WAP125에서 패킷 캡처 구성

목표

패킷 캡처 기능을 사용하면 WAP(Wireless Access Point)에서 수신 및 전송된 패킷을 캡처하고 저장할 수 있습니다. 그런 다음 네트워크 프로토콜 분석기가 캡처된 패킷을 분석하여 문제 해결 또는 성능 최적화를 수행할 수 있습니다.패킷 캡처 방법에는 두 가지가 있습니다.

- 이 디바이스에 파일 저장 — 캡처된 패킷은 WAP의 파일에 저장됩니다.WAP는 파일을 TFTP(Trivial File Transport Protocol) 서버로 전송할 수도 있습니다.파일 관리 패킷 캡처는 pcap 형식으로 포맷되며 Wireshark 및 OmniPeek와 같은 도구를 사용하여 검사할 수 있습니다.
- 원격 호스트로 스트림 — 캡처된 패킷은 Wireshark 툴을 실행하는 외부 컴퓨터로 실시간으로 리디렉션됩니다.

이 문서는 WAP에서 패킷 캡처를 구성하고 이러한 패킷 캡처를 로컬에서 또는 원격으로 받는 방법에 대해 설명하고 안내하는 데 목적이 있습니다.

적용 가능한 디바이스

- WAP125

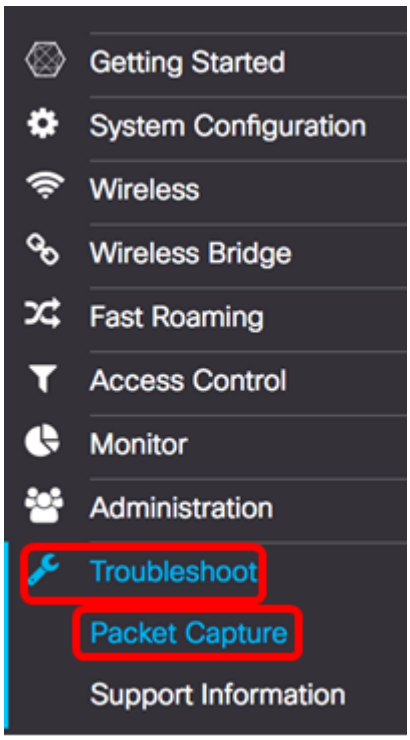
소프트웨어 버전

- 1.0.0.3

패킷 캡처 구성

패킷 캡처 설정 구성

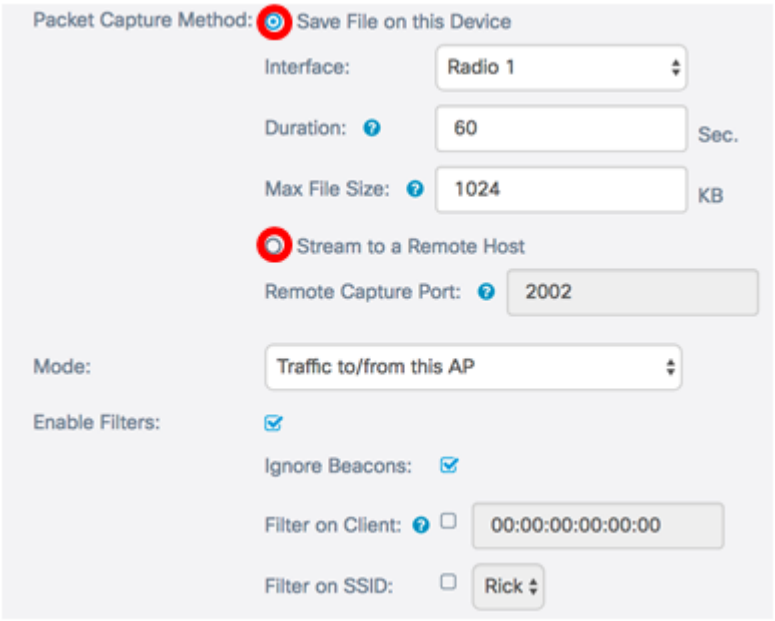
1단계. 웹 기반 유틸리티에 로그인하고 Troubleshoot(문제 해결) **> Packet Capture(패킷 캡처)를** 선택합니다.



2단계. 다음 패킷 캡처 방법 라디오 버튼 중 하나를 선택합니다.

