

# Using Wireshark on a Cisco Business WAP for Packet Analysis: Stream Directly to Wireshark

## Objective

This article explains how to perform a packet capture of network traffic using a Cisco Business Wireless Access Point (WAP), and stream it directly to Wireshark.

## Table of Contents

- [Introduction and Frequently Asked Questions](#)
- [What is a packet capture?](#)
- [What types of packets can be captured?](#)
- [What are the ways a packet capture can be done on a WAP?](#)
- [Where can I stream the packet?](#)
- [Applicable Devices and Software Version](#)
- [Download Wireshark](#)
- [Log into the WAP](#)
- [Remote Packet Capture Explanation](#)
- [Stream a Capture Straight to Wireshark](#)

## Introduction and Frequently Asked Questions

Configuration changes, monitoring, and troubleshooting are something a network administrator has to deal with often. Having a simple tool to use is invaluable! The goal of this article is to get more comfortable with the basics of packet captures as well as how to stream the packets to Wireshark. If you are not familiar with this process, let us answer some questions you might have already.

First things first, Wireshark is a free packet analyzer for anyone looking to troubleshoot their network. Wireshark provides many options for the capture as well as sorting traffic by several different parameters. Head to [Wireshark](#) for details on this open-source option.

### What is a packet capture?

A packet capture, also known as a PCAP file, is a tool that can be helpful in troubleshooting. It can record every packet sent between devices in your network, in real time. Capturing packets allows you to dig into the details of the network traffic, which can include everything from device discovery, protocol conversations, and failed authentication. You can see the path of specific traffic flow and every interaction between devices on selected networks. These packets can be saved for further analysis as needed. It's like an x-ray of the network's inner workings via the transfer of packets.

### What types of packets can be captured?

The WAP device can capture the following types of packets:

- 802.11 packets received and transmitted wirelessly on the radio interfaces. Packets captured on the radio interfaces include the 802.11 header.
- 802.3 packets received and transmitted on the Ethernet interface.
- 802.3 packets received and transmitted on the internal logical interfaces, such as Virtual Access Points (VAPs) and Wireless Distribution System (WDS) interfaces.

## What are the ways a packet capture can be done on a WAP?

There are two methods of packet capture available:

1. *Local Capture Method* – Captured packets are stored in a file on the WAP device. The WAP device can transfer the file to a Trivial File Transfer Protocol (TFTP) server. The file is formatted in PCAP format and can be examined using Wireshark. You can choose *Save File on this Device* to select the local capture method.

If you prefer the local capture method, featuring latest Web User Interface (UI), check out [Using Wireshark on a WAP for Packet Analysis: Upload File](#).

If you prefer to view an article that uses the older GUI for the local capture method, check out [Configure Packet Capture to Optimize Performance on a Wireless Access Point](#).

2. *Remote Capture Method* – Captured packets are redirected in real time to an external computer running Wireshark. You can choose *Stream to a Remote Host* to select the remote capture method. The advantage of this method is that there is no limit to the volume of packets that can be captured.

The focus of this article is to Stream to a Remote Host, so if that is your preference, read on!

## Where can I stream the packet?

The wireless packet capture feature enables capturing and storing the packets received and transmitted by the WAP device. The captured packets can then be analyzed by a network protocol analyzer for troubleshooting or performance optimization. There are many third-party packet analyzer applications available online. In this article, we focus on Wireshark.

Some models of Cisco Business WAPs have the ability to send packets in real time to CloudShark, a web-based packet decoder and analyzer site. It is similar to the Wireshark User Interface (UI) for packet analysis that includes many added options with a subscription. You can choose *Stream to CloudShark* to select the remote capture method. For more information, click on the following links:

- [CloudShark](#) (their official website)
- [Integrating CloudShark for Packet Analysis on a WAP125 or WAP581](#)
- [CloudShark Integration with WAP571 and WAP571E](#)

Neither Wireshark or CloudShark are owned or supported by Cisco. They are included for demonstration purposes only. For support, contact [Wireshark](#) or [CloudShark](#).

## Applicable Devices and Software Version

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


## Download Wireshark

### Step 1

Go to the [Wireshark](#) website. Select the appropriate version. Click **Download**. You will see the progress of the download at the bottom left of the screen.

