# Configuration de la capture de paquets AP sur les contrôleurs sans fil Catalyst 9800

## Table des matières


- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configuration
  - Diagramme du réseau
    - Configurations
- Vérifier
- Dépannage


## Introduction

Ce document décrit comment utiliser la fonctionnalité de capture de paquets du point d'accès (AP).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Accès aux contrôleurs sans fil via l'interface de ligne de commande (CLI) ou l'interface utilisateur graphique (GUI).
- Serveur FTP
- fichiers .pcap

### Composants utilisés

- WLC 9800 v16.10
- AP 3700
- Serveur FTP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

# Informations générales

Cette fonctionnalité n'est disponible que pour les points d'accès Cisco IOS® (comme AP 3702) et est donc déconseillée après la version 17.3 de Cisco IOS® XE.

Cette solution est remplacée par la capture intelligente avec Cisco DNA, ou comme une alternative, en configurant le point d'accès en mode renifleur.

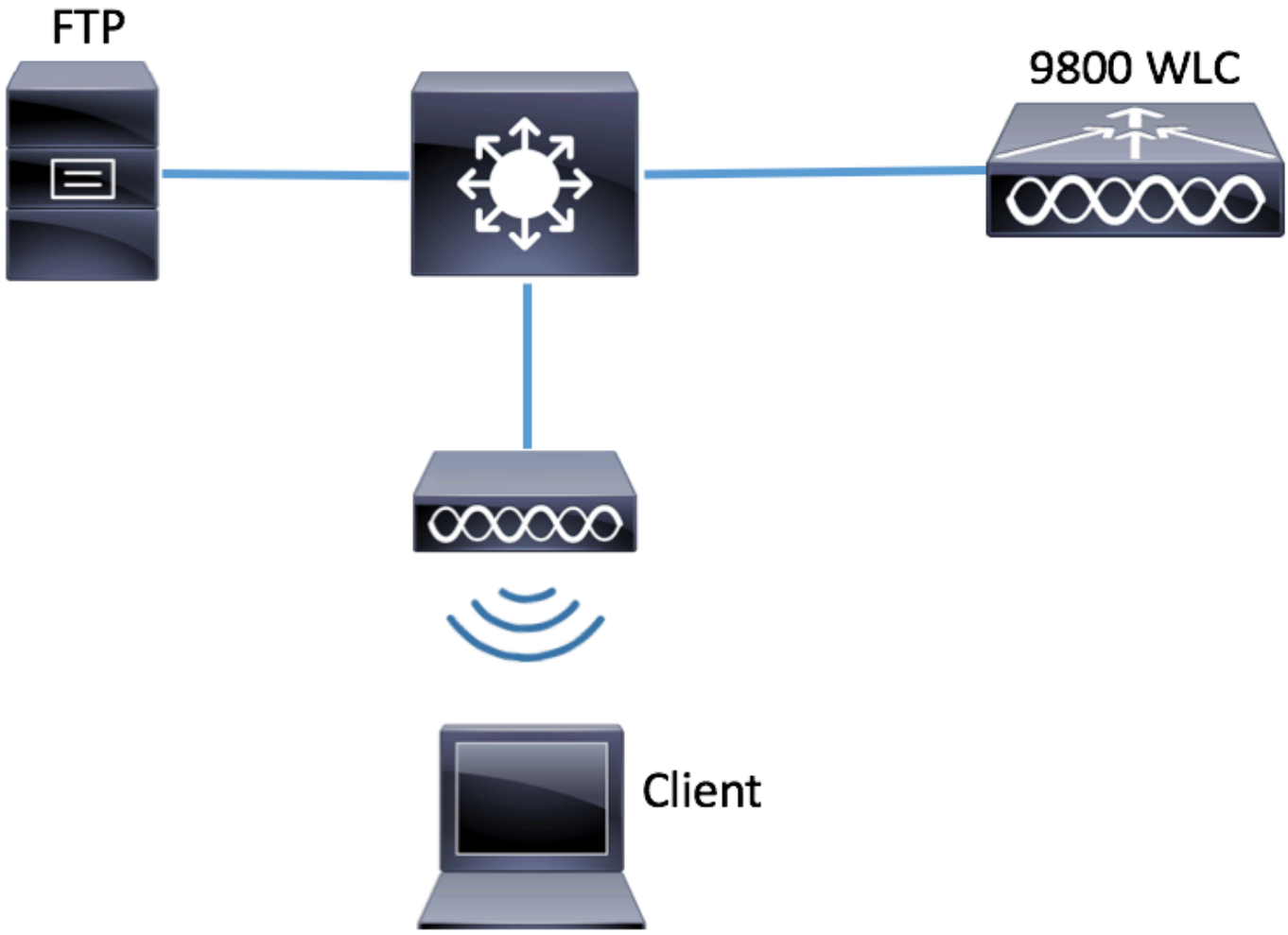
La fonction de capture de paquets AP vous permet d'effectuer des captures de paquets sur l'air avec peu d'effort. Lorsque la fonctionnalité est activée, une copie de tous les paquets et trames sans fil spécifiés envoyés et reçus depuis/vers les points d'accès depuis/vers une adresse MAC sans fil spécifique par liaison radio, est transmise à un serveur FTP (File Transfer Protocol), où vous pouvez la télécharger sous la forme d'un fichier .pcap et l'ouvrir avec votre outil d'analyse de paquets préféré.

