Uso de Wireshark en un WAP empresarial de Cisco para el análisis de paquetes: Transmitir directamente a Wireshark

Objetivo

En este artículo se explica cómo realizar una captura de paquetes del tráfico de red mediante un punto de acceso inalámbrico Cisco Business (WAP) y cómo transmitirlo directamente a Wireshark.

Table Of Contents

Introducción y preguntas frecuentes

Los cambios de configuración, la supervisión y la resolución de problemas son algo que el administrador de red debe tratar a menudo. Disponer de una herramienta sencilla es muy valioso. El objetivo de este artículo es sentirse más cómodo con los fundamentos de las capturas de paquetes, así como de cómo transmitir los paquetes a Wireshark. Si no está familiarizado con este proceso, conteste a algunas preguntas que podría haber hecho ya.

En primer lugar, Wireshark es un analizador de paquetes gratuito para cualquier persona que desee solucionar problemas en su red. Wireshark proporciona muchas opciones para la captura, así como para ordenar el tráfico mediante varios parámetros diferentes. Diríjase a Wireshark para obtener detalles sobre esta opción de código abierto.

¿Qué es una captura de paquetes?

Una captura de paquetes, también conocida como un archivo PCAP, es una herramienta que puede ser útil en la resolución de problemas. Puede registrar cada paquete enviado entre dispositivos de la red en tiempo real. La captura de paquetes le permite profundizar en los detalles del tráfico de red, que puede incluir desde la detección de dispositivos, conversaciones de protocolo y autenticación fallida. Puede ver la ruta del flujo de tráfico específico y cada interacción entre los dispositivos en las redes seleccionadas. Estos paquetes se pueden guardar para un análisis adicional según sea necesario. Es como una radiografía del funcionamiento interno de la red a través de la transferencia de paquetes.

¿Qué tipos de paquetes se pueden capturar?

El dispositivo WAP puede capturar los siguientes tipos de paquetes:

·paquetes 802.11 recibidos y transmitidos de forma inalámbrica en las interfaces de radio. Los paquetes capturados en las interfaces de radio incluyen el encabezado 802.11.

·paquetes 802.3 recibidos y transmitidos en la interfaz Ethernet.

·paquetes 802.3 recibidos y transmitidos en las interfaces lógicas internas, como las interfaces Virtual Access Points (VAP) y Wireless Distribution System (WDS).

¿Cuáles son las maneras en que se puede realizar una captura de paquetes en un WAP?

Hay dos métodos de captura de paquetes disponibles:

1. *Método de captura local*: los paquetes capturados se almacenan en un archivo en el dispositivo WAP. El dispositivo WAP puede transferir el archivo a un servidor de protocolo de transferencia de archivos trivial (TFTP). El archivo tiene formato PCAP y se puede examinar mediante Wireshark. Puede elegir *Guardar archivo en este dispositivo* para seleccionar el método de captura local.

Si prefiere el método de captura local, con la interfaz de usuario web más reciente, desprotéjase Uso de Wireshark en un WAP para el análisis de paquetes: Cargar archivo.

Si prefiere ver un artículo que utiliza la GUI más antigua para el método de captura local, consulte Configurar captura de paquetes para optimizar el rendimiento en un punto de acceso inalámbrico.

2. *Método de captura remota*: los paquetes capturados se redirigen en tiempo real a un equipo externo que ejecuta Wireshark. Puede elegir *Stream to a Remote Host* para seleccionar el método de captura remota. La ventaja de este método es que no hay límite en el volumen de paquetes que se pueden capturar.

El objetivo de este artículo es transmitir a un host remoto, por lo que si así lo prefiere, lea.

¿Dónde puedo transmitir el paquete?

La función de captura de paquetes inalámbricos permite capturar y almacenar los paquetes recibidos y transmitidos por el dispositivo WAP. Los paquetes capturados pueden entonces ser analizados por un analizador de protocolo de red para la resolución de problemas o la optimización del rendimiento. Hay muchas aplicaciones de analizador de paquetes de terceros disponibles en línea. En este artículo, nos centramos en Wireshark.

Algunos modelos de WAP empresariales de Cisco tienen la capacidad de enviar paquetes en tiempo real a CloudShark, un sitio web de análisis y descodificador de paquetes. Es similar a la interfaz de usuario (IU) de Wireshark para el análisis de paquetes que incluye muchas opciones añadidas con una suscripción. Puede elegir *Stream to CloudShark* para seleccionar el método de captura remota. Para obtener más información, haga clic en los siguientes enlaces:

- CloudShark (su sitio web oficial)
- Integración de CloudShark para el análisis de paquetes en un WAP125 o WAP581

- Integración de CloudShark con WAP571 y WAP571E

Ni Wireshark ni CloudShark son propiedad de Cisco ni son compatibles con ella. Se incluyen únicamente con fines de demostración. Para obtener asistencia, póngase en contacto con Wireshark o CloudShark.