- 이 장치에 파일 저장 — 캡처된 패킷을 WAP의 파일로 저장합니다.로컬로 저장할 인터페이스, 기간 및 최대 파일 크기를 구성합니다.
- 원격 호스트로 스트림 — 캡처된 패킷을 실시간으로 네트워크 프로토콜 분석기 툴을 실행하는 외부 컴퓨터로 리디렉션합니다.이 옵션을 선택한 경우 6단계로 건너뜁니다.

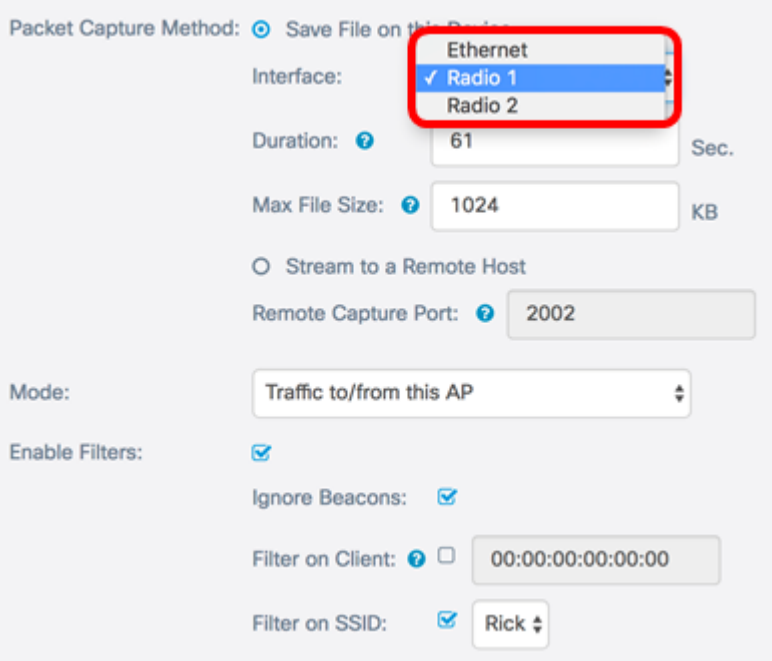
참고:이 예에서는 이 장치에 파일 저장을 선택합니다.



3단계. Interface 드롭다운 목록에서 Capture Interface 드롭다운 목록에서 패킷을 캡처할 인터페이스를 선택합니다.옵션은 다음과 같습니다.

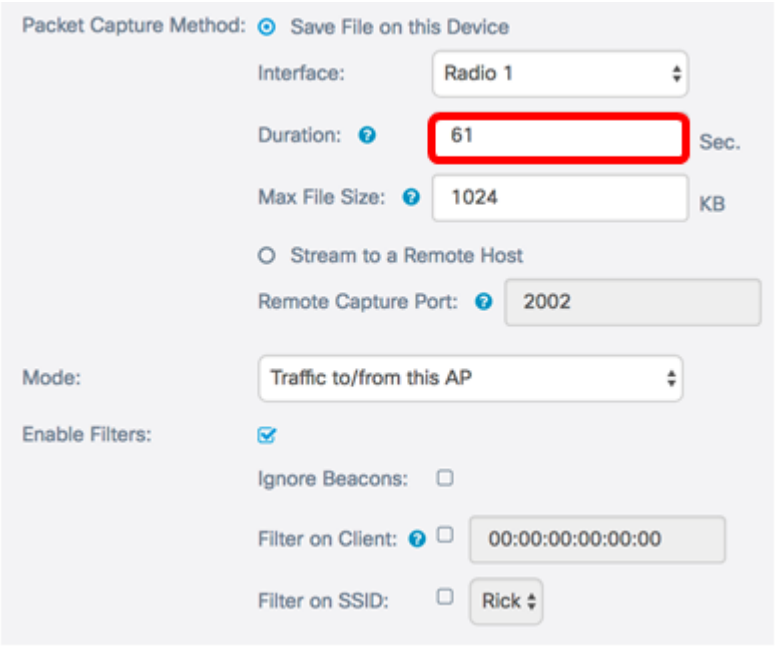
- 이더넷 — 이더넷 포트의 802.3 트래픽.
- 라디오 1 — 라디오 인터페이스 1의 802.11 트래픽.
- 무선 2 — 무선 인터페이스 2의 802.11 트래픽.

참고:이 예에서는 라디오 1이 선택됩니다.