Une fois la capture de paquets démarrée, l'AP auquel le client est associé crée un nouveau fichier .pcap sur le serveur FTP (assurez-vous que le nom d'utilisateur spécifié pour la connexion FTP dispose de droits d'écriture). Si le client se déplace, le nouvel AP crée un nouveau fichier .pcap sur le serveur FTP. Si le client se déplace entre les SSID (Service Set Identifiers), le point d'accès maintient la capture de paquets active afin que vous puissiez voir toutes les trames de gestion lorsque le client s'associe au nouveau SSID.

Si vous effectuez la capture sur un SSID ouvert (pas de sécurité), vous pouvez voir le contenu des paquets de données, mais si le client est associé à un SSID sécurisé (un SSID protégé par mot de passe ou la sécurité 802.1x), alors la partie données des paquets de données est chiffrée et ne peut pas être vue en texte clair.

# Configuration

## Diagramme du réseau



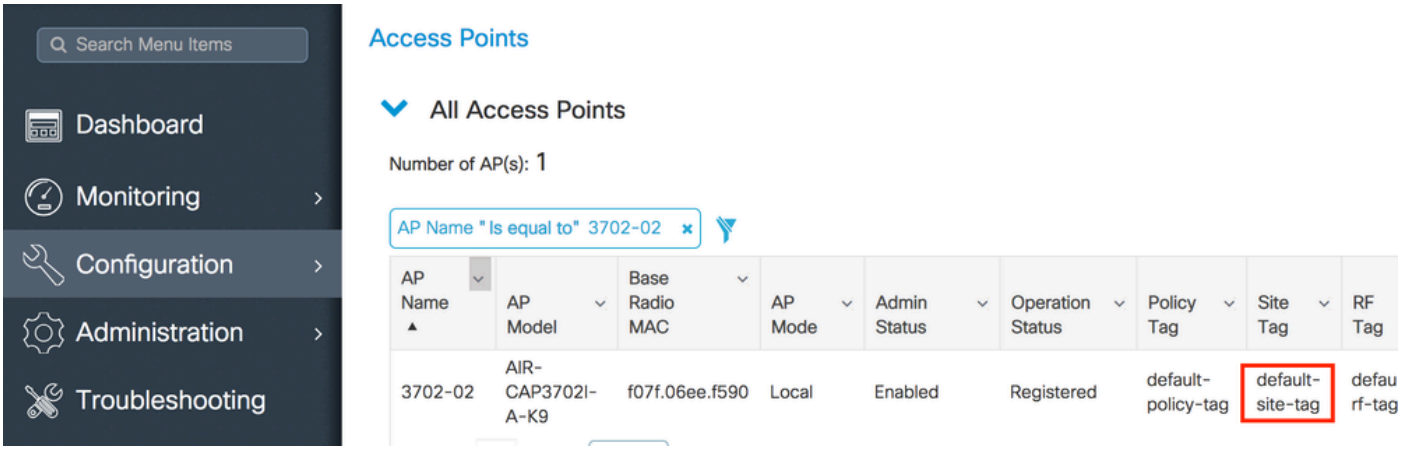

Configurations

Avant la configuration, vérifiez quels sont les points d'accès auxquels le client sans fil peut se connecter.

Étape 1 : vérification de la balise Site actuelle associée aux points d'accès que le client sans fil peut utiliser pour se connecter

IUG:

Accédez à Configuration > Wireless > Access Points.



CLI :

