

Configuración de la captura interna de paquetes por cable en Wave 2 y Wifi 6 AP

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo recopilar la captura interna de paquetes por cable (PCAP) de la interfaz de línea de comandos (CLI) del punto de acceso (AP) con el servidor de protocolo de transferencia de archivos trivial (TFTP).

Contribuida por Jasia Ahsan, ingeniera del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso CLI a AP con Secure Shell (SSH) o acceso a consola.
- servidor TFTP
- archivos .PCAP

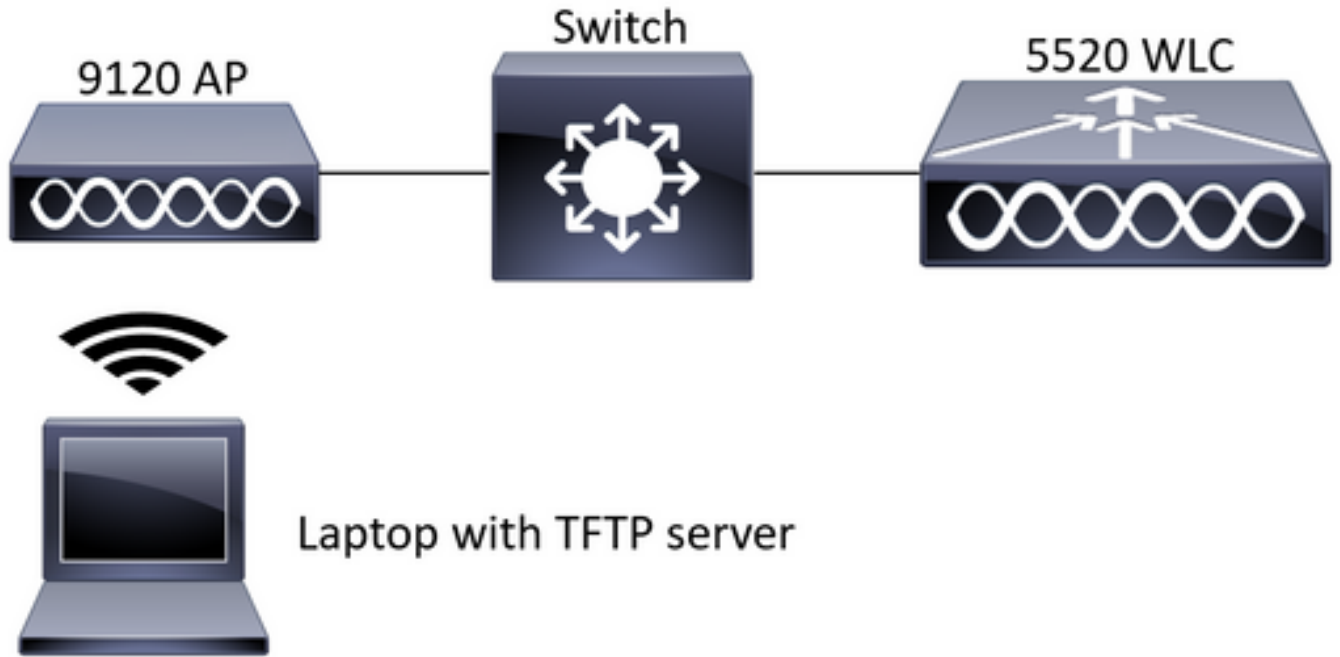
Componentes Utilizados

- 5520 Wireless Lan Controller (WLC) en 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



Configuraciones

La configuración PCAP se ha realizado con SSH a AP. Se pueden seleccionar tres tipos de tráfico IP, TCP y UDP. En este caso, se ha seleccionado el tráfico IP.

Paso 1. Inicie sesión en AP CLI con SSH.

Paso 2. Inicie PCAP para el tráfico IP y ejecute 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)
```

Paso 3. Observe que el resultado se escribe en un archivo en la carpeta /tmp/pcap con el nombre AP agregado al archivo pcap.

Paso 4. Inicie una prueba de ping para capturar el tráfico IP.

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

Paso 5. Detenga la captura.

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

Paso 6. Copie el archivo en un servidor tftp.

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

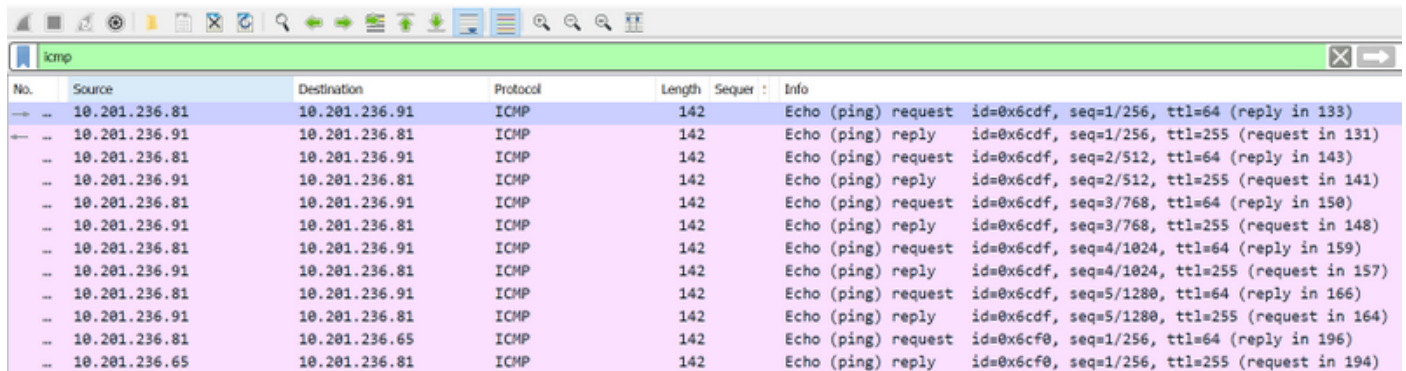
100.0%

Nota: Hay un espacio antes de la dirección ip del servidor tftp.

Verificación

Abra el archivo con cualquier herramienta de análisis de paquetes. Wireshark se utiliza aquí para abrir este archivo.

Los resultados de la prueba de ping se pueden ver en la imagen.



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

No.	Source	Destination	Protocol	Length	Sequencia	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

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.