Catalyst 9800ワイヤレスコントローラでのAPパケットキャプチャの設定

内容

概要

このドキュメントでは、アクセスポイント(AP)のパケットキャプチャ機能の使用方法について説明します。

背景説明

この機能はCisco IOS AP（AP 3702など）でのみ使用できるため、Cisco IOS XEバージョン17.3以降では廃止されています。

このソリューションは、DNACを使用したIntelligent Captureに取って代わり、またはAPをスニファモードに設定する代替手段として使用されます。

APパケットキャプチャ機能を使用すると、少ない労力で空中のパケットキャプチャを実行できます。この機能を有効にすると、APとの間で送受信される特定の無線MACアドレスに対して無線で送受信されるすべての指定された無線パケットとフレームのコピーがFTP(File Transfer Protocol)サーバに転送されます。FTPサーバでは、.pcapファイルとしてダウンロードし、任意のパケット分析ツールで開くことができます。

パケットキャプチャが開始されると、クライアントが関連付けられているAPはFTPサーバ上に新しい.pcapファイルを作成します（FTPログインに指定されたユーザ名に書き込み権限があることを確認します）。クライアントがローミングすると、新しいAPはFTPサーバに新しい.pcapファイルを作成します。クライアントがService Set Identifier(SSID)間を移動すると、APはパケットキャプチャを有効に保つため、クライアントが新しいSSIDに関連付けられたときにすべての管理フレームを確認できます。

オープンSSID（セキュリティなし）でキャプチャを行うと、データパケットの内容を表示できますが、クライアントがセキュアSSID（パスワードで保護されたSSIDまたは802.1xセキュリティ）に関連付けられている場合、データパケットのデータ部分は暗号化され、クリアテキストでは表示されません。

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。

- ワイヤレスコントローラへのコマンドラインインターフェイス(CLI)またはグラフィックユーザインターフェイス(GUI)アクセス。
- FTP サーバ
- .pcapファイル

