# Configurazione di AP Packet Capture sui controller wireless Catalyst 9800

## Sommario



## Introduzione

In questo documento viene descritto come usare la funzione di acquisizione pacchetti del punto di accesso (AP).

### Premesse

La funzione AP Packet Capture consente di acquisire i pacchetti via etere con il minimo sforzo. Quando la funzione è abilitata, una copia di tutti i pacchetti wireless e dei frame specificati inviati e ricevuti da/ai punti di accesso da/a uno specifico indirizzo MAC wireless via etere, viene inoltrata a un server FTP (File Transfer Protocol), dove è possibile scaricarla come file .pcap e aprirla con lo strumento di analisi dei pacchetti preferito.

Una volta avviata l'acquisizione del pacchetto, l'access point a cui è associato il client crea un nuovo file .pcap sul server FTP (assicurarsi che il nome utente specificato per l'accesso FTP abbia diritti di scrittura). Se il client esegue il roaming, il nuovo punto di accesso crea un nuovo file con estensione pcap sul server FTP. Se il client si sposta tra gli SSID (Service Set Identifier), l'access point mantiene attiva l'acquisizione del pacchetto in modo che sia possibile visualizzare tutti i frame di gestione quando il client si associa al nuovo SSID.

Se si esegue l'acquisizione su un SSID aperto (nessuna protezione), è possibile visualizzare il contenuto dei pacchetti di dati, ma se il client è associato a un SSID protetto (un SSID protetto da password o la protezione 802.1x) la parte dei pacchetti di dati viene crittografata e non può essere visualizzata in testo non crittografato.

Questa funzione è disponibile solo per gli access point IOS (come AP 3702).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso ai controller wireless tramite interfaccia a riga di comando (CLI) o interfaccia grafica (GUI).
- server FTP
- file pcap

