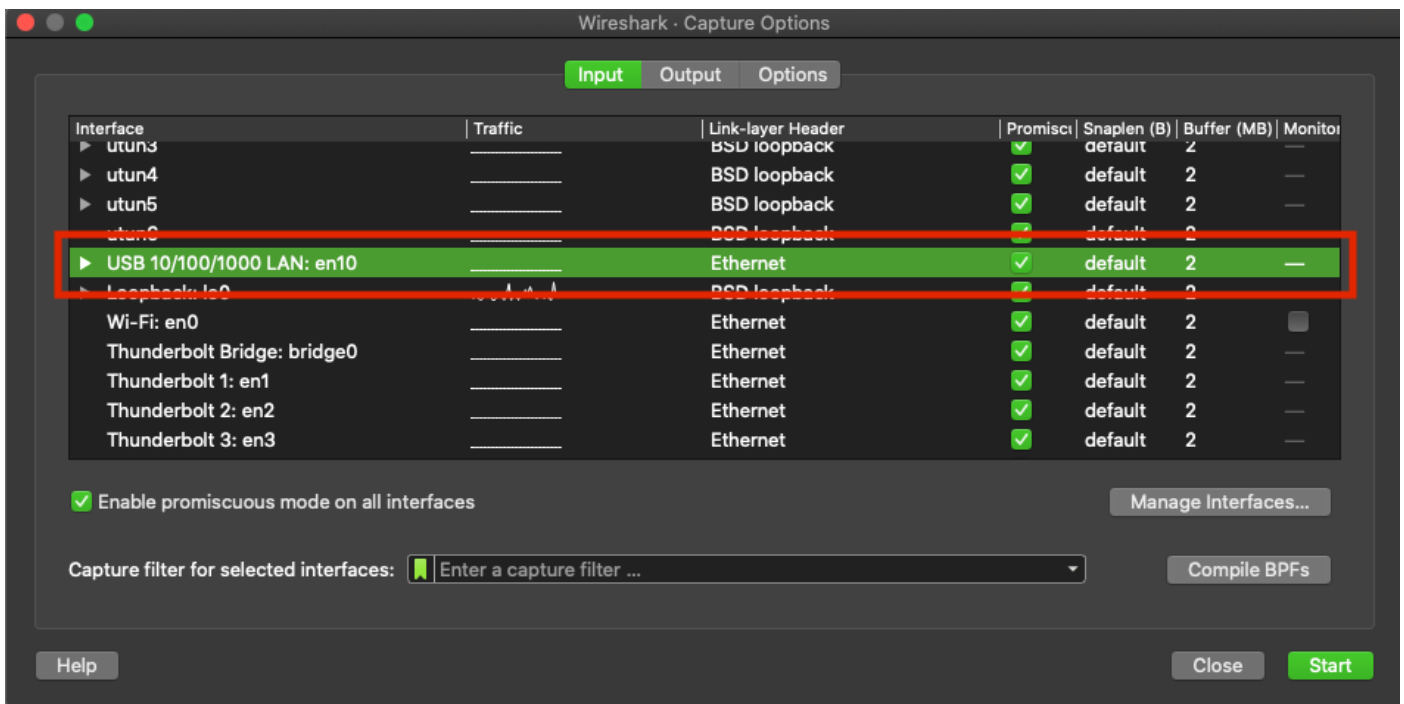
Configurazione di Wireshark per la raccolta dell'acquisizione del pacchetto

Passaggio 1. Avviare Wireshark.

