

# Catalyst 9800ワイヤレスコントローラのスニファモードでのアクセスポイントの設定

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[GUIによるスニファモードでのAPの設定](#)

[CLIによるスニファモードでのAPの設定](#)

[GUIを使用してチャンネルをスキャンするようにAPを設定する](#)

[CLIを使用してチャンネルをスキャンするためのAPの設定](#)

[パケットキャプチャを収集するためのWiresharkの設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

このドキュメントでは、Graphic User Interface(GUI)またはCommand Line Interface ( CLI ; コマンドラインインターフェイス ) を使用して、Catalyst 9800シリーズワイヤレスコントローラ (9800 WLC)のスニファモードでアクセスポイント(AP)を設定する方法と、Air(PCAP)を収集する方法について説明しますワイヤレスビヘイビアのトラブルシューティングと分析を行うために、スニファAPを使用します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- 9800 WLCの設定
- 802.11規格の基礎知識

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- AP 2802
- 9800 WLC Cisco IOS®-XEバージョン17.3.2a

- Wireshark 3.X

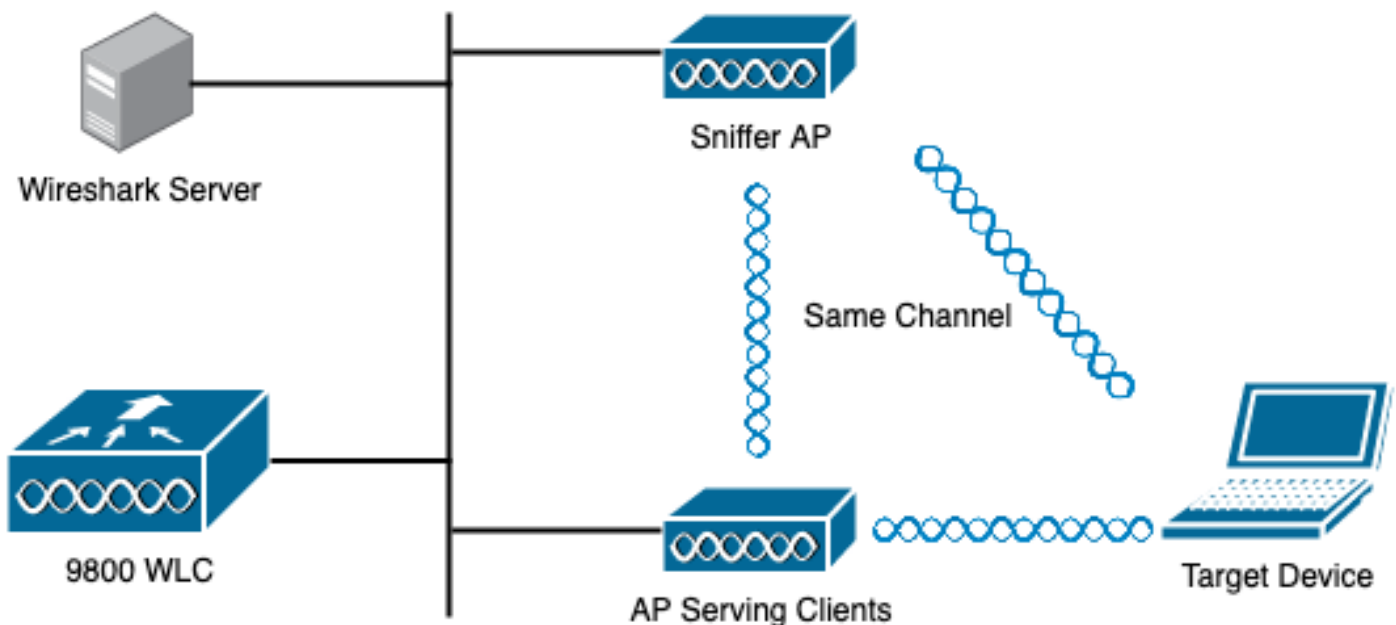
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

考慮すべき事柄:

- スニファAPをターゲットデバイスと、このデバイスが接続されているAPの近くにすることを推奨します。
- 使用する802.11チャンネルと幅、クライアントデバイスとAPを確認します。

## ネットワーク図



## 設定

### GUIによるスニファモードでのAPの設定

ステップ1: 図に示すように、9800 WLC GUIで、**[Configuration] > [Wireless] > [Access Points] > [All Access Points]**に移動します。



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

ステップ2 : スニファモードで使用するAPを選択します。図に示すように[General]タブで、APの名前を更新します。

Cisco Catalyst 9800-CL Wireless Controller 17.3.2a

Welcome admin

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Blk 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

ステップ3：図に示すように、[Admin Status] が[Enabled] であることを確認し、[AP Mode]を [Sniffer]に変更します。

Cisco Catalyst 9800-CL Wireless Controller 17.3.2a

Welcome admin

Configuration > Wireless > Access Points

All Access Points

Number of AP(s): 1

AP Name	AP Model	Slots	Admin Status	IP Address	Blk M
2802-carcerva	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**

