Gebruik van WirelessShark op een Cisco Business WAP voor pakketanalyse: Direct stream naar draadloos

Doel

Dit artikel legt uit hoe u een pakketvastlegging van netwerkverkeer kunt uitvoeren met een Cisco Business Wireless Access Point (WAP) en het rechtstreeks naar Wireless-shark stroomt.

Inhoud

Inleiding en vaak gestelde vragen

De configuratie verandert, controleert en probleemoplossing is iets waar een netwerkbeheerder vaak mee moet omgaan. Een eenvoudig te gebruiken instrument is van onschatbare waarde. Het doel van dit artikel is om comfortabeler te worden met de basislijnen van pakketvastlegging en hoe de pakketten naar Wireshark te stromen. Als u niet bekend bent met dit proces, laten we dan een paar vragen beantwoorden die u misschien al hebt.

Eerst is Wireshark een gratis pakketanalyzer voor iedereen die hun netwerk wil oplossen. Wireshark biedt veel opties voor de opname en het sorteren van verkeer door verschillende parameters. Ga naar Wireshark voor meer informatie over deze opensource-optie.

Wat is een pakketvastlegging?

Een pakketvastlegging, ook bekend als een PCAP-bestand, is een gereedschap dat kan helpen bij het oplossen van problemen. Het kan elk pakket opnemen dat tussen apparaten in uw netwerk wordt verzonden, in real time. Het opnemen van pakketten staat u toe om in de details van het netwerkverkeer te graven, dat alles van apparatenontdekking, protocol gesprekken, en mislukte authenticatie kan omvatten. U kunt het pad van specifieke verkeersstroom en elke interactie tussen apparaten op geselecteerde netwerken zien. Deze pakketten kunnen indien nodig worden opgeslagen voor verdere analyse. Het is als een röntgenstraal van de binnenwerking van het netwerk via de overdracht van pakketten.

Welke typen pakketten kunnen worden opgenomen?

Het WAP-apparaat kan de volgende typen pakketten opslaan:

· 802.11 pakketten die draadloos op de radiointerfaces zijn ontvangen en verzonden. Packets die worden opgenomen op de radio-interfaces bevatten de header 802.11.

· 802.3 pakketten die op de Ethernet-interface zijn ontvangen en verzonden.

· 802.3 pakketten die op de interne logische interfaces worden ontvangen en verzonden, zoals Virtual Access Point (VAP's) en Wireless Distribution System (WDS) interfaces.

Hoe kan een pakketvastlegging op een WAP worden uitgevoerd?

Er zijn twee methoden voor de pakketvastlegging beschikbaar:

1. *Local Capture Methode* - De opgenomen pakketten worden in een bestand op het WAP-apparaat opgeslagen. Het WAP-apparaat kan het bestand naar een TFTP-server (Trivial File Transfer Protocol) overbrengen. Het bestand is opgemaakt in de PCAP-indeling en kan worden onderzocht met behulp van Wireshark. U kunt kiezen *Opslaan op dit apparaat* om de lokale opnamemethode te selecteren.

Als u de lokale opnamemethode liever hebt, met behulp van de nieuwste Web User Interface (UI), kunt u uitkijken met Wireshark op een WAP voor pakketanalyse: Uploadbestand.

Als u liever een artikel bekijkt dat de oudere GUI voor de lokale opnamemethode gebruikt, controleer dan het configureren van pakketvastlegging om prestaties op een draadloos access point te optimaliseren.

2. *Remote Capture Methode* - De opgenomen pakketten worden in realtime opnieuw gericht op een externe computer waarop Wireless-Shark wordt uitgevoerd. U kunt *Stream naar een Remote Host* kiezen om de afstandsopnamemethode te selecteren. Het voordeel van deze methode is dat er geen grens is aan de hoeveelheid pakketten die kan worden opgenomen.

De focus van dit artikel is op Stream naar een Remote Host, dus als dat uw voorkeur is, lees dan op!

Waar kan ik het pakje bedelen?

De draadloze pakketvastlegging functie maakt het mogelijk de pakketten op te nemen en op te slaan die door het WAP-apparaat worden ontvangen en verzonden. De opgenomen pakketten kunnen dan door een netwerkprotocolanalyzer worden geanalyseerd om problemen op te lossen of prestaties te optimaliseren. Er zijn veel online toepassingen voor pakketanalyzer van derden beschikbaar. In dit artikel richten we ons op Wireshark.