### Step 2

Go to *Downloads* on your computer and select the Wireshark file to install its application.

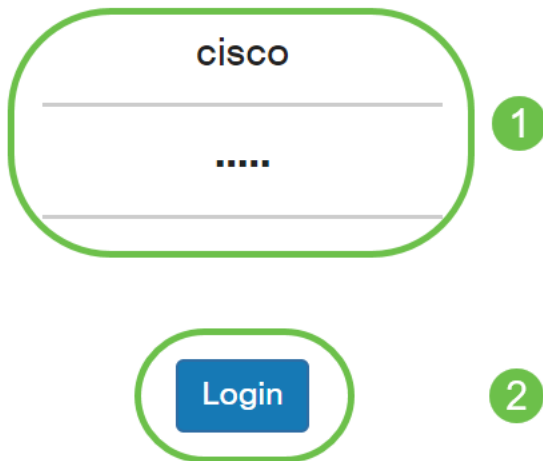
 Wireshark-win64-3.0.6.exe	10/30/2019 4:05 PM	Application	57,887 KB
--	--------------------	-------------	-----------

## Log into the WAP

In your web browser, enter the IP address of the WAP. Enter your credentials. If this is your first time accessing this device or you did a factory reset, the default username and password is *cisco*. If you need instructions on how to log in, you may follow the steps in the [Access the Web-based Utility of the Wireless Access Point \(WAP\)](#) article.



## Wireless Access Point



## Remote Packet Capture Explanation

The Remote Packet Capture feature enables you to specify a remote port as the destination port for packet captures. This feature works in conjunction with the Wireshark network analyzer tool for Windows. A packet capture server runs on the WAP device and sends the captured packets through a Transmission Control Protocol (TCP) connection to the Wireshark tool.

A Microsoft Windows computer running the Wireshark tool allows you to display, log, and analyze the captured traffic. The remote packet capture facility is a standard feature of the Wireshark tool for Windows.

While the remote packet capture is not supported by Linux, the Wireshark tool works under Linux and already created capture files can be viewed.

When the remote capture mode is in use, the WAP device does not store any captured data locally in its file system.

If a firewall is installed between the Wireshark installed computer and the WAP device, Wireshark must be allowed to pass through the firewall policy of the computer. The firewall must also be configured to allow the Wireshark computer to initiate a TCP connection to the WAP device.

## Stream a Capture Straight to Wireshark

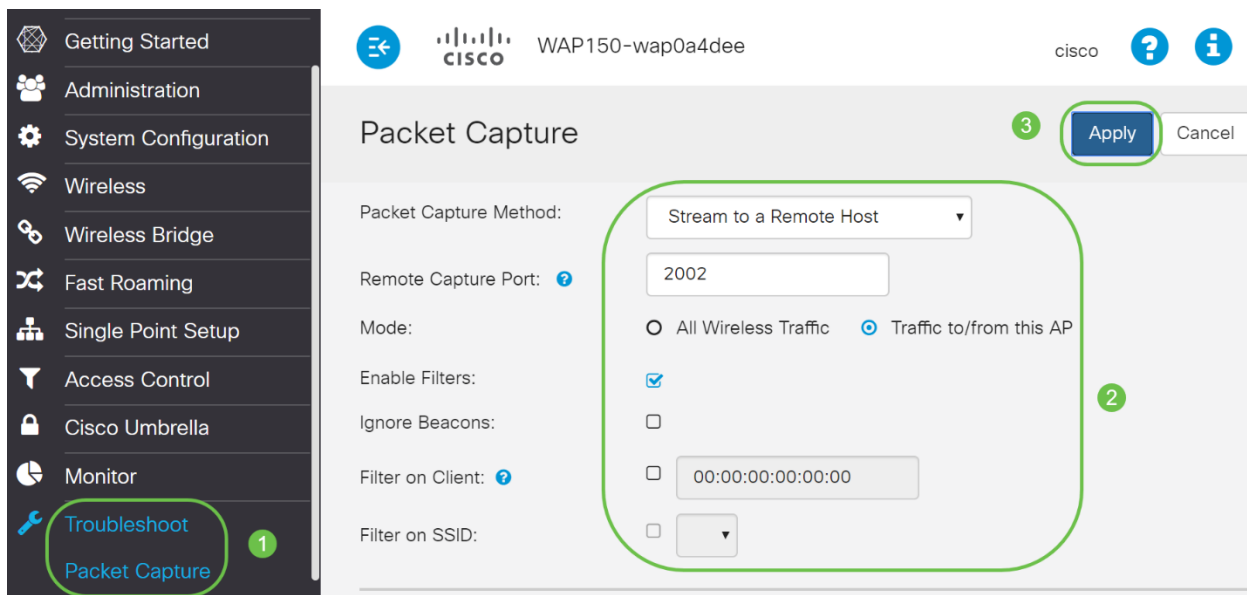
To initiate a remote capture on a WAP device using the *Stream to a Remote Host* option, follow the steps listed below.