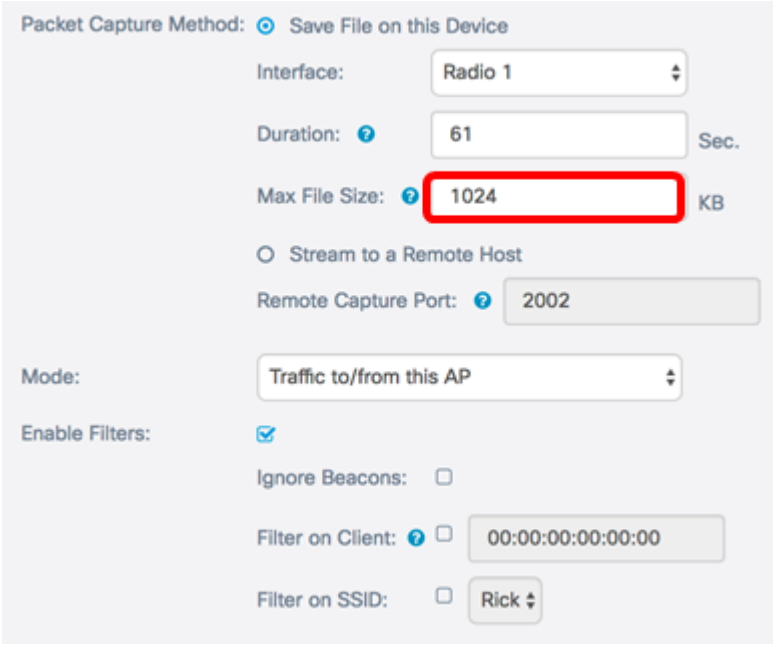


4단계. Duration(기간) 필드에 10~3600초 범위의 캡처 기간을 입력합니다.기본값은 60초입니다.

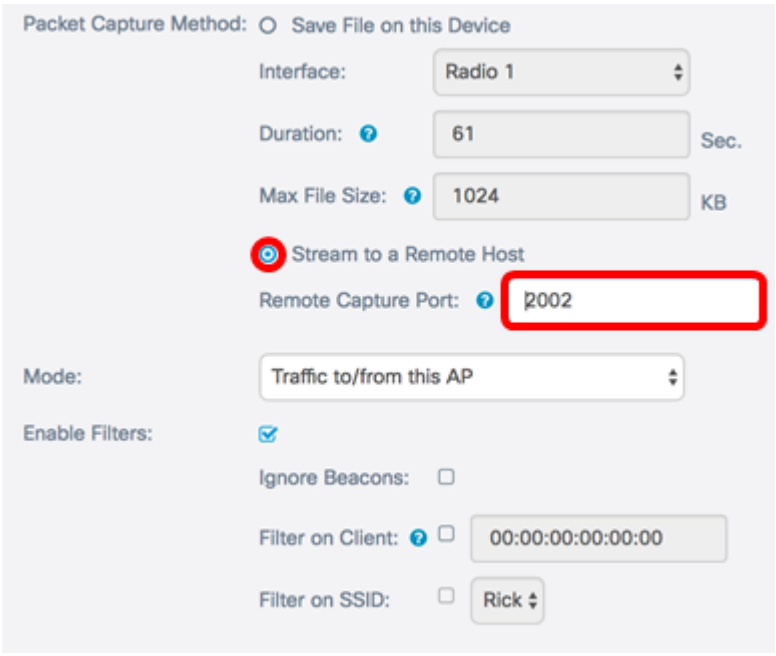
참고:이 예에서는 61이 사용됩니다.



5단계. *Max File Size*(최대 파일 크기) 필드에 64~4096KB 범위의 최대 캡처 파일 크기를 입력합니다.기본값은 1024KB입니다.