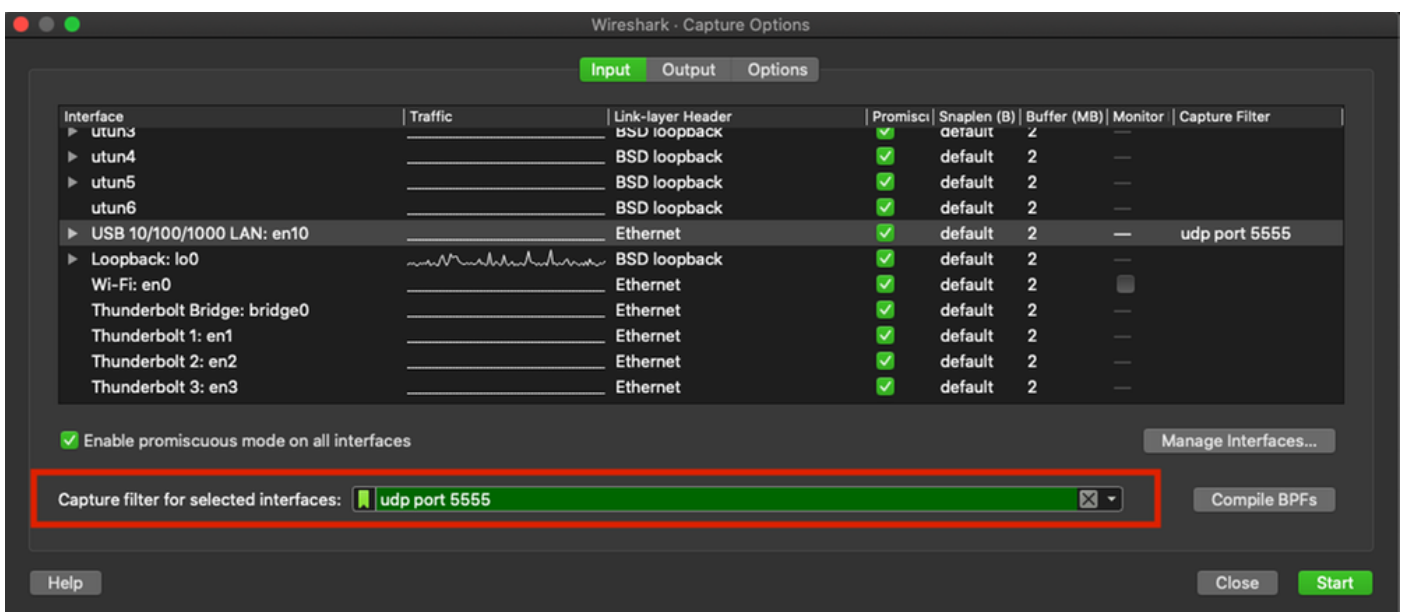
Passaggio 2. Selezionare l'icona del menu **Capture options** da Wireshark, come mostrato nell'immagine.



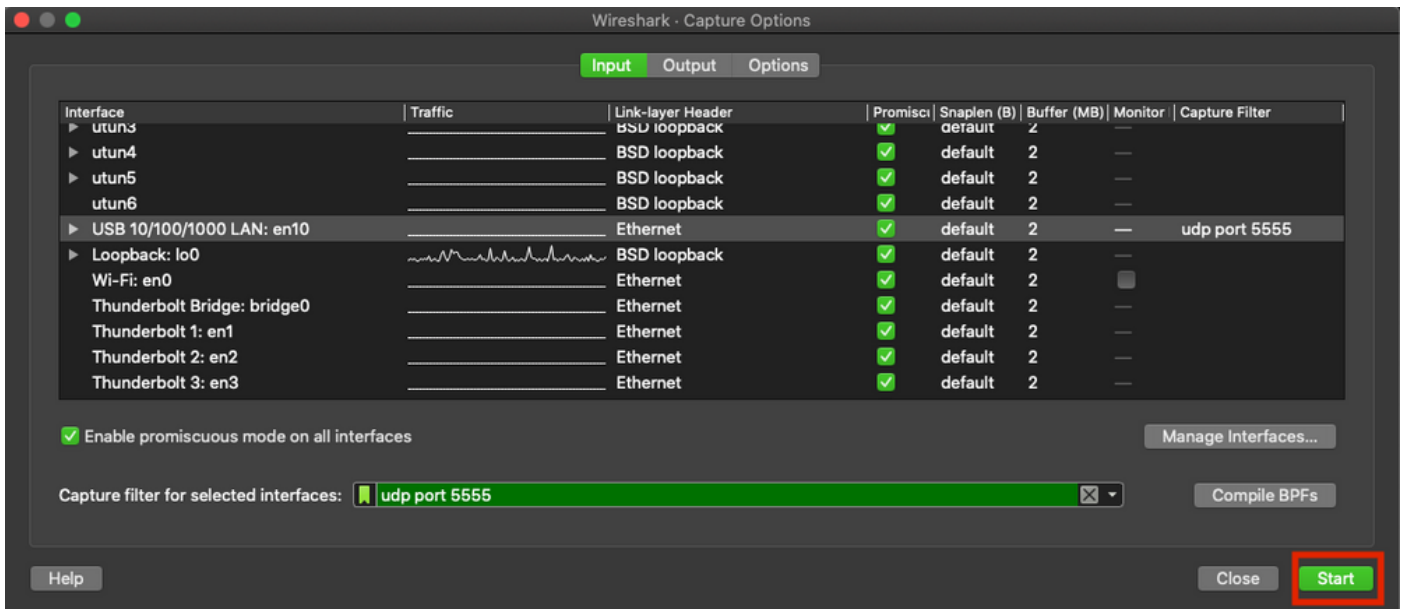
Passaggio 3. Viene visualizzata una finestra popup. Selezionate dall'elenco Interfaccia cablata (Wired Interface) come origine della cattura, come mostrato nell'immagine.