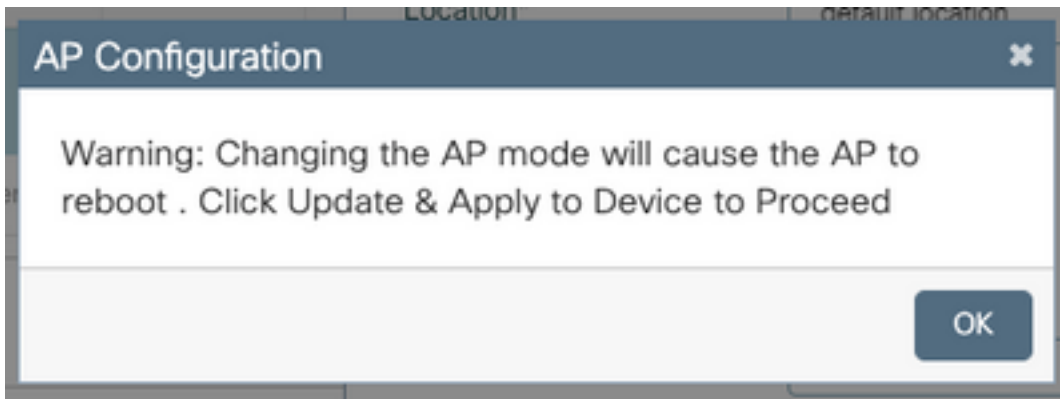
AP Mode Sniffer

Operation Status Registered

次の注記がポップアップに表示されます。

"警告：APモードを変更すると、APがリブートします。[Update & Apply to Device to Proceed]をクリックします。

図に示すように[OK]を選択します。



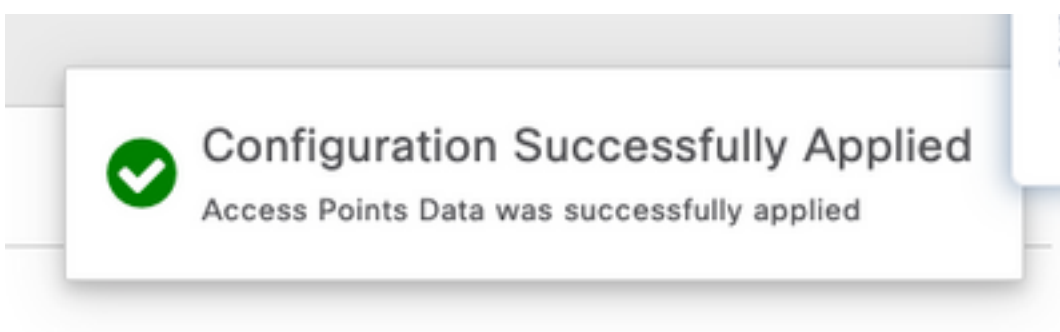
ステップ4 : 図に示すように、[Update & Apply to Device]をクリックします。

The screenshot shows the "Edit AP" configuration page. At the top, there are tabs for "General", "Interfaces", "High Availability", "Inventory", "ICap", "Advanced", and "Support Bundle". The "General" tab is selected. The page is divided into two main sections: "General" and "Version".  

General		Version	
AP Name*	2802-carcerva-sniffer	Primary Software Version	17.3.2.32
Location*	default location	Predownloaded Status	N/A
Base Radio MAC	a03d.6f92.9400	Predownloaded Version	N/A
Ethernet MAC	00a2.eedf.6114	Next Retry Time	N/A
Admin Status	ENABLED <input checked="" type="checkbox"/>	Boot Version	1.1.2.4
AP Mode	Sniffer ▼	IOS Version	17.3.2.32
Operation Status	Registered	Mini IOS Version	0.0.0.0
Fabric Status	Disabled	IP Config	
LED State	ENABLED <input checked="" type="checkbox"/>	CAPWAP Preferred Mode	IPv4
LED Brightness Level	8 ▼	DHCP IPv4 Address	172.16.0.125
		Static IP (IPv4/IPv6)	<input type="checkbox"/>

At the bottom of the page, there is a "Cancel" button on the left and an "Update & Apply to Device" button on the right, which is highlighted with a red rectangle. A "Guided Assistance" sidebar is visible on the right side of the page.