Dispositivos y versión de software aplicables

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

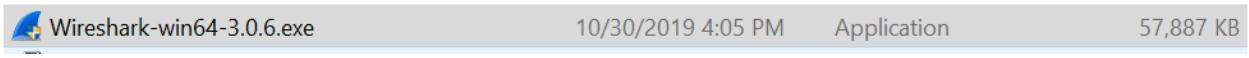
Descargar Wireshark

Paso 1

Vaya al sitio web de Wireshark. Seleccione la versión adecuada. Haga clic en **Descarga**. Verá el progreso de la descarga en la parte inferior izquierda de la pantalla.

Paso 2

Vaya a *Descargas* en su equipo y seleccione el archivo Wireshark para instalar su aplicación.



Inicie sesión en WAP

En el explorador Web, introduzca la dirección IP del WAP. Introduzca sus credenciales. Si es la primera vez que accede a este dispositivo o ha realizado un restablecimiento de fábrica, el nombre de usuario y la contraseña predeterminados son *cisco*. Si necesita instrucciones sobre cómo iniciar sesión, puede seguir los pasos del artículo Acceso a la utilidad basada en Web del punto de acceso inalámbrico (WAP).

Explicación de captura remota de paquetes

La función Captura remota de paquetes permite especificar un puerto remoto como puerto de destino para las capturas de paquetes. Esta función funciona junto con la herramienta de análisis de red Wireshark para Windows. Un servidor de captura de paquetes se ejecuta en el dispositivo WAP y envía los paquetes capturados a través de una conexión de protocolo de control de transmisión (TCP) a la herramienta Wireshark.

Un equipo de Microsoft Windows que ejecuta la herramienta Wireshark permite mostrar, registrar y analizar el tráfico capturado. La función de captura remota de paquetes es una función estándar de la herramienta Wireshark para Windows.

Aunque Linux no soporta la captura remota de paquetes, la herramienta Wireshark funciona con Linux y se pueden ver los archivos de captura ya creados.

Cuando el modo de captura remota está en uso, el dispositivo WAP no almacena ningún dato capturado localmente en su sistema de archivos.

Si se instala un firewall entre el equipo instalado de Wireshark y el dispositivo WAP, se debe permitir que Wireshark pase a través de la política de firewall del equipo. El firewall también se debe configurar para permitir que el equipo Wireshark inicie una conexión TCP al dispositivo WAP.

Transmitir una captura directamente a Wireshark

Para iniciar una captura remota en un dispositivo WAP usando la opción *Stream to a un host*

remoto, siga los pasos enumerados a continuación.

Paso 1

En el WAP, navegue hasta **Troubleshooting > Packet Capture**.

Para el *método de captura de paquetes*:

1. Seleccione **Stream to a Remote Host** en el menú desplegable.
2. En el campo *Puerto de captura remota*, utilice el puerto predeterminado de **2002**, o si está utilizando un puerto que no sea el predeterminado, ingrese el número de puerto deseado utilizado para conectar Wireshark al dispositivo WAP. El intervalo de puertos está comprendido entre 1025 y 65530.
3. Hay dos *modos* para las opciones de captura de paquetes. Seleccione lo que mejor se adapte a su situación.

·*Todo el tráfico inalámbrico*: captura todos los paquetes inalámbricos en el aire.

·*Tráfico hacia/desde este AP* - Capture el paquete enviado desde el AP o el AP recibido.

