

在Wave 2和Wifi 6 AP中配置内部有线数据包捕获

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

简介

本文档介绍如何通过简单文件传输协议(TFTP)服务器从接入点(AP)命令行界面(CLI)收集内部有线数据包捕获(PCAP)。

作者：Jasia Ahsan，Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- 通过安全外壳(SSH)或控制台访问对AP的CLI访问。
- TFTP 服务器
- .PCAP文件

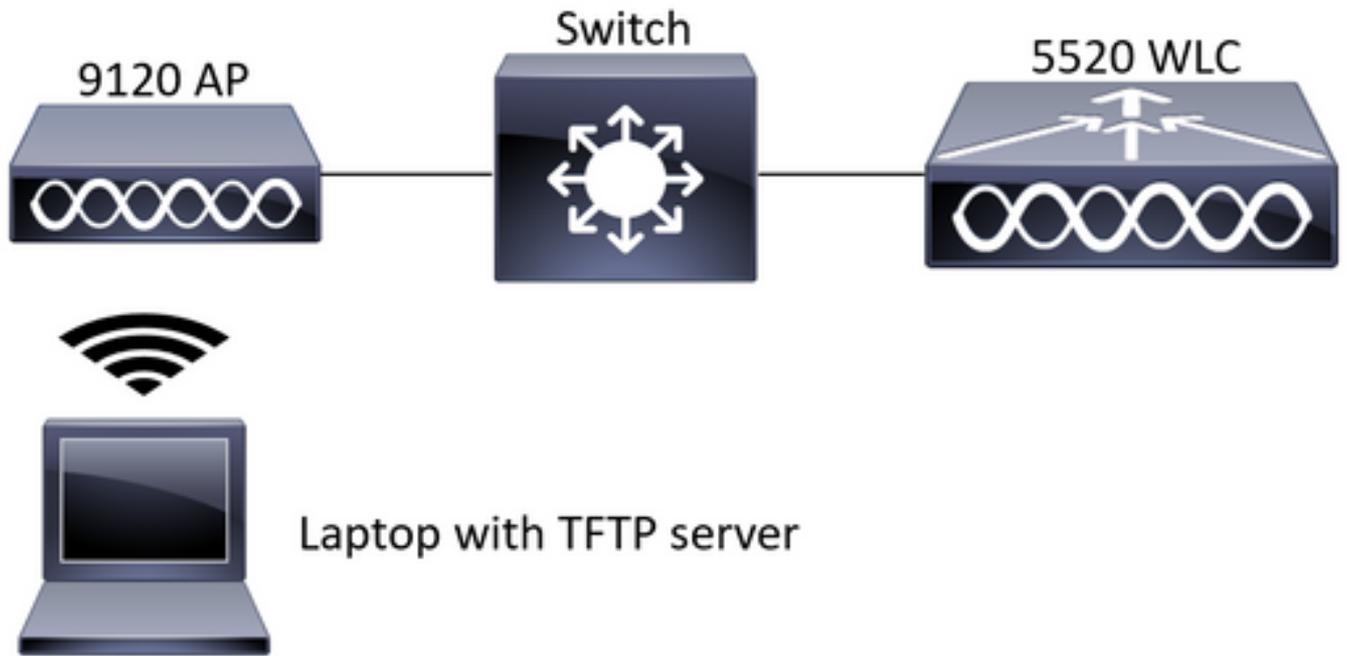
使用的组件

- 8.10.112上的5520无线LAN控制器(WLC)代码。
- AP 9120AXI
- TFTP 服务器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



配置

PCAP配置已通过SSH完成到AP。可以选择三种流量类型：IP、TCP和UDP。在这种情况下，已选择IP流量。

步骤1.使用SSH登录AP CLI。

步骤2.启动IP流量的PCAP并运行此命令，

```
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)
```

步骤3.注意，输出将写入/tmp/pcap文件夹中的文件，其中AP名称已添加到pcap文件。

步骤4.开始ping测试以捕获IP流量。

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

步骤5.停止捕获。

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

步骤6.将文件复制到tftp服务器。

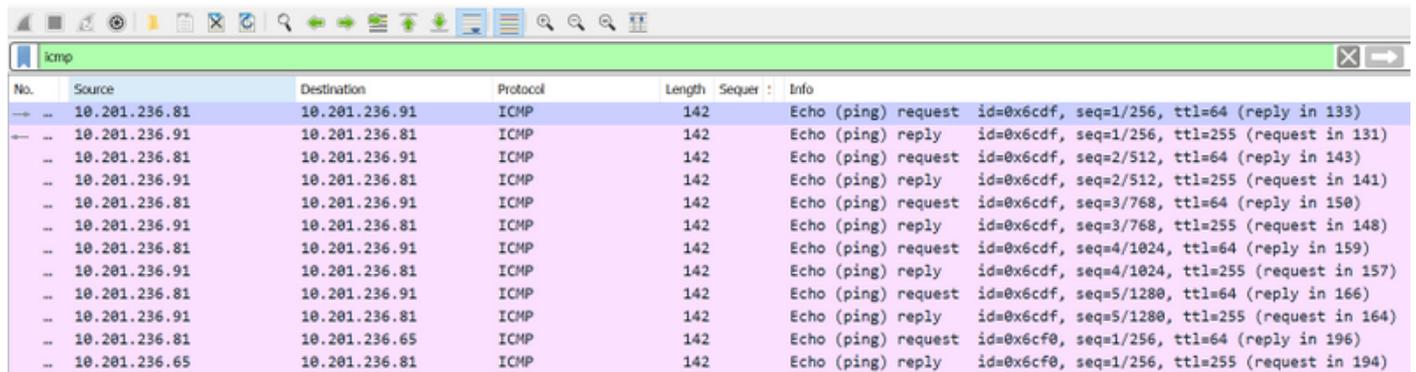
```
CLI:
# copy pcap 2802_capture.pcap0 tftp: 10.201.236.33
#####
##### 100.0%
```

注意：tftp服务器IP地址前有一个空格。

验证

使用任何数据包分析工具打开文件。此处使用Wireshark打开此文件。

在映像中可以看到ping测试结果。



The image shows a Wireshark packet capture window titled 'icmp'. The main pane displays a list of 19 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 last two packets (18 and 19) show a change in destination to 10.201.236.65.

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

故障排除

目前没有针对此配置的故障排除信息。