図に示すように、変更とAPのバウンスを確認するポップアップが表示されます。



## CLIによるスニファモードでのAPの設定

ステップ1: スニファモードとして使用するAPを特定し、AP名を取得します。

ステップ2: AP名を変更します。

このコマンドは、AP名を変更します。ここで、<AP-name>はAPの現在の名前です。

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

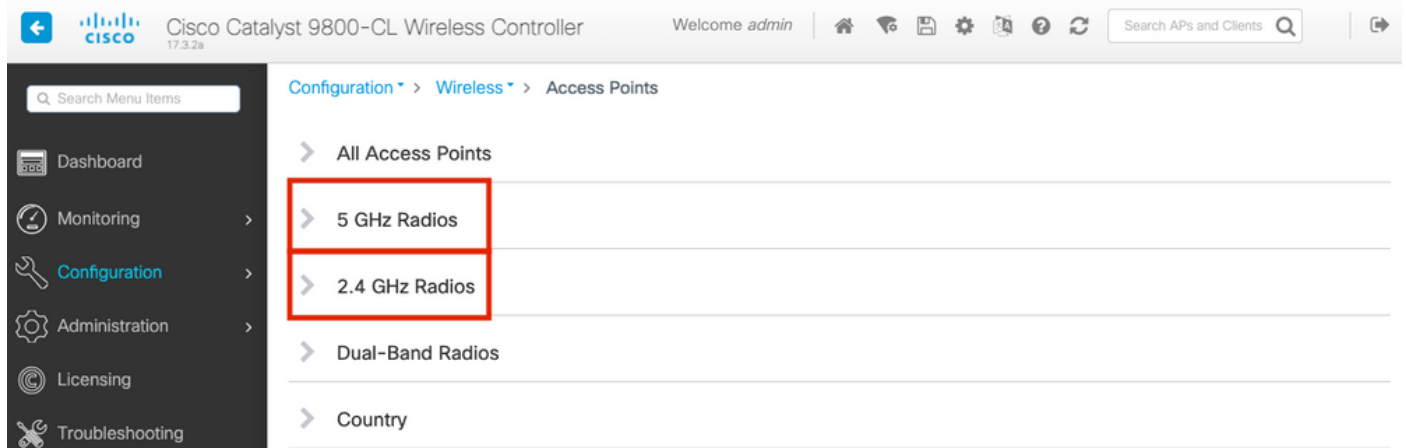
ステップ3: スニファモードでAPを設定します。

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

## GUIを使用してチャンネルをスキャンするようにAPを設定する

ステップ1: 9800 WLC GUIで、[Configuration] > [Wireless] > [Access Points]に移動します。

ステップ2: [アクセスポイント]ページで、[5 GHz Radios]または[2.4 GHz Radios]メニューリストを表示します。これは、図に示すように、スキャンするチャンネルによって異なります。



ステップ2: APを検索します。矢印をクリックして検索ツールを表示し、ドロップダウンリストから[Contains]を選択し、図に示すようにAP名を入力します。

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

ステップ3:APを選択し、図に示すように、[Configure] > [Sniffer Channel Assignment]の下の [Enable Sniffer]チェックボックスをオンにします。

Cisco Catalyst 9800-CL Wireless Controller 17.3.2a

Welcome admin

Configuration > Wireless > Edit Radios 5 GHz Band

Configure Detail

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

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

Cancel

ステップ4：図に示すように、[Sniff Channel]ドロップダウンリストから[Channel]を選択し、[Sniffer IP address (Server IP address with Wireshark)]を入力します。

The screenshot shows the configuration page for 'Edit Radios 5 GHz Band' on a Cisco Catalyst 9800-CL Wireless Controller. The 'Configure' tab is active. The 'Sniffer Channel Assignment' section is highlighted, showing the following settings:

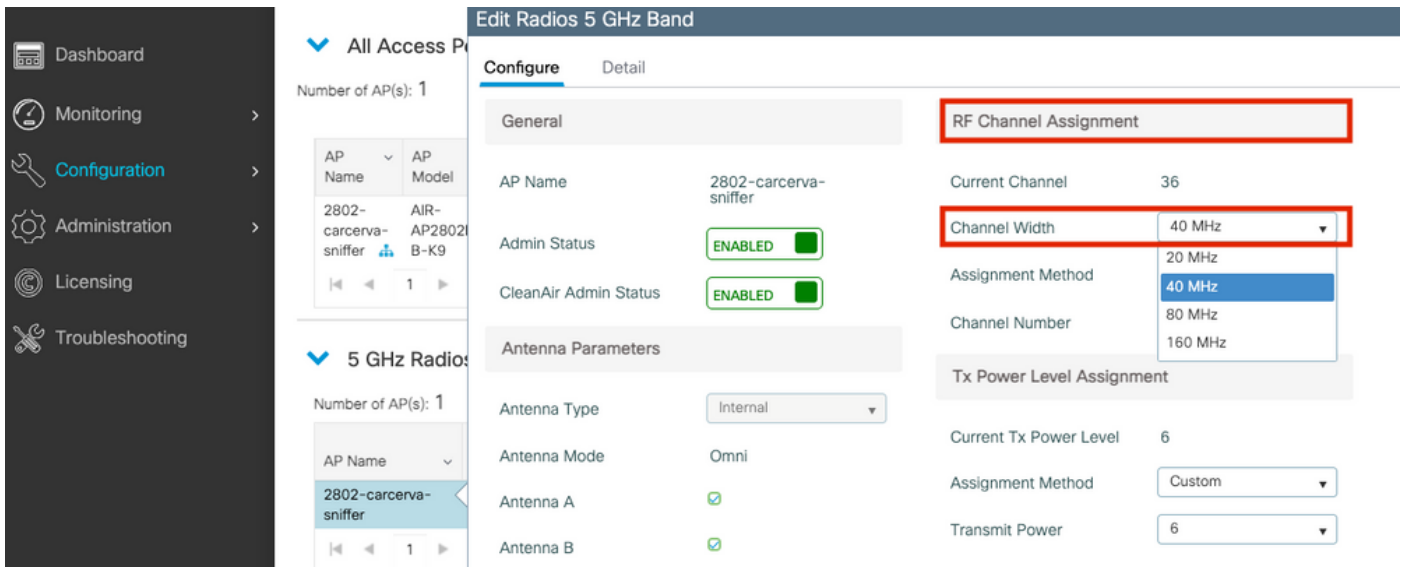
Field	Value
Enable Sniffing	<input checked="" type="checkbox"/>
Sniff Channel	36
Sniffer IP*	172.16.0.190
Sniffer IP Status	Valid

At the bottom of the configuration area, there is a 'Cancel' button.