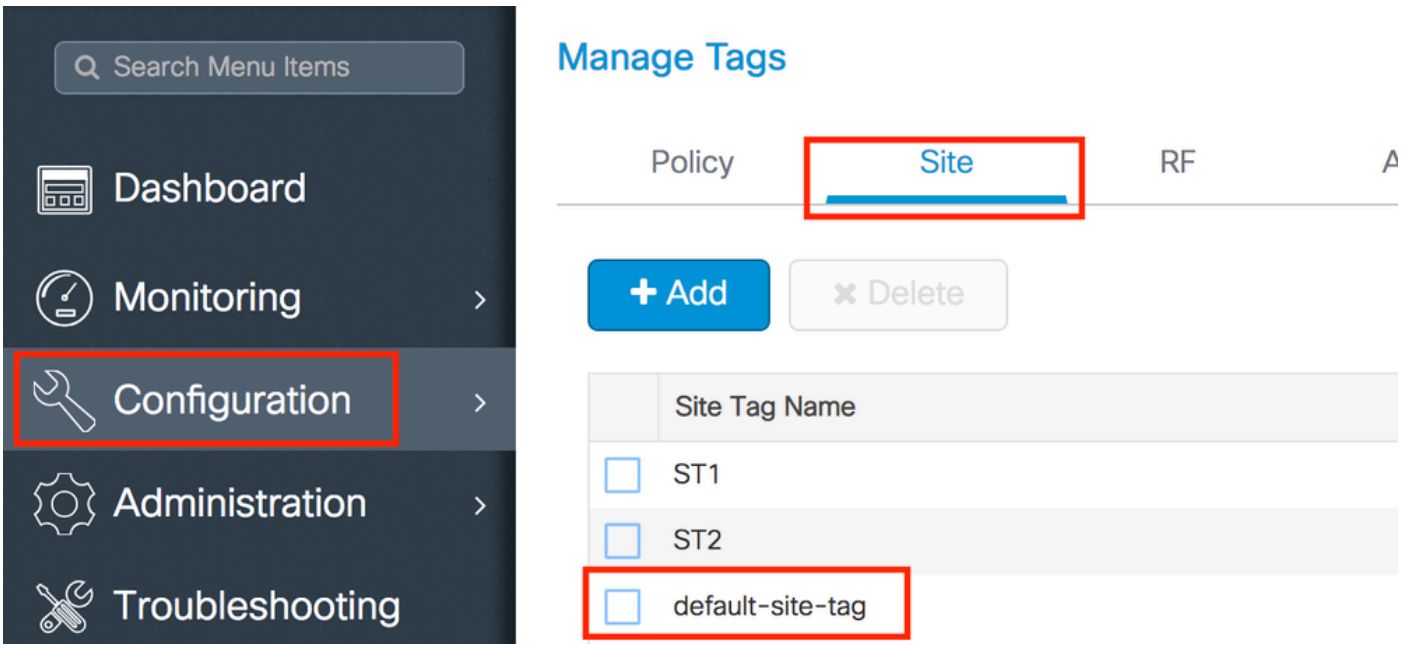
```
<#root>
# show ap tag summary | inc 3702-02


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

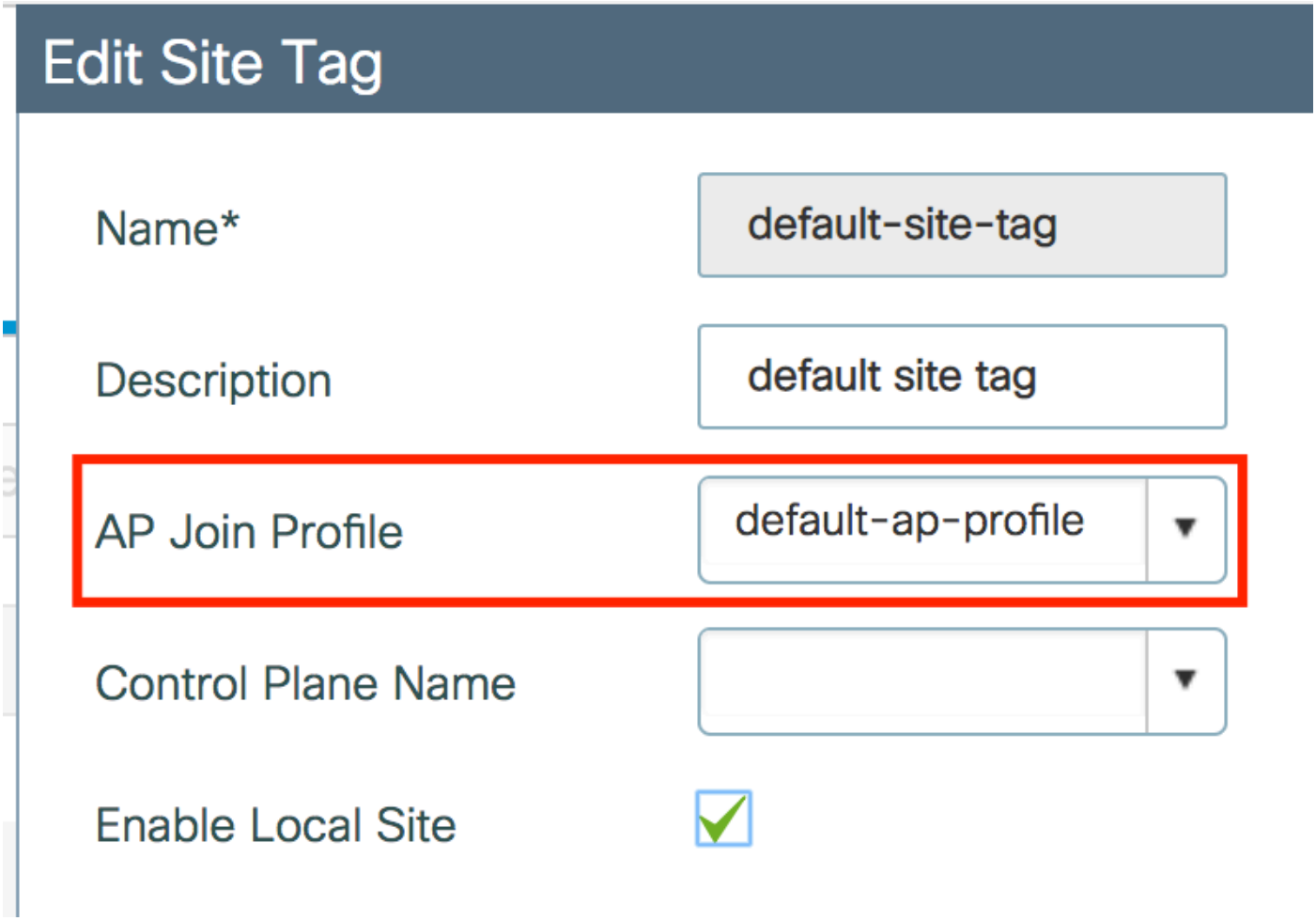
Étape 2 : vérification du profil de connexion AP associé à cette balise de site

IUG:

Accédez à Configuration > Tags & Profiles > Tags > Site > Site Tag Name.




Prenez note du profil de jonction AP associé.




CLI :

<#root>

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