Sommige modellen van Cisco Business WAP's hebben de mogelijkheid om pakketten in real-time te verzenden naar CloudShark, een webgebaseerde pakketdecoder en analyzer-website. Het is gelijk aan de Wireless User Interface (UI) voor pakketanalyse die veel toegevoegde opties met een abonnement bevat. U kunt *Stream naar CloudShark* kiezen om de afstandsopnamemethode te selecteren. Klik op de volgende koppelingen voor meer informatie:

- CloudShark (hun officiële website)
- Cloud-haai integreren voor pakketanalyse op een WAP125 of WAP581
- CloudShark-integratie met WAP571 en WAP571E

Noch Wireshark of CloudShark is eigendom van of ondersteund door Cisco. Zij zijn uitsluitend voor demonstratiedoeleinden opgenomen. Neem voor ondersteuning contact op met Wireshark of CloudShark.

Toepasselijk apparaat en softwareversie

- WAP125 versie 1.0.2.0
- WAP150 versie 1.1.1.0
- WAP121 versie 1.0.6.8
- WAP361 versie 1.1.1.0
- WAP581 versie 1.0.2.0
- WAP571 versie 1.1.0.4
- WAP571E versie 1.1.0.4

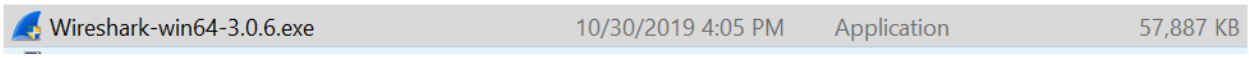
Download Wireshark

Stap 1

Ga naar de website Wireshark. Selecteer de gewenste versie. Klik op **Download (Downloaden).** De voortgang van de download staat linksonder op het scherm.

Stap 2

Ga naar *downloads* op uw computer en selecteer het Help-bestand om de toepassing te installeren.



Inloggen op WAP

Voer in uw webbrowser het IP-adres van de WAP in. Voer je geloofsbrieven in. Als dit de eerste keer is dat u dit apparaat opent of als u een fabrieksreset hebt uitgevoerd, dan zijn de standaardgebruikersnaam en het wachtwoord *Cisco*. Als u instructies nodig hebt over het inloggen, kunt u de stappen in het Access the Web-Based Utility of the Wireless Access Point (WAP) artikel volgen.

Uitleg afstandsbediening van pakketvastlegging

Met de functie Remote Packet Capture kunt u een externe poort instellen als de doelpoort voor pakketvastlegging. Deze functie werkt in combinatie met het gereedschap Windows-netwerkanalyzer voor Windows. Een pakketopnameserver voert op het WAP-apparaat uit en stuurt de opgenomen pakketten door een TCP-verbinding (Transmission Control Protocol) naar het Wireless-shark-gereedschap.

Met een Microsoft Windows-computer waarop het programma WinShark wordt uitgevoerd, kunt u het opgenomen verkeer weergeven, loggen en analyseren. De voorziening voor pakketvastlegging op afstand is een standaardfunctie van het gereedschap Windows.

Terwijl de externe pakketvastlegging niet wordt ondersteund door Linux, werkt het gereedschap Wireshark onder Linux en kunnen de reeds gemaakte opnamestanden worden bekeken.

Wanneer de externe opnamemodus in gebruik is, slaat het WAP-apparaat geen lokaal opgenomen gegevens in het bestandssysteem op.

Als een firewall is geïnstalleerd tussen de Wireless-shark geïnstalleerde computer en het WAP-apparaat, moet Wireless-shark het firewallbeleid van de computer kunnen doorlopen. De firewall moet ook worden geconfigureerd om de Wireshark computer in staat te stellen om een TCP-verbinding naar het WAP-apparaat te initiëren.

Stream a Capture Straight to Wireless-Shark

Om een externe opname op een WAP-apparaat te starten met behulp van de *Stream naar een*

Remote Host-optie, volgt u de onderstaande stappen.

Stap 1

navigeren in WAP naar **probleemoplossing > Packet Capture**.

Voor de *Packet Capture Methode*:

1. Selecteer **Stream naar een Remote Host** in het vervolgkeuzemenu.
2. In het veld *Remote Capture Port*, gebruikt u de standaardpoort van **2002**, of als u een andere poort gebruikt dan de standaard, voert u het gewenste poortnummer in dat wordt gebruikt om Wireless-shark aan te sluiten op het WAP-apparaat. Het poortbereik loopt van 1025 tot 65530.
3. Er zijn twee *modi* voor de pakketvastlegging. Selecteer wat het beste is voor uw scenario.

- *Al het draadloze verkeer* - Leg alle draadloze pakketten in de lucht vast.
- *Verkeer naar/van deze AP* - Leg het pakket vast dat van AP of AP wordt verzonden.