ステップ5：接続先デバイスとAPで使用するチャネル幅を選択します。

図に示すように、[Configure] > [RF Channel Assignment]に移動してこれを設定します。





## CLIを使用してチャンネルをスキャンするためのAPの設定

ステップ1: APでチャンネルスニフを有効にします。次のコマンドを実行します。

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

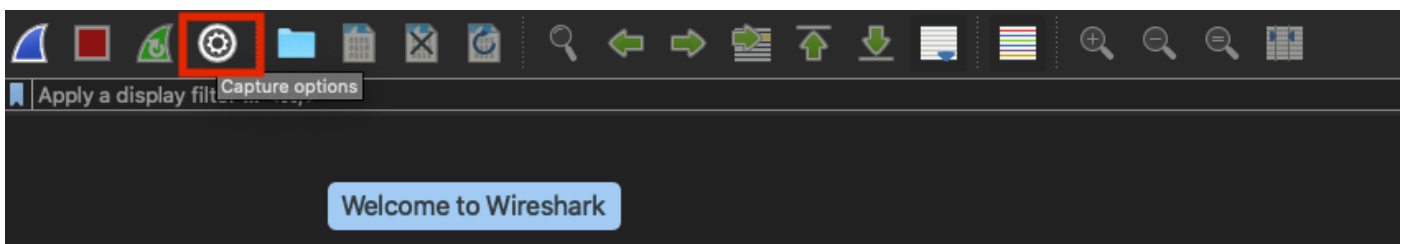
例 :

