Konfigurieren der internen Paketerfassung in Wave 2 und WiFi 6 AP

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die interne PCAP (kabelgebundene Paketerfassung) von der Befehlszeilenschnittstelle (CLI) des Access Point (AP) mit dem TFTP-Server (Trivial File Transfer Protocol) erfasst wird.

Unterstützt von Jasia Ahsan, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CLI-Zugriff auf AP mit Secure Shell (SSH) oder Konsolenzugriff.
- TFTP-Server
- .PCAP-Dateien

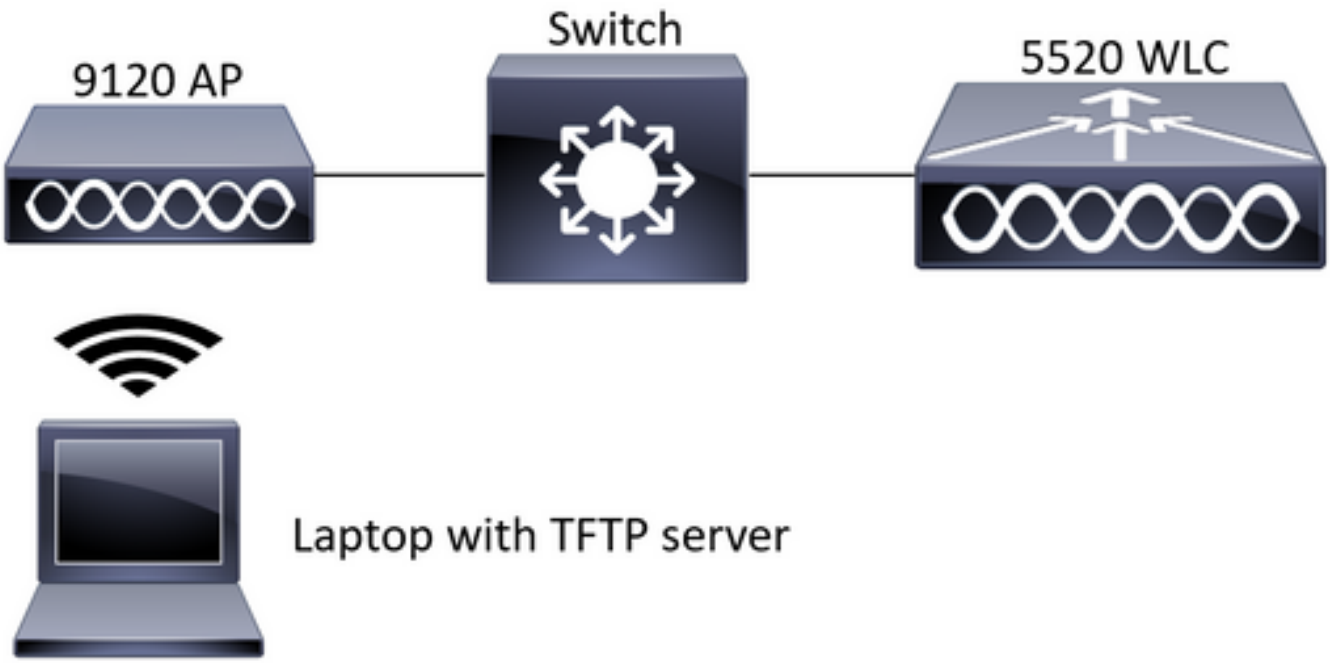
Verwendete Komponenten

- 5520 Wireless LAN Controller (WLC) mit Code 8.10.112.
- AP 9120AXI
- TFTP-Server

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerkdiagramm



Konfigurationen

Die PCAP-Konfiguration wurde mit SSH zu AP durchgeführt. Es können drei Datenverkehrstypen ausgewählt werden: IP, TCP und UDP. In diesem Fall wurde IP-Datenverkehr ausgewählt.

Schritt 1: Melden Sie sich mit SSH bei der AP-CLI an.

Schritt 2: Starten Sie die PCAP für IP-Datenverkehr, und führen Sie den folgenden Befehl aus:

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)
```

Schritt 3: Beachten Sie, dass die Ausgabe in eine Datei im Ordner /tmp/pcap geschrieben wird, wobei der AP-Name der pcap-Datei hinzugefügt wird.

Schritt 4: Starten Sie einen Ping-Test, um den IP-Datenverkehr zu erfassen.

CLI:

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

Schritt 5: Stoppen Sie die Erfassung.

CLI:

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

Schritt 6: Kopieren Sie die Datei auf einen TFTP-Server.

CLI:

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

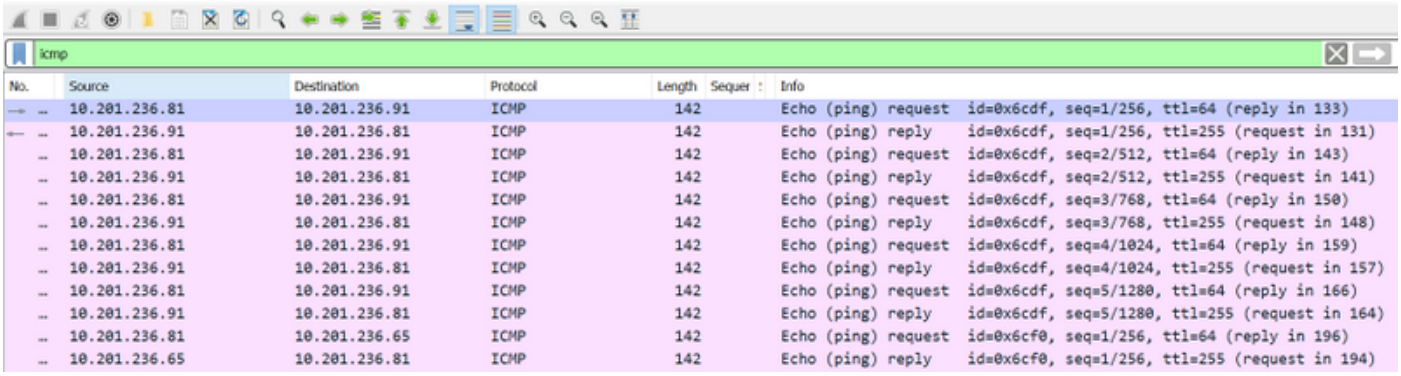
```
################################################## 100.0%
```

Hinweis: Vor der IP-Adresse des TFTP-Servers ist ein Leerzeichen vorhanden.

Überprüfen

Öffnen Sie die Datei mit einem Paketanalyse-Tool. Wireshark wird hier verwendet, um diese Datei zu öffnen.

Die Ping-Testergebnisse sind im Bild zu sehen.



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)

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.