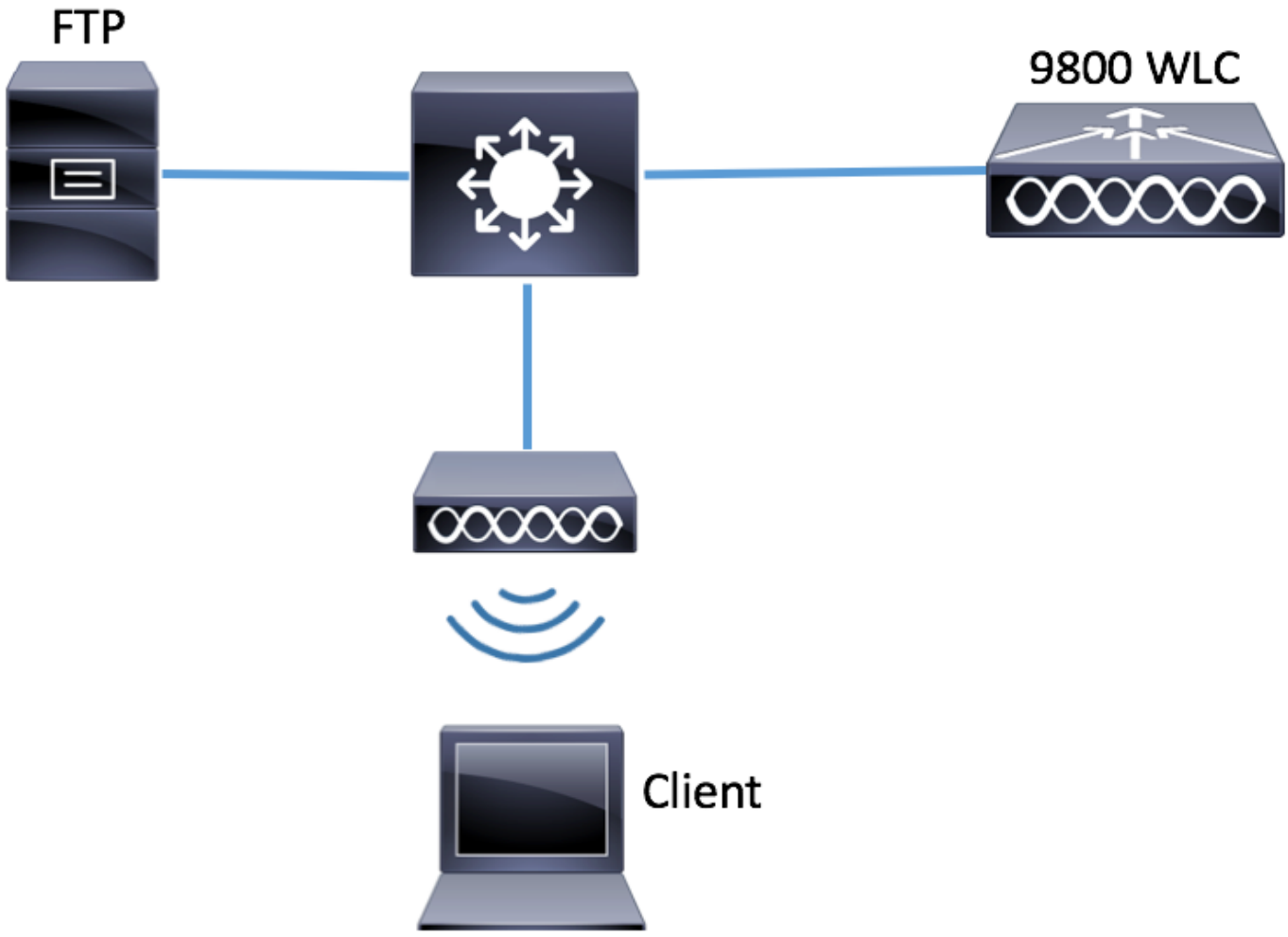
## Componenti usati

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

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

### Esempio di rete



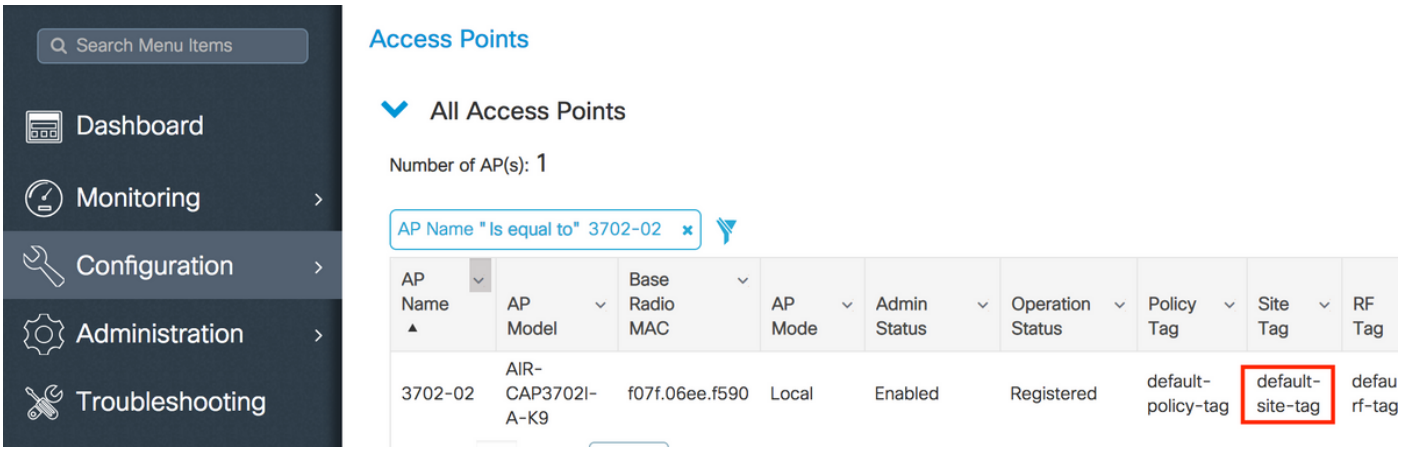

### Configurazioni

Prima di eseguire la configurazione, verificare quali sono i punti di accesso ai quali il client wireless può connettersi.

Passaggio 1. Verificare il tag del sito corrente associato agli access point che il client wireless può utilizzare per connettersi.

GUI:

Selezionare **Configuration > Wireless > Access Point**



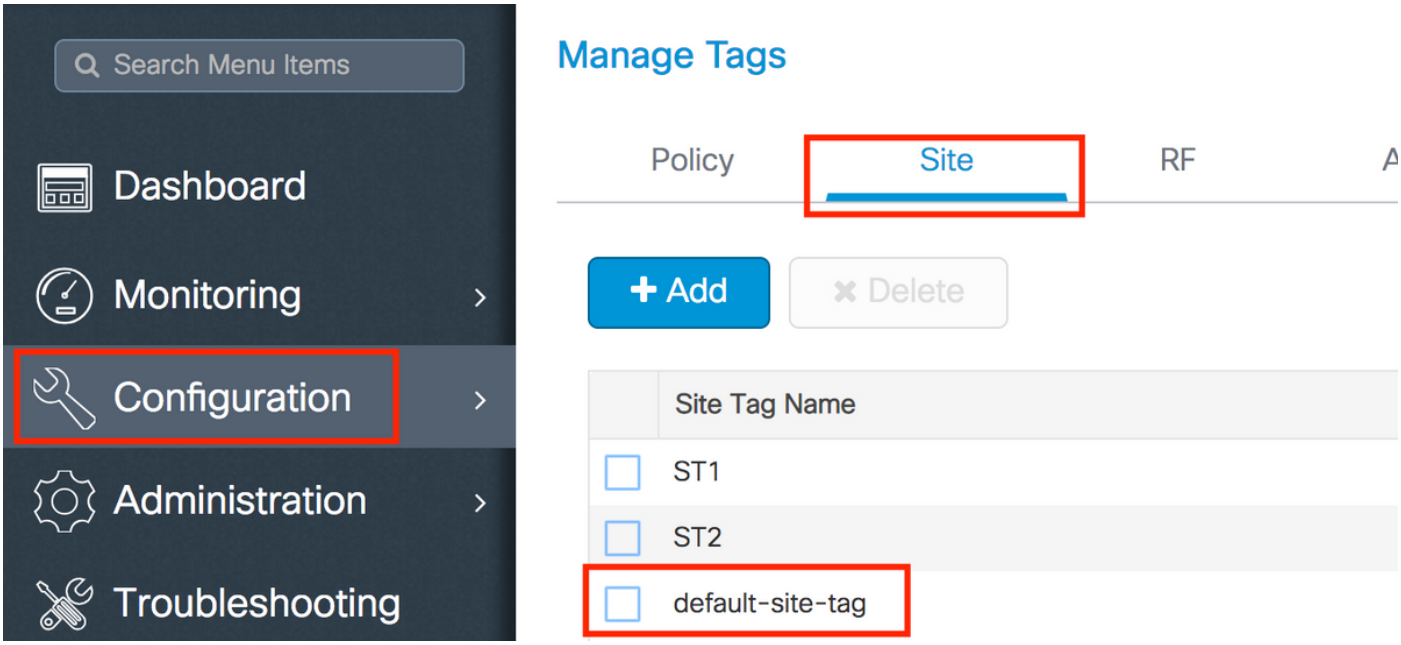

CLI:

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

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

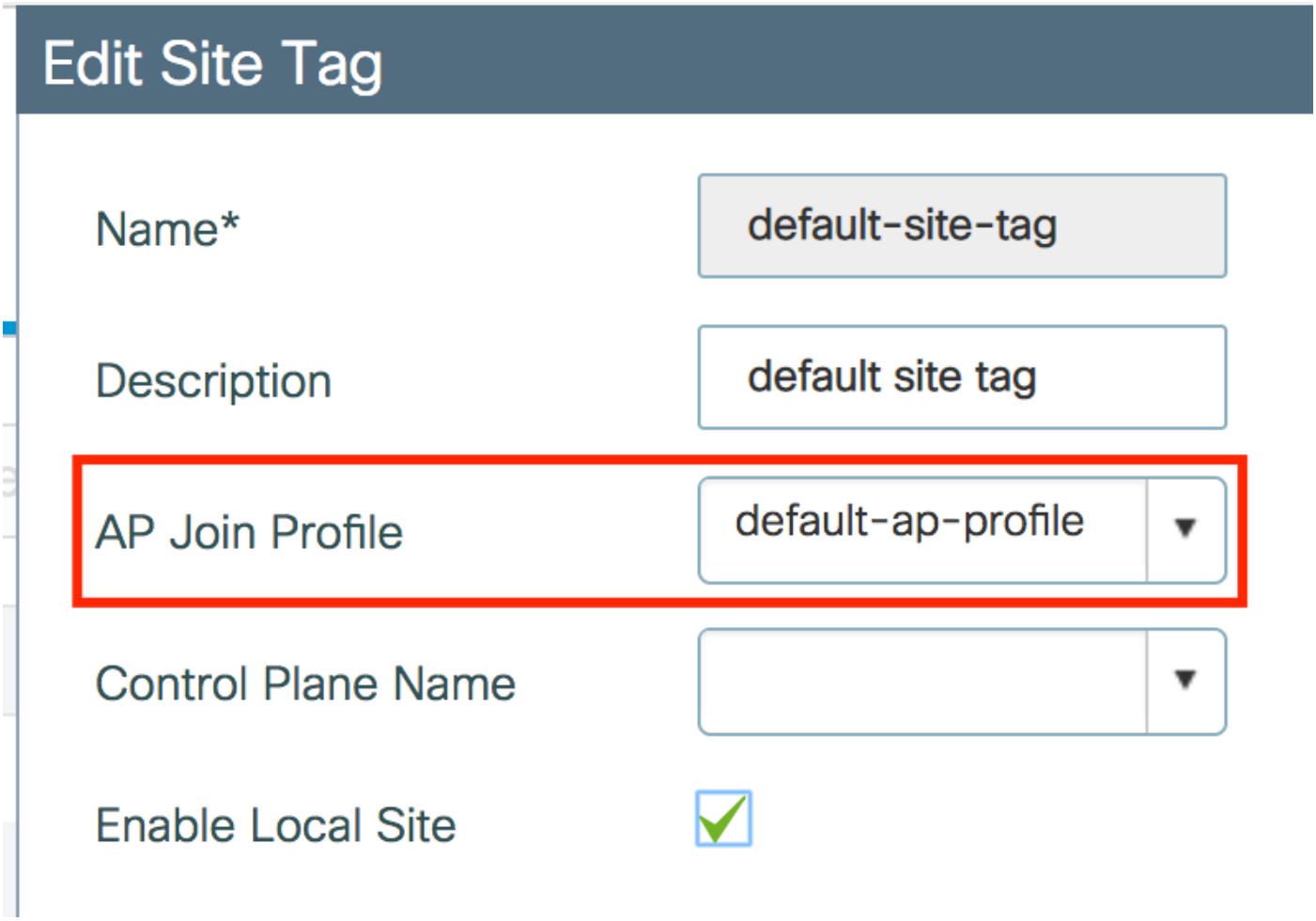
Passaggio 2. Controllare il profilo di aggiunta AP associato al tag del sito

GUI:

Selezionare **Configurazione > Tag e profili > Tag > Sito > Nome tag sito**




Prendere nota del profilo di aggiunta AP associato



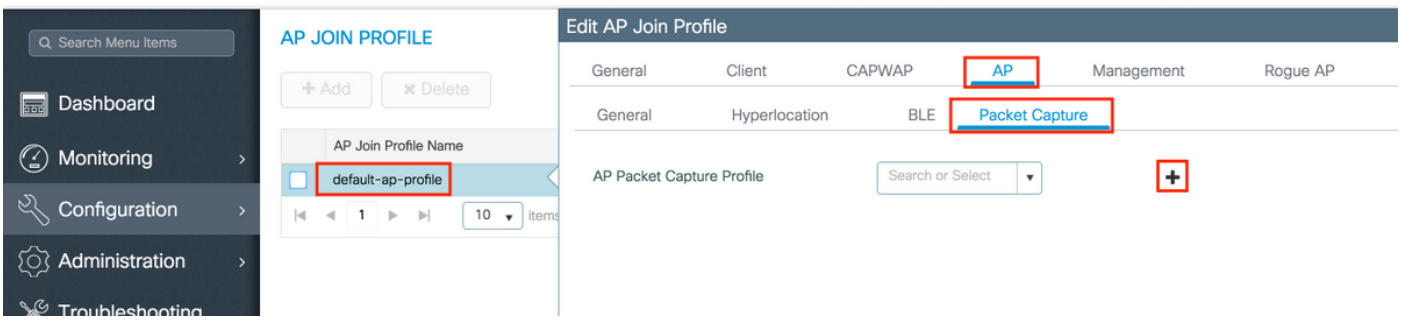

CLI:

```
# 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
```

Passaggio 3. Aggiungere le impostazioni di acquisizione pacchetti nel profilo di aggiunta all'access point

GUI:

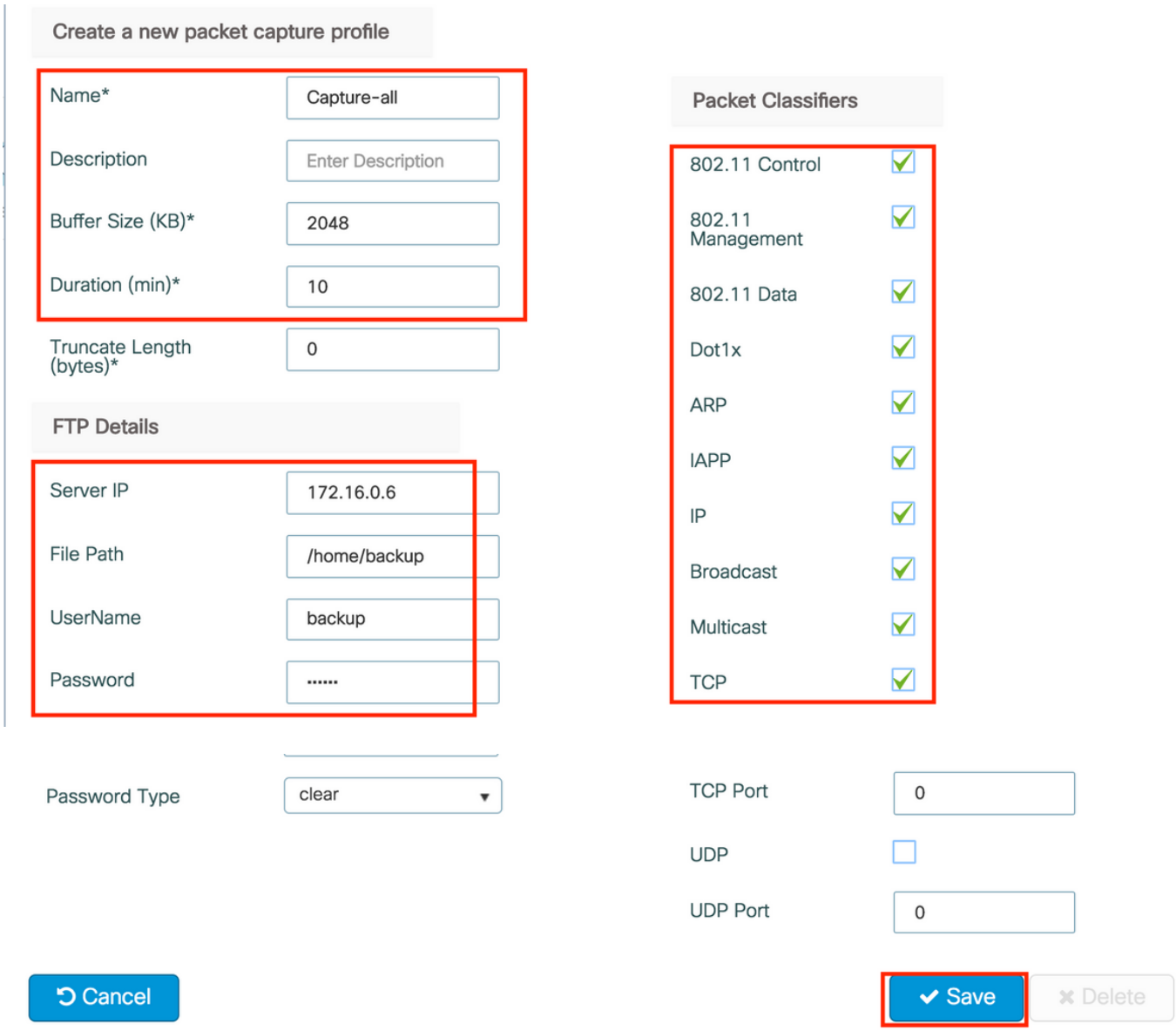
Selezionare **Configurazione > Tag e profili > AP Join > AP Join Profile Name > AP > Packet Capture** e aggiungere un nuovo **profilo AP Packet Capture.**