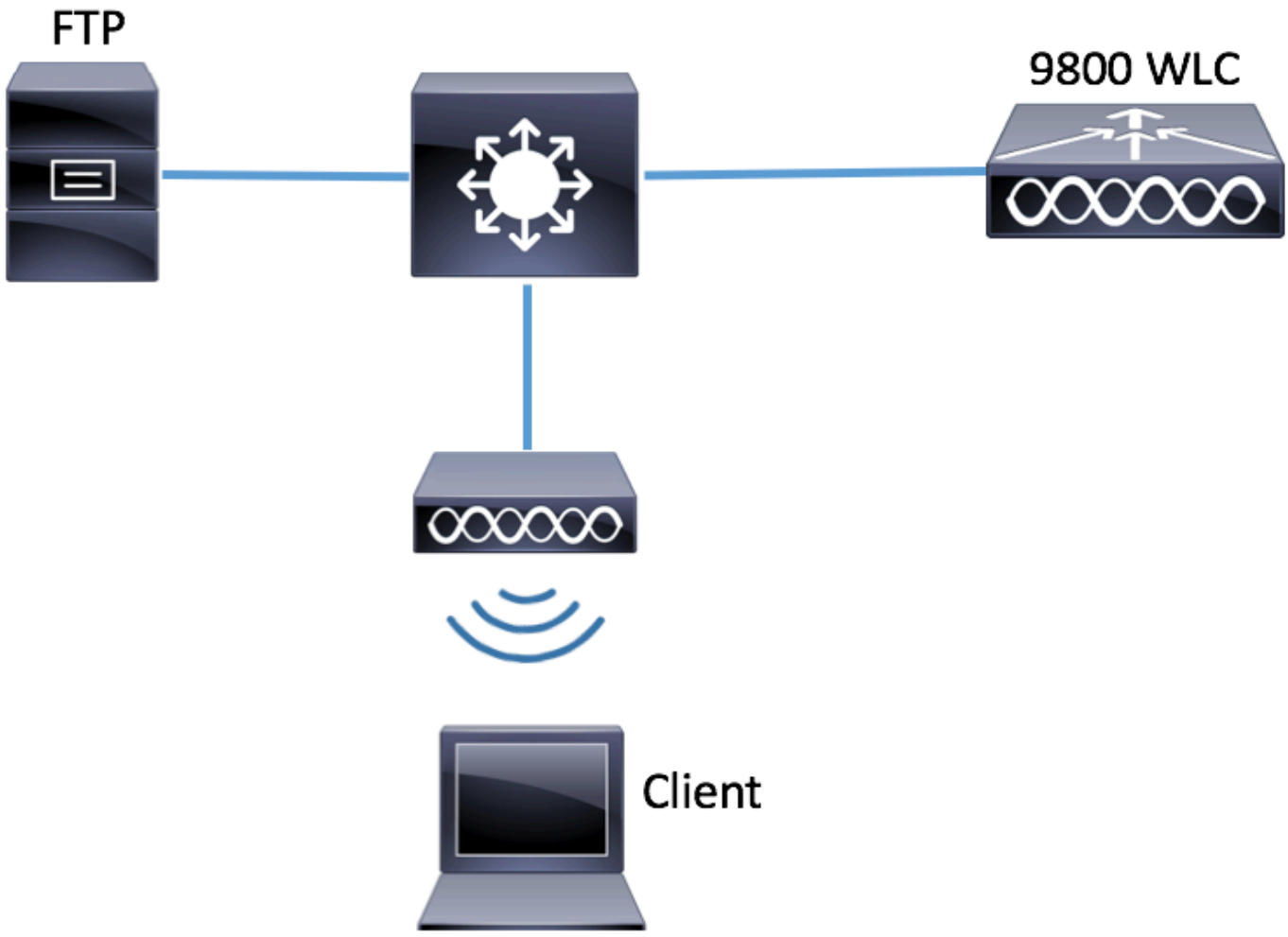
使用するコンポーネント

- 9800 WLC v16.10
- AP 3700
- FTP サーバ

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。

コンフィギュレーション

ネットワーク図



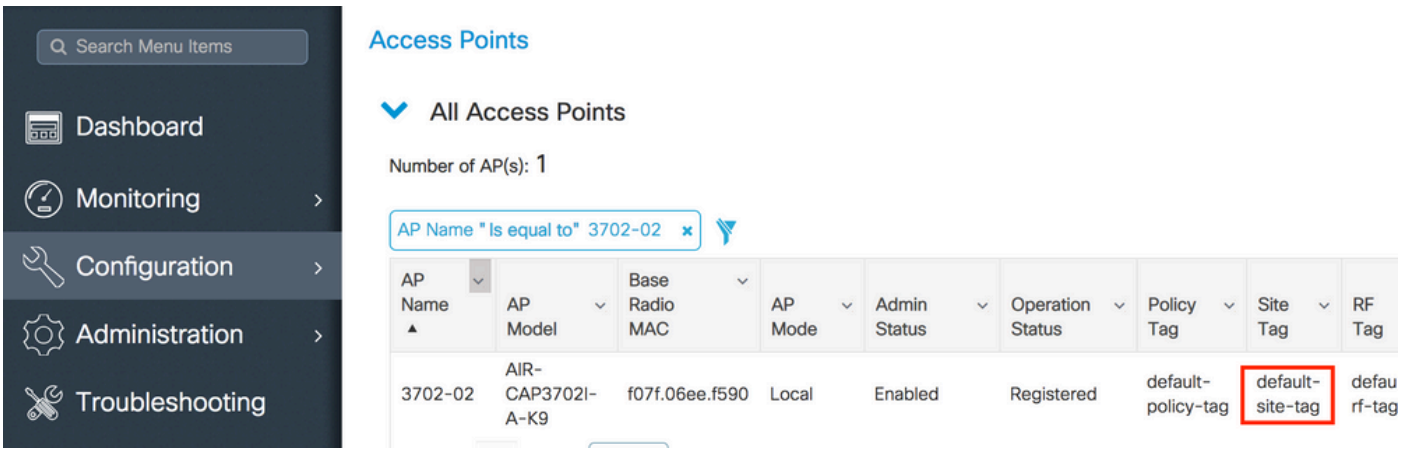
設定

設定を行う前に、ワイヤレスクライアントが接続できるAPを確認します。

ステップ 1：ワイヤレスクライアントが接続に使用できるAPに関連付けられた現在のサイトタグを確認します。

GUI：

[Configuration] > [Wireless] > [Access Points] に移動します。



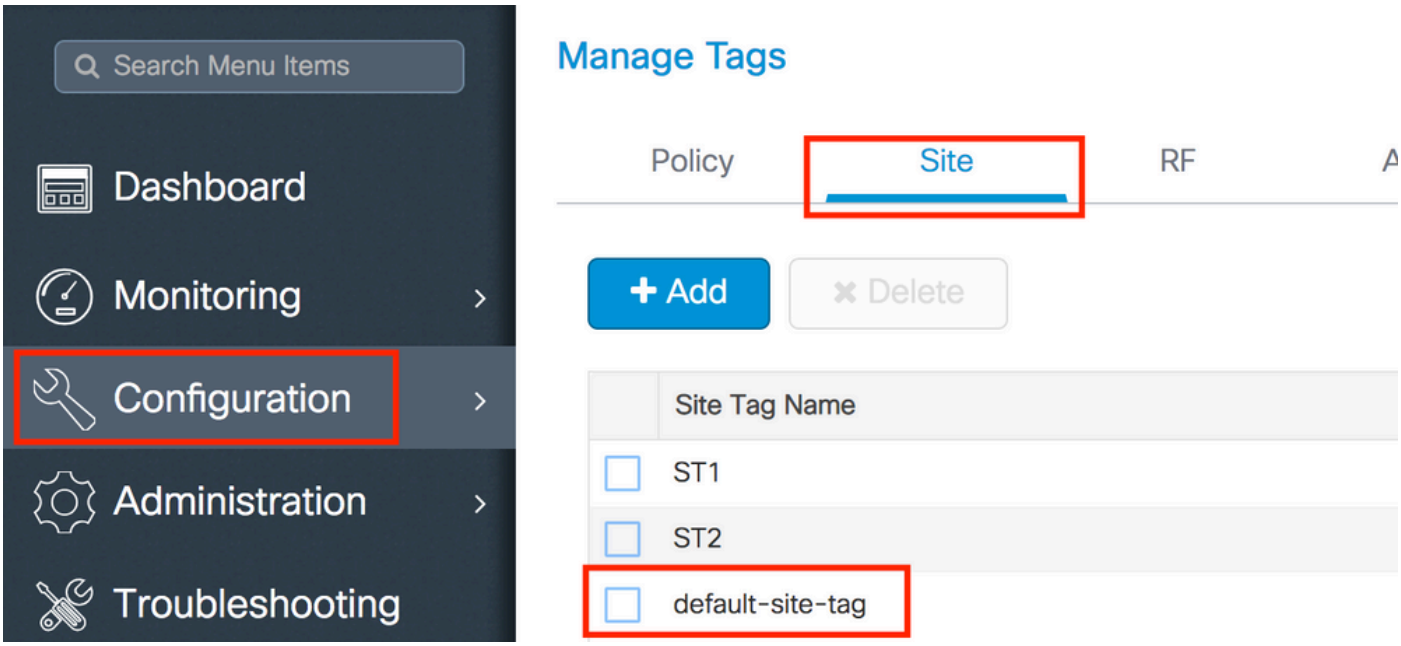
CLI：

```
# show ap tag summary | inc 3702-02

3702-02 f07f.06e1.9ea0 default-site-tag default-policy-tag default-rf-tag No Default
```