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

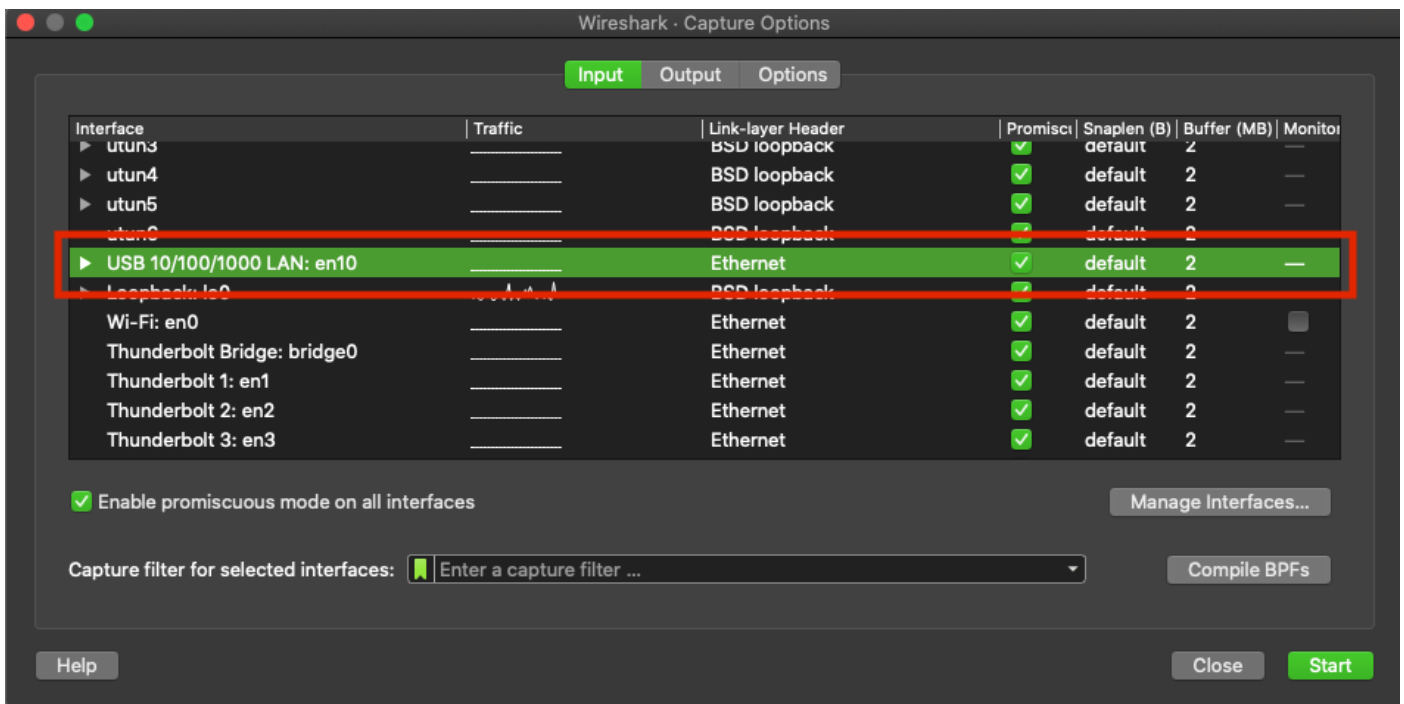
## パケットキャプチャを収集するためのWiresharkの設定

ステップ1: Wiresharkを起動します。

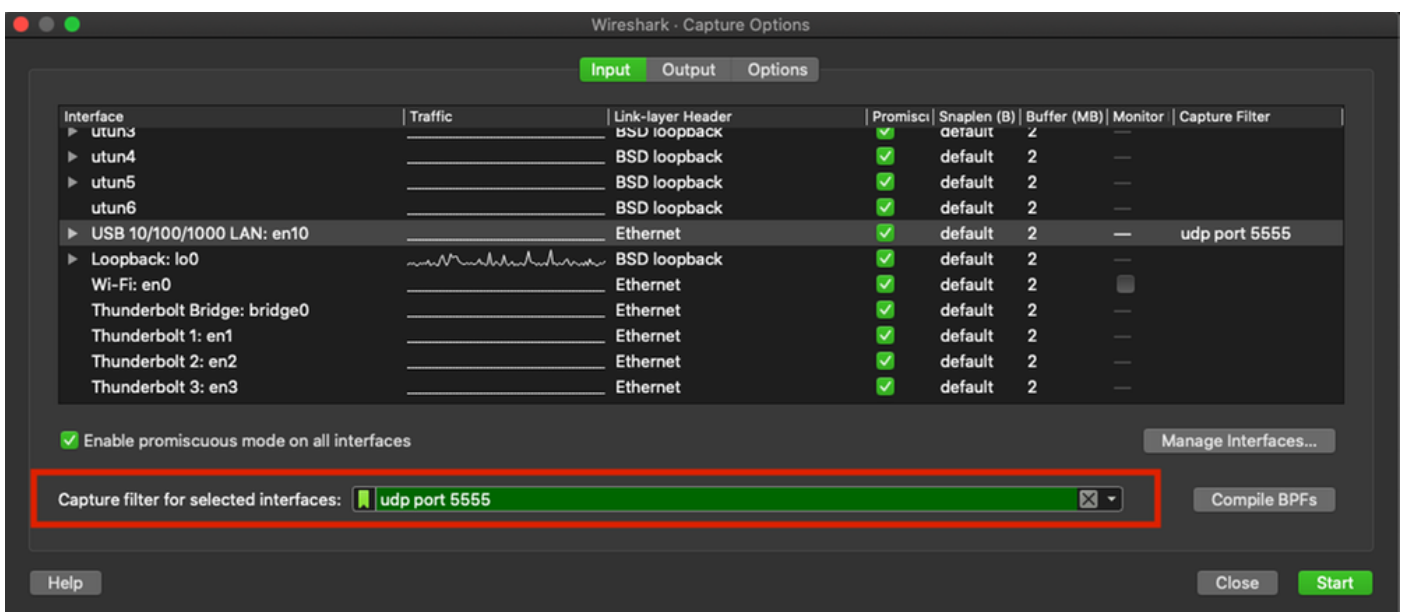
ステップ2 : 図に示すように、Wiresharkから[Capture options]メニューアイコンを選択します。



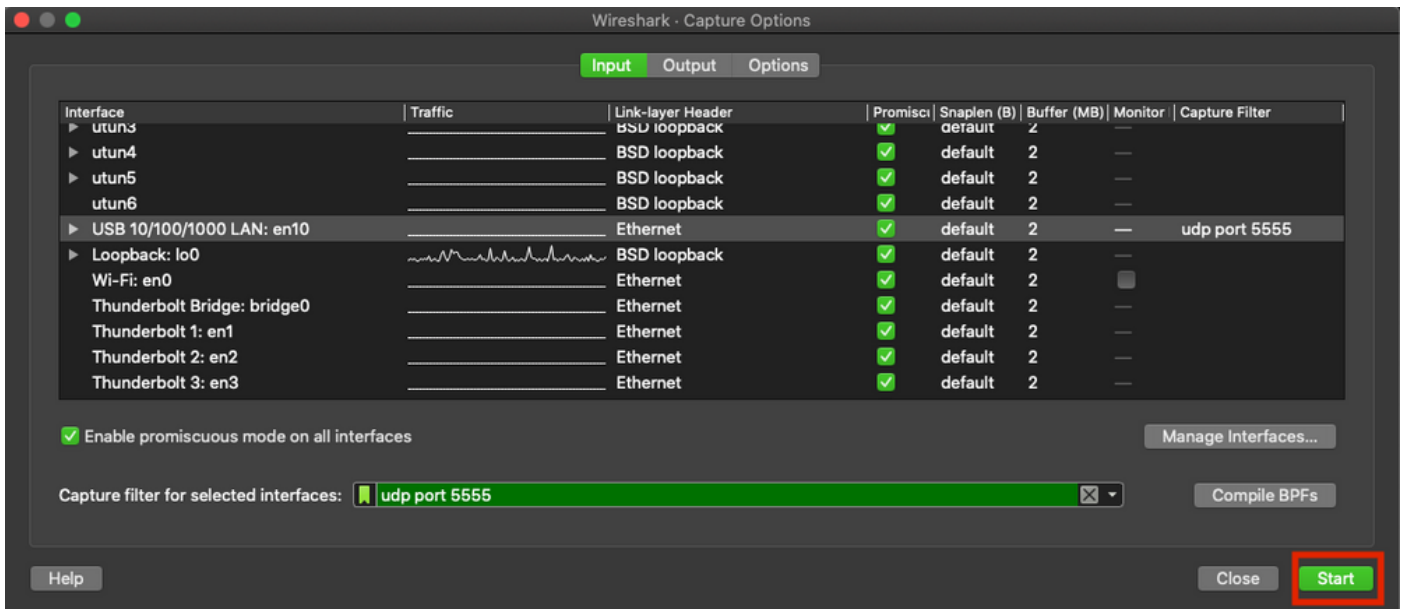
ステップ3 : ポップアップウィンドウが表示されます。図に示すように、キャプチャのソースとして[Wired Interface]をリストから選択します。