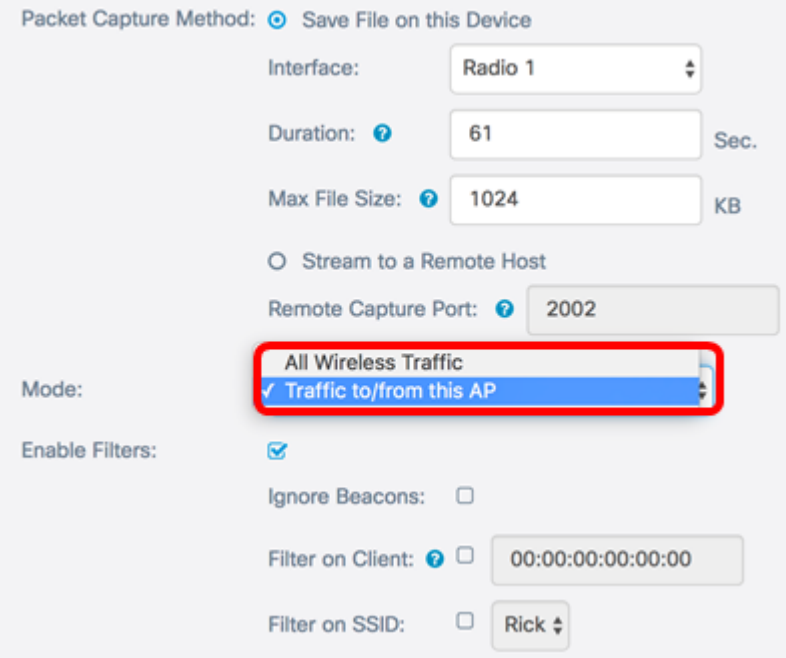


6단계. 원격 패킷 캡처 방법을 선택한 경우 *Remote Capture Port* 필드에 1~65530 범위의 포트 번호를 입력합니다.기본값은 2002입니다.

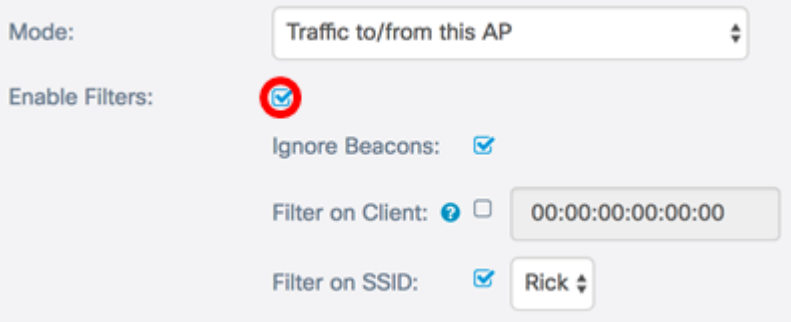


7단계. Mode 드롭다운 목록에서 캡처할 패킷을 선택합니다.옵션은 다음과 같습니다.

- All Wireless Traffic(모든 무선 트래픽) - 다른 네트워크에서 전송되는 무선 패킷을 포함하여 모든 무선 패킷을 캡처합니다.
- 이 AP를 오가는 트래픽 — WAP와 클라이언트 간에 전송되는 패킷을 캡처합니다.

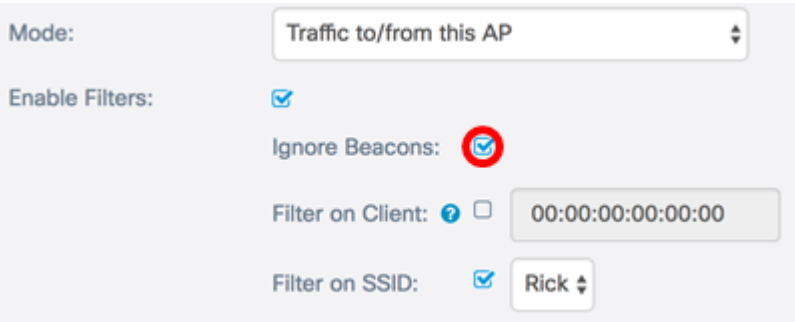


8단계. Enable Filters(필터 **활성화)** 확인란을 선택하여 패킷 캡처에 대한 특정 필터를 허용합니다.



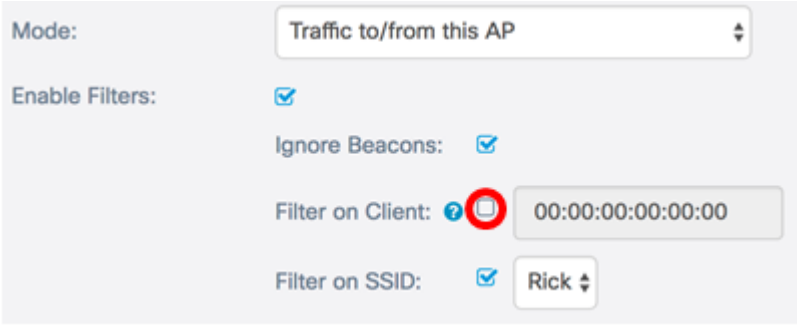
9단계. (선택 사항) 무선이 탐지하거나 전송하는 802.11 신호의 캡처를 비활성화하려면 신호 무시 확인란을 선택합니다.비컨 프레임은 주기적으로 전송되어 WLAN(Wireless Local Area Network)이 있음을 알립니다.