## Step 1

On the WAP, navigate to **Troubleshoot > Packet Capture**.

For the *Packet Capture Method*:

1. Select **Stream to a Remote Host** from the drop-down menu.
2. In the *Remote Capture Port* field, use the default port of **2002**, or if you are using a port other than the default, enter the desired port number used to connect Wireshark to the WAP device. The port range is from 1025 to 65530.
3. There are two *Modes* for packet capture options. Select what is best for your scenario.
  - *All Wireless Traffic* – Capture all wireless packets in the air.
  - *Traffic to/from this AP* – Capture the packet sent from the AP or the AP received.
4. Check **Enable Filters**.
5. Choose from the following options:
  - *Ignore Beacons* – Enable or disable the capturing of 802.11 beacons detected or transmitted by the radio. Beacon frames are broadcast frames that carry information regarding a network. The purpose of a beacon is to advertise an existing wireless network.
  - *Filter on Client* – Once enabled, specify the MAC address for WLAN Client filter. Note that the Client filter is active only when a capture is performed on an 802.11 interface.
  - *Filter on SSID* - This option will be greyed out for this *Stream to a Remote Host* option.
6. Click **Apply** to save the settings.







## Step 2

Click on the **Start Capture** icon.

**Packet Capture Status**

Current Capture Status:	Not started
Packet Capture Time:	00:00:00
Packet Capture File Size:	0 KB

**Refresh**


   

### Step 3

A *confirm* pop-up window will open. Click on **Yes** to start the capture.

**Confirm** ×

---

 Are you ready to start remote packet capture?

---

**Yes** **No**





### Step 4

Click on the **Refresh** button to check the current status.

**Packet Capture Status**

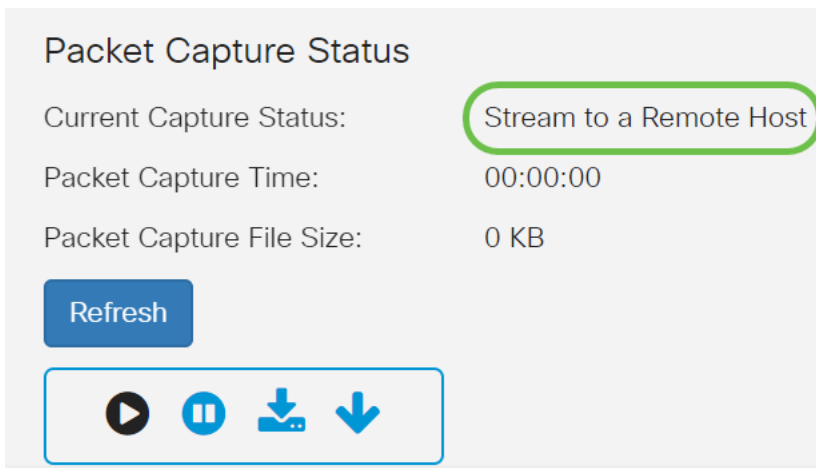
Current Capture Status:	Not started
Packet Capture Time:	00:00:00
Packet Capture File Size:	0 KB