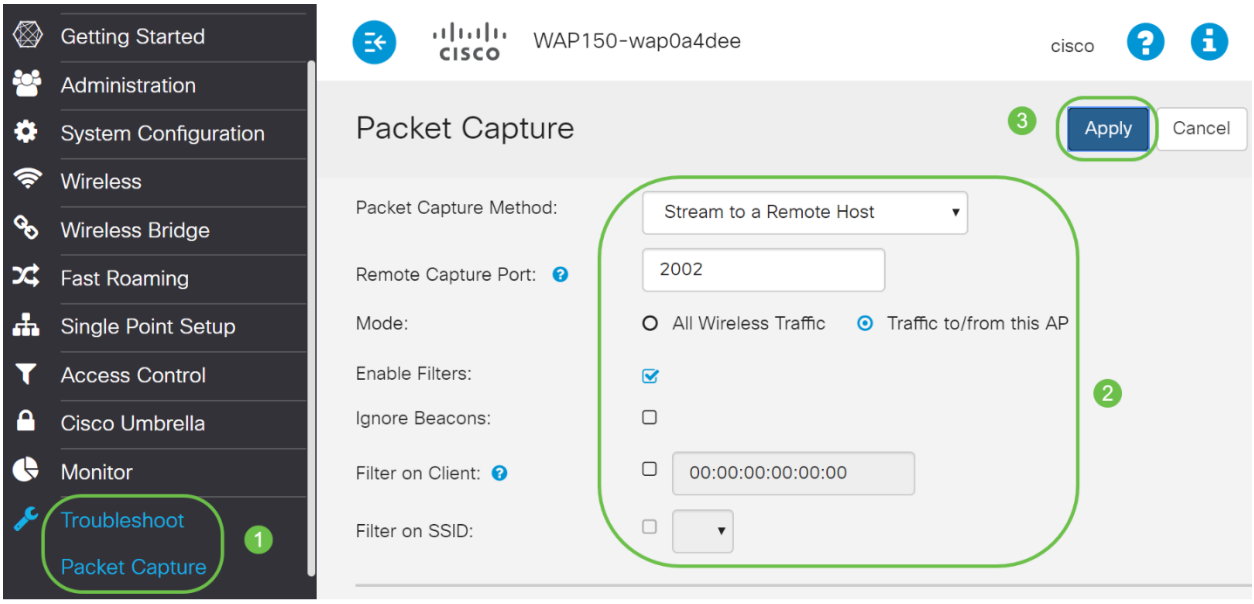
4. Controleer **Filters inschakelen**.
5. Kies uit de volgende opties:

- *Negeren Beacons* - Schakel de opname van 802.11 bakens die door de radio zijn gedetecteerd of verzonden in of uit. Baken-frames zijn uitzendframes die informatie over een netwerk bevatten. Het doel van een baken is het adverteren van een bestaand draadloos netwerk.

- *Filter op client* - Nadat deze geactiveerd is, specificeert u het MAC-adres voor WLAN-clientfilter. Merk op dat het clientfilter alleen actief is als er een opname op een 802.11-interface wordt uitgevoerd.

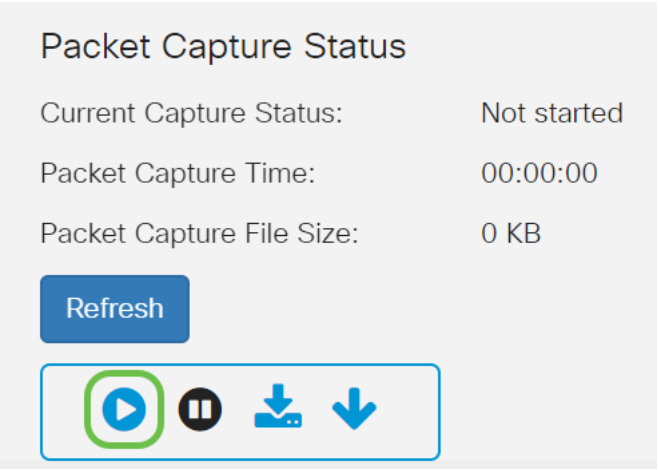
- *Filter op SSID* - Deze optie zal voor deze *Stream* aan *een Remote Host* optie worden gegraveerd.