참고:이 예에서는 신호 무시가 활성화됩니다.



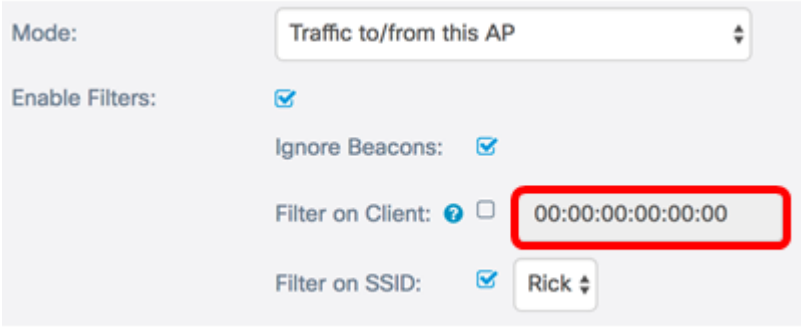
10단계. (선택 사항) Filter on Client 확인란을 선택하여 무선 클라이언트의 MAC 주소를 지정합니다.

참고:이 예에서는 Filter on Client(클라이언트의 필터)가 선택되지 않았습니다.

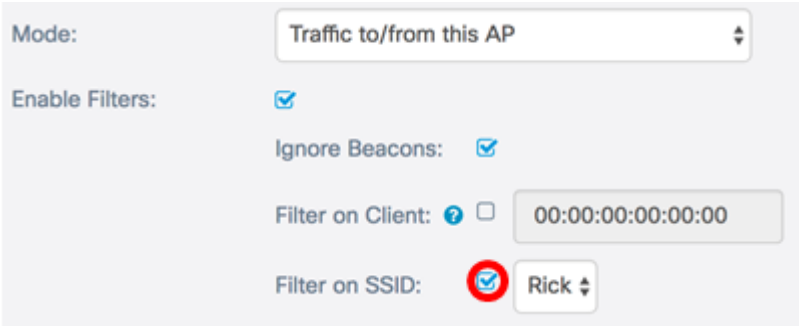


11단계. (선택 사항) Filter on Client(클라이언트의 *필터*) 필드에 클라이언트의 MAC 주소를 입력합니다.

참고:이는 무선 인터페이스에서 패킷 캡처를 수행하는 경우에만 활성화됩니다.

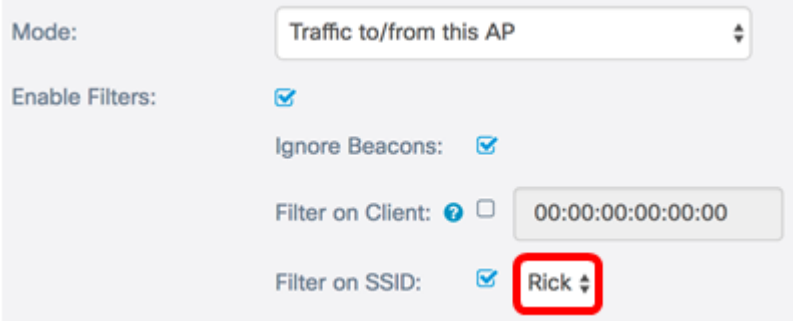


12단계. Filter **on SSID** 확인란을 선택하여 특정 SSID의 패킷을 캡처합니다.



13단계. SSID 드롭다운 목록에서 패킷을 캡처할 SSID를 선택합니다.

참고:드롭다운 목록에 표시되는 SSID는 선택한 인터페이스 및 구성된 SSID 수에 따라 달라집니다.이 예에서는 Rick이 선택됩니다.