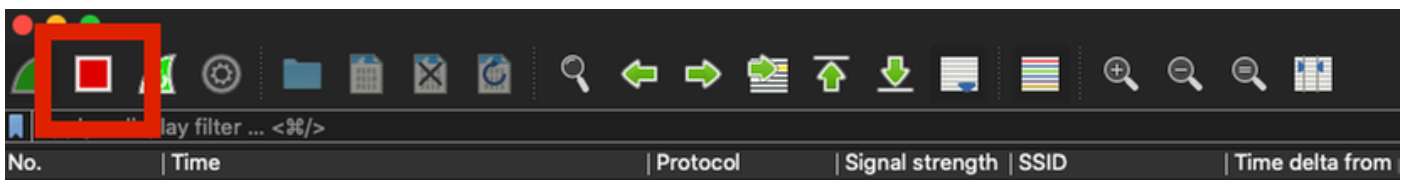
ステップ4:[Capture filter for selected interfaces: 図]に示すように、フィールドボックスにudpポート555と入力します。



ステップ5 : 図に示すように、[Start]をクリックします。

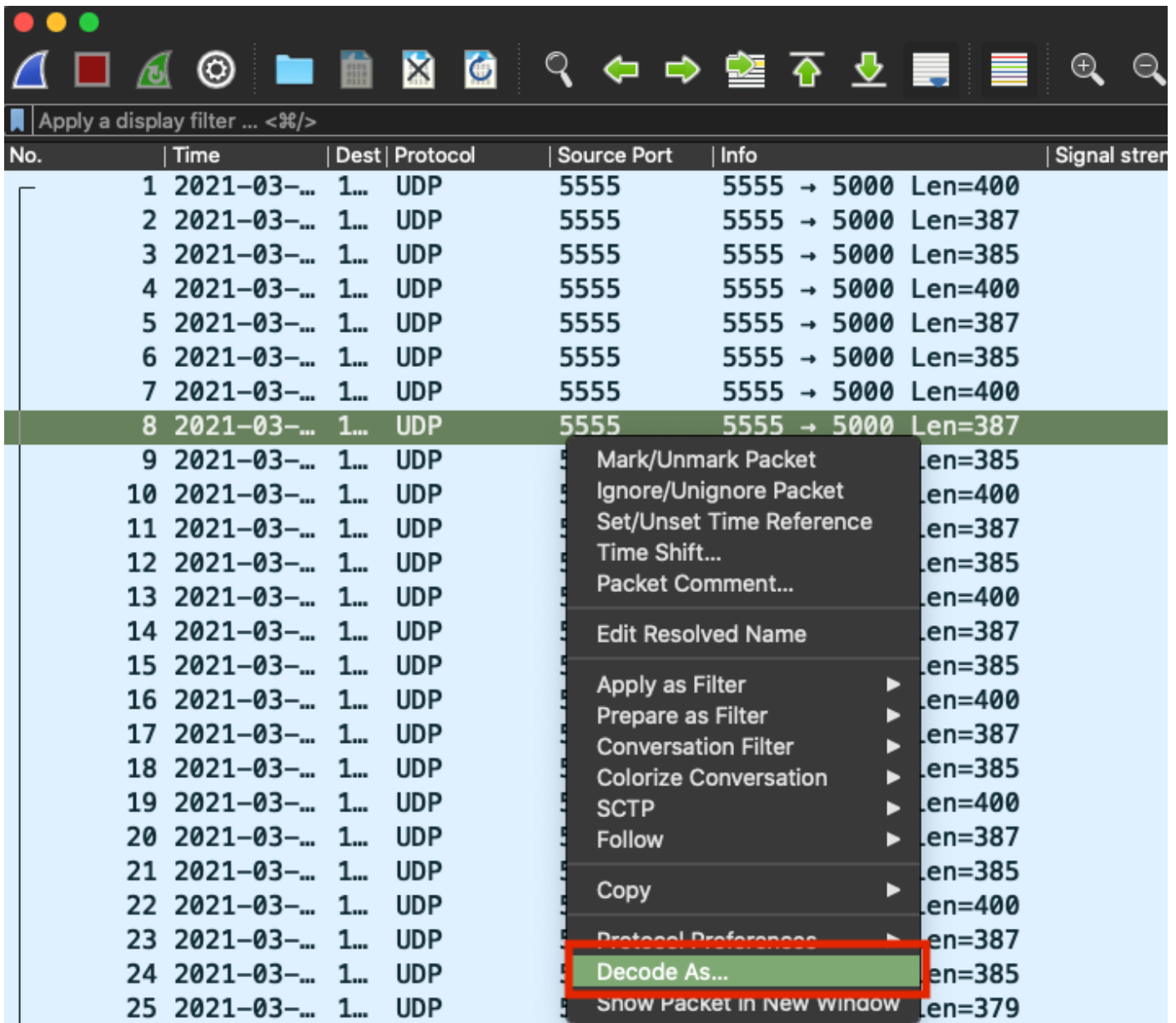


ステップ6 : 図に示すように、Wiresharkが必要な情報を収集するのを待ち、Wiresharkから [Stop]ボタンを選択します。

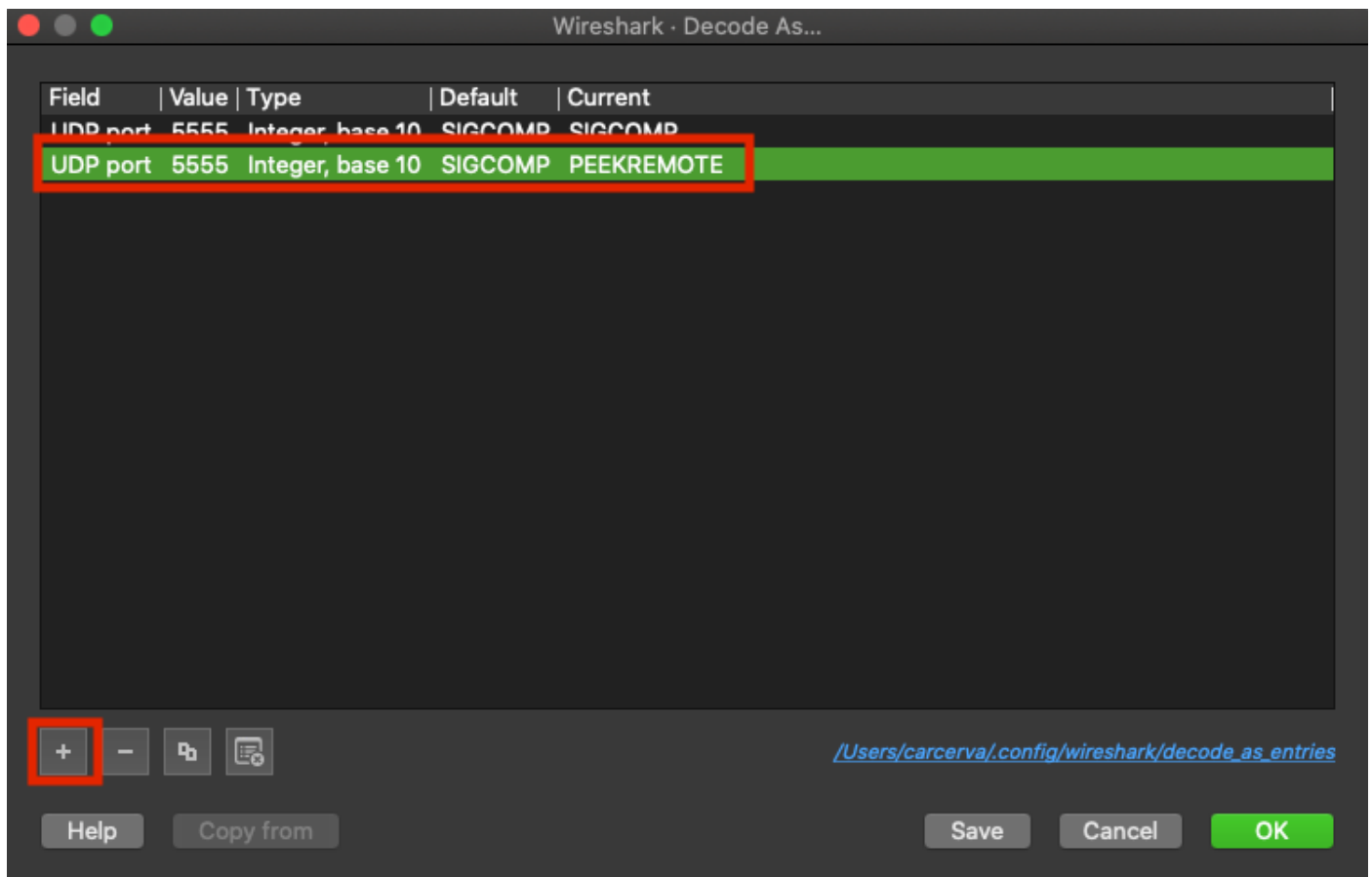


ヒント : WLANで事前共有キー(PSK)などの暗号化が使用されている場合は、APと目的のクライアント間の4ウェイハンドシェイクがキャプチャされることを確認します。これは、デバイスがWLANに関連付けられる前にOTA PCAPが起動する場合、またはキャプチャの実行中にクライアントの認証と再認証が解除された場合に実行できます。

ステップ7:Wiresharkはパケットを自動的にデコードしません。パケットをデコードするには、キャプチャから行を選択し、右クリックしてオプションを表示し、図に示すようにDecode As...を選択します。



ステップ8：ポップアップウィンドウが表示されます。[add]ボタンを選択して新しいエントリを追加し、次のオプションを選択します。図に示すように、フィールドからのUDPポート、値から5555、デフォルトからSIGCOMP、および現在からPEEKREMOTE。



手順 9 : [OK] をクリックします。パケットがデコードされ、分析を開始する準備が整います。

## 確認

ここでは、設定が正常に機能しているかどうかを確認します。

9800 GUIからAPがスニファモードであることを確認するには、次の手順を実行します。

ステップ1:9800 WLC GUIで、[Configuration] > [Wireless] > [Access Points] > [All Access Points]に移動します。

