

# Configurar a Captura de Pacote com Fio Interno no AP Wave 2 e Wifi 6

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Verificar](#)

[Troubleshoot](#)

## Introduction

Este documento descreve como coletar PCAP (Captura de Pacote com Fio) interno da Interface de Linha de Comando (CLI - Command Line Interface) do Ponto de Acesso (AP - Access Point) com o servidor TFTP (Trivial File Transfer Protocol).

Contribuído por Jasia Ahsan, engenheira do TAC da Cisco.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso CLI ao AP com Shell Seguro (SSH) ou Acesso de Console.
- servidor TFTP
- arquivos .PCAP

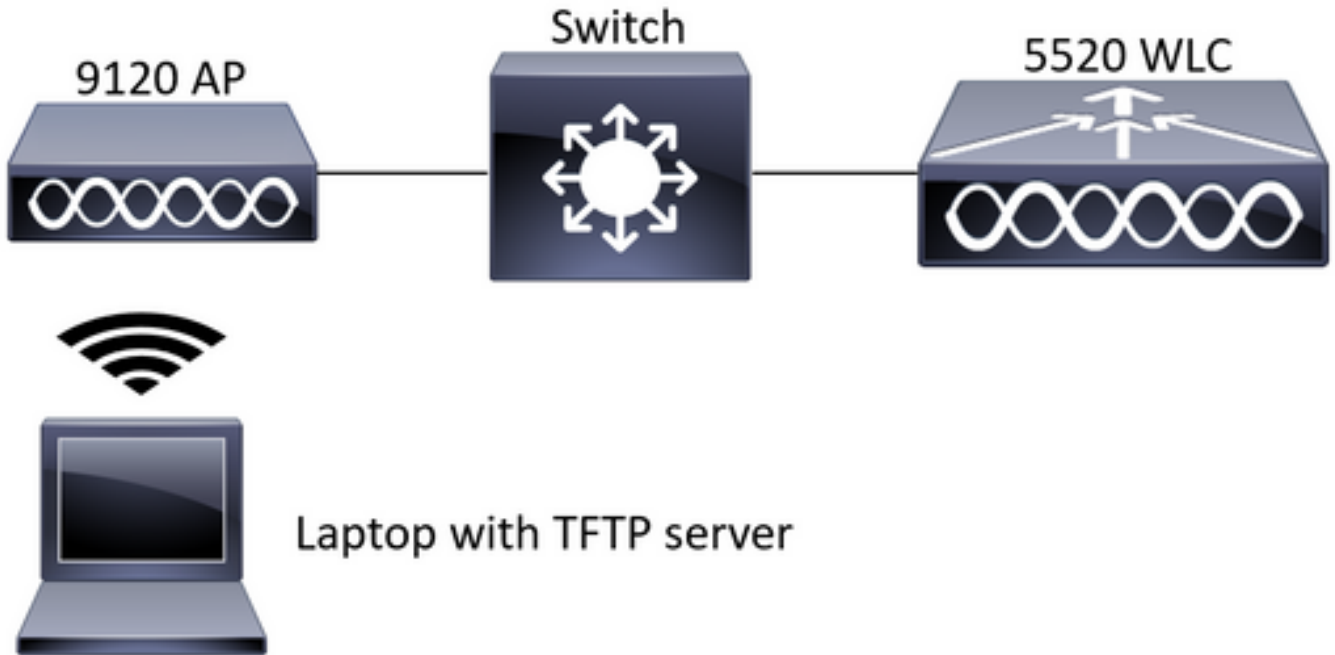
### Componentes Utilizados

- 5520 Wireless Lan Controller (WLC) no código 8.10.112.
- AP 9120AXI
- servidor TFTP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

## Diagrama de Rede



## Configurações

A configuração de PCAP foi feita com SSH para AP. Três tipos de tráfego podem ser selecionados IP, TCP e UDP. Nesse caso, o tráfego IP foi selecionado.

Etapa 1. Faça login no AP CLI com SSH.

Etapa 2. Inicie o PCAP para tráfego IP e execute este comando,

```
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)
```

Etapa 3. Observe que a saída é gravada em um arquivo na pasta /tmp/pcap com o nome AP adicionado ao arquivo pcap.

Etapa 4. Inicie um teste de ping para capturar o tráfego IP.

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

Etapa 5. Pare a captura.

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

Etapa 6. Copie o arquivo para um servidor tftp.

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

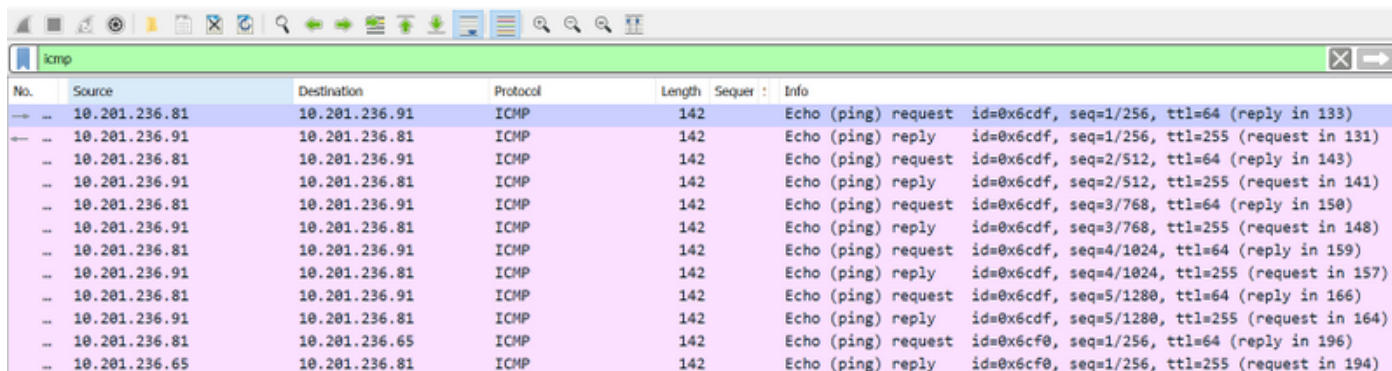
##### 100.0%

**Note:** Há um espaço antes do endereço ip do servidor tftp.

## Verificar

Abra o arquivo com qualquer ferramenta de análise de pacote. O Wireshark é usado aqui para abrir este arquivo.

Os resultados do teste de ping podem ser vistos na imagem.



The screenshot shows a Wireshark capture of ICMP traffic. The table below represents the data shown in the packet list pane.

No.	Source	Destination	Protocol	Length	Sequenc	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)

## Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.