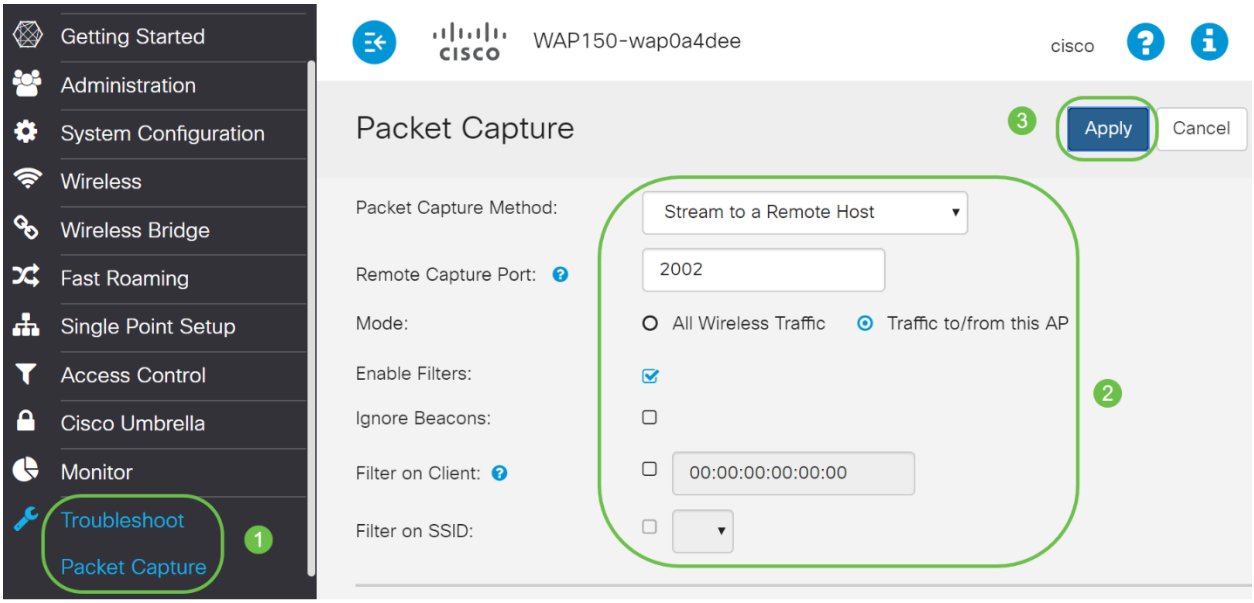
4. Marque **Activar filtros**.
5. Elija una de las siguientes opciones:

·*Ignore Beacons* - Habilite o deshabilite la captura de balizas 802.11 detectadas o transmitidas por la radio. Las tramas de baliza son tramas de broadcast que llevan información relativa a una red. El propósito de una baliza es anunciar una red inalámbrica existente.

·*Filter on Client* - Una vez habilitado, especifique la dirección MAC para el filtro de cliente WLAN. Tenga en cuenta que el filtro Cliente sólo está activo cuando se realiza una captura en una interfaz 802.11.

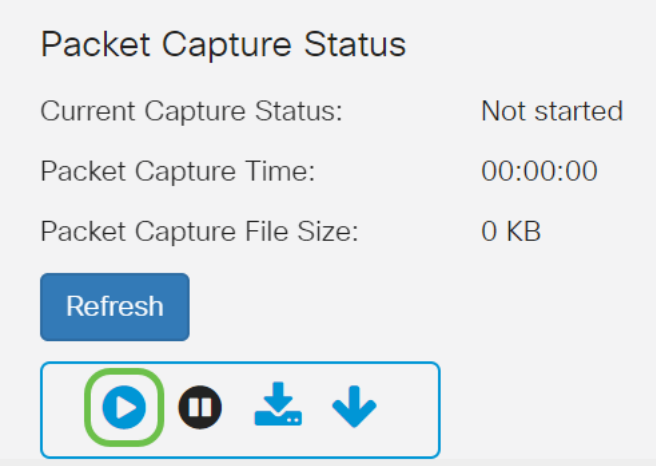
·*Filtro en SSID* - Esta opción se atenuará para esta *opción Transmitir a un host remoto*.

6. Haga clic en **Aplicar** para guardar los parámetros.



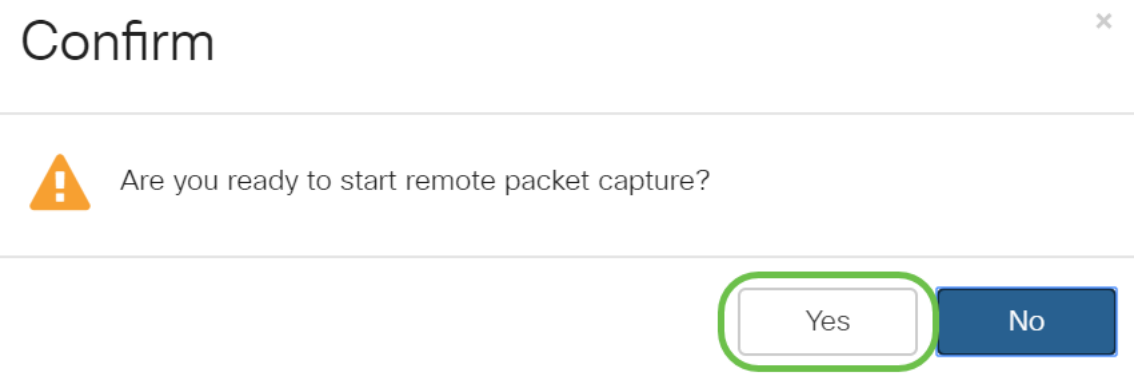
Paso 2

Haga clic en el icono **Iniciar captura**.