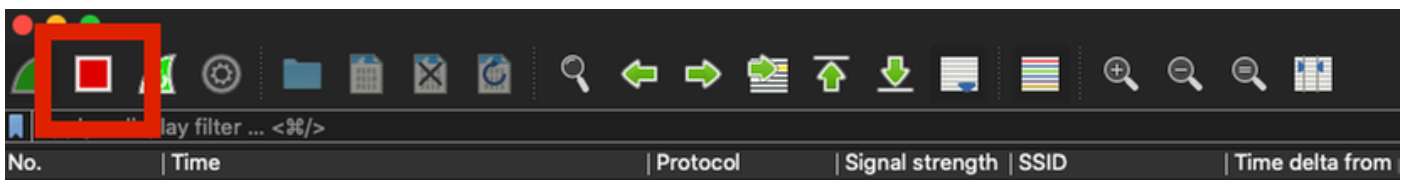
Passaggio 4. Sotto il filtro di acquisizione per le interfacce selezionate: nella casella campo digitare **udp port 5555**, come illustrato nell'immagine.



Passaggio 5. Fare clic su **Start**, come mostrato nell'immagine.

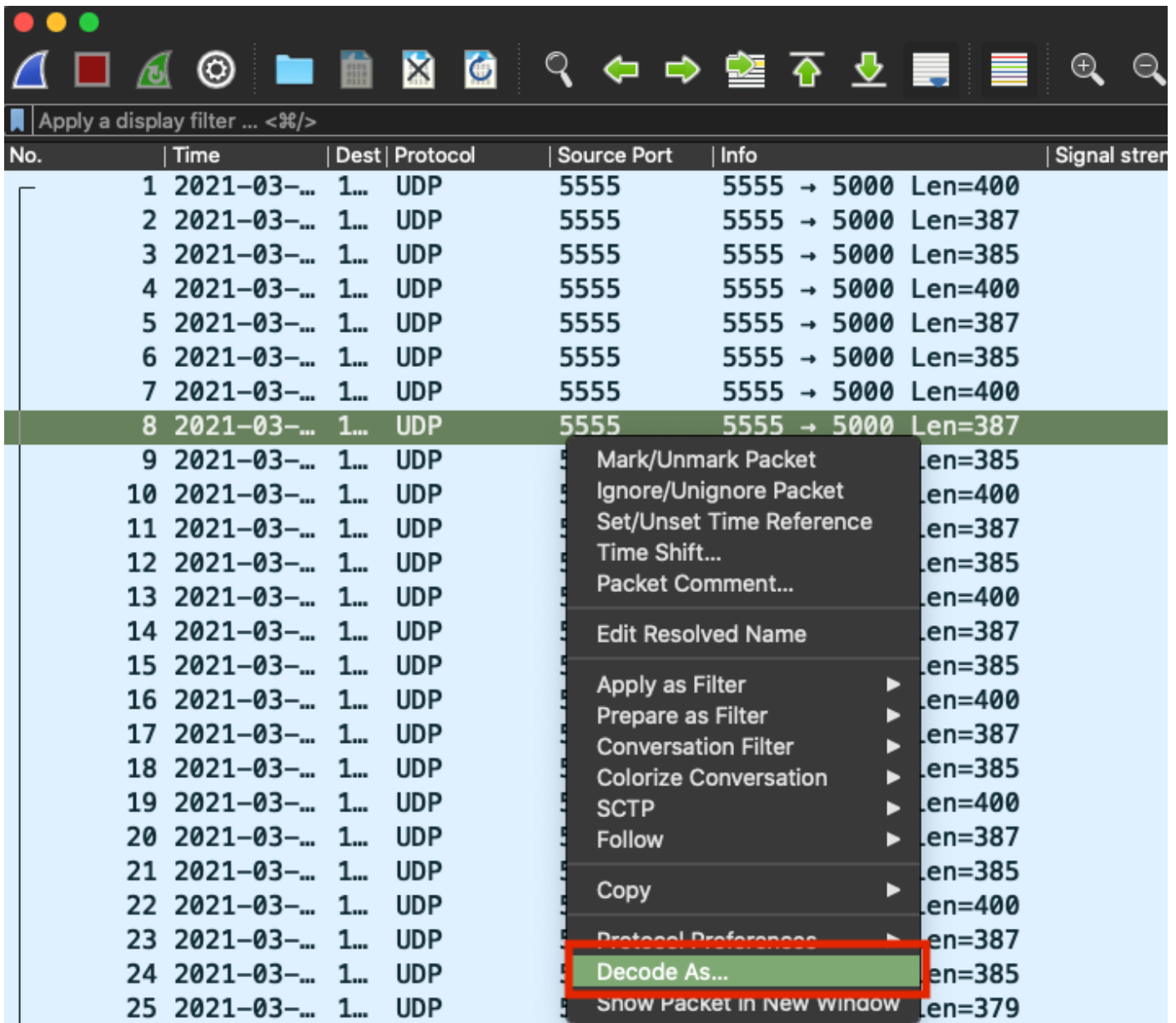


Passaggio 6. Attendere che Wireshark raccolga le informazioni richieste e selezionare il pulsante **Stop** da Wireshark, come mostrato nell'immagine.

