Catalyst 9800 Wireless Controller에서 AP 패킷 캡처 구성

목차

소개

이 문서에서는 액세스 포인트(AP) 패킷 캡처 기능을 사용하는 방법에 대해 설명합니다.

배경 정보

이 기능은 Cisco IOS AP(예: AP 3702)에서만 사용할 수 있으므로 Cisco IOS XE 버전 17.3 이후에는 더 이상 사용되지 않습니다.

이 솔루션은 DNAC를 사용하는 Intelligent Capture로 대체되거나 AP를 스니퍼 모드로 설정하여 대안으로 사용됩니다.

AP Packet Capture 기능을 사용하면 적은 노력으로 공중으로 패킷 캡처를 수행할 수 있습니다. 이 기능이 활성화되면 AP에서 특정 무선 mac 주소로 보내고 받은 모든 지정된 무선 패킷 및 프레임의 복사본이 무선으로 특정 MAC 주소에서 보내고 받는 FTP(File Transfer Protocol) 서버로 전달됩니다. 여기서 파일을 .pcap 파일로 다운로드하고 원하는 패킷 분석 도구로 열 수 있습니다.

패킷 캡처가 시작되면 클라이언트가 연결된 AP가 FTP 서버에 새 .pcap 파일을 만듭니다(FTP 로그인에 대해 지정된 사용자 이름에 쓰기 권한이 있는지 확인). 클라이언트가 로밍하면 새 AP가 FTP 서버에 새 .pcap 파일을 만듭니다. 클라이언트가 SSID(Service Set Identifier) 사이를 이동할 경우, AP는 패킷 캡처를 계속 유지하므로 클라이언트가 새 SSID에 연결할 때 모든 관리 프레임을 볼 수 있습니다.

개방형 SSID(보안 없음)에서 캡처하는 경우 데이터 패킷의 내용을 볼 수 있지만 클라이언트가 보안 SSID(암호로 보호된 SSID 또는 802.1x 보안)에 연결된 경우 데이터 패킷의 데이터 부분이 암호화되며 일반 텍스트로 표시되지 않습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 무선 컨트롤러에 대한 CLI(Command Line Interface) 또는 GUI(Graphic User Interface) 액세스
- FTP 서버
- .pcap 파일