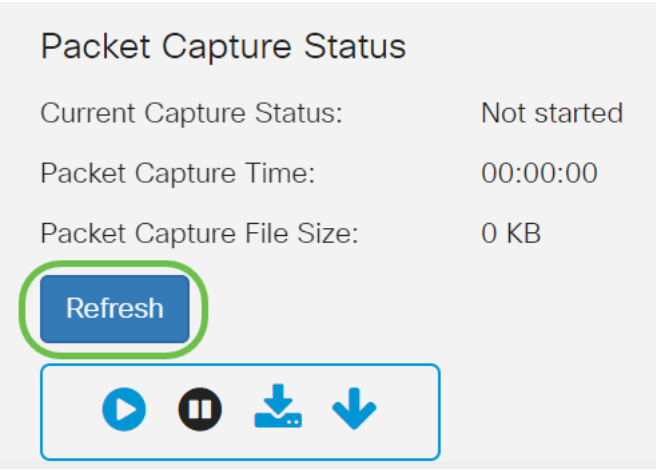
Paso 3

Se abrirá *una* ventana emergente de *confirmación*. Haga clic en **Sí** para iniciar la captura.



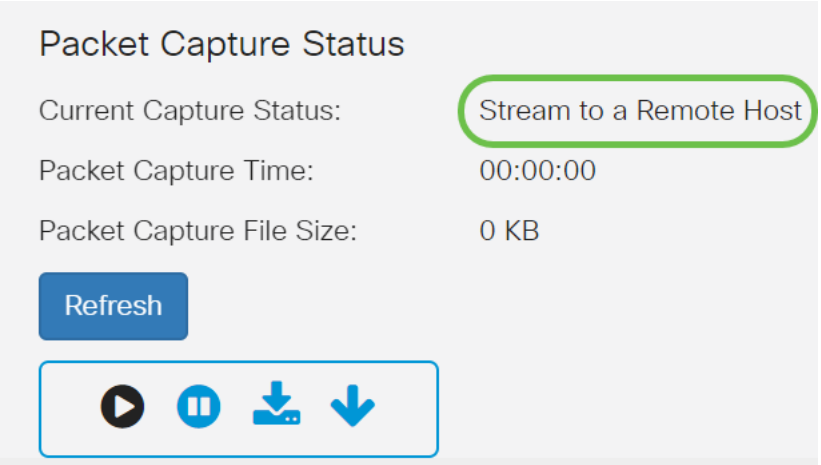
Paso 4

Haga clic en el botón **Refresh** para comprobar el estado actual.



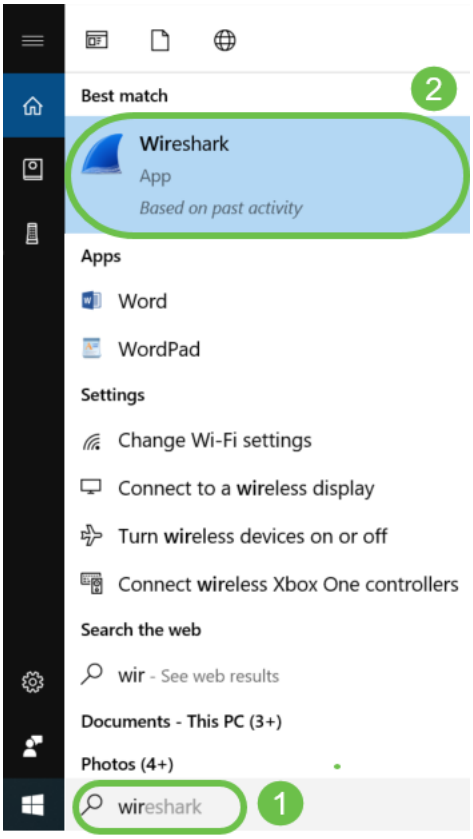
Paso 5

Ahora puede ver que el *Estado de captura actual* será *Transmisión a un Host Remoto*.