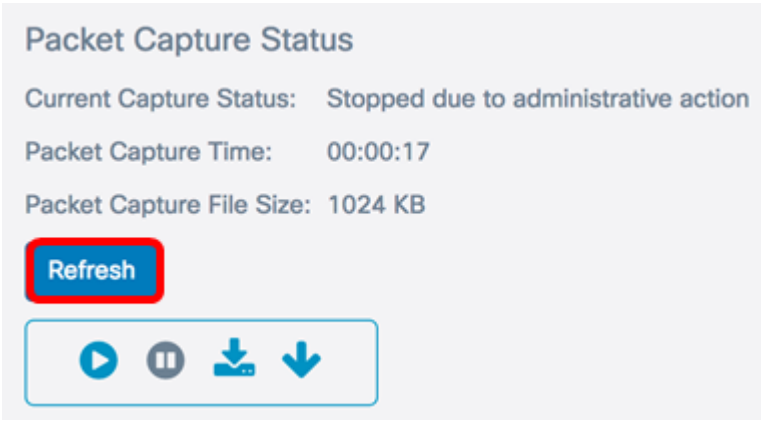


14단계. 을 클릭합니다 Save.

이제 Packet Capture 설정을 성공적으로 구성했어야 합니다.

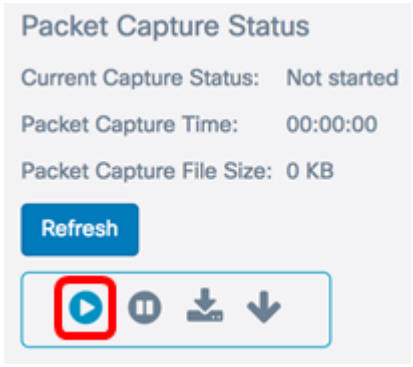
패킷 캡처

15단계. Packet *Capture Status* 영역에는 다음 정보가 포함됩니다.현재 상태를 보려면 **Refresh**(새로 고침)를 클릭합니다.

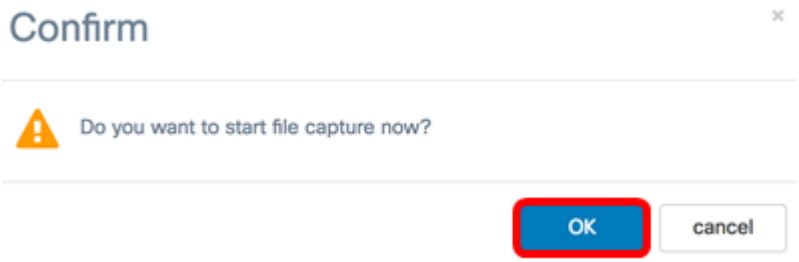


- 현재 캡처 상태 — 현재 패킷 캡처 상태를 표시합니다.이 예에서는 "관리 작업으로 인해 중지됨 "이 현재 상태입니다.
- 패킷 캡처 시간 — 패킷이 캡처되는 기간을 표시합니다.이 예에서는 00:00:17초가 기록되었습니다.
- Packet Capture File Size — 패킷 캡처 파일의 크기를 표시합니다.이 예에서 1024kb는 캡처 크기입니다.

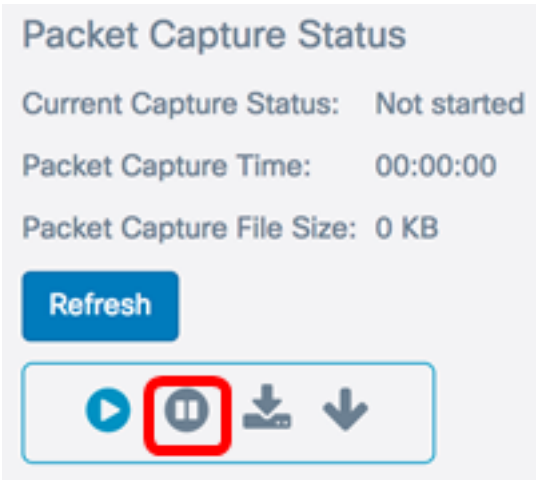
16단계. **Start Capture(캡처 시작)** 버튼을 클릭하여 패킷 캡처 프로세스를 시작합니다.