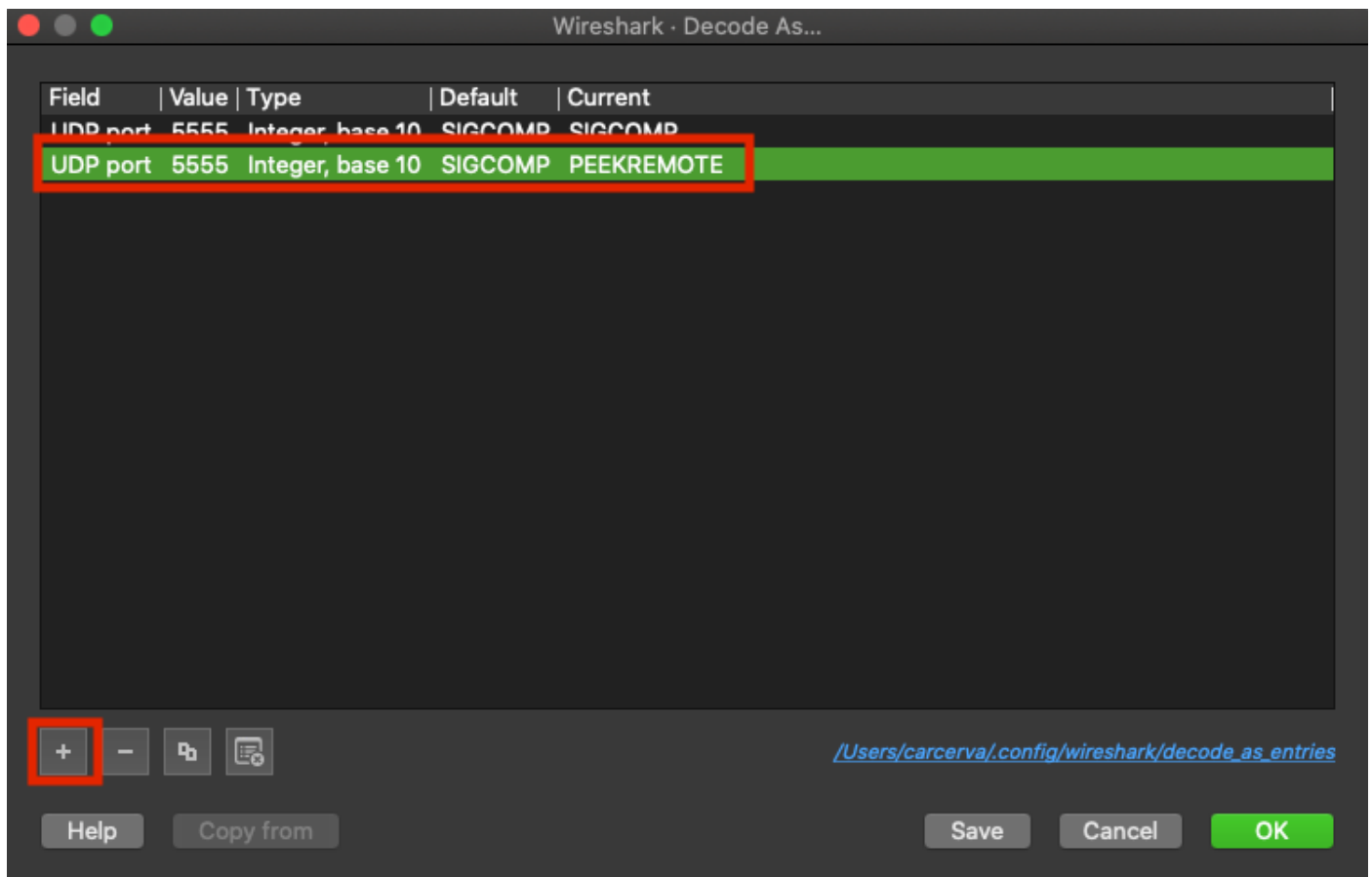


Suggerimento: Se la WLAN utilizza la crittografia, ad esempio la chiave già condivisa (PSK), verificare che l'acquisizione intercetti l'handshake a quattro vie tra l'AP e il client desiderato. Questa operazione può essere eseguita se il PCAP OTA viene avviato prima che il dispositivo sia associato alla WLAN o se il client viene deautenticato e riautenticato durante l'acquisizione.

Passaggio 7. Wireshark non decodifica i pacchetti automaticamente. Per decodificare i pacchetti, selezionare una linea dall'acquisizione, fare clic con il