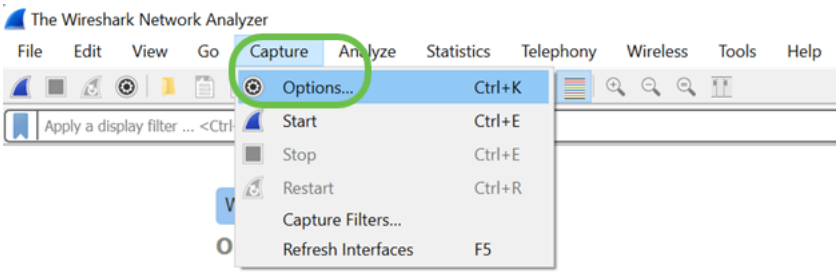
Paso 6

Dado que Wireshark ya se ha descargado, se puede acceder a él escribiendo **Wireshark** en la barra de búsqueda de Microsoft Windows y seleccionando la aplicación cuando se trata de una opción.



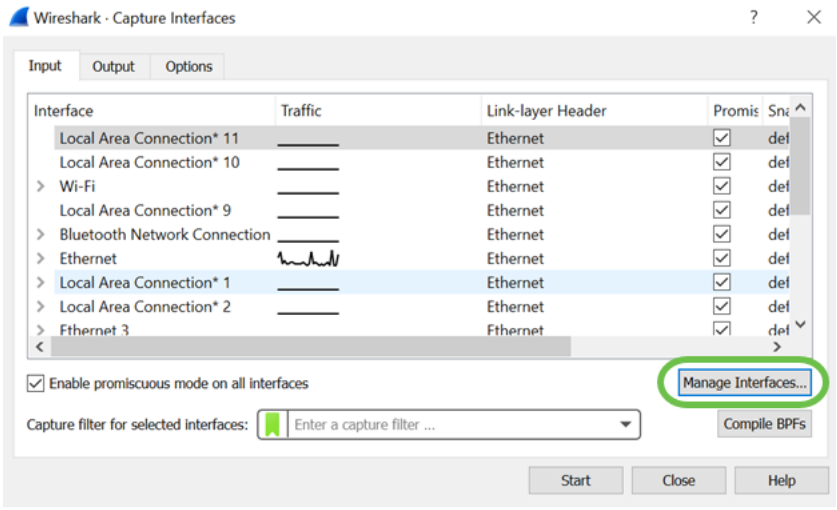
Paso 7

Vaya a **Captura > Opciones...**



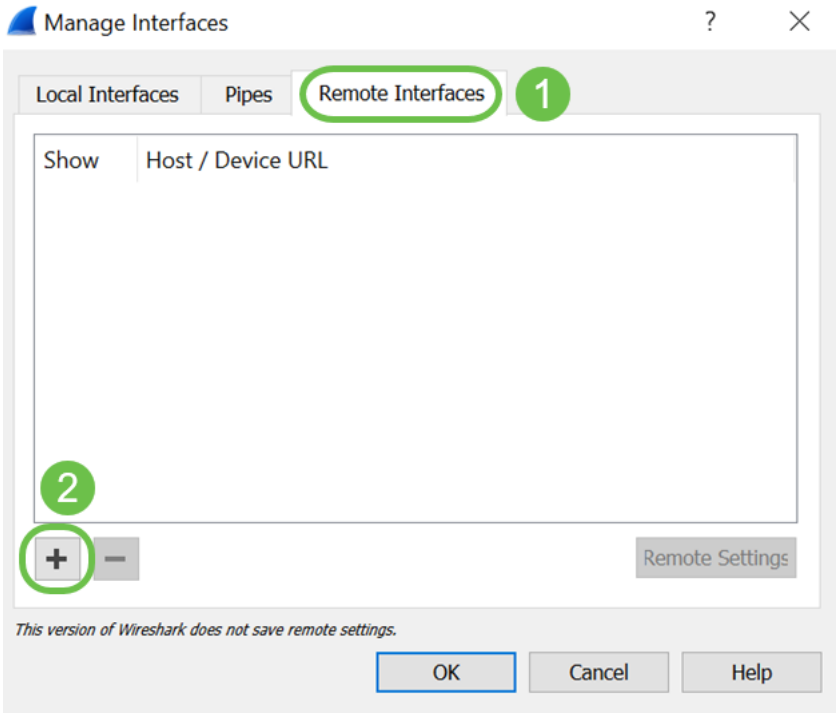
Paso 8

En la nueva ventana *Wireshark - Capture Interfaces*, haga clic en **Administrar interfaces**...