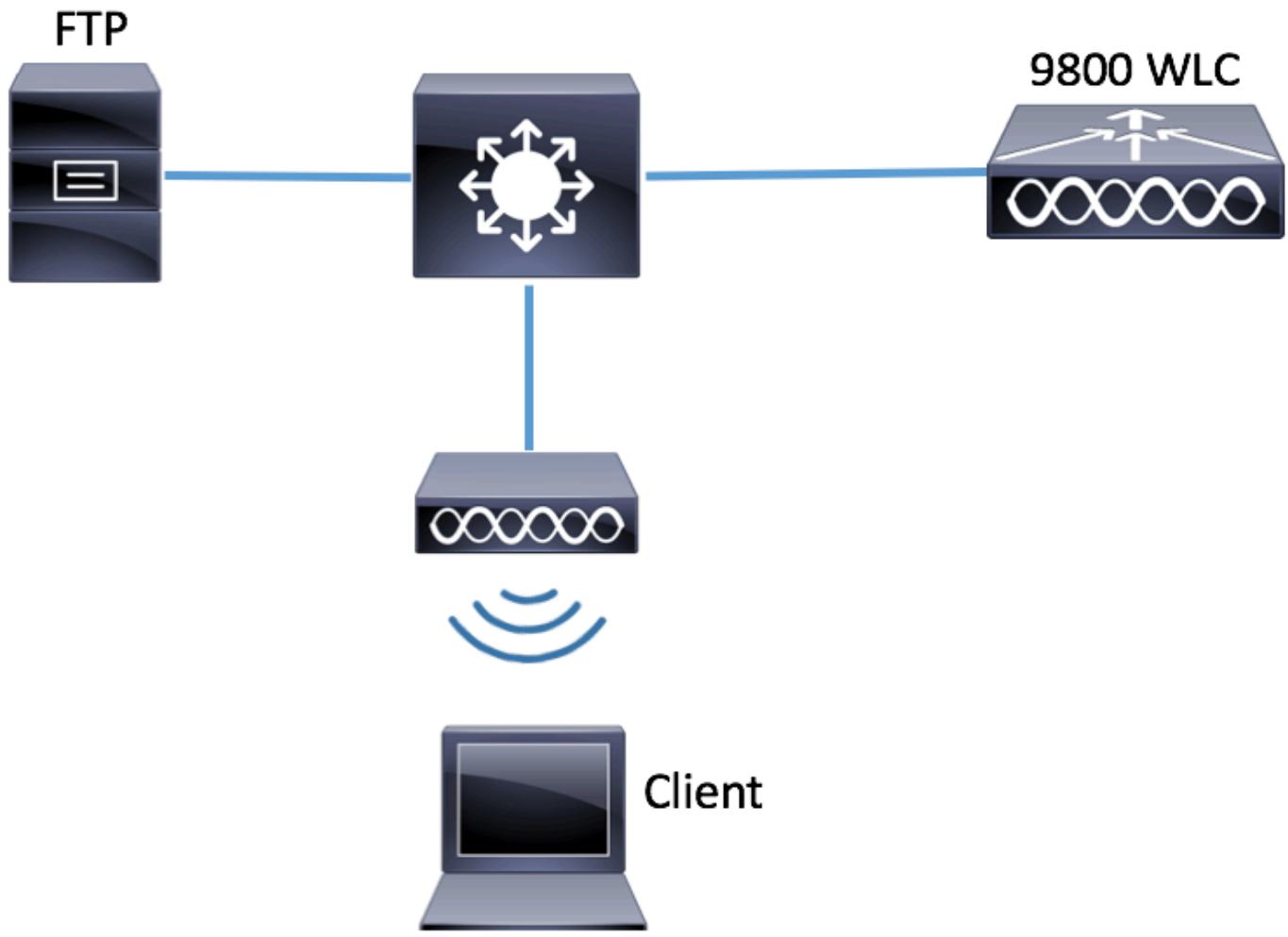
사용되는 구성 요소

- 9800 WLC v16.10
- AP 3700
- FTP 서버

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

설정

네트워크 다이어그램



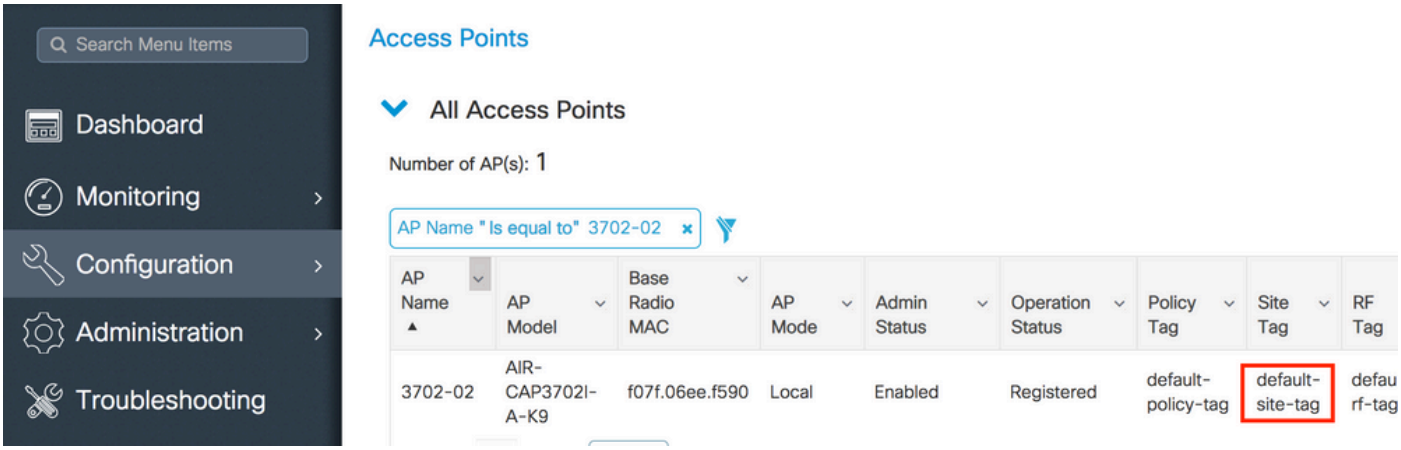
설정

컨피그레이션 전에 무선 클라이언트가 연결할 수 있는 AP를 선택합니다.

1단계. 무선 클라이언트가 연결에 사용할 수 있는 AP와 연결된 현재 사이트 태그를 확인합니다.

GUI:

Configuration(컨피그레이션) **> Wireless(무선) > Access Points(액세스 포인트)로 이동합니다**



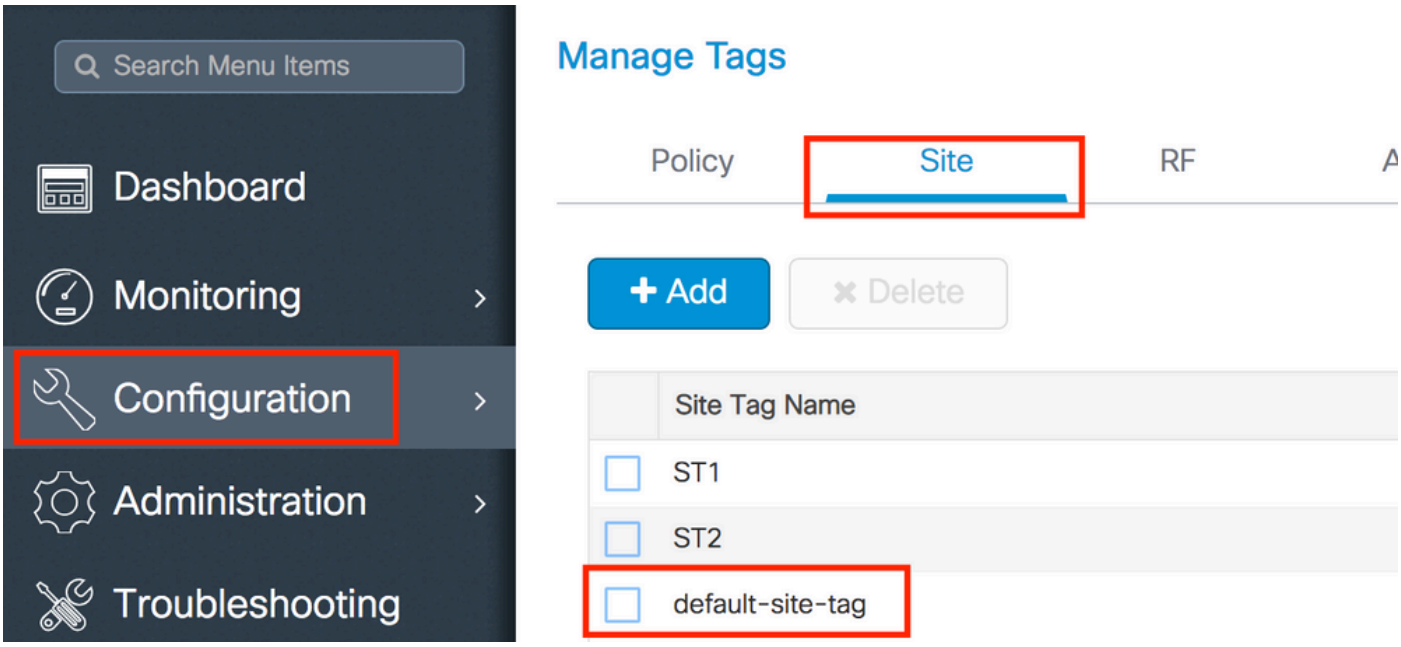
CLI:

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

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

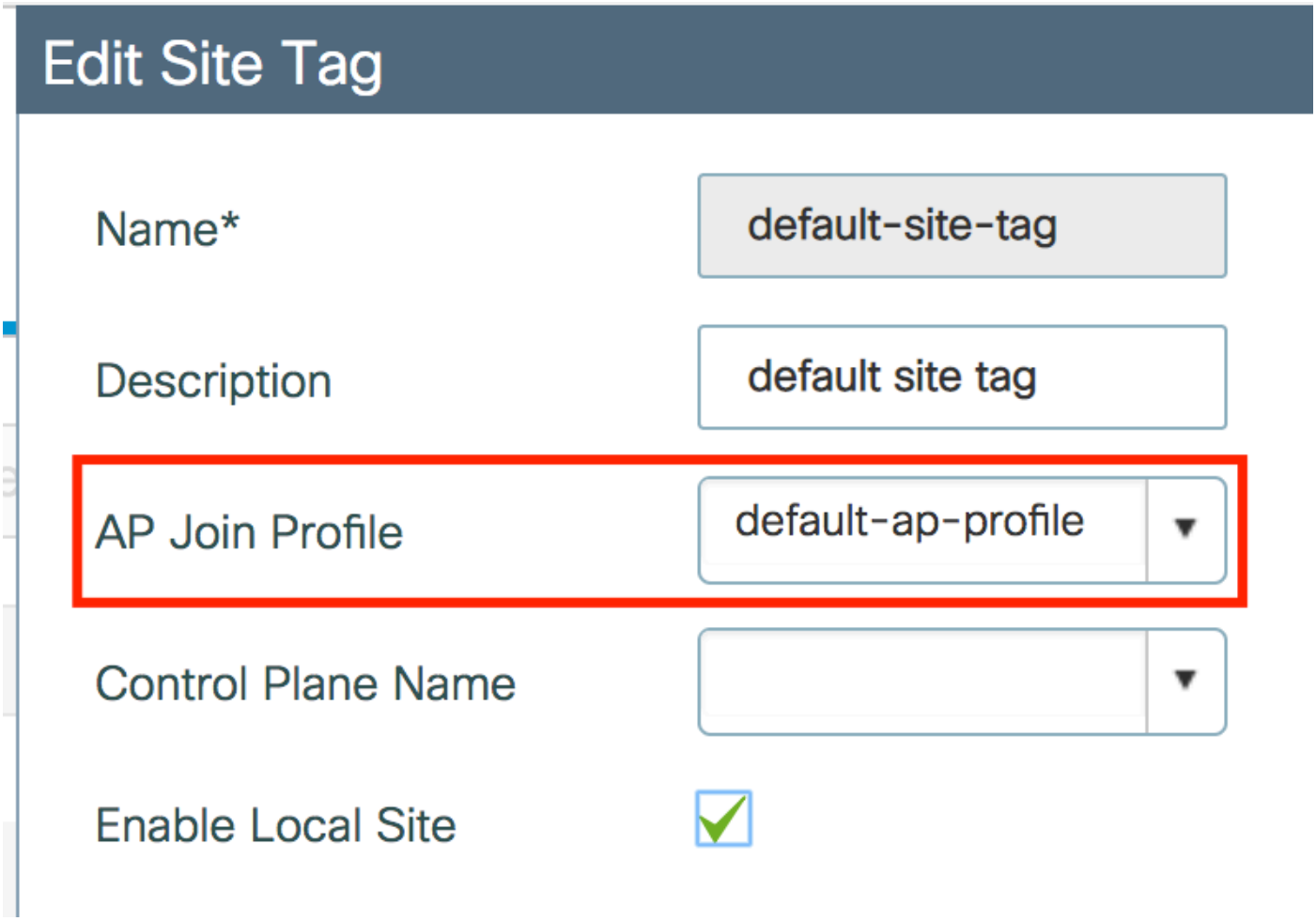
2단계. 해당 사이트 태그와 연결된 AP 가입 프로필을 확인합니다.