6. Klik op **Toepassen** om de instellingen op te slaan.



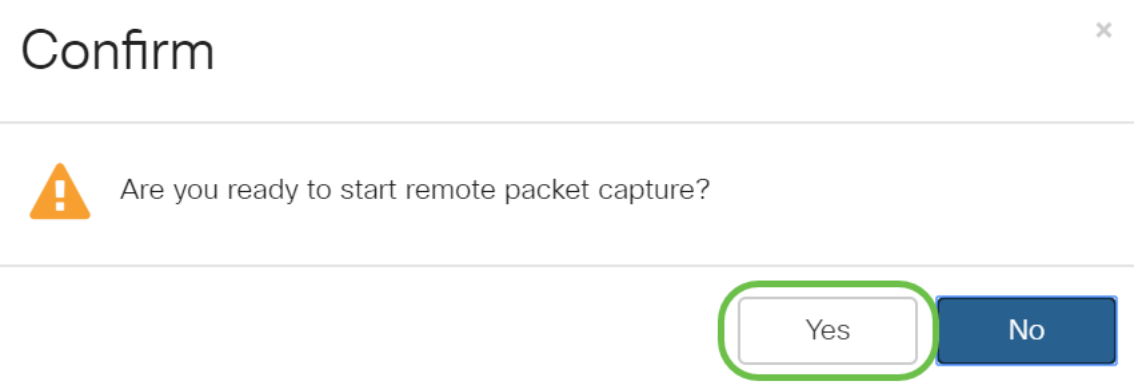
Stap 2

Klik op het pictogram **Start**.



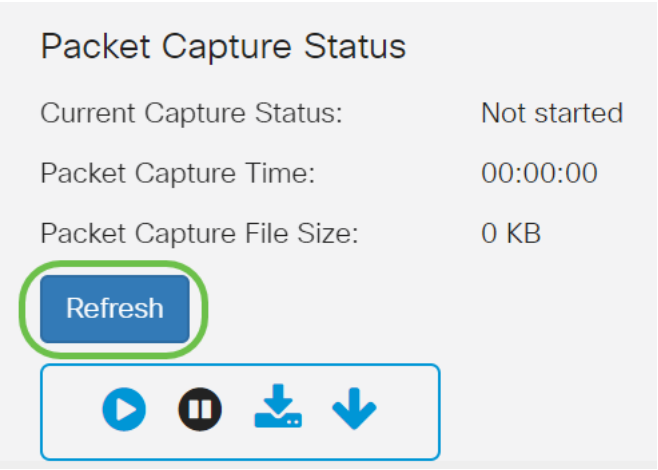
Stap 3

Er wordt een pop-upvenster geopend. Klik op **Ja** om de opname te starten.



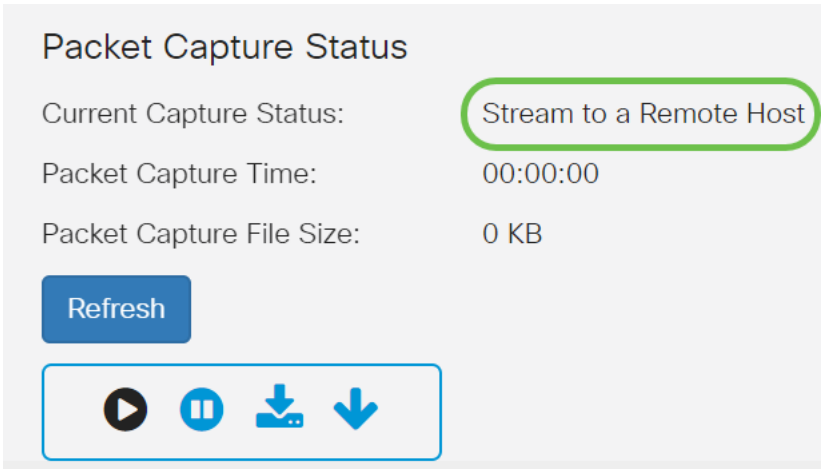
Stap 4

Klik op de knop **Vernieuwen** om de huidige status te controleren.



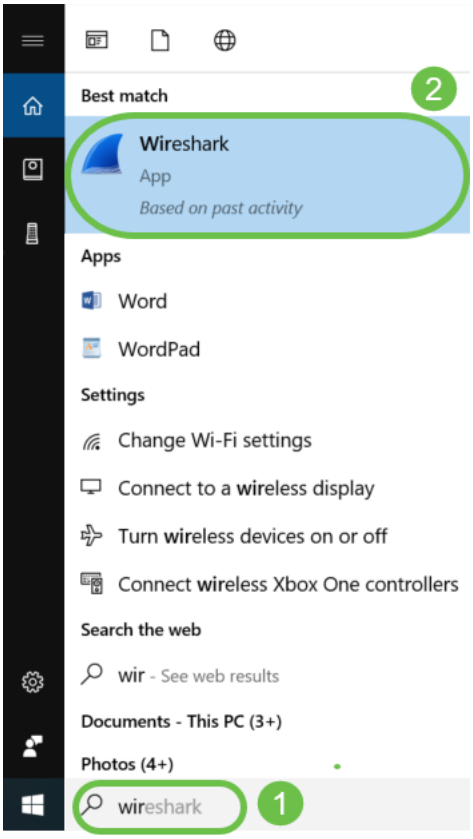
Stap 5

U kunt nu zien dat de *huidige opnamestatus stream naar een Remote Host* is.