**Refresh**

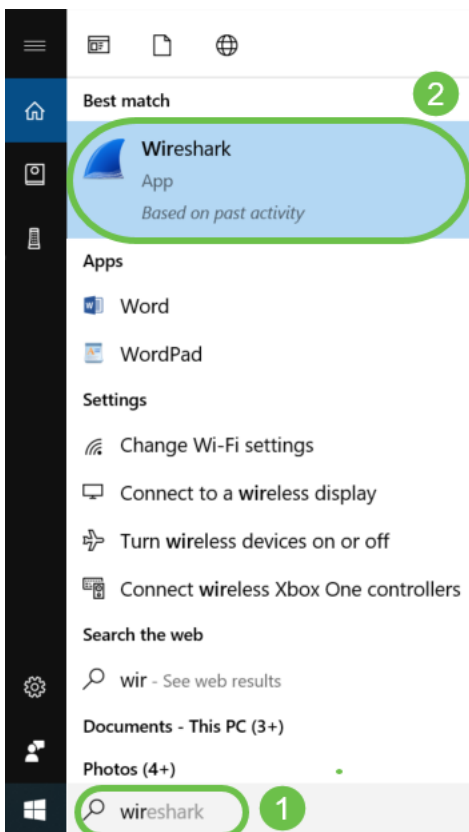
### Step 5

You can now see the *Current Capture Status* will be *Stream to a Remote Host*.



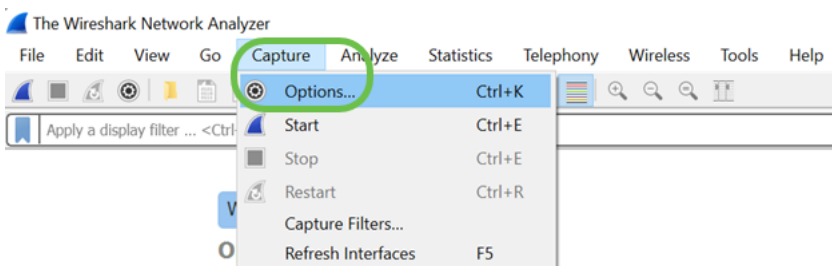
## Step 6

Since Wireshark has already been downloaded, it can be accessed by typing **Wireshark** in the search bar of Microsoft Windows and selecting the application when it is an option.