GUI:

Configuration(컨피그레이션) **> Tags & Profiles(태그 및 프로필) > Tags(태그) > Site(사이트) > Site Tag Name(사이트 태그 이름)으로 이동합니다.**



연결된 AP 가입 프로필을 확인합니다



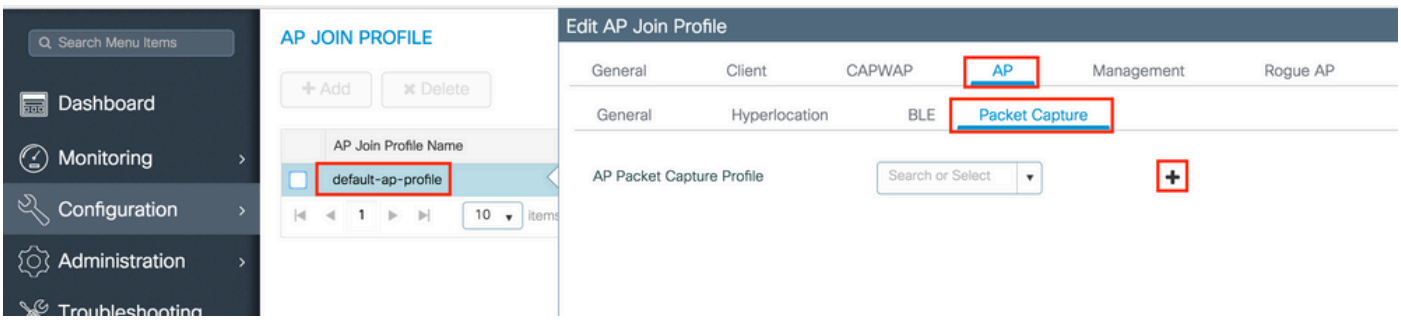
CLI:

```
# 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
```

3단계. AP 가입 프로필에 패킷 캡처 설정 추가

GUI:

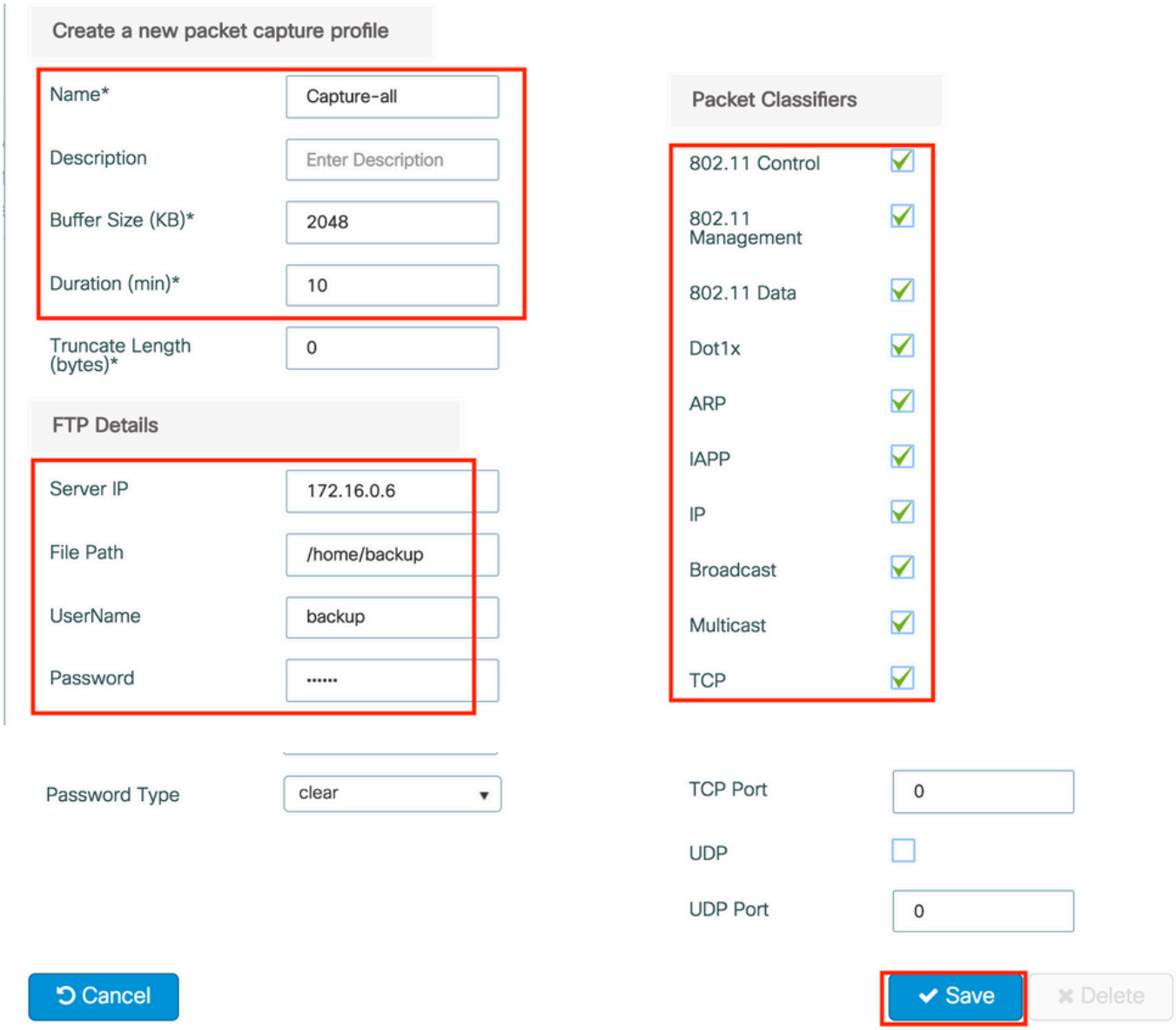
Configuration(컨피그레이션) > Tags & Profiles(태그 및 프로필) > AP Join(AP 조인) > AP Join Profile Name(AP 조인 프로필 이름) > AP > Packet Capture(패킷 캡처)로 이동하고 새 AP Packet Capture Profile(AP 패킷 캡처 프로필)을 추가합니다.