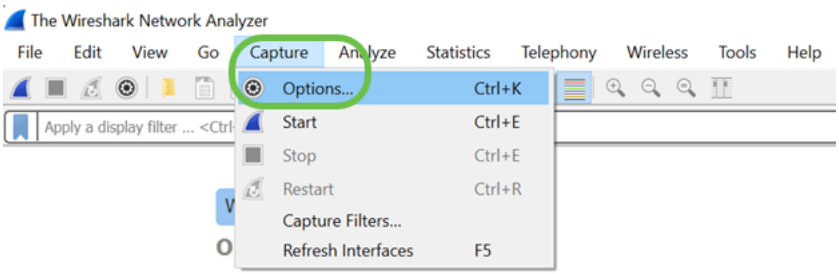
Stap 6

Aangezien Wireshark al is gedownload, kan het worden benaderd door **Wireshark** te typen in de zoekbalk van Microsoft Windows en de toepassing te selecteren wanneer deze een optie is.



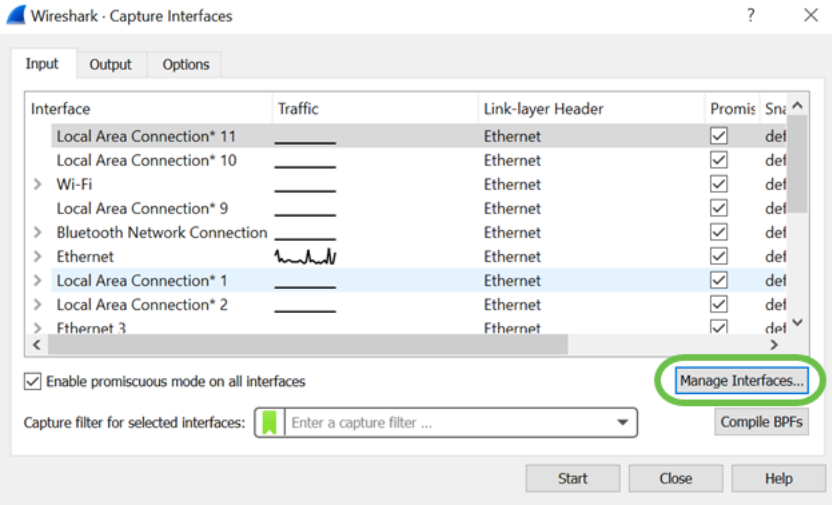
Stap 7

Navigeren in **Opname > Opties...**



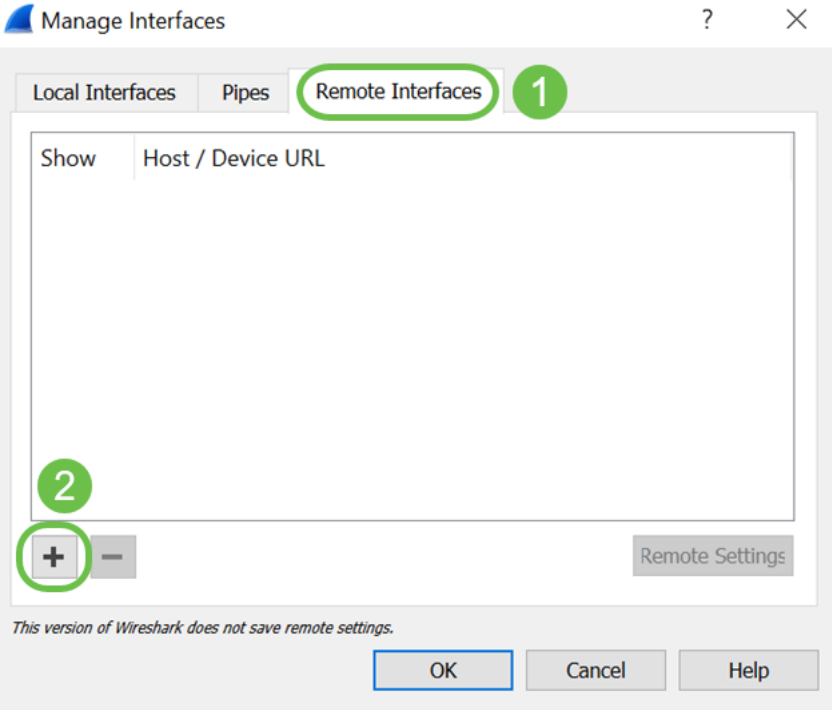
Stap 8

In het nieuwe pop-up *Wireless-shark - Capture interfaces* venster klikt u op **Interfaces beheren**.



