Wave 2 및 Wifi 6 AP에서 내부 유선 패킷 캡처 구성

목차

소개

이 문서에서는 TFTP(Trivial File Transfer Protocol) 서버가 있는 AP(Access Point) CLI(Command Line Interface)에서 내부 유선 PCAP(Packet Capture)를 수집하는 방법에 대해 설명합니다.

기고자: Jasia Ahsan, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SSH(Secure Shell) 또는 콘솔 액세스를 통해 AP에 대한 CLI 액세스
- TFTP 서버
- .PCAP 파일

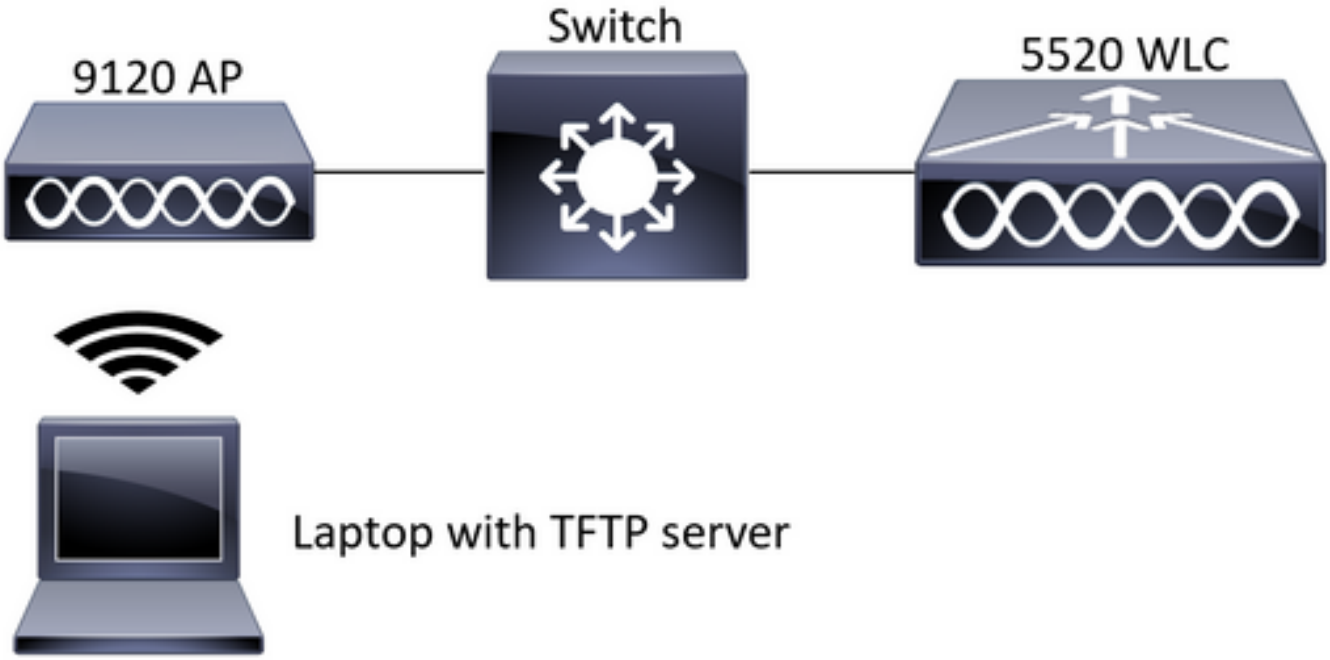
사용되는 구성 요소

- 8.10.112 코드의 5520 WLC(Wireless Lan Controller)
- AP 9120AXI
- TFTP 서버

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

구성

네트워크 다이어그램



구성

AP에 대한 SSH를 사용하여 PCAP 컨피그레이션이 완료되었습니다.IP, TCP 및 UDP를 선택할 수 있는 트래픽 유형은 세 가지가 있습니다.이 경우 IP 트래픽이 선택되었습니다.

1단계. SSH를 사용하여 AP CLI에 로그인합니다.

2단계. IP 트래픽용 PCAP를 시작하고 이 명령을 실행합니다.

CLI:

```
# debug traffic wired ip capture % Writing packets to "/tmp/pcap/2802_capture.pcap0" #reading
from file /dev/click_wired_log, link-type EN10MB (Ethernet)
```

3단계. 출력이 /tmp/pcap 폴더의 파일에 기록되고 AP 이름이 pcap 파일에 추가됩니다.

4단계. IP 트래픽을 캡처하기 위해 ping 테스트를 시작합니다.