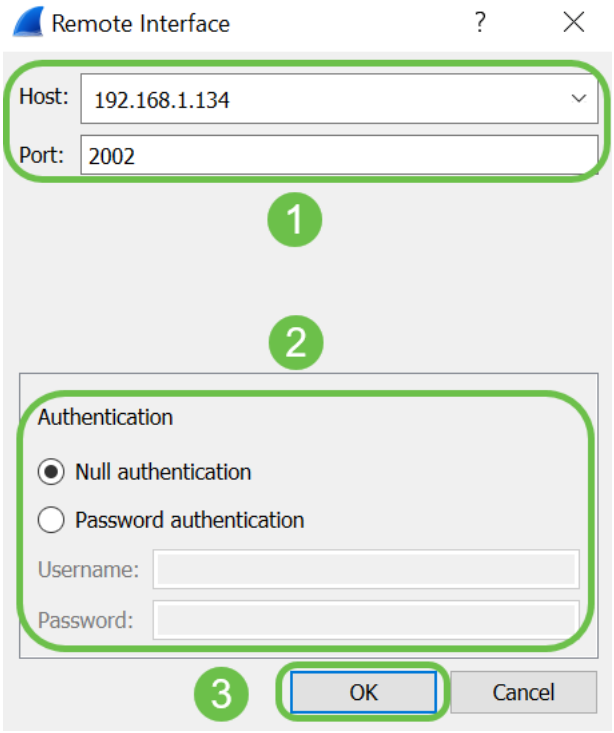
Paso 9

En la nueva ventana emergente *Administrar interfaces*, navegue hasta **Interfaces remotas** y haga clic en el **icono más** para agregar la interfaz.



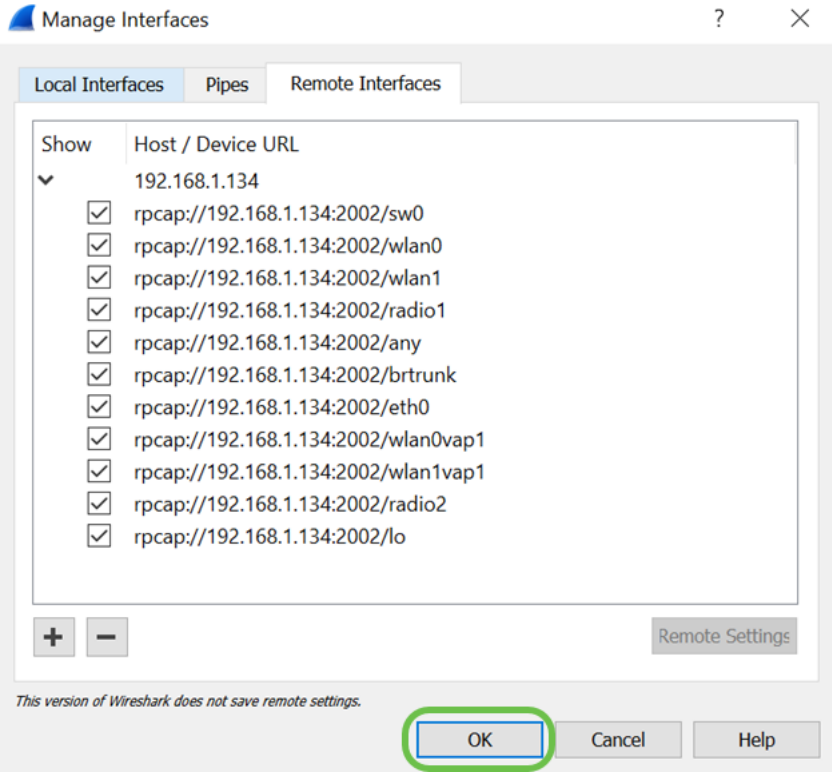
Paso 10

En la nueva ventana emergente *Remote Interface*, ingrese el *Host:* Detalles de la dirección IP (la IP del dispositivo WAP donde ha iniciado la captura remota) y *Puerto:* número (configurado en WAP para captura remota). En este caso, la IP del dispositivo WAP era 192.168.1.134. Puede seleccionar la opción *Null authentication* o *Password authentication* en función de sus parámetros. Si selecciona esta opción, introduzca los detalles *Nombre de usuario* y *Contraseña* en consecuencia. Click OK.