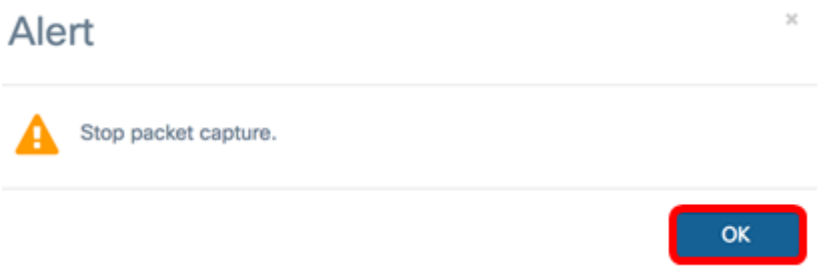
17단계. 이제 *패킷 캡처*가 시작됨을 알리는 창이 나타납니다.OK(**확인**)를 클릭하여 계속합니다.



18단계. Stop **Capture(캡처 중지)** 버튼을 클릭하여 패킷 캡처 프로세스를 중지합니다.



19단계. 패킷 캡처를 종료할지 확인하는 창이 나타납니다.계속하려면 **확인**을 클릭합니다.

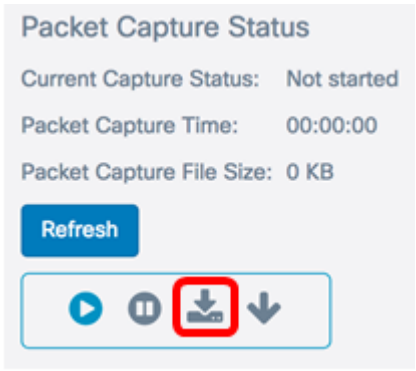


이제 WAP125에서 성공적으로 패킷을 캡처해야 합니다.

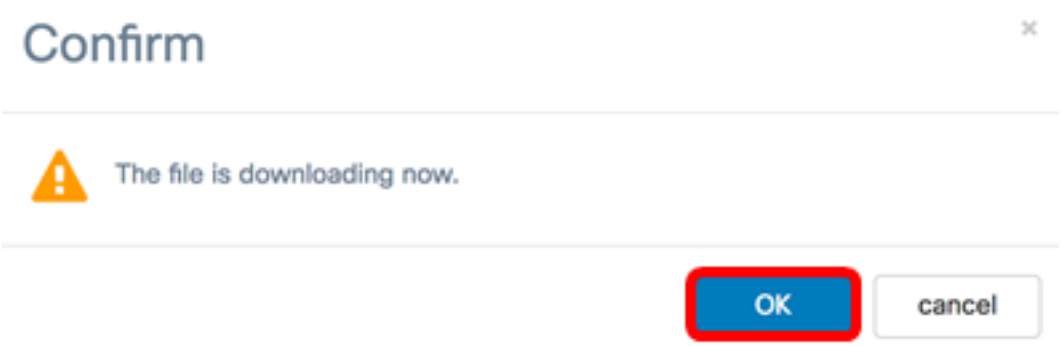
패킷 캡처 파일 다운로드

이 장치에 다운로드

1단계. **Download** to this Device 버튼을 클릭합니다.

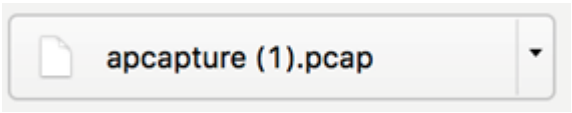


2단계. 다운로드가 시작되는 창이 나타납니다.OK(**확인**)**를** 클릭합니다.



다운로드가 완료되면 다운로드한 파일이 브라우저 다운로드 기록에 나타납니다.파일은 HTTP/HTTPS로 다운로드되며 파일 형식은 .pcap입니다.

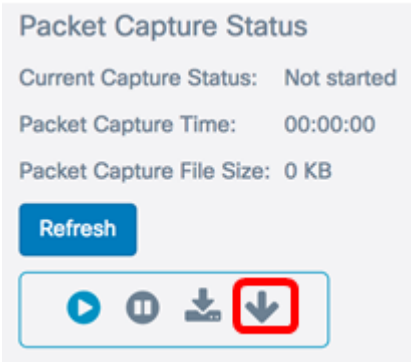
참고:이 예에서 apcapture(1).pcap은 다운로드한 파일입니다.



WAP125에서 패킷 캡처 파일을 성공적으로 다운로드했습니다.