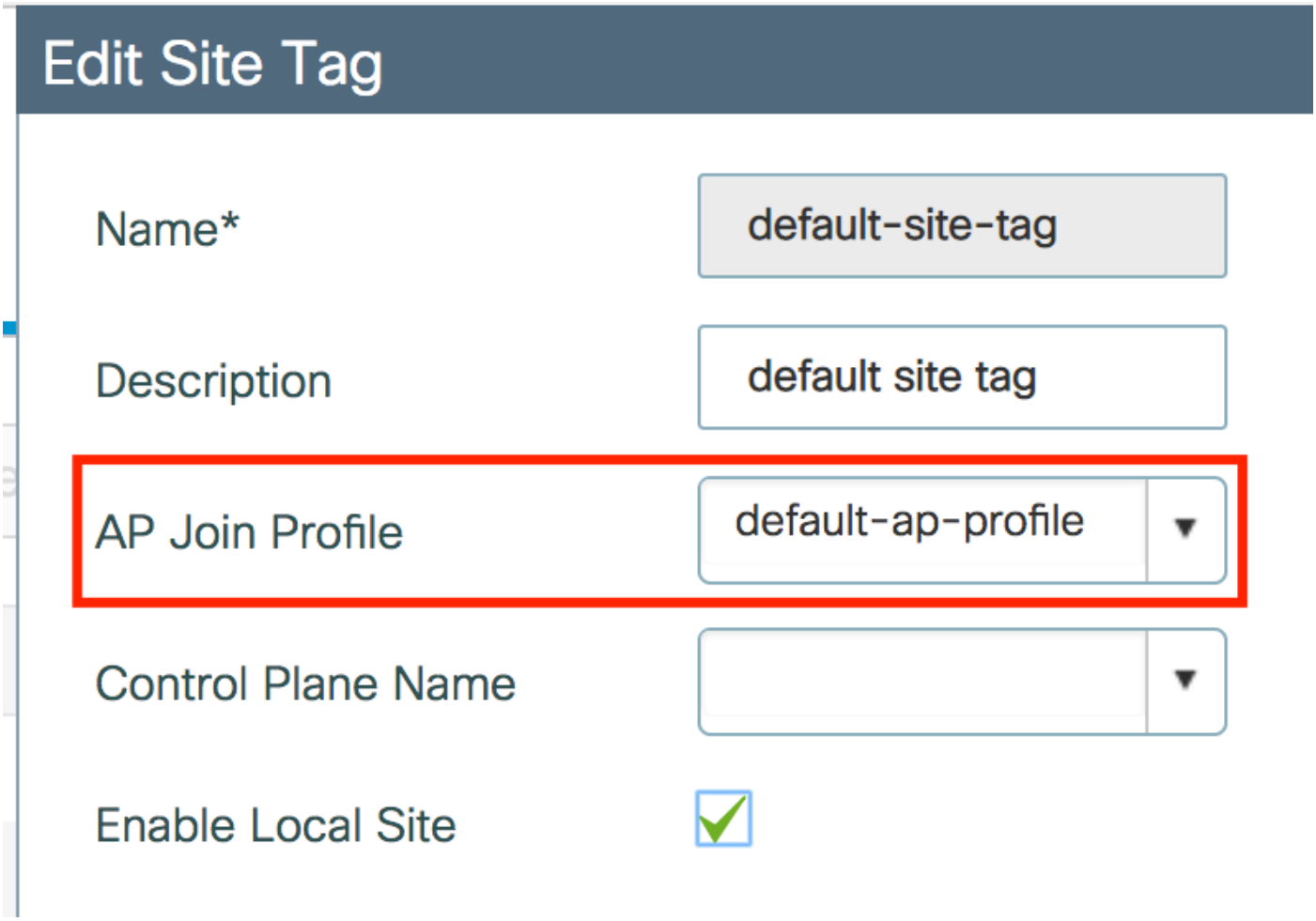
ステップ 2：そのサイトタグに関連付けられているAP加入プロファイルを確認します

