Configurazione dell'acquisizione interna di pacchetti cablati nell'access point Wave 2 e Wifi 6

Sommario

Introduzione

In questo documento viene descritto come raccogliere i pacchetti PCAP (Wired Packet Capture) interni dall'interfaccia della riga di comando (CLI) del punto di accesso con il server TFTP (Trivial File Transfer Protocol).

Contributo di Jasia Ahsan, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso CLI all'access point con Secure Shell (SSH) o accesso alla console.
- Server TFTP
- file PCAP

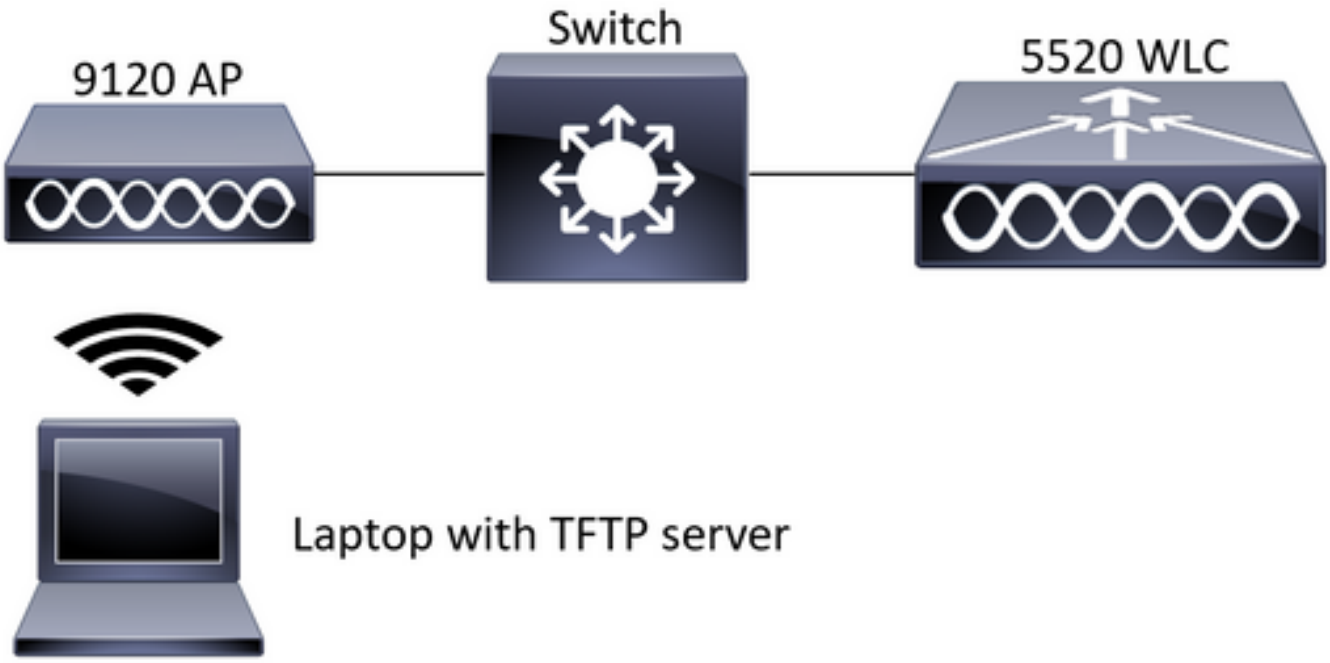
Componenti usati

- 5520 Wireless Lan Controller (WLC) su codice 8.10.112.
- AP 9120AXI
- Server TFTP

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Configurazioni

La configurazione PCAP è stata eseguita con SSH nell'access point. È possibile selezionare tre tipi di traffico: IP, TCP e UDP. In questo caso è stato selezionato il traffico IP.

Passaggio 1. Accedere alla CLI dell'access point con SSH.

Passaggio 2. Avviare PCAP per il traffico IP ed eseguire questo 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)
```

Passaggio 3. Si noti che l'output viene scritto in un file nella cartella /tmp/pcap con il nome AP aggiunto al file pcap.

Passaggio 4. Avviare un test ping per acquisire il traffico IP.

CLI:

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

Passaggio 5. Interrompere l'acquisizione.

CLI:

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

Passaggio 6. Copiare il file su un server tftp.

CLI:

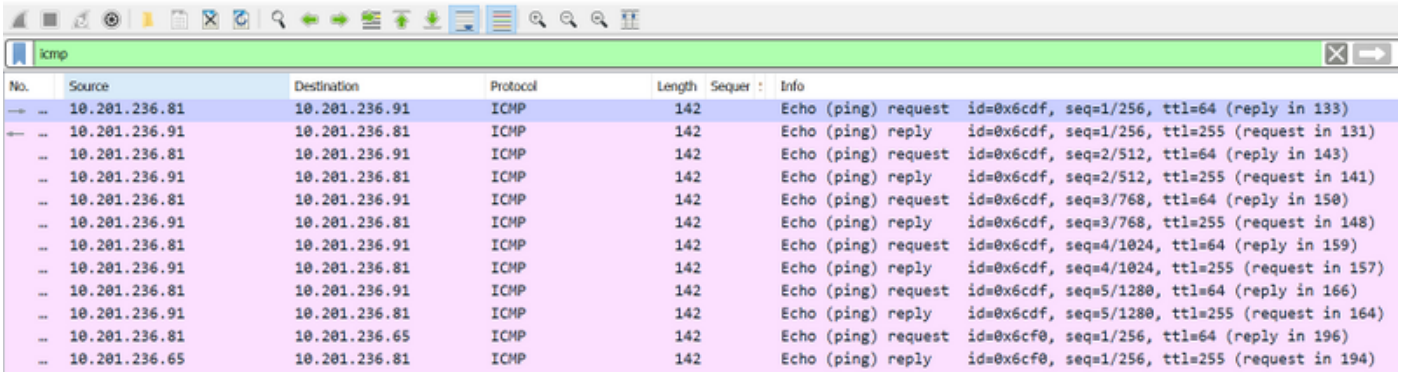
```
# copy pcap 2802_capture.pcap0 tftp: 10.201.236.33
###############################################################################################################
########################################################## 100.0%
```

Nota: È presente uno spazio prima dell'indirizzo IP del server tftp.

Verifica

Aprire il file con uno strumento di analisi dei pacchetti. Wireshark viene utilizzato qui per aprire questo file.

I risultati del ping sono visibili nell'immagine.



icmp

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)

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.