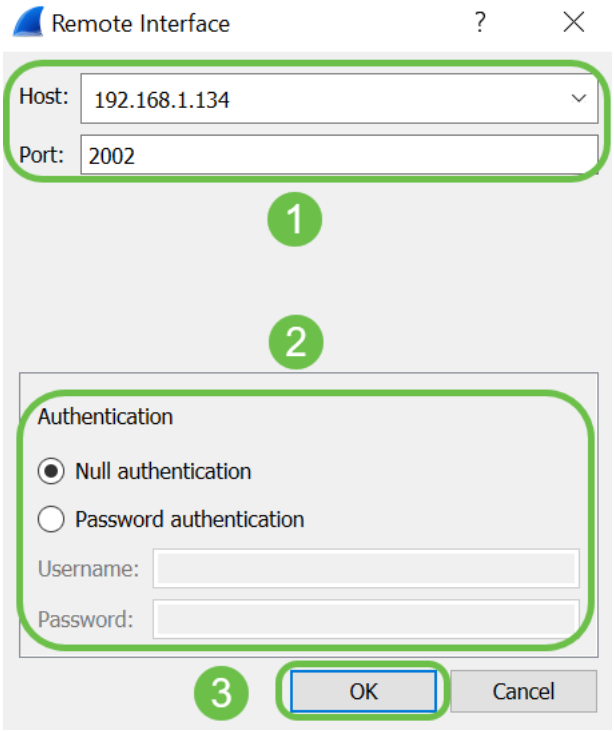
Stap 9

In het nieuwe pop-upvenster *Interfaces beheren*, navigeer naar **externe interfaces** en klik op het **plus-pictogram** om de interface toe te voegen.



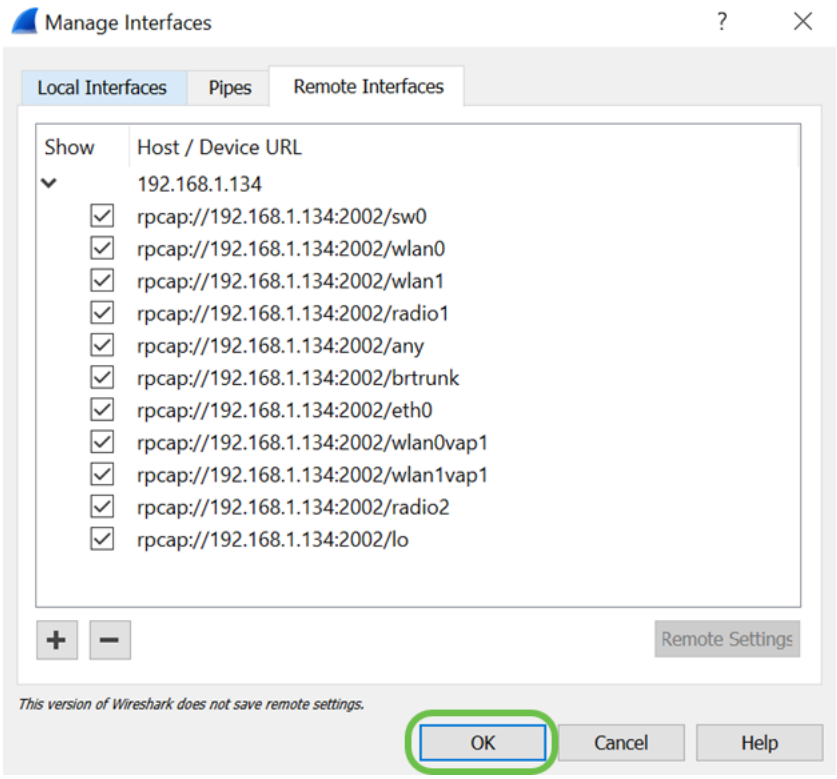
Stap 10

Voer in het pop-upvenster *Remote Interface* de *host in:* IP-adresdetails (het WAP-apparaat IP waar u de afstandsopname hebt gestart) en *Port:* aantal (ingesteld op WAP voor externe opname). In dit geval was IP-apparaat voor WAP 192.168.1.134. U kunt op basis van uw instellingen *volledige verificatie* of *wachtwoordverificatie* selecteren. Als u deze optie selecteert, voert u de *gebruikersnaam* en *de* wachtwoordgegevens in. Klik op **OK**.