GUI：

[Configuration] > [Tags & Profiles] > [Tags] > [Site] > [Site Tag Name] に移動します。



関連付けられたAP加入プロファイルをメモします



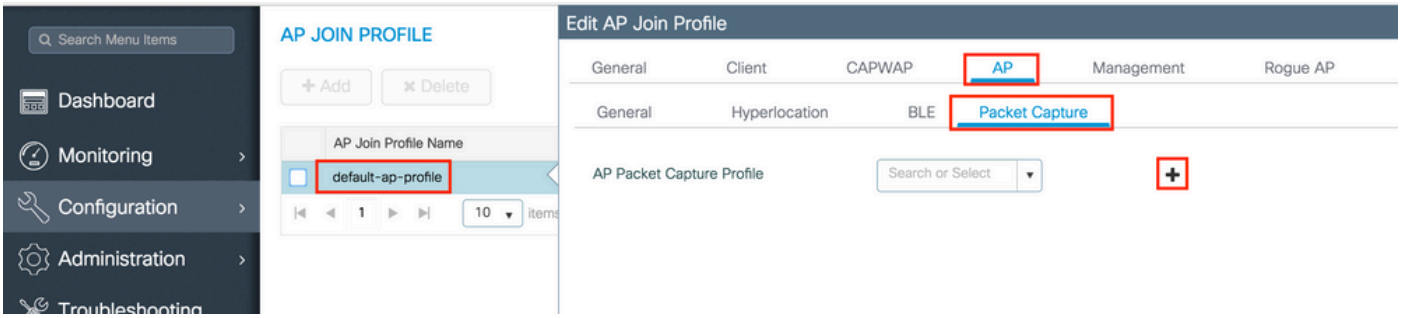
CLI：

```
# show wireless tag site detailed default-site-tag

Site Tag Name : default-site-tag
Description : default site tag
-------------------------------------
AP Profile : default-ap-profile
Local-site : Yes
Image Download Profile: default-me-image-download-profile
```

ステップ 3：AP加入プロファイルにパケットキャプチャ設定を追加します。

GUI：

[Configuration] > [Tags & Profiles] > [AP Join] > [AP Join Profile Name] > [AP] > [Packet Capture] に移動し、新しいAPパケットキャプチャプロファイルを追加します。