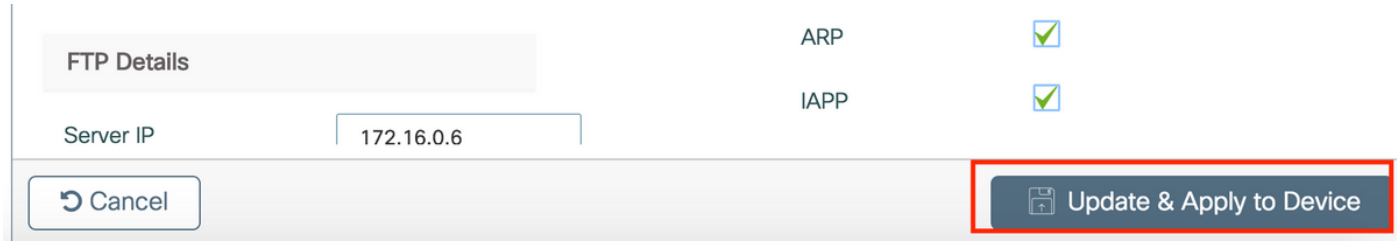
Selezionare un nome per il profilo di acquisizione pacchetto, immettere i dettagli del server FTP a cui gli access point inviano l'acquisizione pacchetto. Accertarsi inoltre di selezionare il tipo di pacchetti da monitorare.

Dimensione buffer = 1024-4096

Durata = 1-60




Una volta salvato il profilo di cattura, fare clic su **Update & Apply to Device** (Aggiorna e applica alla periferica).




CLI:

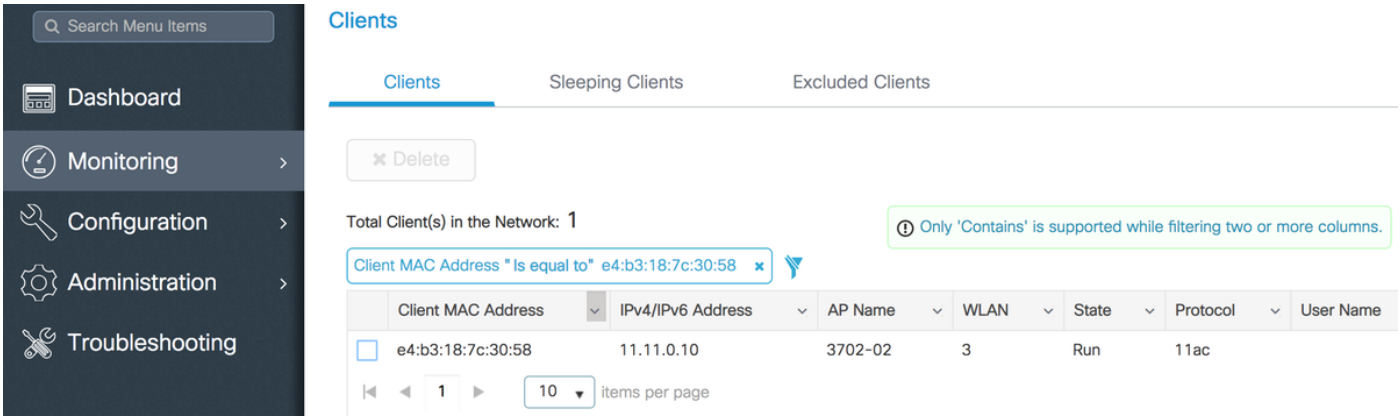
```
# config t
# wireless profile ap packet-capture Capture-all
# classifier arp
# classifier broadcast
# classifier data
# classifier dot1x
# classifier iapp
# classifier ip
# classifier tcp
# ftp password 0 backup
# ftp path /home/backup
# ftp serverip 172.16.0.6
# ftp username backup
# exit

# 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
```

Passaggio 4. Verificare che il client wireless che si desidera monitorare sia già associato a uno degli SSID e a uno degli AP a cui è stato assegnato il tag in cui è stato assegnato il profilo di join AP con le impostazioni di acquisizione dei pacchetti. In caso contrario, non sarà possibile avviare l'acquisizione.

> **Suggerimento**: se si desidera risolvere il problema relativo al motivo per cui un client non è in grado di connettersi a un SSID, è possibile connettersi a un SSID che funziona correttamente e quindi eseguire il roaming al SSID con errori, l'acquisizione segue il client e acquisisce tutte le relative attività.

GUI:

Selezionare **Monitoraggio > Wireless > Client**



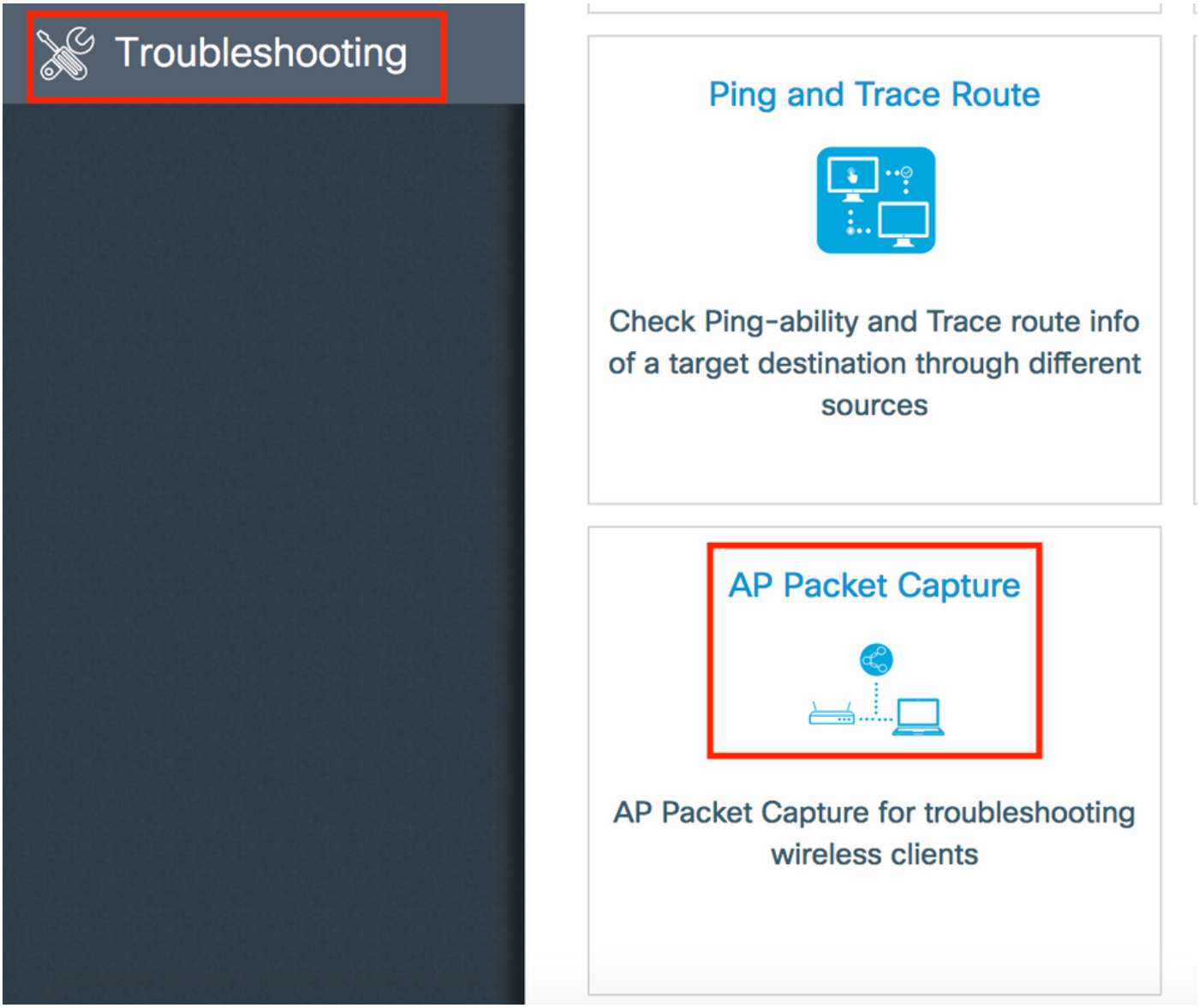

CLI:

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

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

Passaggio 5. Avviare l'acquisizione

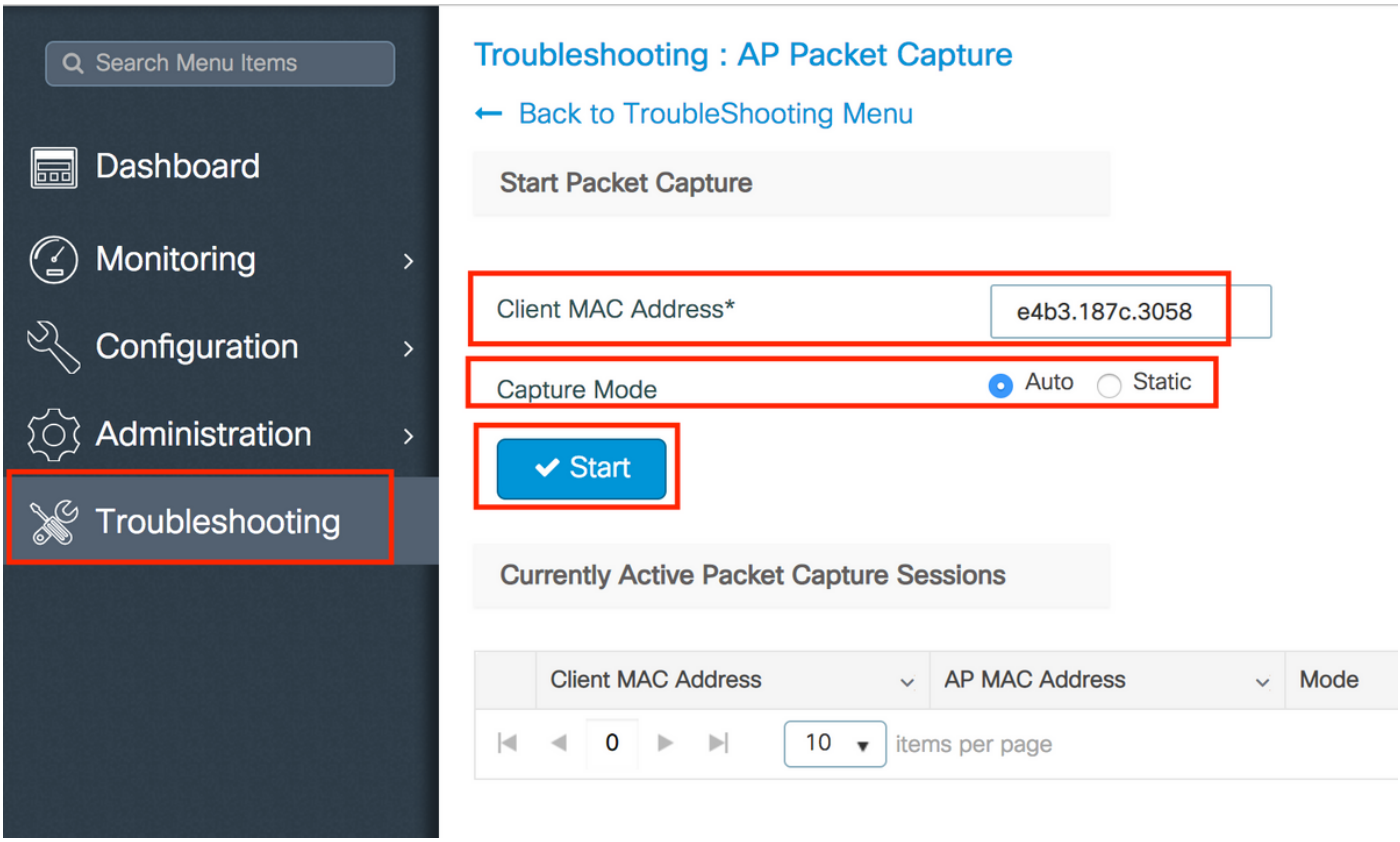
GUI:

Selezionare **Risoluzione dei problemi > Acquisizione pacchetti AP**

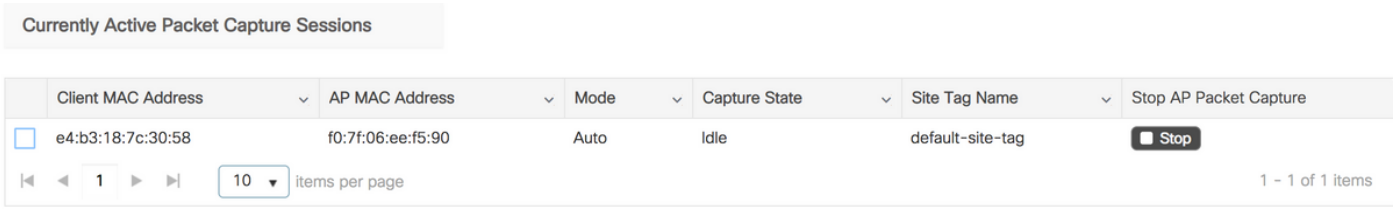



Immettere l'indirizzo MAC del client che si desidera monitorare e selezionare la **modalità di acquisizione. Auto** significa che ogni access point a cui si connette il client wireless crea automaticamente un nuovo file .pcap. **Static** consente di scegliere un access point specifico per monitorare il client wireless.

Avviare la cattura con **Start.**




Viene quindi visualizzato lo stato corrente dell'acquisizione:



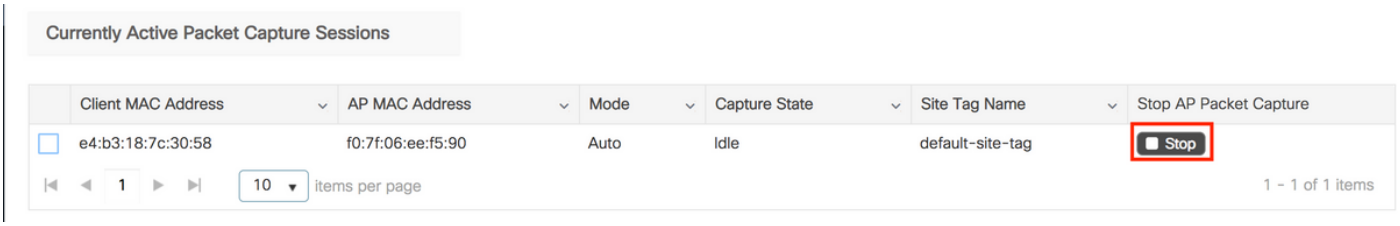

CLI:

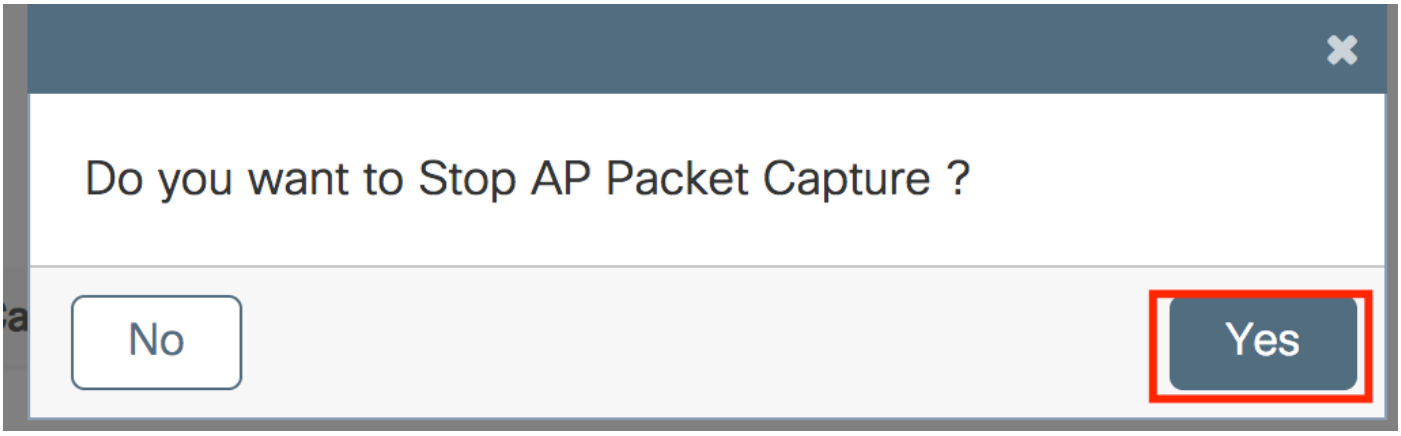
```
# ap packet-capture start <E4B3.187C.3058> auto
```

Passaggio 6. Interrompere l'acquisizione

Una volta acquisito il comportamento desiderato, arrestare l'acquisizione tramite GUI o CLI:

GUI:



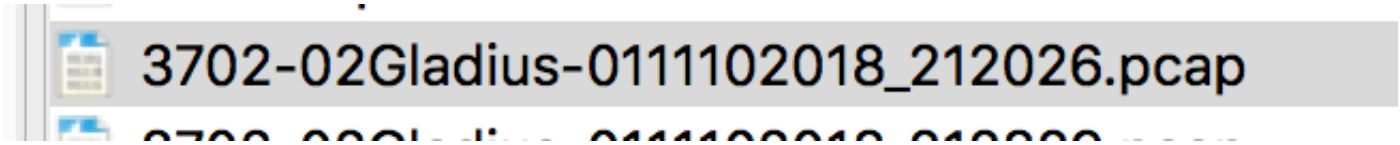



CLI:

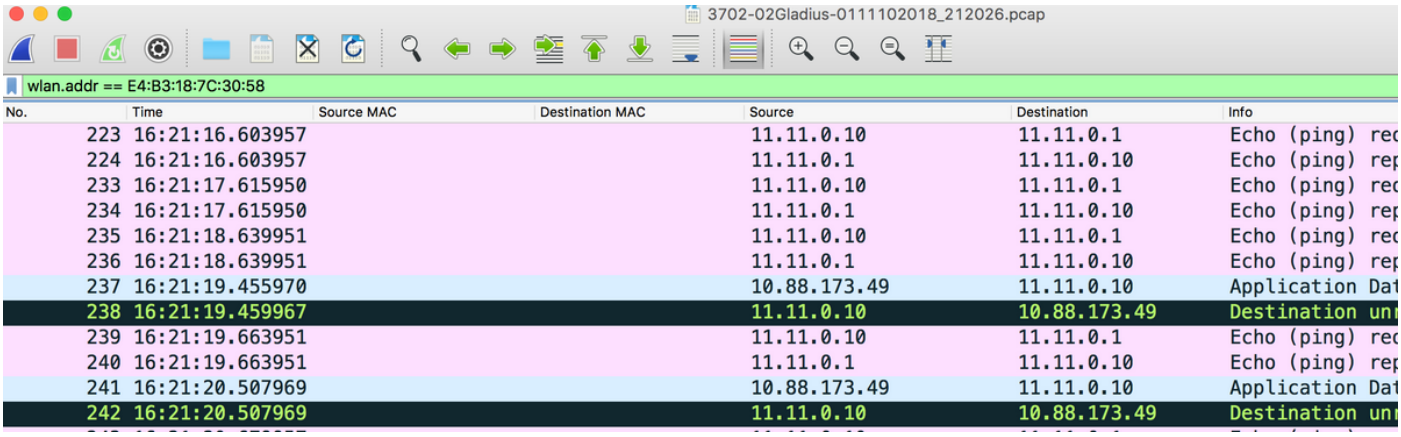
```
# ap packet-capture stop <E4B3.187C.3058> all
```

Passaggio 7. Raccogliere il file pcap dal server FTP

Il file con nome <ap-name><9800-wlc-name>-<##-file><day><month><year>_<hour><minute><second>.pcap




Passaggio 8. È possibile aprire il file con lo strumento di analisi dei pacchetti preferito.




# Verifica

Èpossibile utilizzare questi comandi per verificare la configurazione della funzione di acquisizione dei pacchetti.

```
# 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
```

# Risoluzione dei problemi

Per risolvere il problema, procedere come segue:

Passaggio 1. Abilitare la condizione di debug

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

Passaggio 2. Riprodurre il comportamento

Passaggio 3. Verificare il tempo del controller corrente per poter tenere traccia del tempo di accesso

```
# show clock
```

Passaggio 4. Raccogliere i registri

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

Passaggio 5. Ripristinare le impostazioni predefinite della condizione dei registri.

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

> **Nota**: dopo una sessione di risoluzione dei problemi è molto importante impostare nuovamente i livelli dei log per evitare la generazione di log non necessari.