pulsante destro del mouse per visualizzare le opzioni, quindi selezionare **Decodifica con nome...**, come mostrato nell'immagine.



Passaggio 8. Viene visualizzata una finestra popup. Selezionare il pulsante Aggiungi e aggiungere una nuova voce. Selezionare le opzioni seguenti: Porta UDP da Field, 5555 da Value, SIGCOMP da Default e PEEKREMOTE da Current, come mostrato nell'immagine.



Passaggio 9. Fare clic su **OK**. I pacchetti vengono decodificati e pronti per iniziare l'analisi.

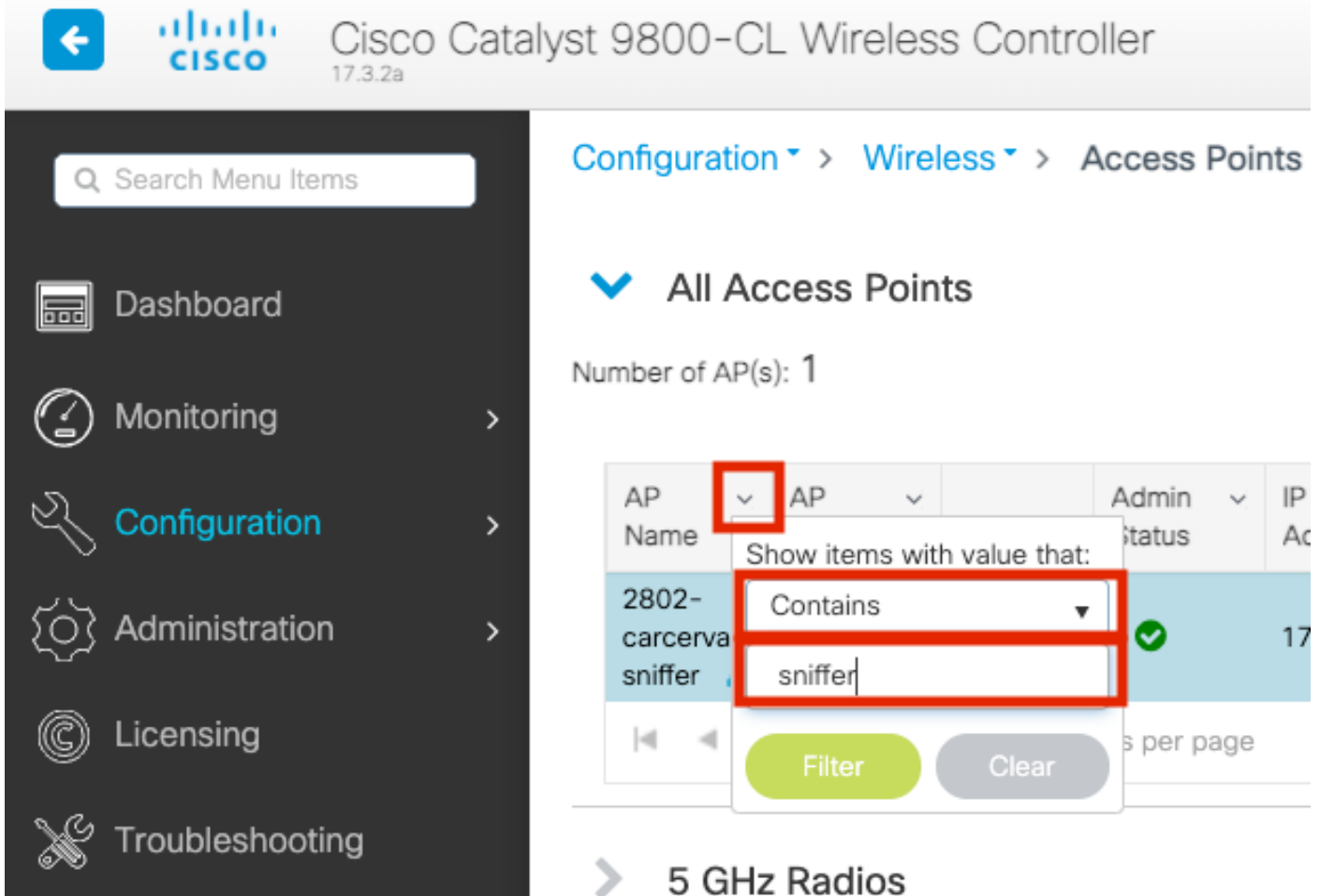
Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