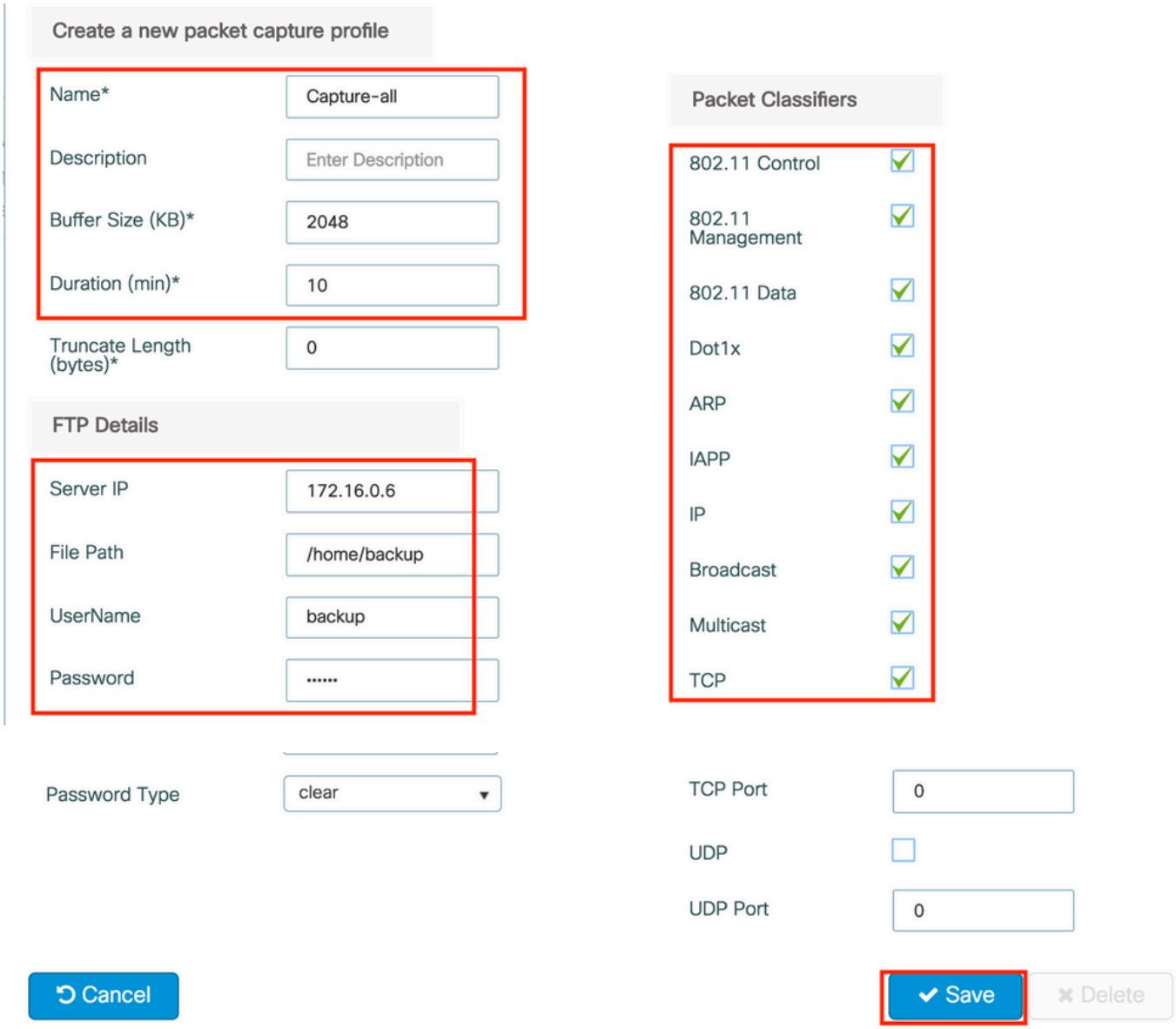


パケットキャプチャプロファイルの[Name]を選択し、APがパケットキャプチャを送信するFTPサ

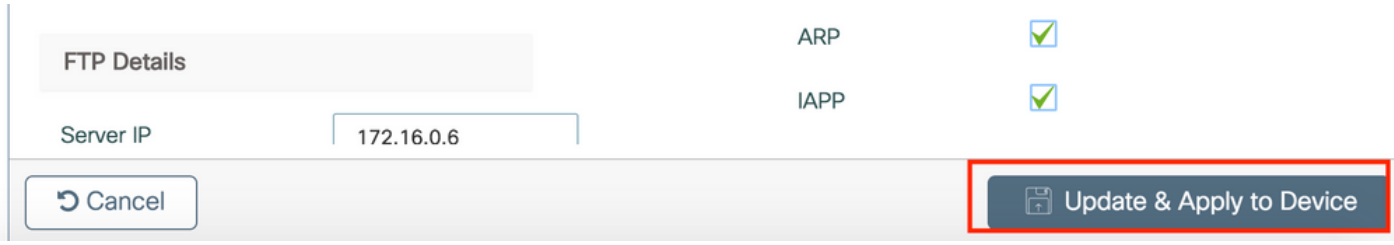
ーバの詳細を入力します。また、モニタするパケットの種類も選択します。

バッファサイズ= 1024 ～ 4096

期間= 1 ～ 60



キャプチャプロファイルを保存したら、[Update & Apply to Device] をクリックします。



CLI：

```
# config t
# wireless profile ap packet-capture Capture-all
# classifier arp
```

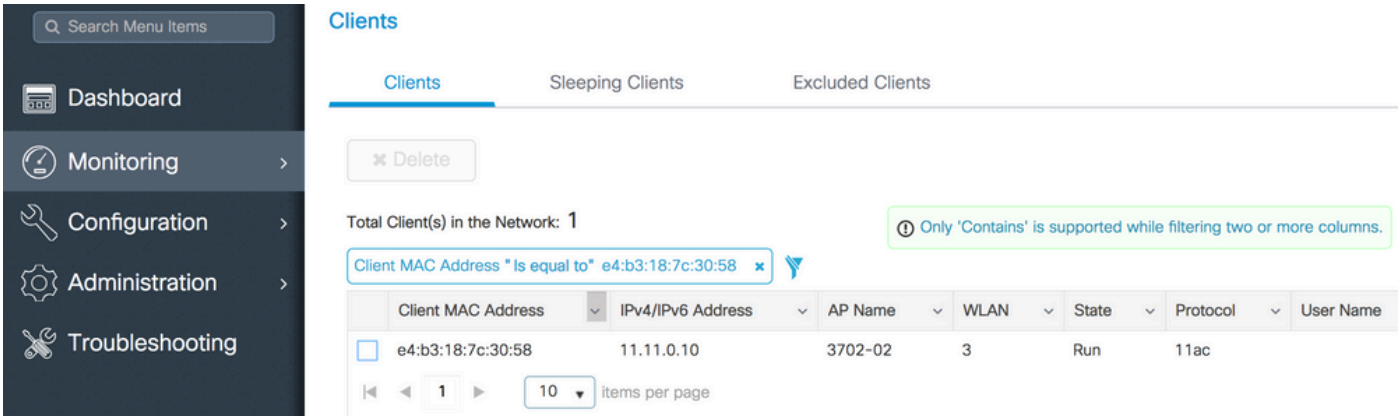
```
# classifier broadcast
# classifier data
# classifier dot1x
# classifier iapp
# classifier ip
# classifier tcp
# ftp password 0 backup
# ftp path /home/backup
# ftp serverip 172.16.0.6
# ftp username backup
# exit

# ap profile default-ap-profile
# packet-capture Capture-all
# end

# show wireless profile ap packet-capture detailed Capture-all

Profile Name : Capture-all
Description  :
-----------------------------------------------------
Buffer Size       : 2048 KB
Capture Duration  : 10 Minutes
Truncate Length   : packet length
FTP Server IP     : 172.16.0.6
FTP path          : /home/backup
FTP Username      : backup

Packet Classifiers
  802.11 Control  : Enabled
  802.11 Mgmt     : Enabled
  802.11 Data     : Enabled
  Dot1x           : Enabled
  ARP             : Enabled
  IAPP            : Enabled
  IP              : Enabled
  TCP             : Enabled
  TCP port        : all
  UDP             : Disabled
  UDP port        : all
  Broadcast       : Enabled
  Multicast       : Disabled
```

ステップ 4：モニタするワイヤレスクライアントが、いずれかのSSIDと、パケットキャプチャ設定を持つAP加入プロファイルが割り当てられたタグを割り当てたAPのいずれかに、すでに関連付けられていることを確認します。関連付けられていない場合、キャプチャは開始できません。

> **ヒント**:クライアントがSSIDに接続できない原因をトラブルシューティングする場合は、正常に動作するSSIDに接続し、障害のあるSSIDにローミングします。キャプチャはクライアントに従い、そのアクティビティをすべてキャプチャします。

