

配置波形2和Wifi 6 AP的内部有线的数据包捕获

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

本文描述如何从接入点(AP)命令行界面(CLI)收集内部有线的数据包Capture(PCAP)用简单文件传输协议(TFTP)服务器。

贡献用Jasia Ahsan , Cisco TAC工程师。

[先决条件](#)

[要求](#)

Cisco 建议您了解以下主题：

- 对AP的CLI访问与安全壳SSH或控制台访问。
- TFTP 服务器
- .PCAP文件

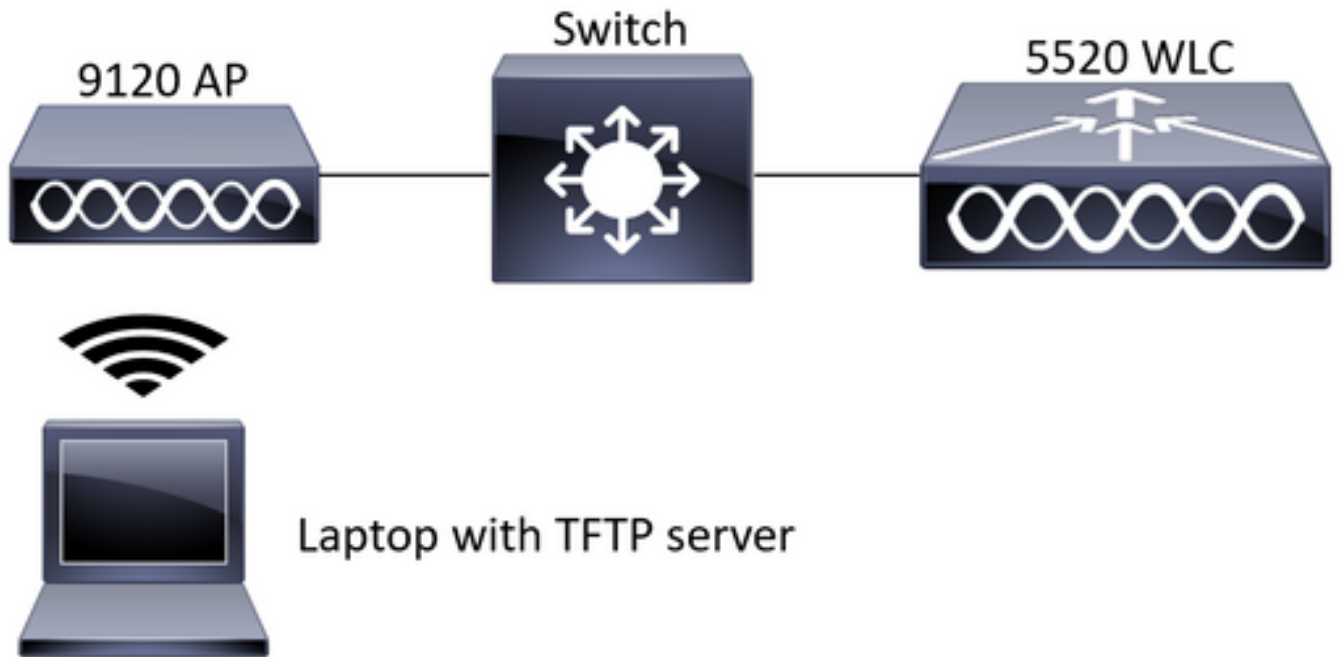
[使用的组件](#)

- 在8.10.112代码的5520个无线局域网Controller(WLC)。
- 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配置是完成与SSH对AP。三流量类型可以是选择的IP、TCP和UDP。在这种情况下IP数据流选择。

步骤1.对AP CLI的登录与SSH。

步骤2.开始IP数据流的PCAP并且运行此命令，

```
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)
```

第 3 步：注意输出写入到在/tmp/pcap文件夹的一个文件有AP名称的被添加到pcap文件。

步骤4.开始ping测试捕获IP数据流。

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

步骤5.终止捕获。

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

步骤6.复制文件对TFTP server。

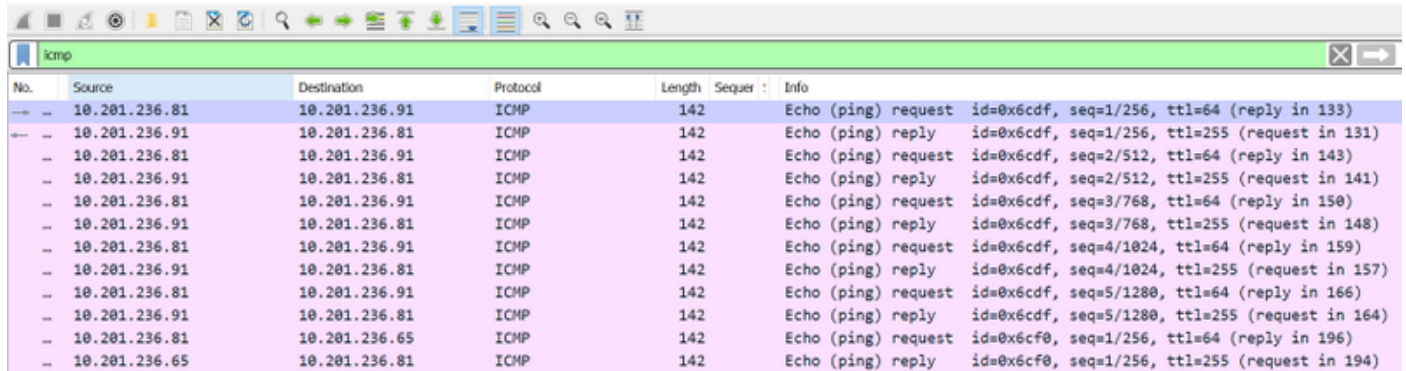
```
CLI:
# copy pcap 2802_capture.pcap0 tftp: 10.201.236.33
#####
##### 100.0%
```

Note:有空间在TFTP服务器IP地址前。

验证

打开文件用所有数据包分析工具。Wireshark用于得这里打开此文件。

ping测试检验结果在镜像能被看到。



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 back 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。