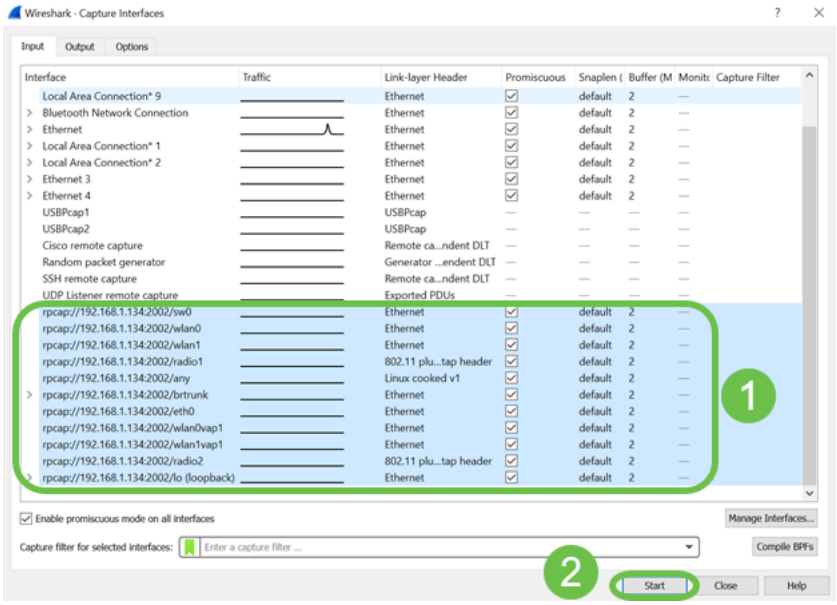
Stap 11

Onder het tabblad *Remote Interfaces* kunt u alle interfaces van het elders geplaatste WAP-apparaat zien. Selecteer bepaalde opties alleen om het opgenomen aantal pakketten te verminderen. Je laat de radiointerfaces geselecteerd als je bakken-pakketten wilt zien. Klik op **OK**.



Stap 12

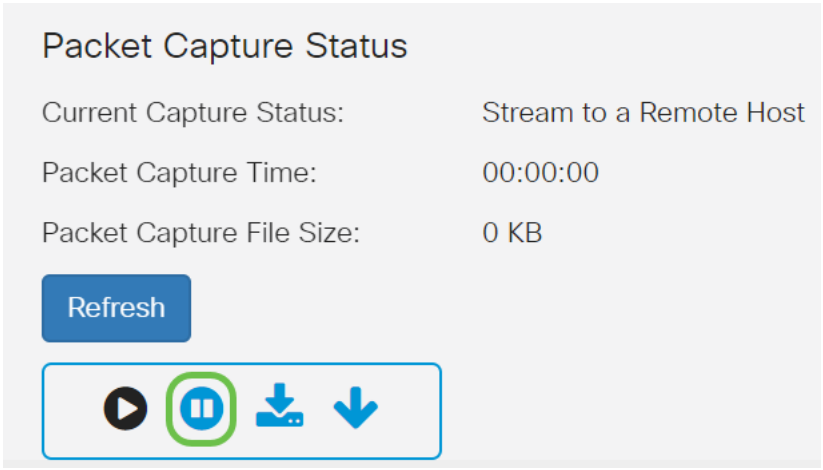
Nu zullen de nieuwe interfaces hun weerslag hebben op het venster *Wireshark - Capture Interfaces*. **Selecteer** de interface die u wilt bewaken en klik op **Start** om de pakketten te bekijken.



Als u problemen ondervindt wanneer u probeert de pakketten te bekijken, betekent dit dat de service *Remote Packet Capture Protocol* niet aan uw systeem werkt. De Remote Packet Capture Protocol-service moet eerst op het doelplatform worden uitgevoerd voordat Wireless-shark er verbinding mee kan maken. Klik voor meer informatie op de link *Remote Capture Interfaces* via Wireshark.