CLI:

```
#ping 10.201.236.91 Sending 5, 100-byte ICMP Echos to 10.201.236.91, timeout is 2 seconds !!!!!
```

5단계. 캡처를 중지합니다.

CLI:

```
#no debug traffic wired ip capture
```

6단계. 파일을 tftp 서버에 복사합니다.

CLI:

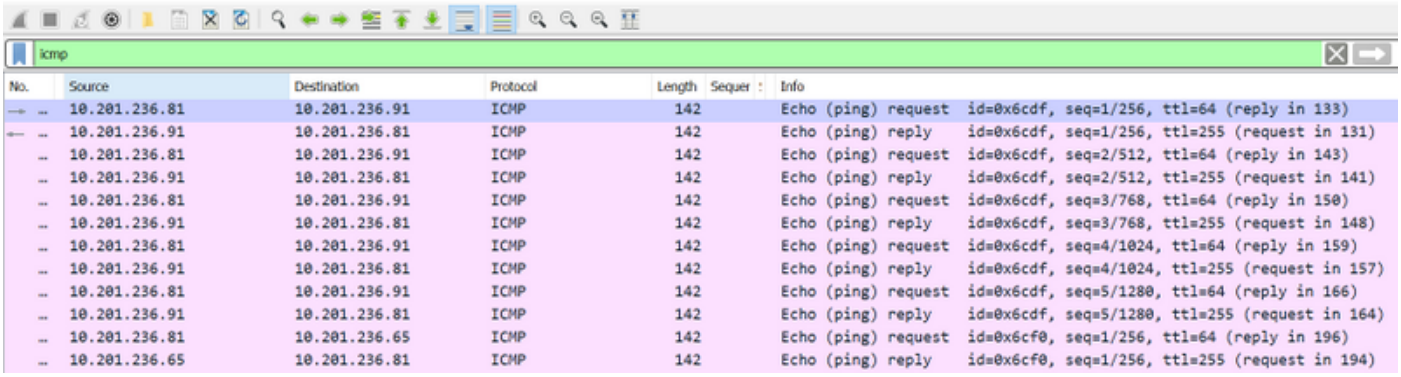
```
# copy pcap 2802_capture.pcap0 tftp: 10.201.236.33
##################################################################################################
##################################################### 100.0%
```

참고:tftp 서버 ip 주소 앞에 공백이 있습니다.

다음을 확인합니다.

패킷 분석 도구로 파일을 엽니다.Wireshark는 이 파일을 여는 데 사용됩니다.

Ping 테스트 결과는 이미지에서 확인할 수 있습니다.



icmp

No.	Source	Destination	Protocol	Length	Sequer	Info
→	10.201.236.81	10.201.236.91	ICMP	142		Echo (ping) request id=0x6cdf, seq=1/256, ttl=64 (reply in 133)
←	10.201.236.91	10.201.236.81	ICMP	142		Echo (ping) reply id=0x6cdf, seq=1/256, ttl=255 (request in 131)
	10.201.236.81	10.201.236.91	ICMP	142		Echo (ping) request id=0x6cdf, seq=2/512, ttl=64 (reply in 143)
	10.201.236.91	10.201.236.81	ICMP	142		Echo (ping) reply id=0x6cdf, seq=2/512, ttl=255 (request in 141)
	10.201.236.81	10.201.236.91	ICMP	142		Echo (ping) request id=0x6cdf, seq=3/768, ttl=64 (reply in 150)
	10.201.236.91	10.201.236.81	ICMP	142		Echo (ping) reply id=0x6cdf, seq=3/768, ttl=255 (request in 148)
	10.201.236.81	10.201.236.91	ICMP	142		Echo (ping) request id=0x6cdf, seq=4/1024, ttl=64 (reply in 159)
	10.201.236.91	10.201.236.81	ICMP	142		Echo (ping) reply id=0x6cdf, seq=4/1024, ttl=255 (request in 157)
	10.201.236.81	10.201.236.91	ICMP	142		Echo (ping) request id=0x6cdf, seq=5/1280, ttl=64 (reply in 166)
	10.201.236.91	10.201.236.81	ICMP	142		Echo (ping) reply id=0x6cdf, seq=5/1280, ttl=255 (request in 164)
	10.201.236.81	10.201.236.65	ICMP	142		Echo (ping) request id=0x6cf0, seq=1/256, ttl=64 (reply in 196)
	10.201.236.65	10.201.236.81	ICMP	142		Echo (ping) reply id=0x6cf0, seq=1/256, ttl=255 (request in 194)

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.