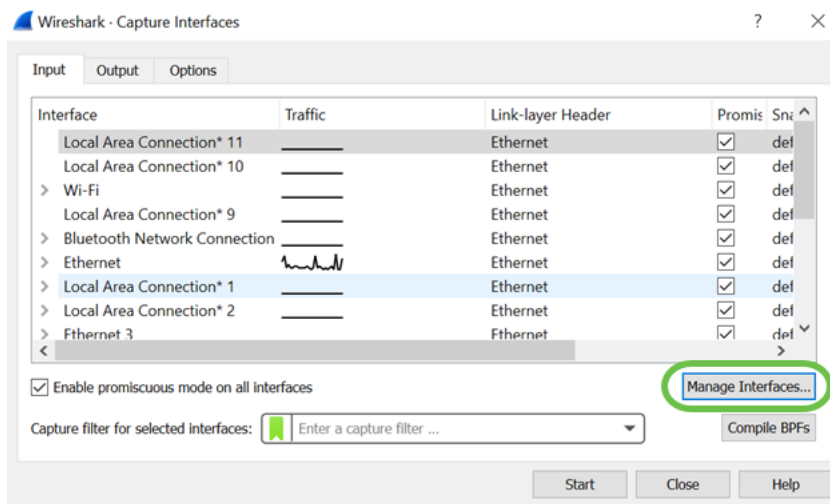
## Step 7

Navigate to **Capture > Options...**



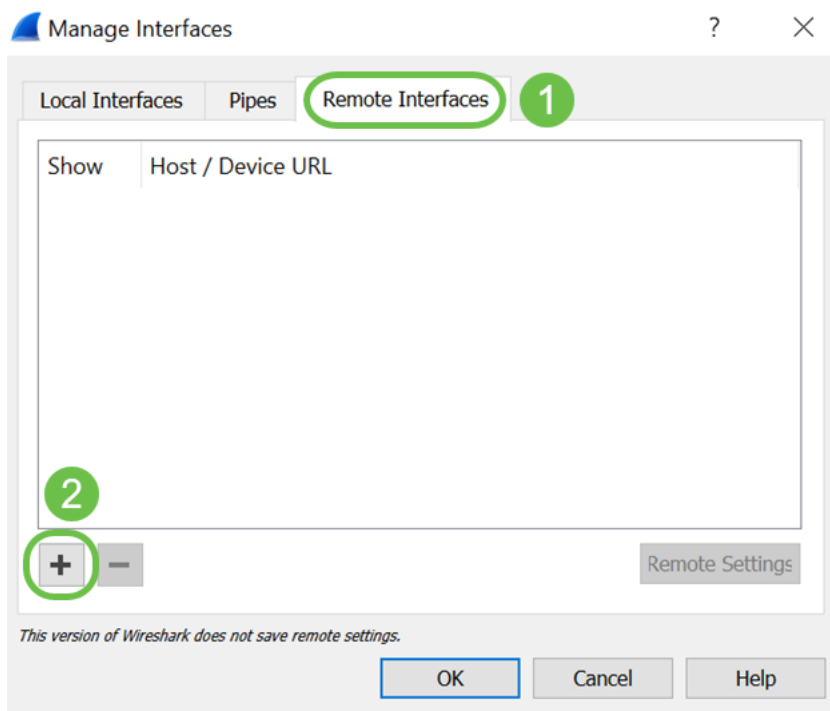
## Step 8

On the new pop-up *Wireshark – Capture Interfaces* window, click **Manage Interfaces...**



## Step 9

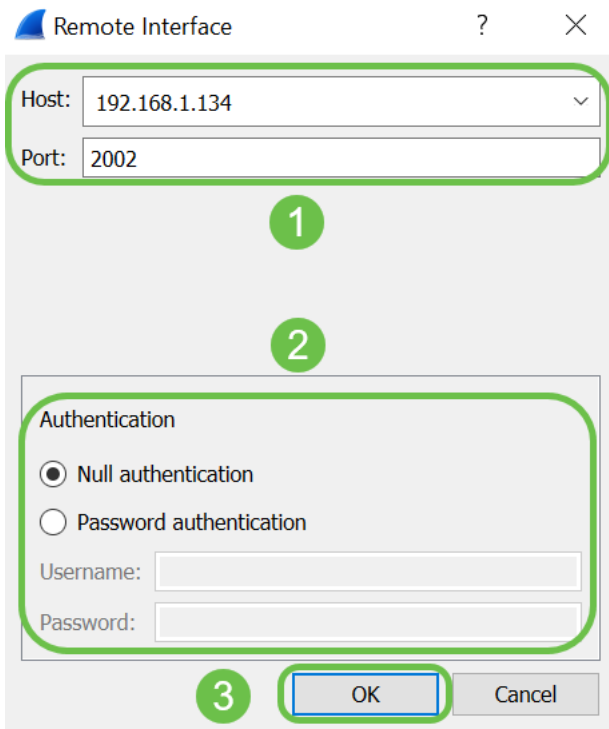
On the new *Manage Interfaces* pop-up window, navigate to **Remote Interfaces** and click on the **plus icon** to add the interface.