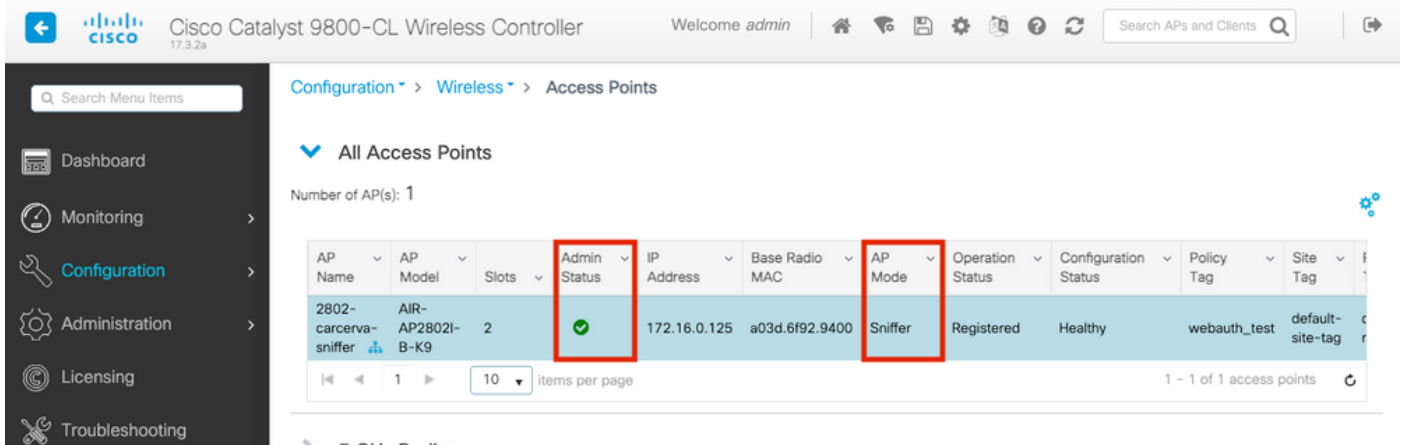
Per verificare che l'access point sia in modalità sniffer dall'interfaccia utente di 9800:

Passaggio 1. Sull'interfaccia utente del WLC del 9800, selezionare **Configuration > Wireless > Access Point > All Access Point**.

Passaggio 2. Cercare nell'access point. Fare clic sulla freccia verso il basso per visualizzare lo strumento di ricerca, selezionare **Contiene** dall'elenco a discesa e digitare il nome dell'access point, come mostrato nell'immagine.



Passaggio 3. Verificare che **Admin Status** (Stato amministratore) sia selezionato con il **segno di spunta in verde** e che **AP Mode (Modalità AP)** sia **Sniffer**, come mostrato nell'immagine.