GUI：

[Monitoring] > [Wireless] > [Clients] に移動します。



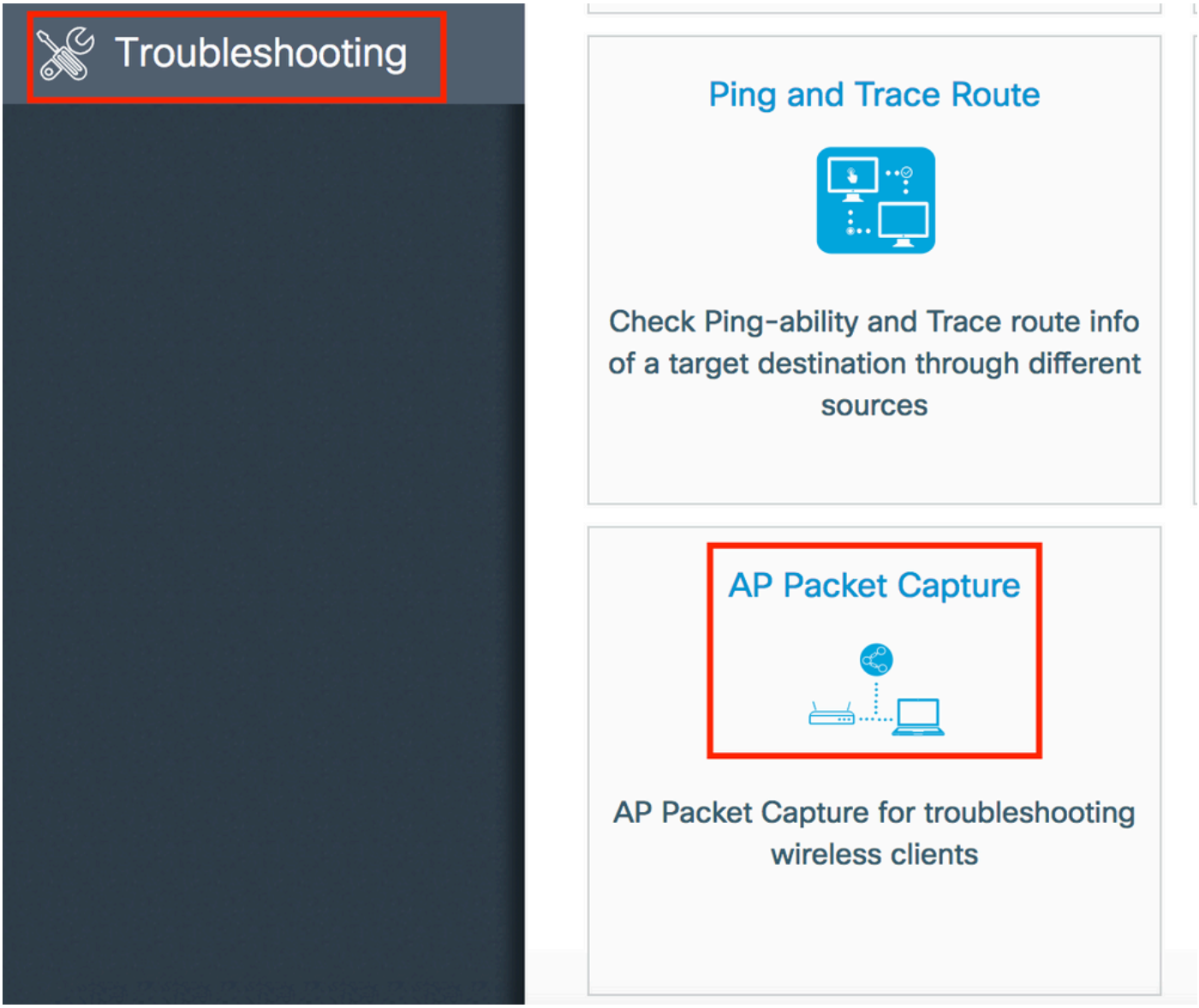
CLI：

```
# show wireless client summary | inc e4b3.187c.3058

e4b3.187c.3058 3702-02 3 Run 11ac
```