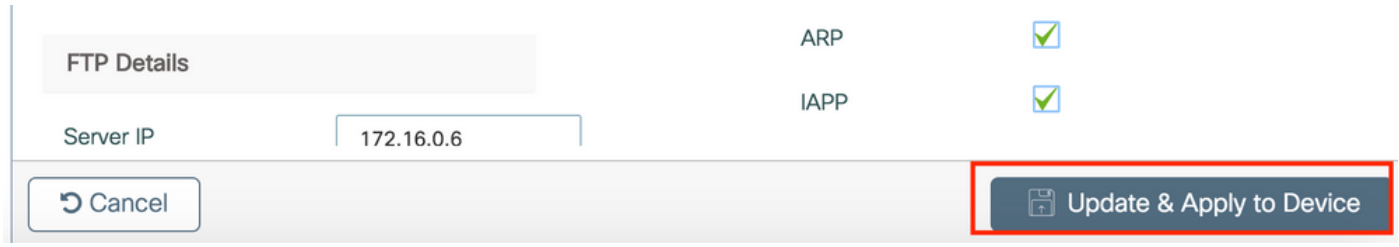
Name for the Packet Capture Profile(패킷 캡처 프로파일 이름)을 선택하고 AP가 패킷 캡처를 전송할 FTP 서버 세부사항을 입력합니다. 또한 모니터링할 패킷의 종류를 선택해야 합니다.

버퍼 크기 = 1024-4096

기간 = 1-60



캡처 프로필이 저장되면 Update & Apply to **Device를 클릭합니다.**



CLI:

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

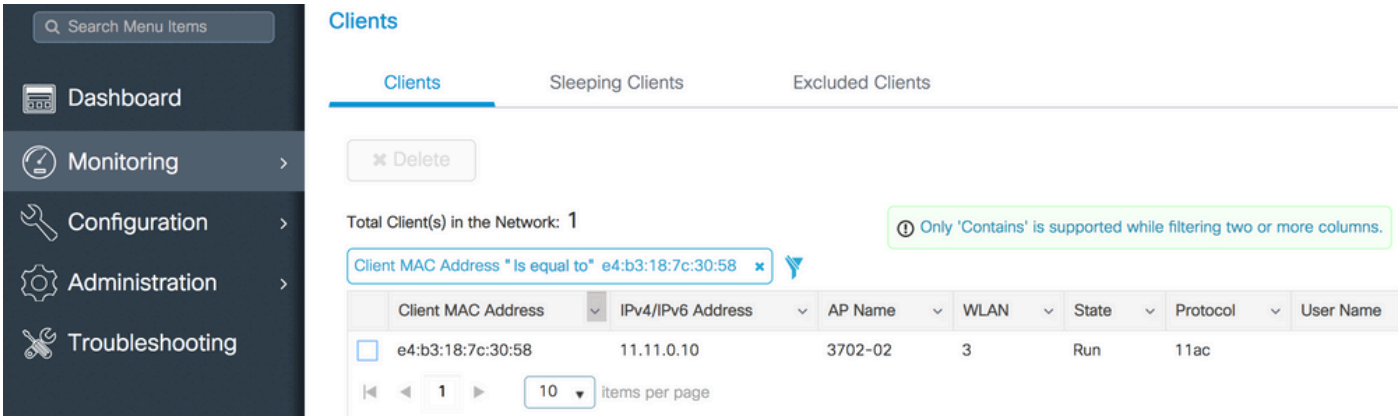
```
# classifier arp
# classifier broadcast
# classifier data
# classifier dot1x
# classifier iapp
# classifier ip
# classifier tcp
# ftp password 0 backup
# ftp path /home/backup
# ftp serverip 172.16.0.6
# ftp username backup
# exit

# 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
```

4단계. 모니터링할 무선 클라이언트가 SSID 및 AP 가입 프로필과 패킷 캡처 설정이 할당된 태그를 할당한 AP 중 하나에 이미 연결되어 있는지 확인합니다. 그렇지 않으면 캡처를 시작할 수 없습니다.

> **팁**: 클라이언트가 SSID에 연결할 수 없는 이유를 트러블슈팅하려면 정상적으로 작동하는 SSID에 연결한 다음 오류가 발생한 SSID로 로밍하면 캡처는 클라이언트를 따르고 모든 활동을 캡처합니다.