TFTP 서버에 다운로드

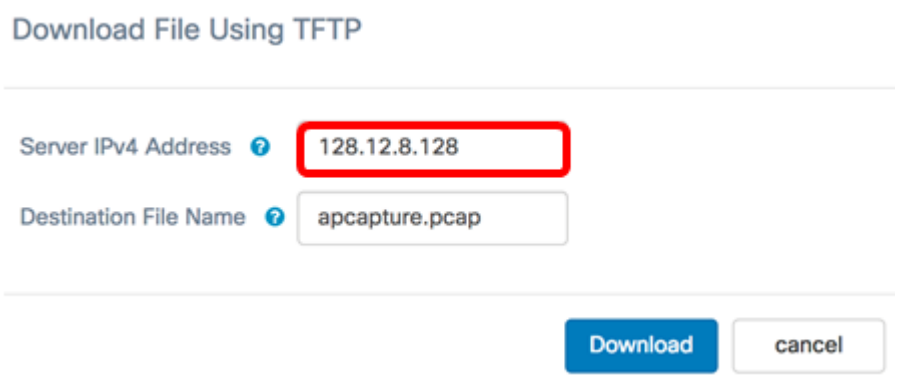
1단계. (선택 사항) 캡처된 파일을 TFTP 서버에서 다운로드해야 하는 경우 **Download to TFTP** Server(TFTP 서버로 다운로드) 버튼을 클릭합니다.



클릭하면 Server IPv4 Address(서버 IPv4 주소) 필드와 Destination File Name(대상 파일 이름) 필드가 있는 창이 나타납니다.

2단계. Server IPv4 Address 필드에 TFTP 서버의 IPv4 주소를 입력합니다.6단계의 *Remote Capture Port* 필드에 입력한 포트 번호가 TFTP 서버 주소에 연결됩니다.

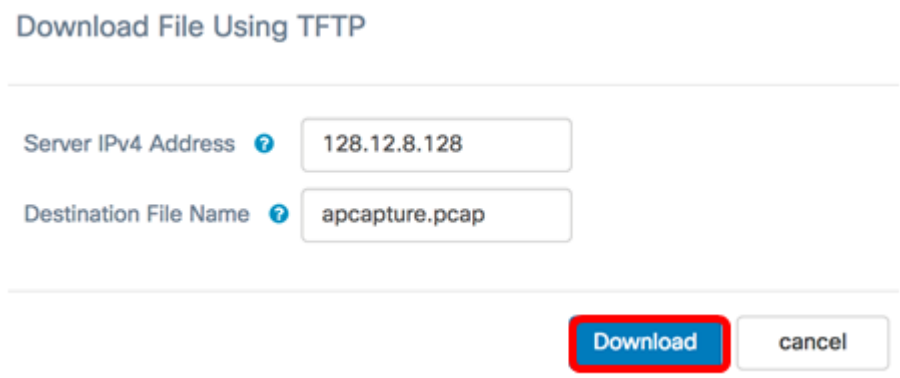
참고:이 예에서는 128.12.8.128이 사용됩니다.



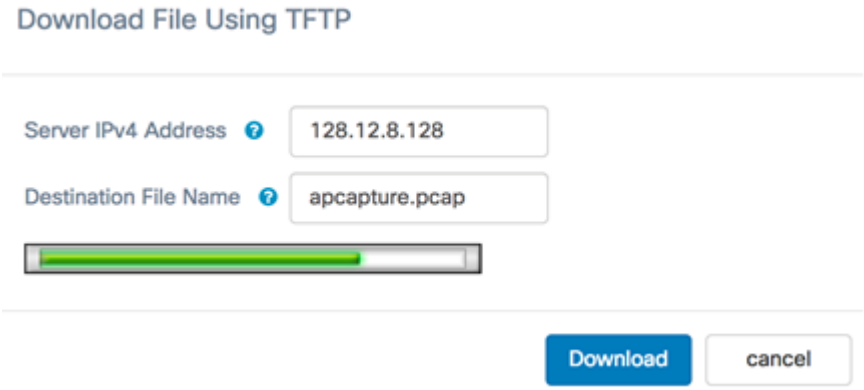
3단계. *대상 파일 이름* 필드에 pcap 형식으로 파일 이름을 입력합니다.

참고:이 예에서는 apcapture.pcap이 사용됩니다.

4단계. **다운로드**를 클릭합니다.



Destination File Name 필드 아래에 진행률 표시줄이 나타납니다.



이제 TFTP 서버를 통해 패킷 캡처 파일을 다운로드해야 합니다.