ステップ 5：キャプチャの開始

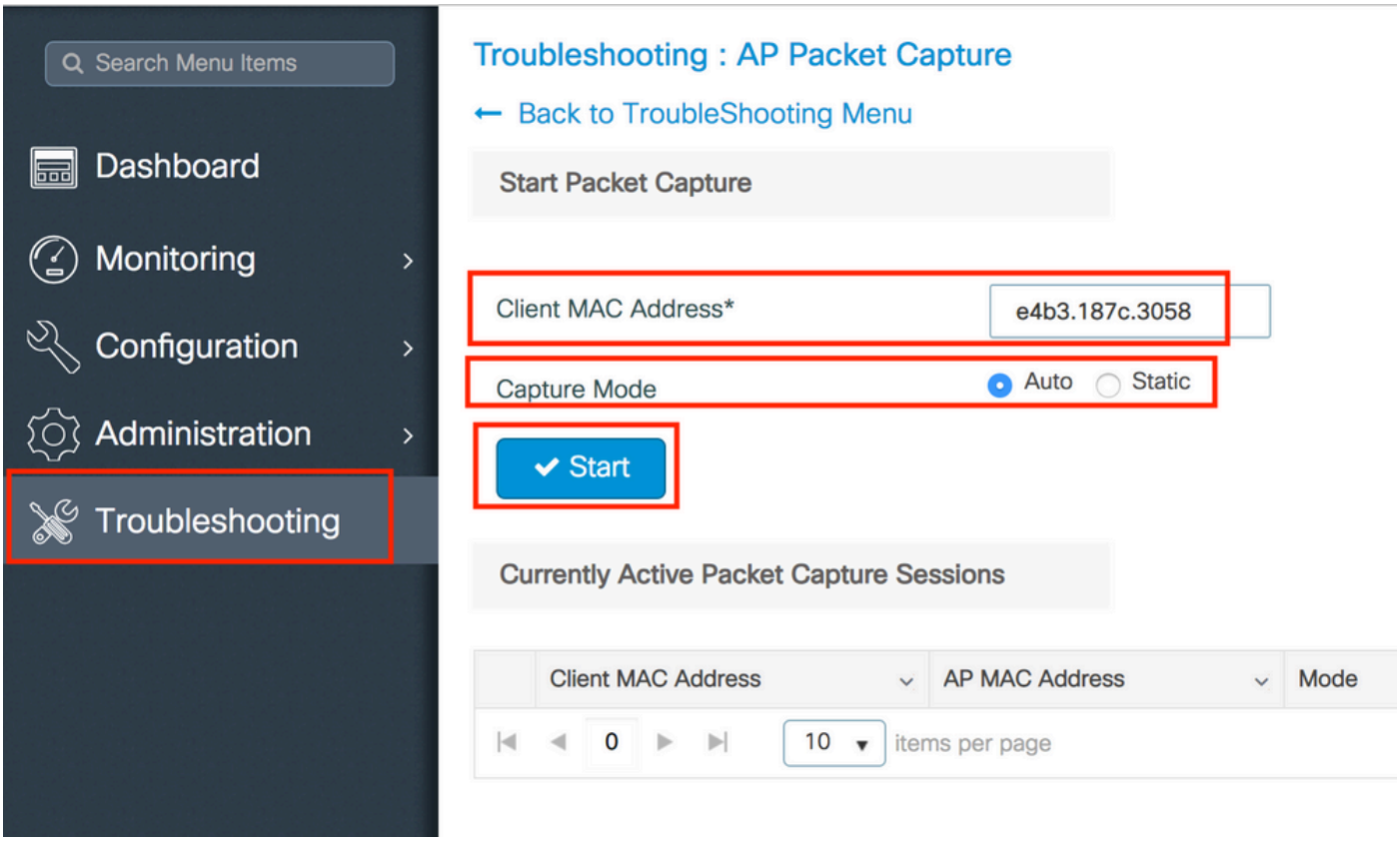
GUI：

[Troubleshooting] > [AP Packet Capture] に移動します。

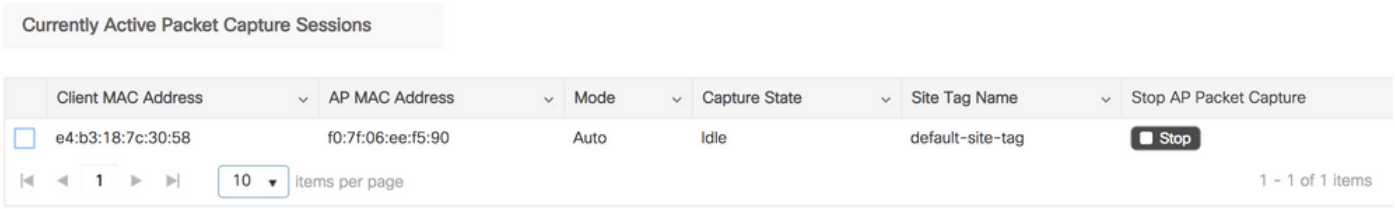


モニタするクライアントのMACアドレスを入力し、[Capture Mode]を選択します。 Autoは、ワイヤレスクライアントが接続するすべてのAPが新しい.pcapファイルを自動的に作成することを意味します。 Staticでは、ワイヤレスクライアントを監視する特定のAPを1つ選択できます。

Startを使用してキャプチャを開始します。



次に、キャプチャの現在の状態を確認できます。



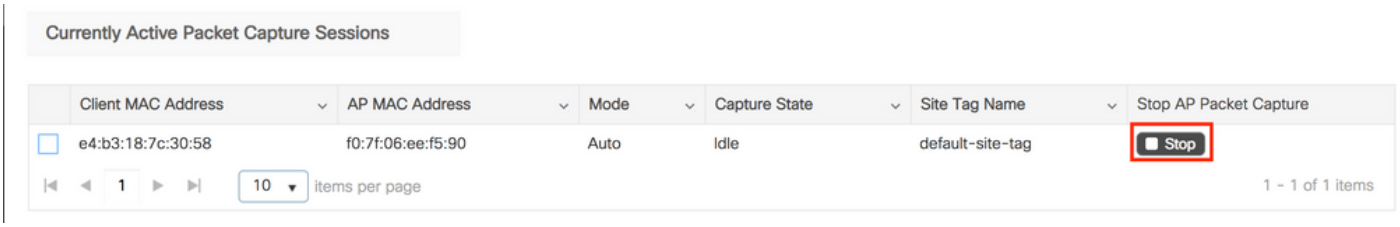
CLI：

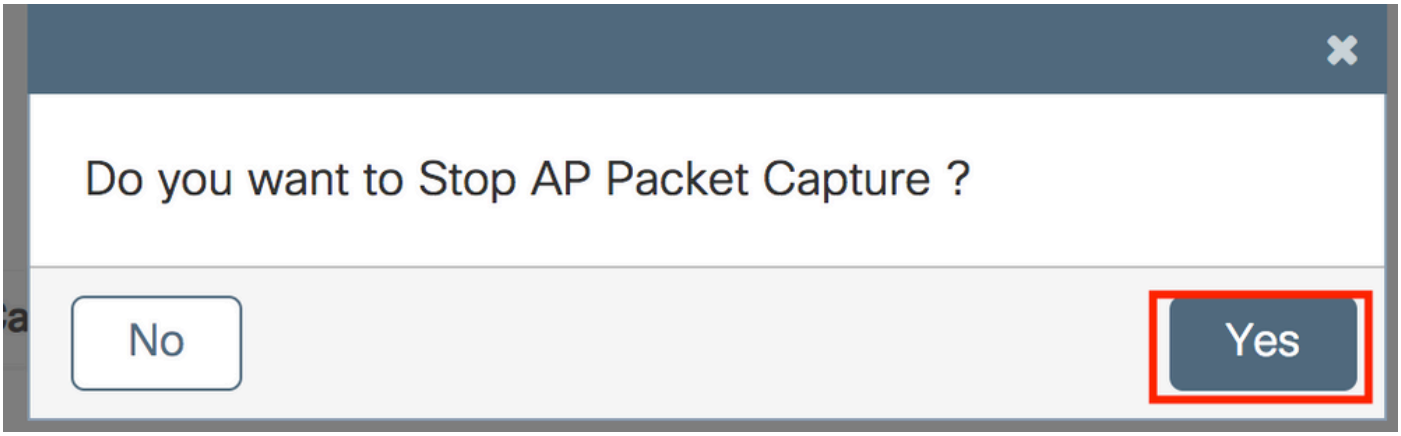
```
# ap packet-capture start <E4B3.187C.3058> auto
```