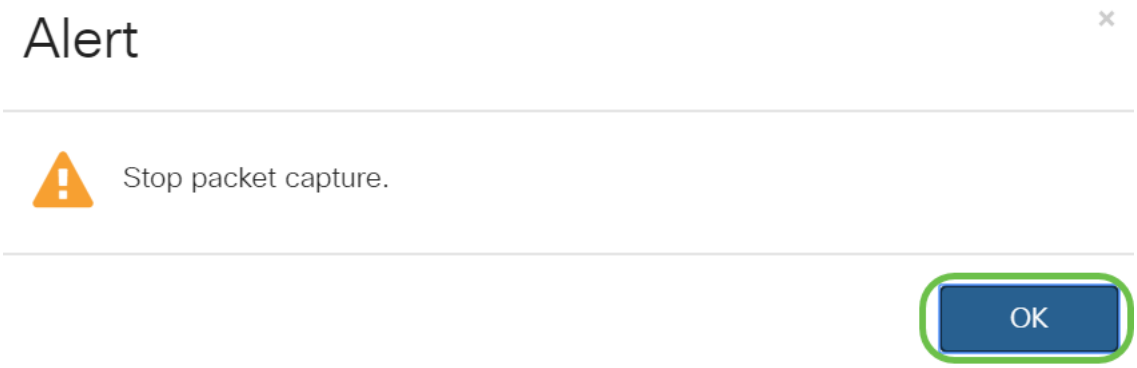
Stap 13

Klik in WAP op het **pictogram Stop Capture** om het opnamproces te stoppen.



Stap 14

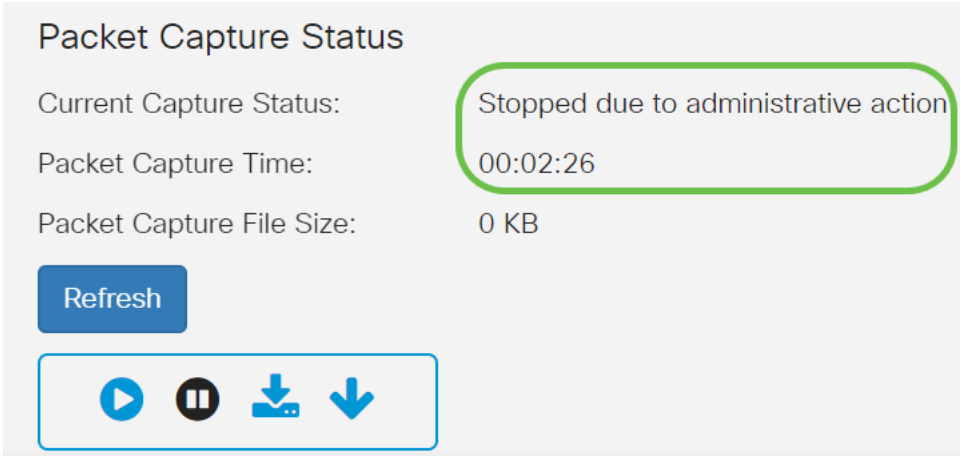
Er verschijnt een pop-upvenster met waarschuwing. Klik op **OK** om de afstandsopname te stoppen.



U kunt de pakketvastlegging ook stoppen door op de knop **Stop** in de applicatie Wireless-shark te klikken.

Stap 15

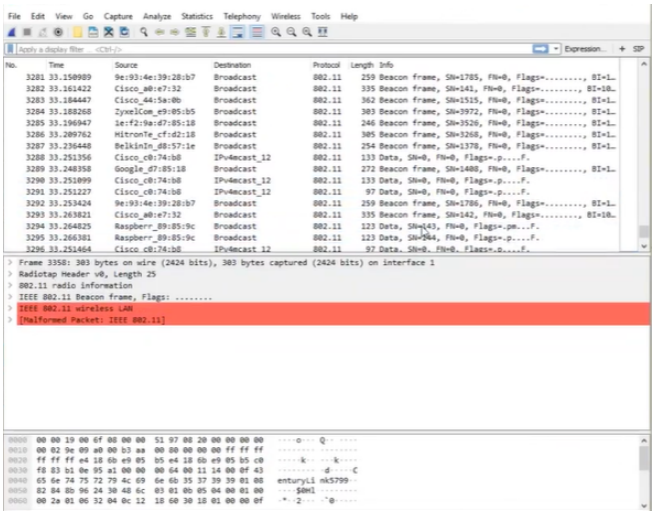
De *huidige Capture Status* zal nu laten zien *als Gestopt door administratieve actie*, en *Packet Capture Time* zal *de* totale opnameduur weergeven.



De grootte van het *Packet Capture File* wordt als *0 KB* weergegeven. Bovendien werken de opties voor het downloaden van bestanden niet in dit scenario.

Stap 16

Op Wireshark kunt u uw pakketvastlegging bekijken.



Conclusie

Je hebt nu de vaardigheden om een pakje rechtstreeks te laten streamen naar Wireshark en je kunt het analyseren. Weet je niet waar je heen moet? Er zijn genoeg video's en artikelen beschikbaar die u online kunt verkennen. Wat je zoekt, hangt af van de behoeften van je situatie. Dit heb je!