```
Site Tag Name : default-site-tag
Description : default site tag
-------------------------------------
AP Profile :
```

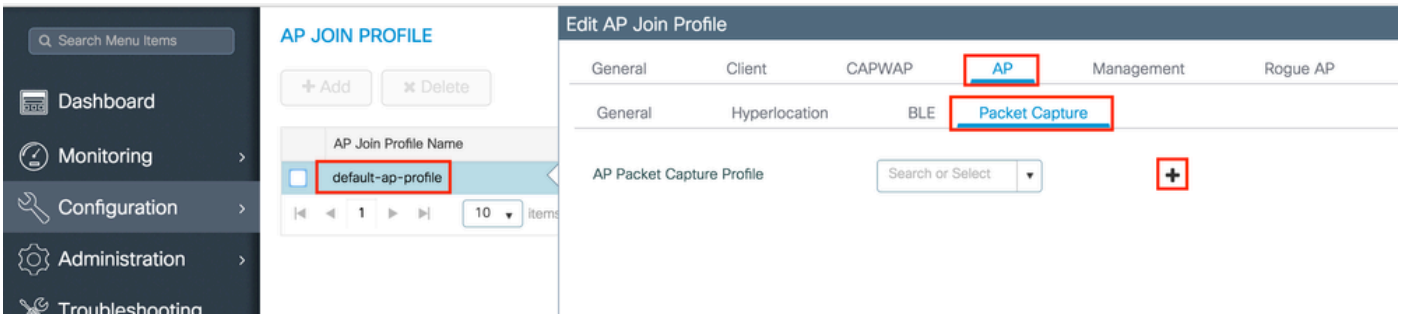
**default-ap-profile**

```
Local-site : Yes
Image Download Profile: default-me-image-download-profile
```

Étape 3 : ajout des paramètres de capture de paquets sur le profil de connexion AP

IUG:

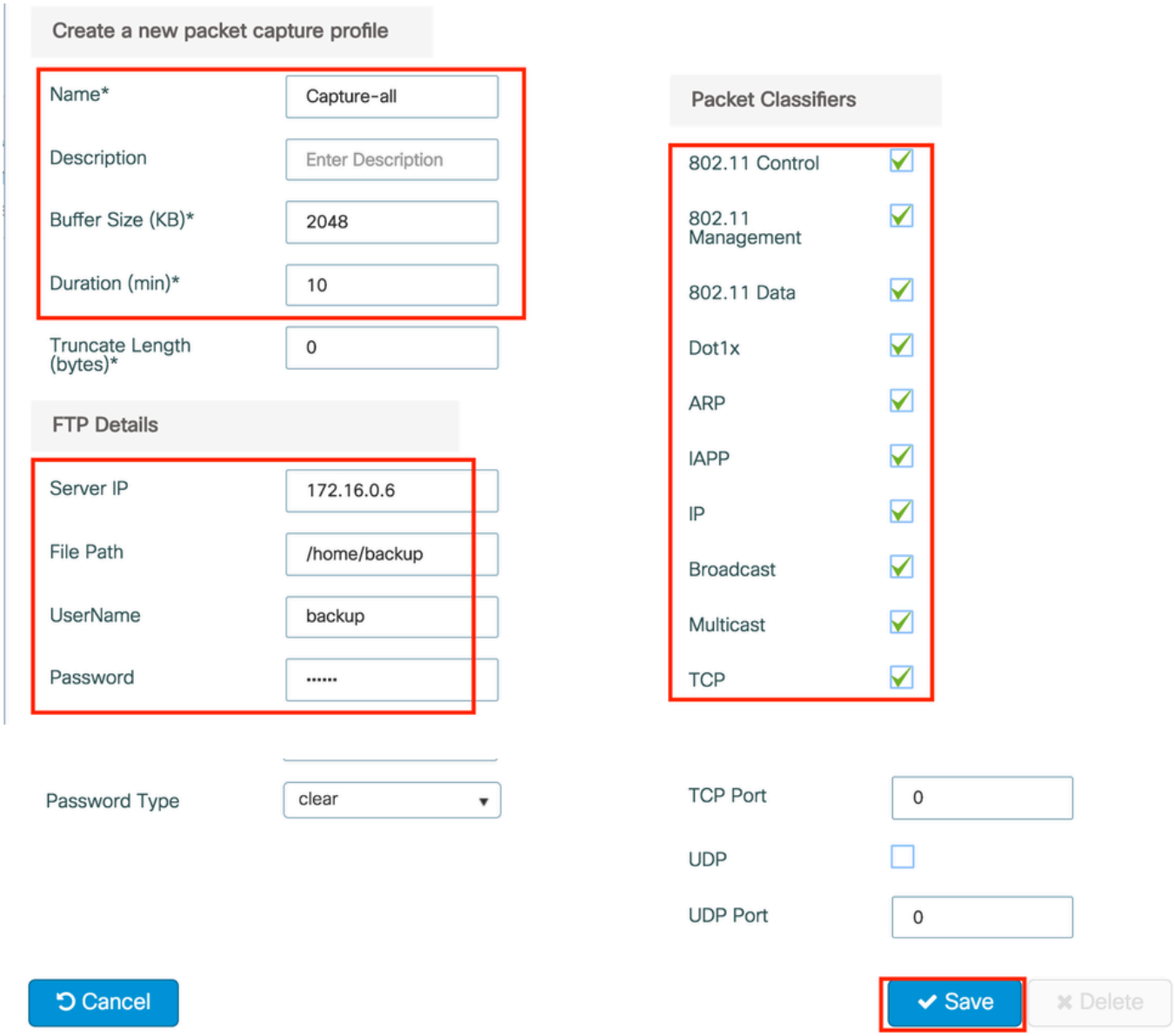
Accédez à Configuration > Tags & Profiles > AP Join > AP Join Profile Name > AP > Packet Capture et ajoutez un nouveau profil de capture de paquets AP.



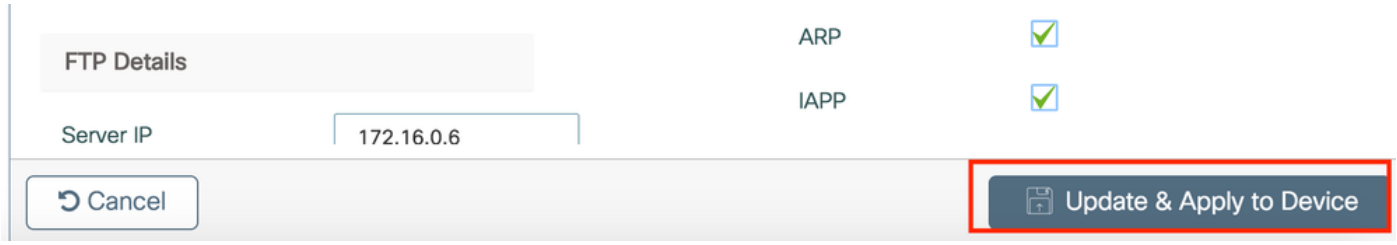

Sélectionnez un nom pour le profil de capture de paquets et entrez les détails du serveur FTP auquel les points d'accès envoient la capture de paquets. Assurez-vous également de sélectionner le type de paquets que vous souhaitez surveiller.

Taille du tampon = 1024-4096

Durée = 1-60




Une fois le profil Capture enregistré, cliquez sur Update & Apply to Device.




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
```