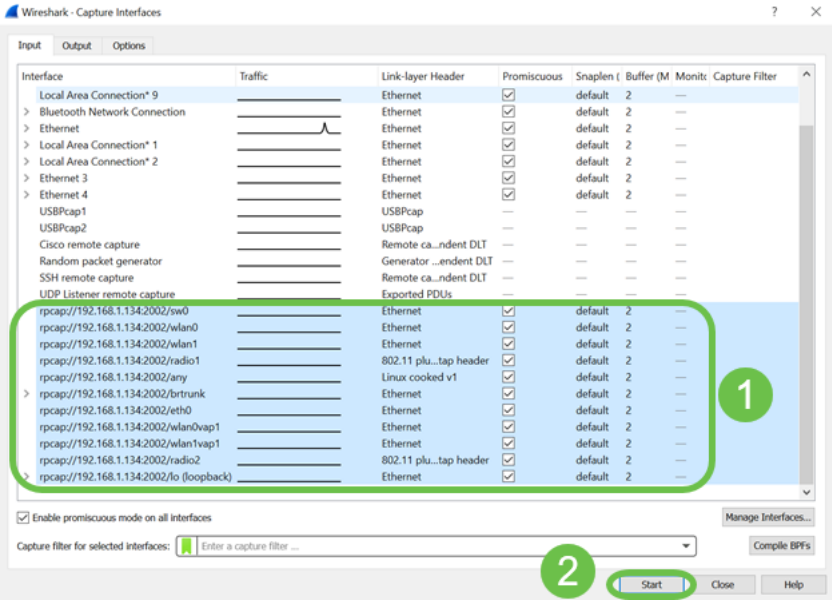
Paso 11

En la pestaña *Interfaces remotas*, podrá ver todas las interfaces del dispositivo WAP remoto. Es posible que sólo desee anular la selección de algunos de estos para reducir el volumen de paquetes capturados. Dejaría las interfaces de radio seleccionadas si desea ver los paquetes de baliza. Click OK.



Paso 12

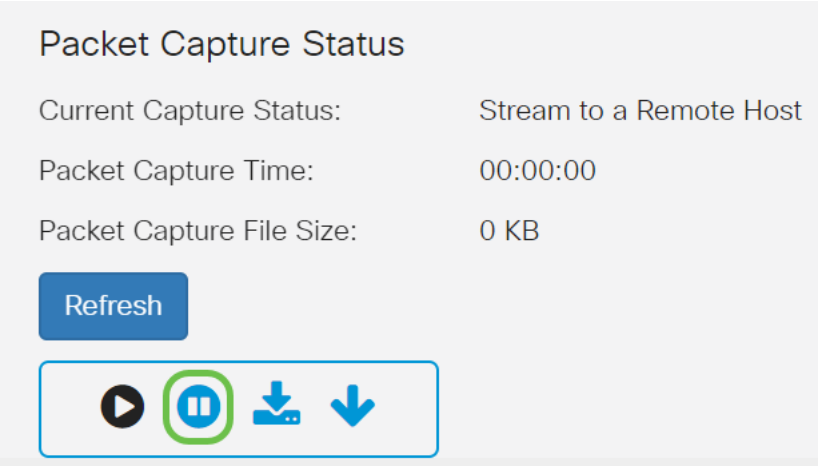
Ahora, las interfaces recién agregadas se reflejarán en la ventana *Wireshark - Capture Interfaces*. **Seleccione** la interfaz que desea monitorear y haga clic en **Start** para ver los paquetes.



Si encuentra problemas cuando intenta ver los paquetes, esto significa que el servicio *Remote Packet Capture Protocol* no está funcionando en su sistema. El servicio Remote Packet Capture Protocol debe estar ejecutándose primero en la plataforma de destino antes de que Wireshark pueda conectarse a ella. Para obtener más información, haga clic en el enlace *Interfaces de captura remota* a través de Wireshark.

