

# Interne bekabelde pakketvastlegging in Wave 2 en WiFi 6 AP configureren

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Verifiëren](#)

[Problemen oplossen](#)

## Inleiding

Dit document beschrijft hoe u interne bekabelde Packet Capture (PCAP) kunt ophalen van Access Point (AP) Opdrachtlijn Interface (CLI) met Trivial File Transfer Protocol (TFTP) server.

Bijgedragen door Jasia Ahsan, Cisco TAC Engineer.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CLI-toegang tot AP met Secure Shell (SSH) of toegang tot console.
- TFTP-server
- .PCAP-bestanden

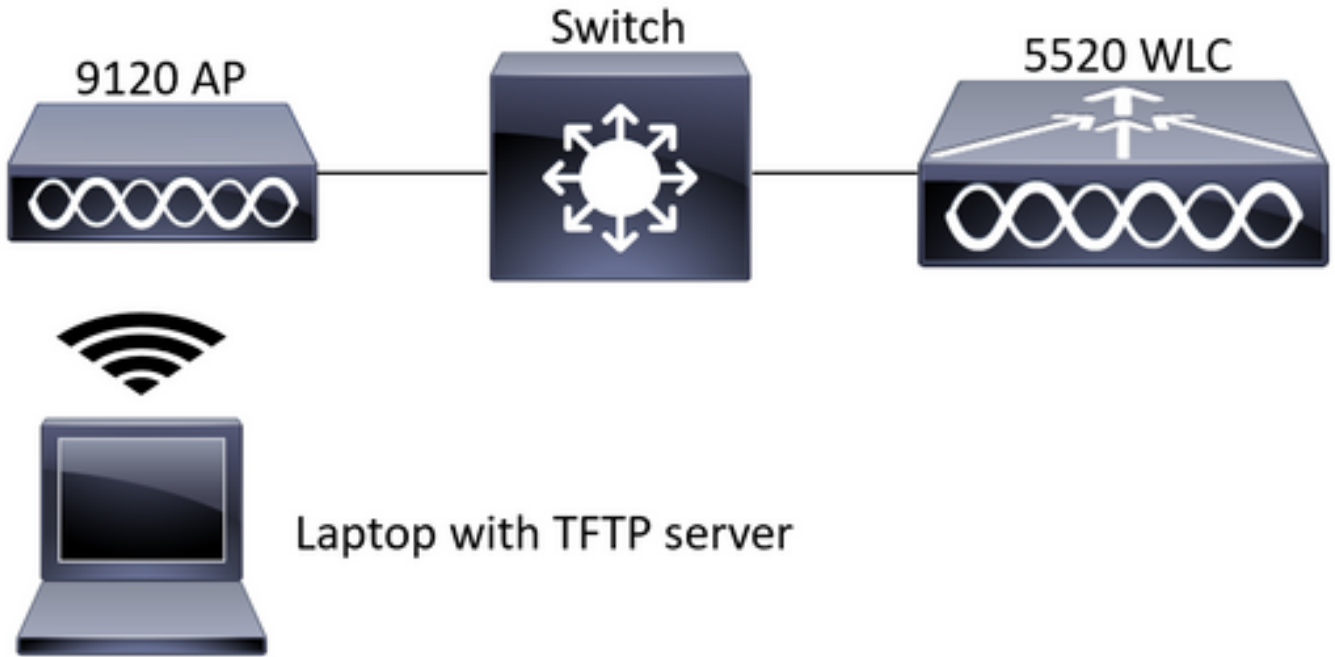
### Gebruikte componenten

- 5520 draadloze LAN-controller (WLC) op 8.10.112-code.
- AP9120AXI
- TFTP-server

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Configureren

## Netwerkdigram



## Configuraties

De PCAP-configuratie is uitgevoerd met SSH naar AP. Er kunnen drie typen verkeer worden geselecteerd: IP, TCP en UDP. In dit geval is IP-verkeer geselecteerd.

Stap 1. Meld u aan bij de AP CLI met SSH.

Stap 2. Start het PCAP voor IP-verkeer en voer deze opdracht uit,

```
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)
```

Stap 3. Let op dat de uitvoer naar een bestand in de map /tmp/pcap is geschreven en dat de AP-naam aan het PDF-bestand is toegevoegd.

Stap 4. Start een ping-test om het IP-verkeer op te nemen.

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

Stap 5. Stop de opname.

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

Stap 6. Kopieer het bestand naar een FTP-server.

```
CLI:
# copy pcap 2802_capture.pcap0 tftp: 10.201.236.33
#####
```

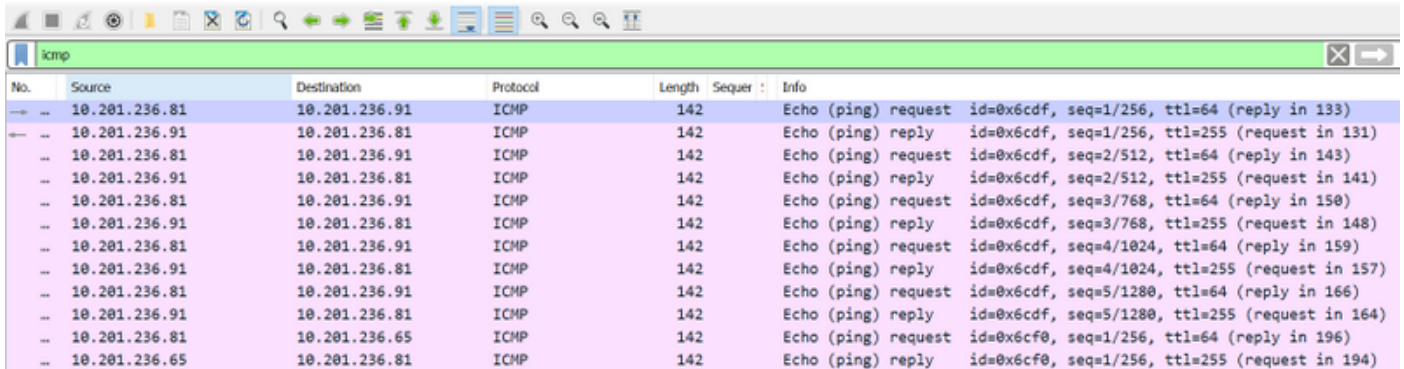
##### 100.0%

Opmerking: Er is een ruimte voor het IP-adres van de tftp server.

## Verifiëren

Open het bestand met een pakketanalyzer. Wireshark wordt hier gebruikt om dit bestand te openen.

De ping-testresultaten kunnen in de afbeelding worden gezien.



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)

## Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.