Étape 4. Assurez-vous que le client sans fil que vous souhaitez surveiller est déjà associé à l'un des SSID et à l'un des points d'accès qui a attribué la balise où le profil de jonction AP avec les paramètres de capture de paquets a été attribué, sinon la capture ne peut pas être démarrée.

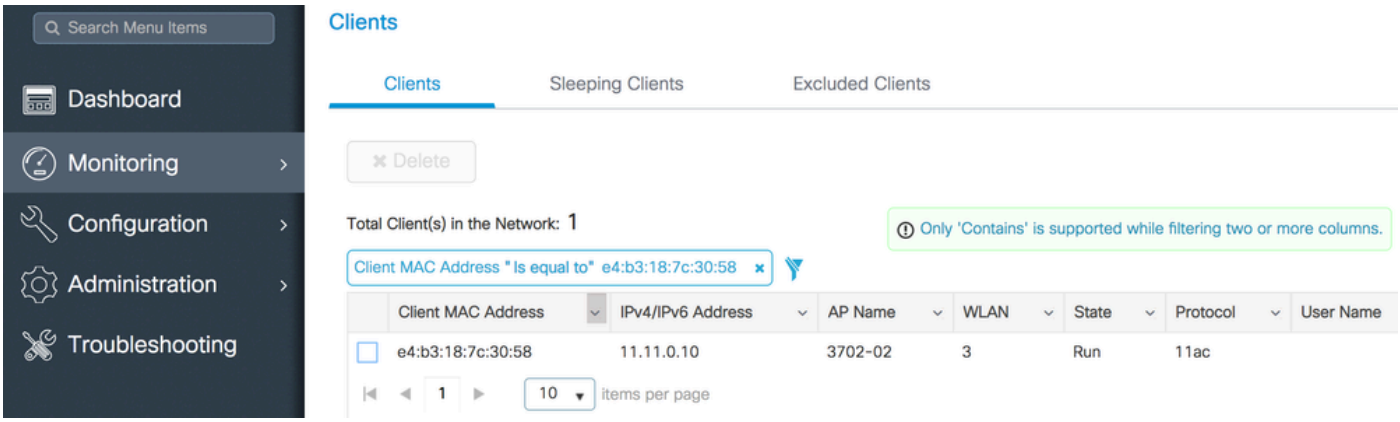
---

Conseil : si vous souhaitez dépanner la raison pour laquelle un client n'est pas en mesure de se connecter à un SSID, vous pouvez vous connecter à un SSID qui fonctionne correctement, puis vous déplacer vers le SSID défaillant, la capture suit le client et capture toute son activité.

---

IUG:

Accédez à Monitoring > Wireless > Clients.