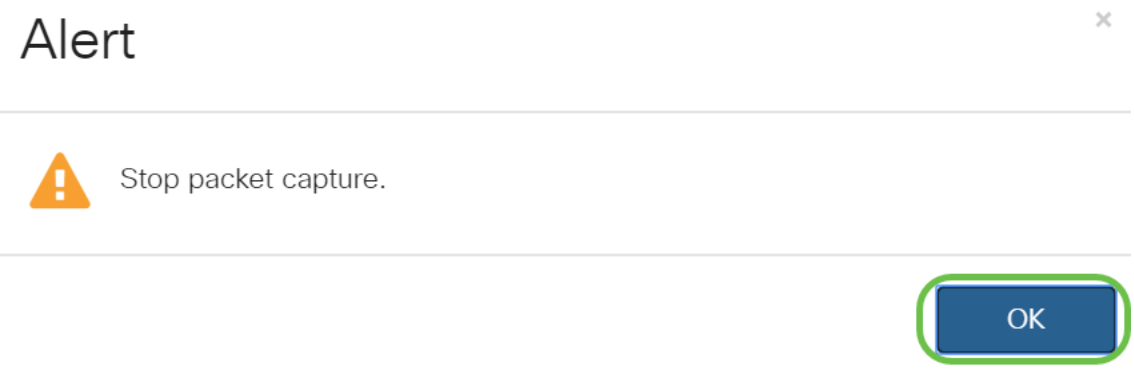
Paso 13

En el WAP, haga clic en el **icono Detener captura** para detener el proceso de captura.



Paso 14

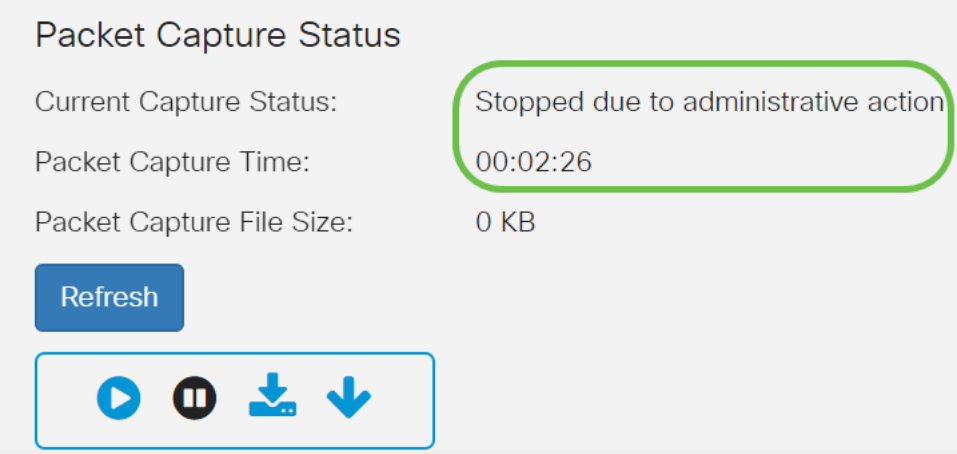
Aparecerá una ventana emergente *Alerta*. Haga clic en **Aceptar** para detener la captura remota.



También puede detener la captura de paquetes haciendo clic en el botón **Stop** en la aplicación Wireshark.

Paso 15

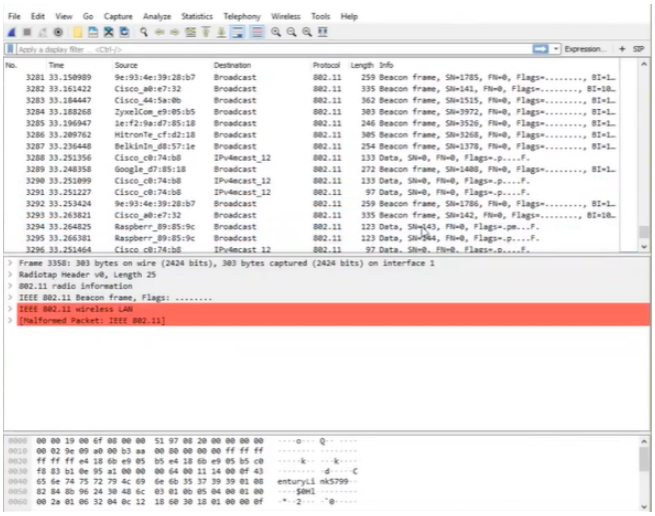
Ahora el *Estado de captura actual* se mostrará como *Detenido debido a la acción administrativa*, y el *Tiempo de captura de paquetes* se reflejará para mostrar la duración total de la captura.



El *tamaño del archivo de captura de paquetes* se mostrará como *0 KB*. Además, las opciones de descarga de archivos no funcionarán en esta situación.

Paso 16

En Wireshark puede ver la captura de paquetes.



Conclusión

Ahora tiene las habilidades para obtener un paquete transmitido directamente a Wireshark y puede trabajar analizándolo. ¿No está seguro de dónde ir desde aquí? Hay muchos videos y artículos disponibles en línea para explorar. Lo que busca depende de las necesidades de su situación. ¡Lo tienes!