

# Configure Internal Wired Packet Capture in Wave 2 and Wifi 6 AP

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Verify](#)

[Troubleshoot](#)

## Introduction

This document describes how to collect internal wired Packet Capture(PCAP) from Access Point (AP) Command Line Interface (CLI) with Trivial File Transfer Protocol (TFTP) server.

Contributed by Jasia Ahsan, Cisco TAC Engineer.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- CLI access to AP with Secure Shell (SSH) or Console Access.
- TFTP server
- .PCAP files

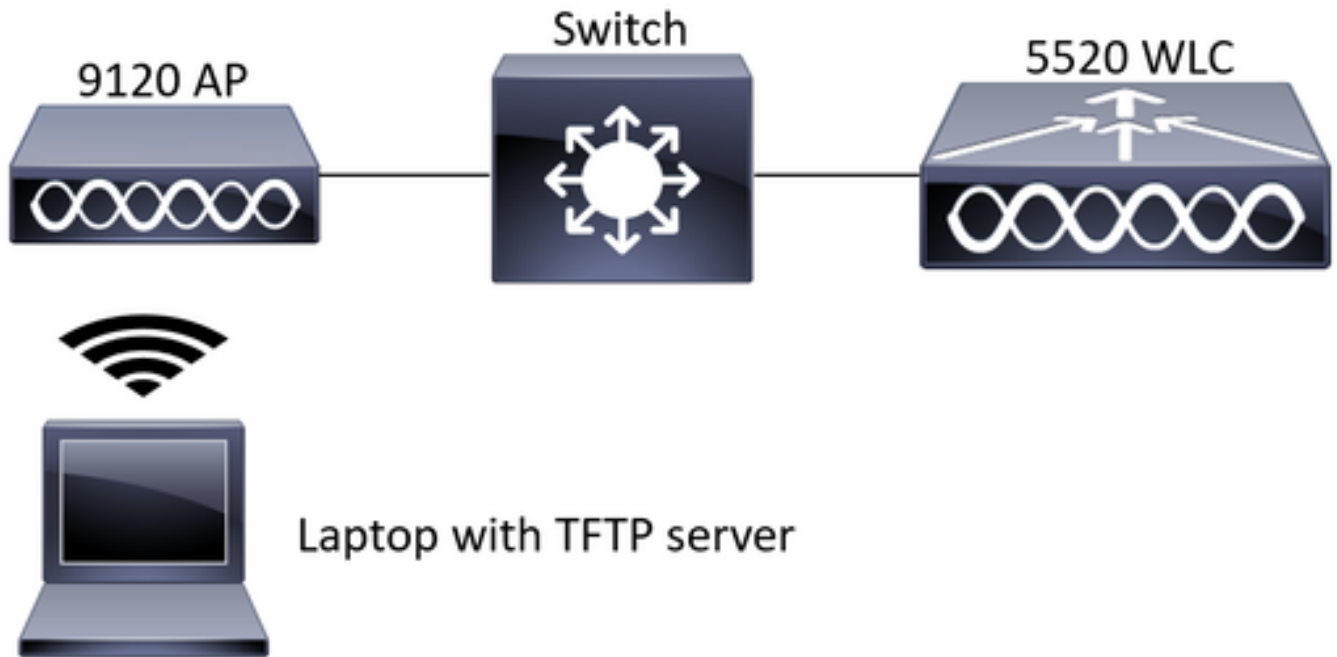
### Components Used

- 5520 Wireless Lan Controller(WLC) on 8.10.112 code.
- AP 9120AXI
- TFTP server

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. If your network is live, ensure that you understand the potential impact of any command.

## Configure

### Network Diagram



## Configurations

The PCAP configuration has been done with SSH to AP. Three traffic types can be selected IP, TCP and UDP. In this case IP traffic has been selected.

Step 1. Log in to the AP CLI with SSH.

Step 2. Start the PCAP for IP traffic and run this command,

```
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)
```

Step 3. Notice the output is written to a file in /tmp/pcap folder with the AP name added to the pcap file.

Step 4. Start a ping test to capture the IP traffic.

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

Step 5. Stop the capture.

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

Step 6. Copy the file to a tftp server.

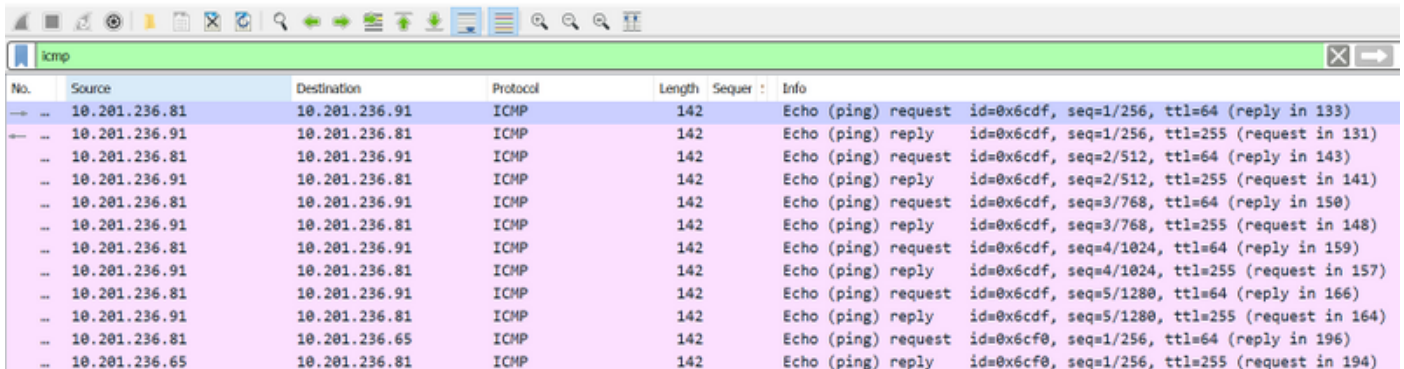
```
CLI:
# copy pcap 2802_capture.pcap0 tftp: 10.201.236.33
#####
##### 100.0%
```

**Note:** There is a space before the tftp server ip address.

# Verify

Open the file with any packet analysis tool. Wireshark is used here to open this file.

The ping test results can be seen in the image.



The image shows a Wireshark packet capture window titled 'icmp'. The main pane displays a list of 18 ICMP packets. The columns are No., Source, Destination, Protocol, Length, Sequer, and Info. The packets alternate between requests and replies, all with a length of 142 bytes. The 'Info' column provides details such as 'Echo (ping) request' or 'Echo (ping) reply', ID, sequence number, and TTL.

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)

# Troubleshoot

There is currently no specific troubleshooting information available for this configuration.