CLI :

<#root>

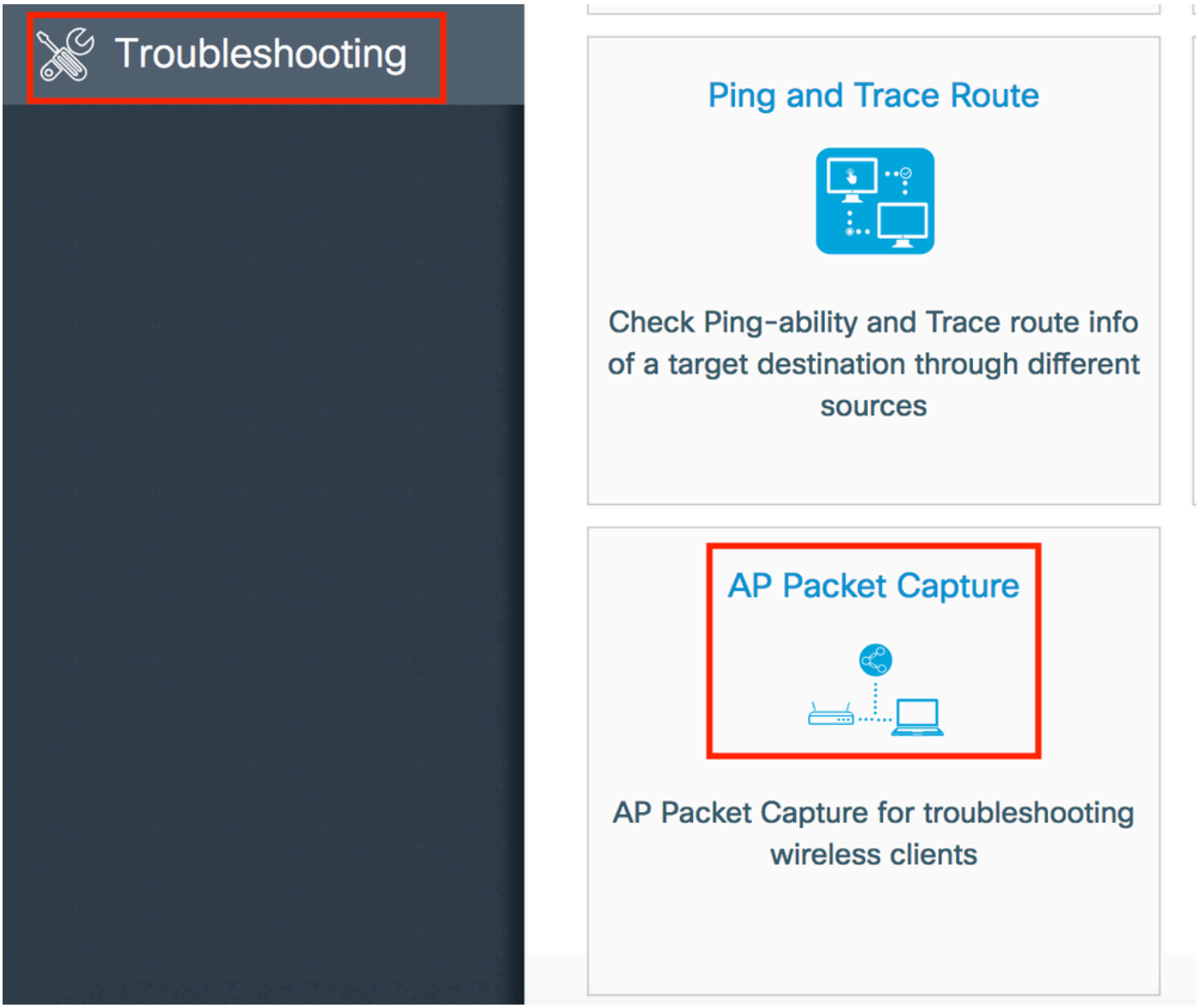
```
# show wireless client summary | inc e4b3.187c.3058
```

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

Étape 5. Démarrez la capture.

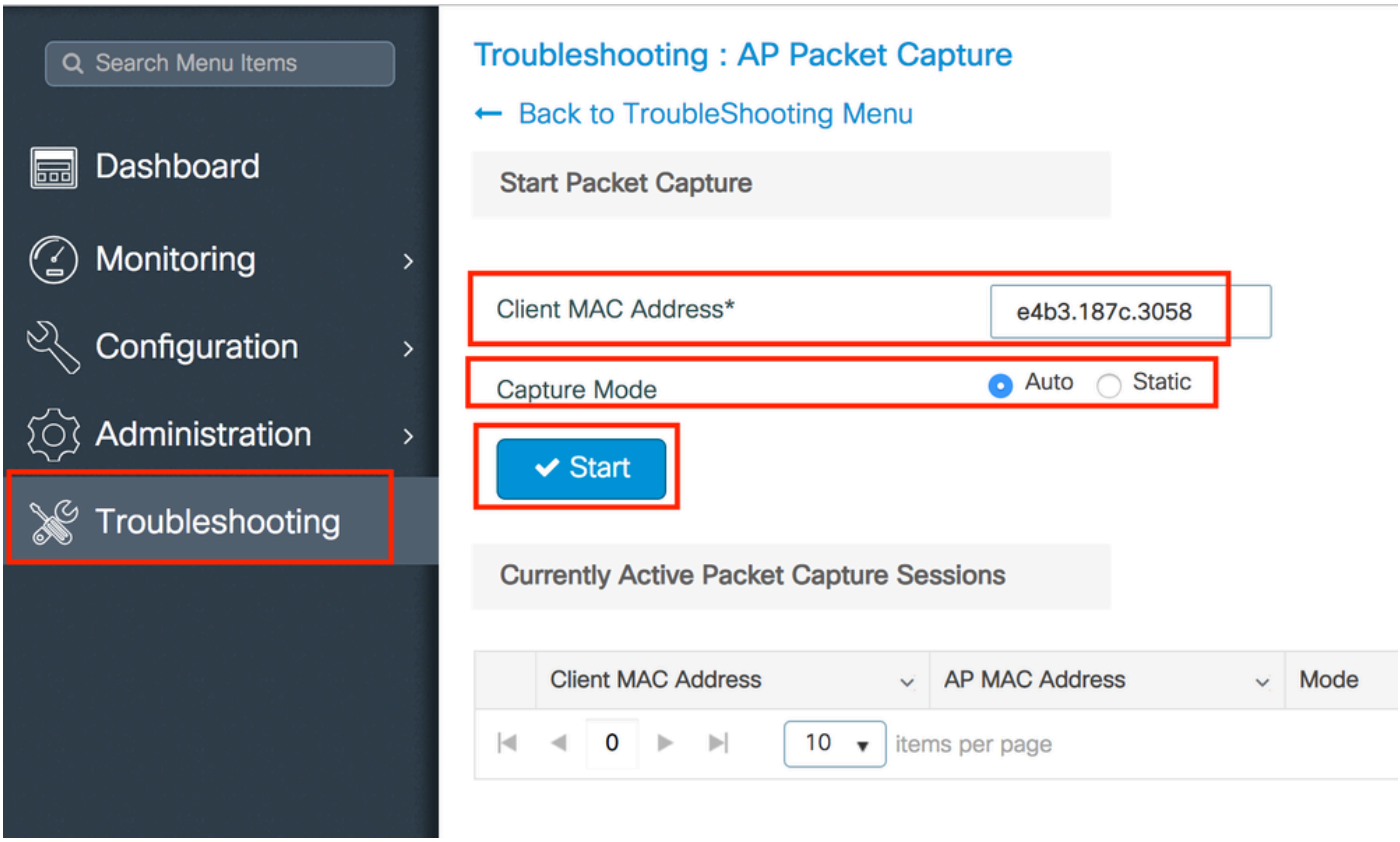
IUG:

Accédez à Troubleshooting > AP Packet Capture.

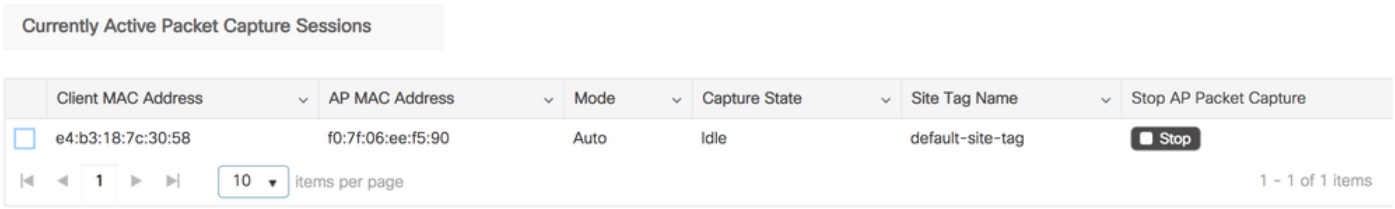



Entrez l'adresse MAC du client que vous voulez surveiller et sélectionnez le mode Capture. Auto signifie que chaque point d'accès auquel le client sans fil se connecte, crée automatiquement un nouveau fichier .pcap. Static vous permet de choisir un point d'accès spécifique pour surveiller le client sans fil.

Commencez la capture par Start.




Ensuite, vous pouvez voir l'état actuel de la capture :



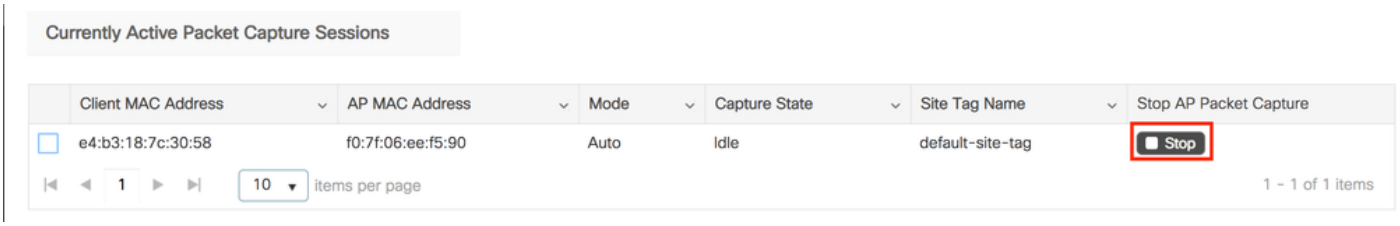

CLI :