手順 6：キャプチャの停止

目的の動作をキャプチャしたら、GUIまたはCLIでキャプチャを停止します。

GUI：



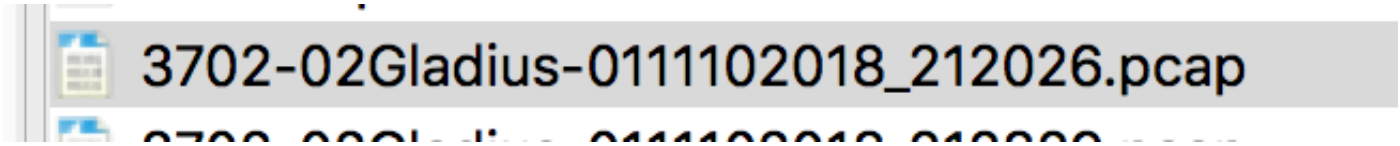


CLI：

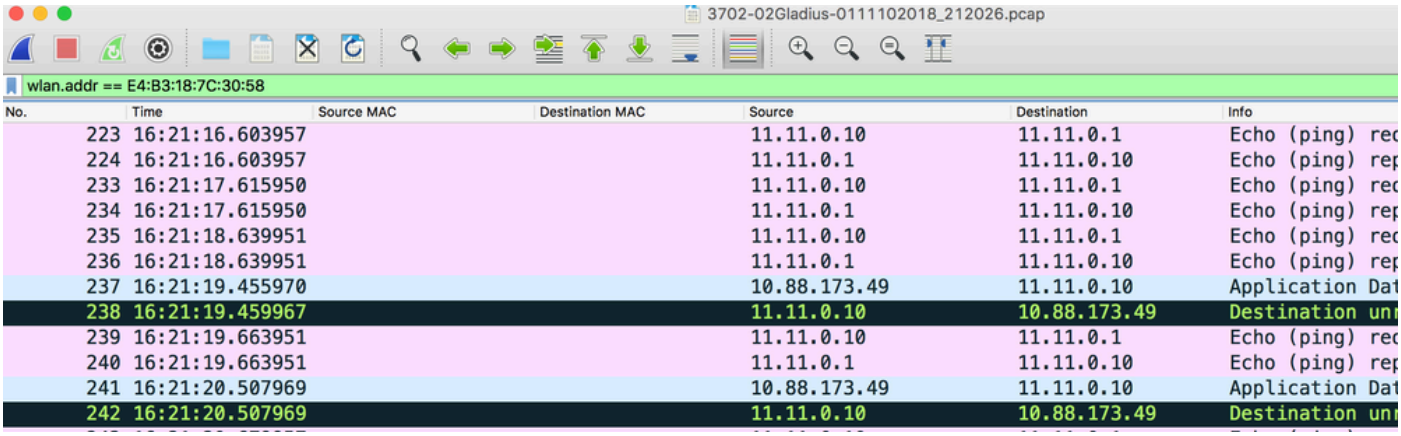
```
# ap packet-capture stop <E4B3.187C.3058> all
```

手順 7：FTPサーバから.pcapファイルを収集します

<ap-name><9800-wlc-name>-<##-file><day><month><year>_<hour><minute><second>.pcapという名前のファイルを見つける必要があります



ステップ 8：このファイルは、任意のパケット分析ツールで開くことができます。



確認

次のコマンドを使用して、パケットキャプチャ機能の設定を確認できます。

```
# show ap status packet-capture

Number of Clients with packet capture started : 1

Client MAC      Duration(secs)   Site tag name            Capture Mode
-----------------------------------------------------------------------
e4b3.187c.3058  600              default-site-tag         auto

# show ap status packet-capture detailed e4b3.187c.3058
```

```
Client MAC Address    : e4b3.187c.3058
Packet Capture Mode   : auto
Capture Duration      : 600 seconds
Packet Capture Site   : default-site-tag

Access Points with status
AP Name                   AP MAC Addr     Status
-----------------------------------------------------
APf07f.06e1.9ea0          f07f.06ee.f590  Started
```

トラブルシュート

この機能をトラブルシューティングするには、次の手順を実行します。

ステップ 1：デバッグ条件を有効にする

```
# set platform software trace wireless chassis active R0 wncmgrd all-modules debug
```

ステップ 2：行動を再現する

ステップ 3：現在のコントローラの時刻を確認して、ログを時間どおりに追跡できるようにします

```
# show clock
```

ステップ 4：ログの収集

```
# show logging process wncmgrd internal | inc ap-packet-capture
```

ステップ 5：ログの状態をデフォルトに戻します。

```
# set platform software trace wireless chassis active R0 wncmgrd all-modules notice
```

> **注**：トラブルシューティングセッションの後、不要なログの生成を避けるためにログレベルを戻すことが非常に重要です。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。