GUI:

Monitoring(**모니터링) > Wireless(무선) > Clients(클라이언트)로 이동합니다.**



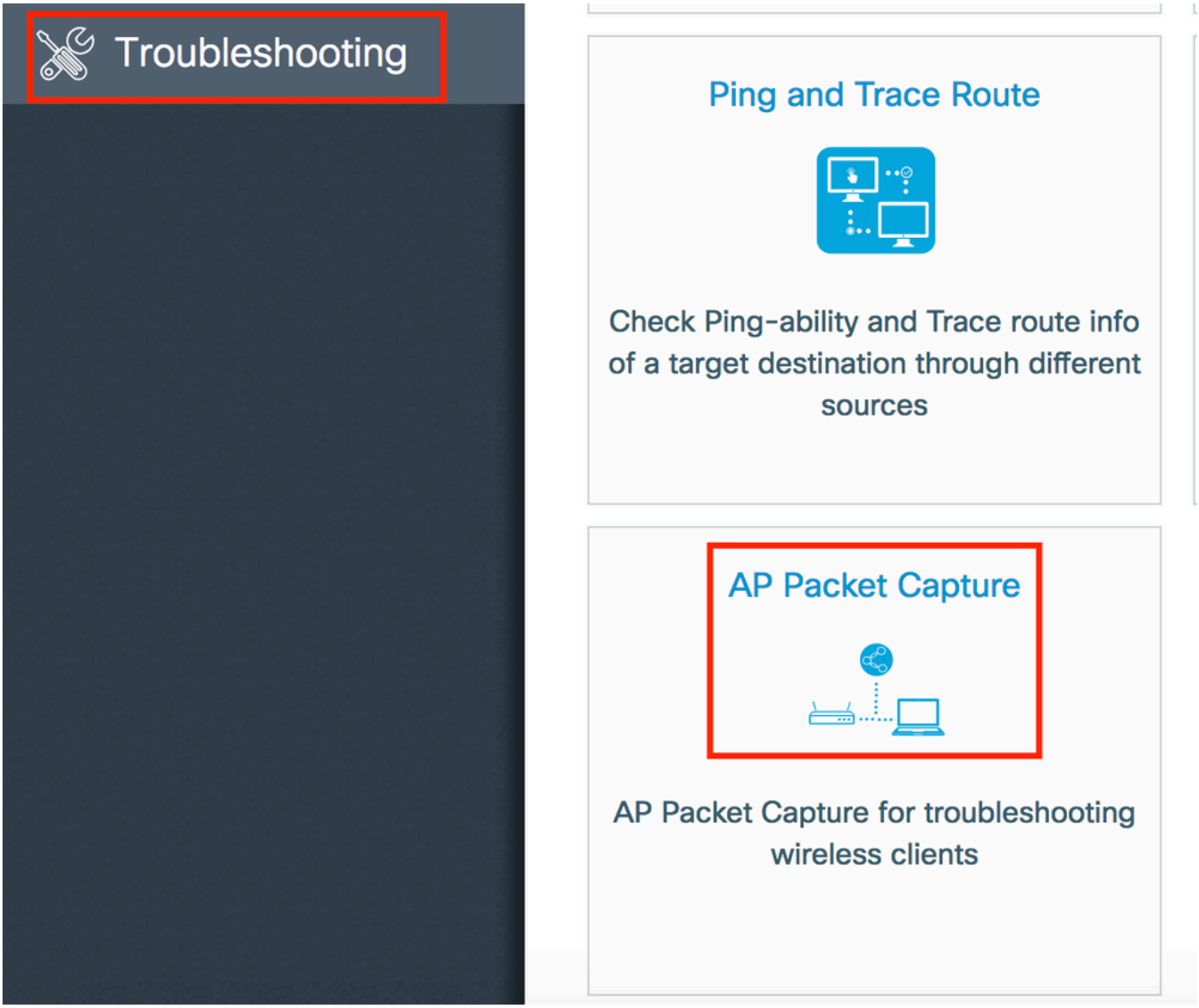
CLI:

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

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

5단계. 캡처 시작

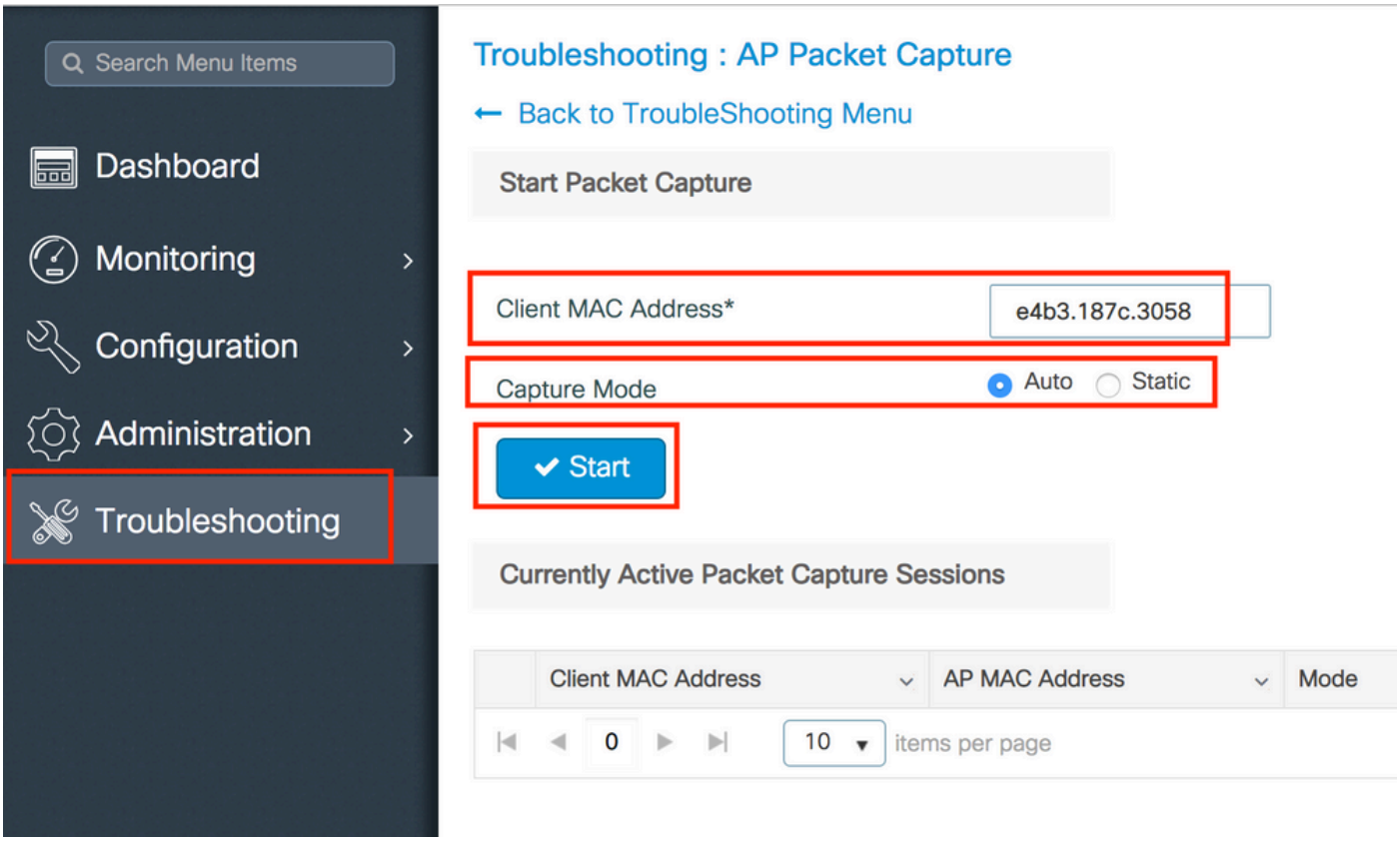
GUI:

Troubleshooting(문제 해결) **> AP Packet Capture(AP 패킷 캡처)로 이동합니다.**

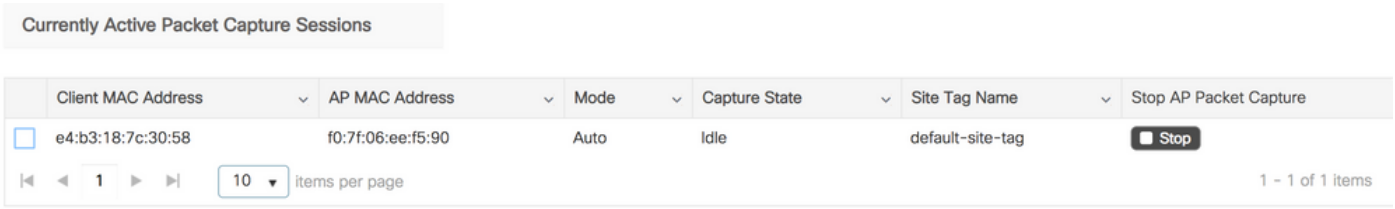


모니터링할 클라이언트의 mac 주소를 입력하고 Capture Mode(**캡처 모드**)를 **선택합니다. Auto**는 무선 클라이언트가 연결되는 모든 AP가 새 .pcap 파일을 자동으로 생성함을 의미합니다. **Static**을 사용하면 무선 클라이언트를 모니터링할 특정 AP를 선택할 수 있습니다.

Start(시작)로 캡처를 **시작합니다.**



그런 다음 캡처의 현재 상태를 볼 수 있습니다.



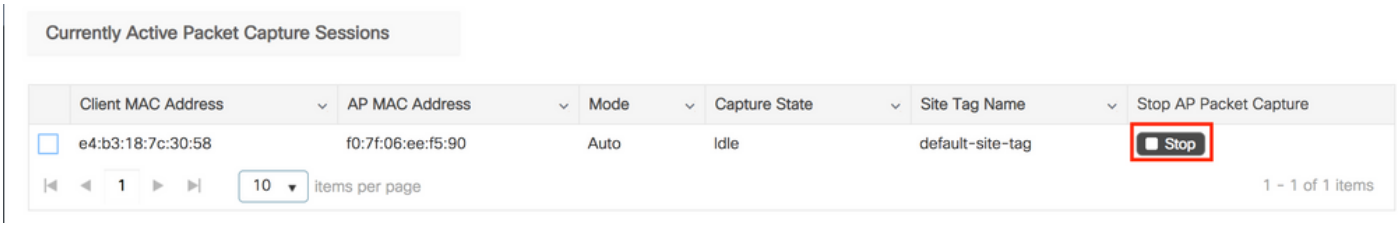
CLI:

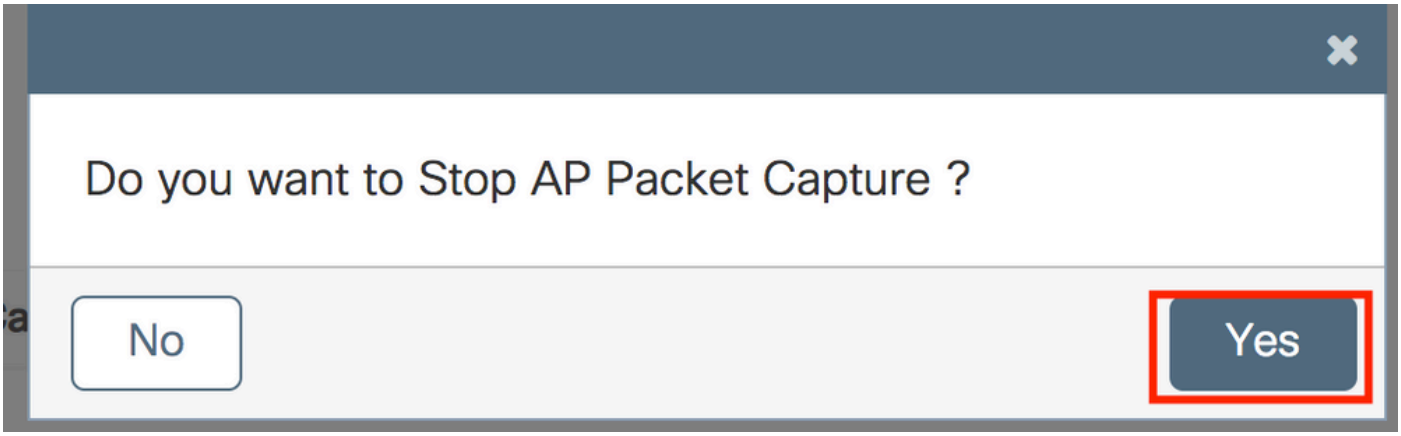
```
# ap packet-capture start <E4B3.187C.3058> auto
```

6단계. 캡처 중지

원하는 동작이 캡처되면 GUI 또는 CLI에서 캡처를 중지합니다.

GUI:



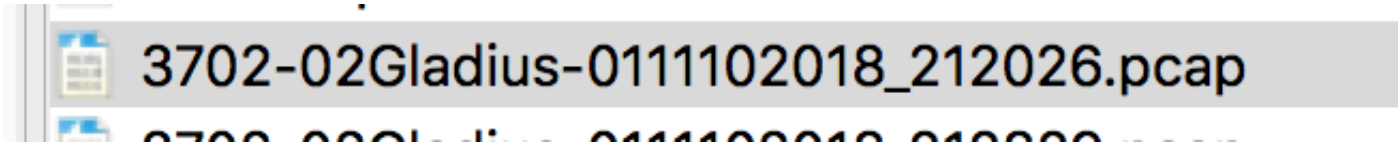


CLI:

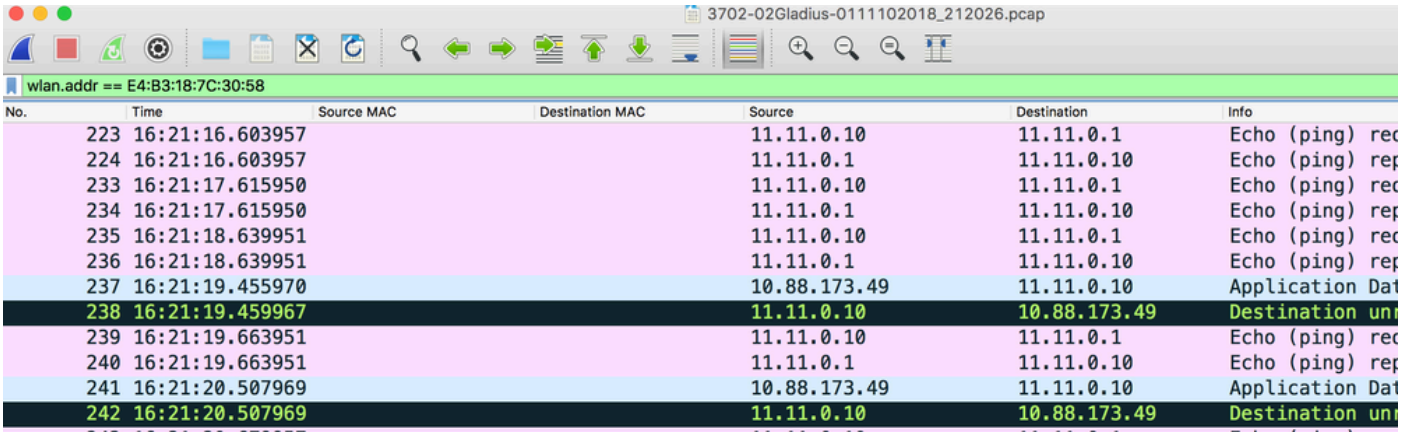
```
# ap packet-capture stop <E4B3.187C.3058> all
```

7단계. FTP 서버에서 .pcap 파일 수집

이름이 <ap-name><9800-wlc-name>-<##-file><day><month><year>_<hour><minute><second>.pcap인 파일을 찾아야 합니다.



8단계. 기본 설정 패킷 분석 도구로 파일을 열 수 있습니다.



다음을 확인합니다.

이러한 명령을 사용하여 패킷 캡처 기능의 컨피그레이션을 확인할 수 있습니다.

```
# 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
```

문제 해결

다음 단계에 따라 이 기능을 트러블슈팅할 수 있습니다.

1단계. 디버그 조건 활성화

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

2단계. 동작 재현

3단계. 현재 컨트롤러 시간을 확인하여 로그를 시간 내에 추적할 수 있습니다.

```
# show clock
```

4단계. 로그 수집

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

5단계. 로그 조건을 기본값으로 다시 설정합니다.

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

> **참고**: 문제 해결 세션 후에는 불필요한 로그가 생성되지 않도록 로그 레벨을 다시 설정하는 것이 매우 중요합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.