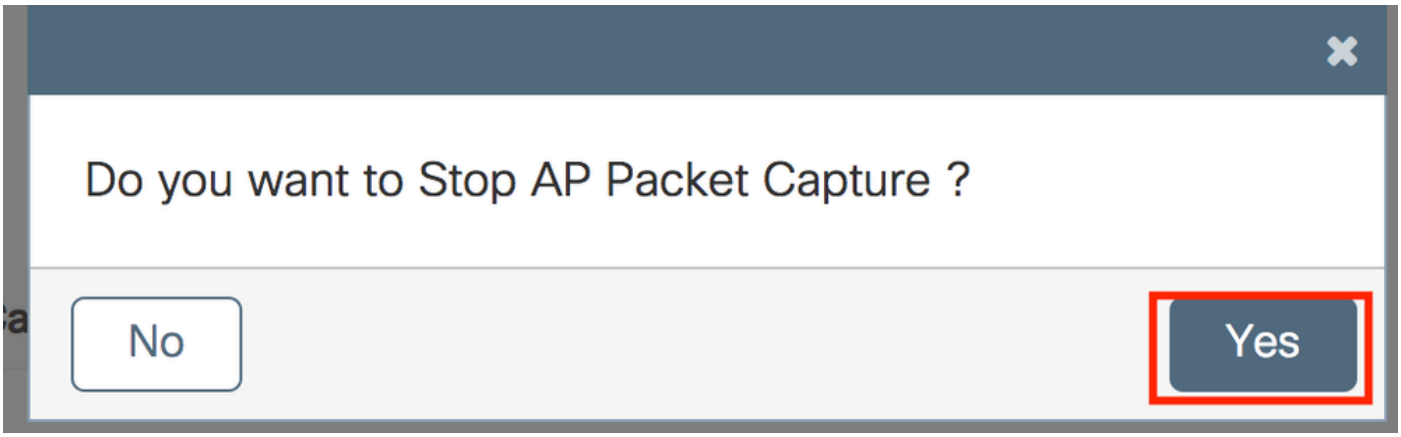
```
# ap packet-capture start <E4B3.187C.3058> auto
```

Étape 6. Arrêtez la capture.

Une fois que le comportement souhaité a été capturé, arrêtez la capture par interface utilisateur graphique ou par interface de ligne de commande :

IUG:



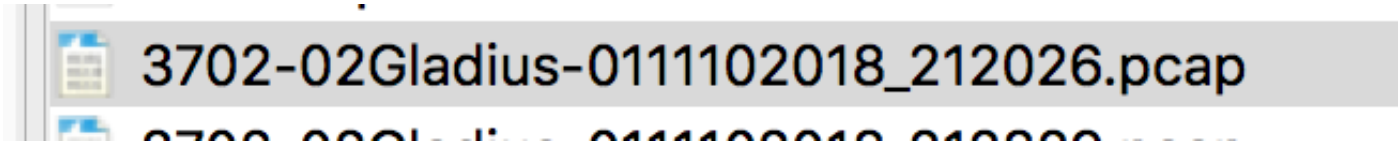



CLI :

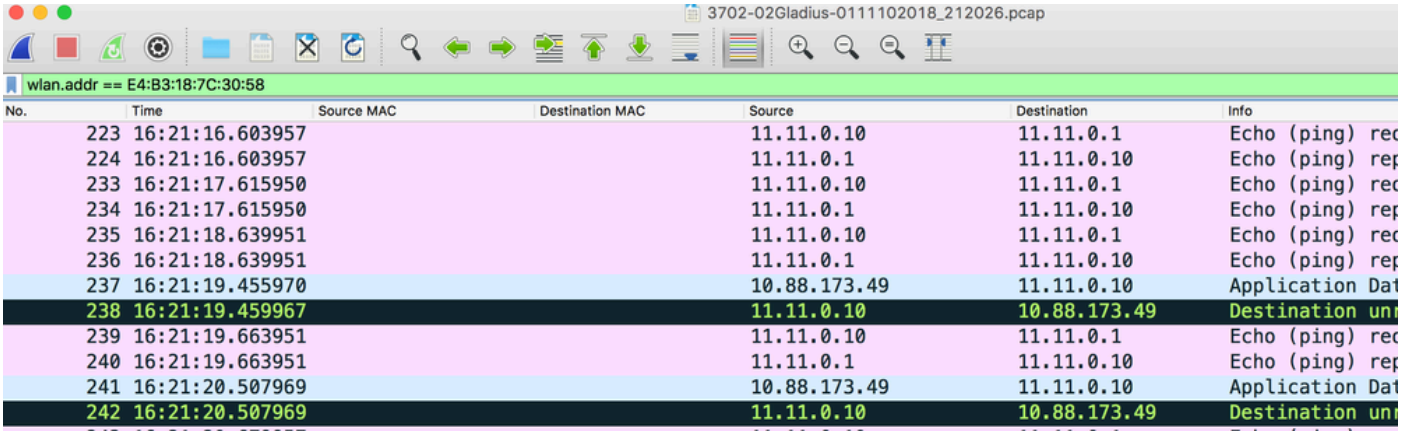
```
# ap packet-capture stop <E4B3.187C.3058> all
```

Étape 7 : collecte du fichier .pcap à partir du serveur FTP

Vous devez trouver un fichier portant le nom <ap-name><9800-wlc-name>-<##-file><day><month><year>_<hour><minute><second>.pcap.




Étape 8. Vous pouvez ouvrir le fichier à l'aide de l'outil d'analyse de paquets de votre choix.




## Vérifier

Vous pouvez utiliser ces commandes pour vérifier la configuration de la fonctionnalité de capture de paquets.

```
# 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
```

# Dépannage

Suivez ces étapes pour dépanner cette fonctionnalité :

Étape 1 : activation de la condition de débogage

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

Étape 2 : reproduction du comportement

Étape 3. Vérifiez l'heure actuelle du contrôleur pour pouvoir suivre les journaux dans le temps.

```
# show clock
```

Étape 4. Collectez les journaux.

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

Étape 5. Rétablissez les paramètres par défaut de la condition des journaux.

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

Remarque : il est très important qu'après une session de dépannage, vous redéfinissiez les niveaux des journaux afin d'éviter la génération de journaux inutiles.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.