

在Wave 2和Wifi 6 AP中配置內部有線資料包捕獲

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[組態](#)

[驗證](#)

[疑難排解](#)

簡介

本文說明如何使用簡單式檔案傳輸通訊協定(TFTP)伺服器從存取點(AP)命令行介面(CLI)收集內部有線封包擷取(PCAP)。

作者：Jasia Ahsan，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- 通過Secure Shell(SSH)或控制檯訪問AP的CLI訪問。
- TFTP伺服器
- .PCAP檔案

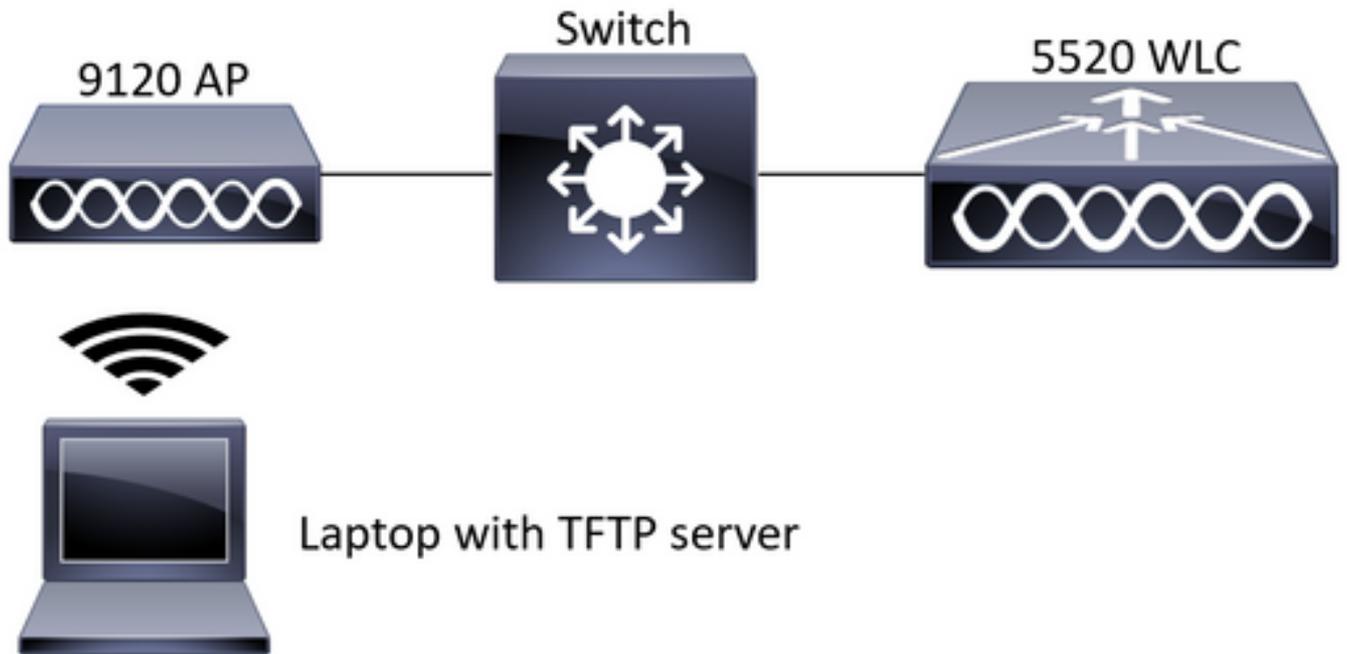
採用元件

- 8.10.112代碼上的5520無線Lan控制器(WLC)。
- AP 9120AXI
- TFTP伺服器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



組態

PCAP配置已通過SSH完成。可以選擇三種流量型別：IP、TCP和UDP。在本例中，已選擇IP流量。

步驟1.使用SSH登入到AP CLI。

步驟2.為IP流量啟動PCAP並運行此命令，

```
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)
```

步驟3.請注意，輸出將寫入到/tmp/pcap資料夾中的檔案中，該檔案的AP名稱已新增到pcap檔案中。

步驟4.開始ping測試以捕獲IP流量。

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

步驟5.停止擷取。

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

步驟6.將檔案複製到tftp伺服器。

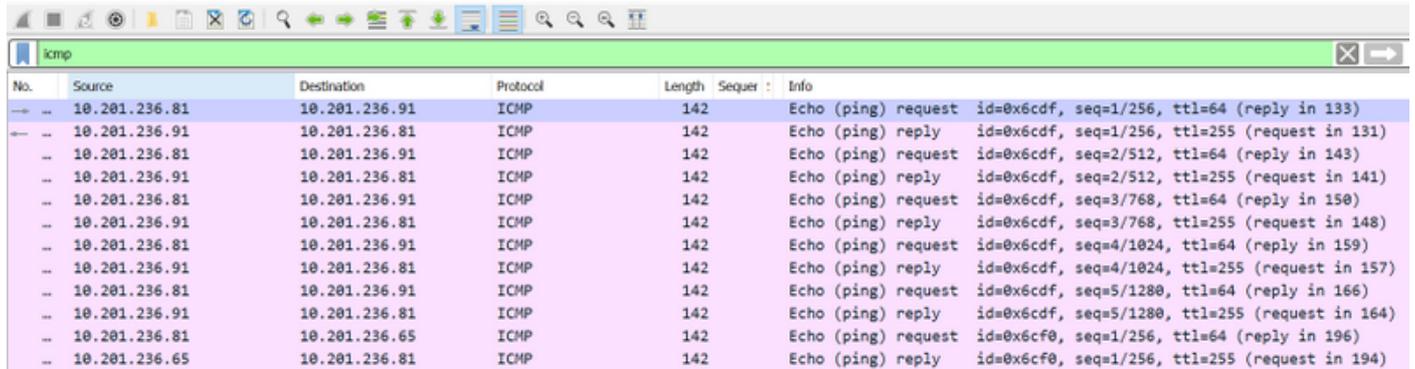
```
CLI:
# copy pcap 2802_capture.pcap0 tftp: 10.201.236.33
#####
##### 100.0%
```

附註：tftp伺服器ip地址前有一個空格。

驗證

使用任何封包分析工具開啟檔案。此處使用Wireshark開啟此檔案。

ping測試結果可在圖中看到。



The image shows a Wireshark packet capture window titled 'icmp'. The main pane displays a list of 19 ICMP packets. The columns are: No., Source, Destination, Protocol, Length, Sequen:, and Info. The packets alternate between requests and replies. Requests are sent from 10.201.236.81 to 10.201.236.91, and replies are sent from 10.201.236.91 to 10.201.236.81. The final two packets (18 and 19) show a change in destination to 10.201.236.65.

No.	Source	Destination	Protocol	Length	Sequen:	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)

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。