ステップ2:APを検索します。矢印をクリックして検索ツールを表示し、ドロップダウンリストから[含む]を選択し、図に示すようにAP名を入力します。



Search Menu Items



Dashboard



Monitoring



Configuration



Administration



Licensing



Troubleshooting

Configuration > Wireless > Access Points

## All Access Points

Number of AP(s): 1

AP Name	AP	Admin Status	IP
2802-carcerva-sniffer	Contains sniffer	<input checked="" type="checkbox"/>	17

5 GHz Radios

ステップ3：図に示すように、[Admin Status]に緑色のチェックマークが付いて、[AP Mode]に [Sniffer] が表示されていることを確認します。



Search Menu Items

Dashboard

Monitoring

Configuration

Administration

Licensing

Troubleshooting

Configuration > Wireless > Access Points

## All Access Points

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	<input checked="" type="checkbox"/>	172.16.0.125	a03d.6f92.9400	Sniffer	Registered	Healthy	webauth_test	default-site-tag

APが9800 CLIからスニファモードであることを確認するために。次のコマンドを実行します。

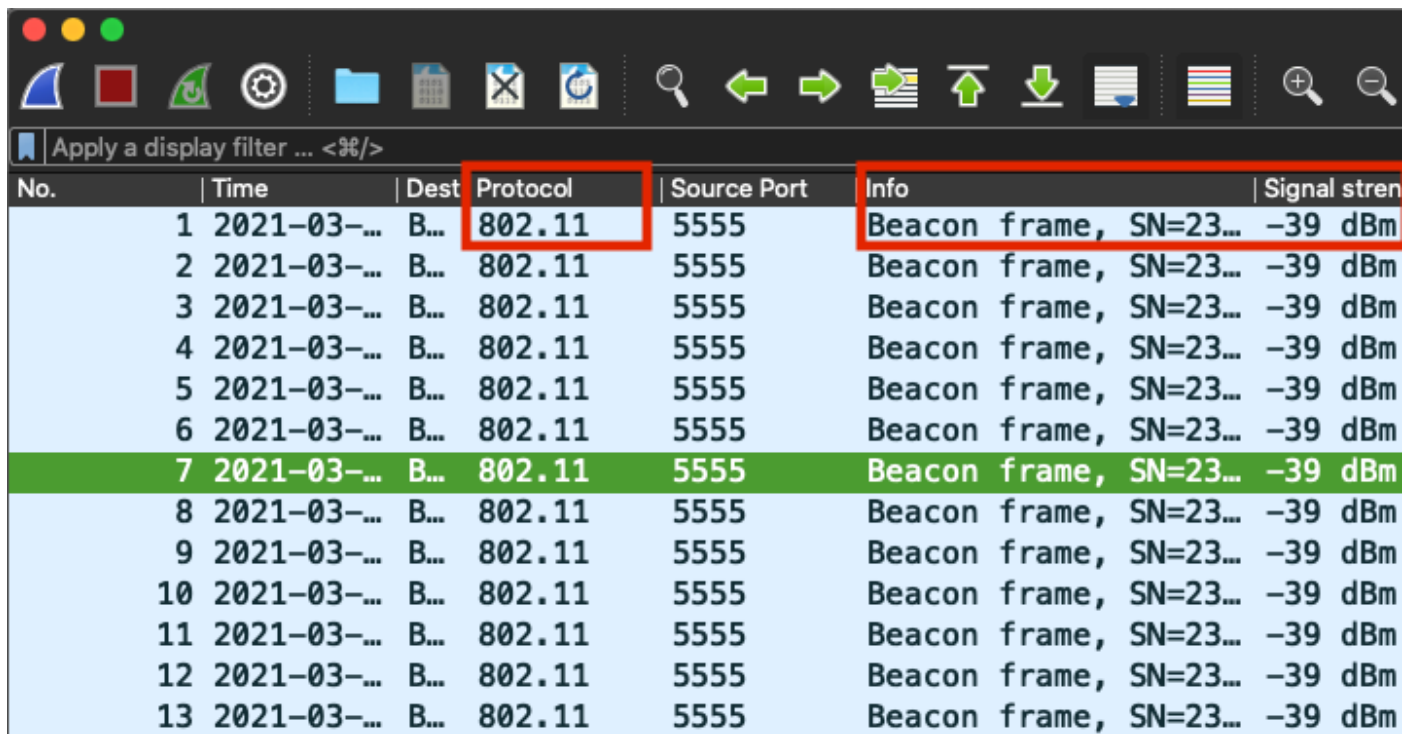
```
carcerva-9k-upg#show ap name 2802-carcerva-sniffer config general | i Administrative  
Administrative State : Enabled
```

```
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

パケットがWiresharkでデコードされたことを確認します。図に示すように、プロトコルがUDPから802.11に変更され、ビーコンフレームが表示されます。



No.	Time	Dest	Protocol	Source Port	Info	Signal strength
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

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

問題 : WiresharkはAPからデータを受信しません。

ソリューション : Wiresharkサーバは、ワイヤレス管理インターフェイス(WMI)によって到達可能である必要があります。WiresharkサーバとWLCからのWMI間の到達可能性を確認してください。

## 関連情報

- [Cisco Catalyst 9800シリーズワイヤレスコントローラソフトウェアコンフィギュレーションガイド、Cisco IOS XE Amsterdam 17.3.x - 章 : スニファモード](#)
- [802.11 ワイヤレス スニフィングの基礎](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)