Per verificare che l'access point sia in modalità sniffer dalla CLI 9800. Eseguire i seguenti comandi:

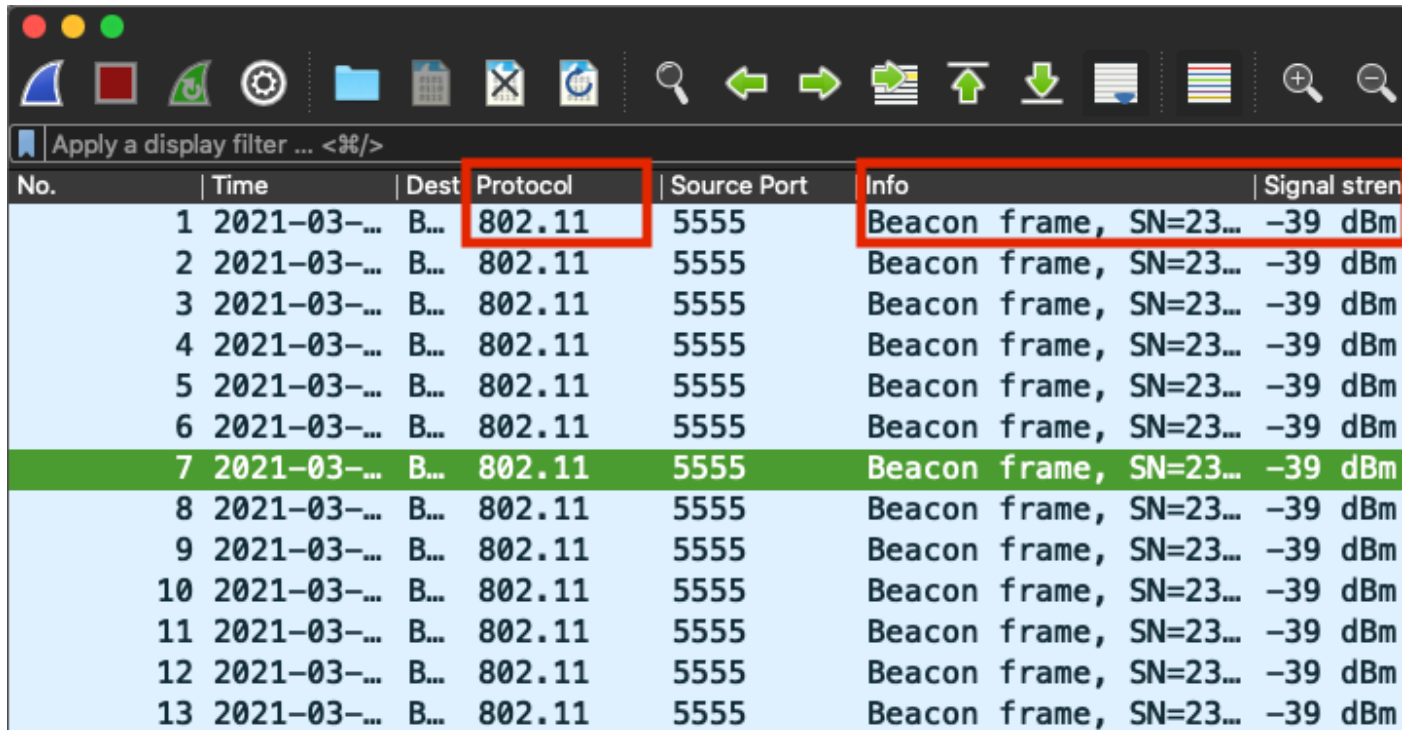
```
carcerva-9k-upg#show ap name 2802-carcerva-sniffer config general | i Administrative
Administrative State : Enabled
```

```
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

Per confermare, i pacchetti vengono decodificati su Wireshark. Il protocollo passa da UDP a 802.11 e vengono visualizzati **frame beacon**, come mostrato nell'immagine.



| 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 |

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Problema: Wireshark non riceve dati dall'access point.

Soluzione: Il server Wireshark deve essere raggiungibile tramite l'interfaccia di gestione wireless (WMI). Verificare la raggiungibilità tra il server Wireshark e WMI dal WLC.

Informazioni correlate

- [Guida alla configurazione del software Cisco Catalyst serie 9800 Wireless Controller, Cisco IOS XE Amsterdam 17.3.x - Capitolo: Modalità Sniffer](#)
- [Nozioni fondamentali sullo sniffing wireless 802.11](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)