## Step 10

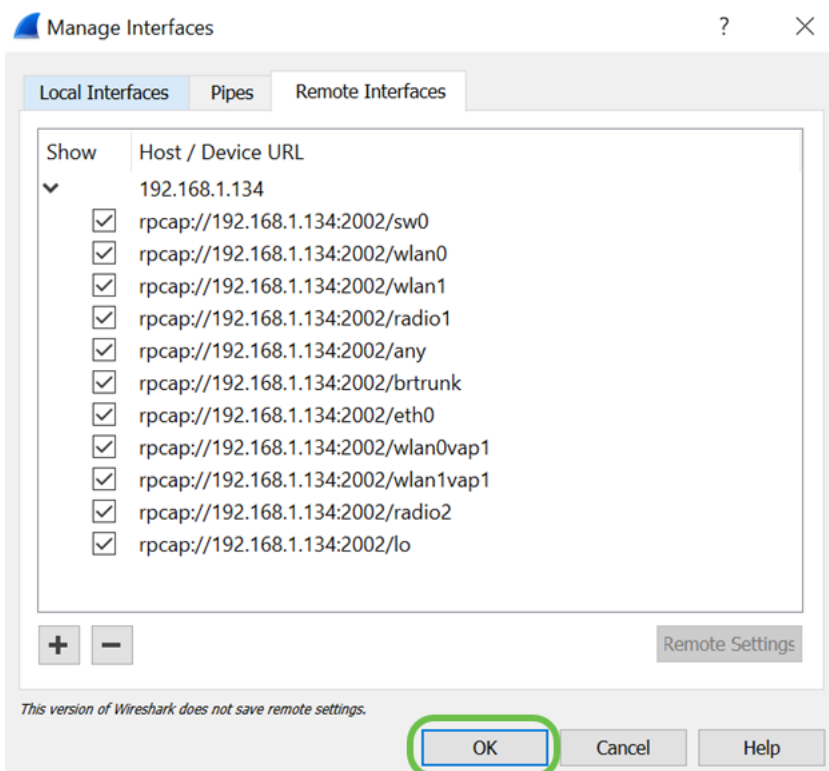
On the new *Remote Interface* pop-up window, enter the *Host*: IP address details (the WAP device IP where you have started the remote capture) and *Port*: number (configured on WAP for remote capture). In this case the WAP device IP was 192.168.1.134. You may select *Null authentication* or *Password authentication* option based on your settings. If you select, *Password authentication* then please enter the *Username* and *Password* details accordingly. Click **OK**.





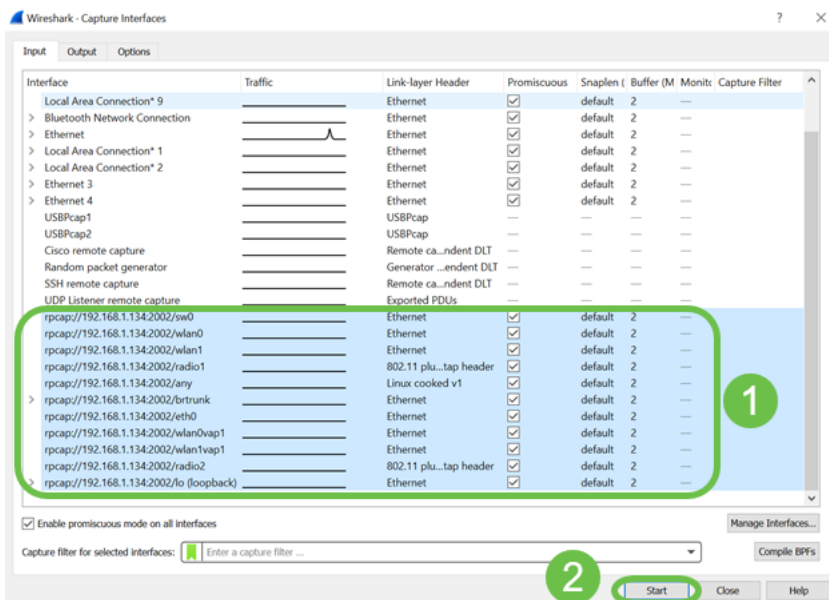
## Step 11

Under the *Remote Interfaces* tab, you will be able to see all the interfaces of the remote WAP device. You may want to only de-select some of these to reduce the volume of packets captured. You would leave the radio interfaces selected if you want to see beacon packets. Click **OK**.



## Step 12

Now newly added interfaces will reflect on the *Wireshark – Capture Interfaces* window. **Select** the interface you want to monitor and click **Start** to view the packets.



If you encounter issues when you attempt to view the packets, this means that the *Remote Packet Capture Protocol* service is not working on your system. The Remote Packet Capture Protocol service must first be running on the target platform before Wireshark can connect to it. For more information, click the link [Remote Capture Interfaces](#) through Wireshark.

### Step 13

On the WAP, click on the **Stop Capture icon** to stop the capture process.

#### Packet Capture Status

Current Capture Status: Stream to a Remote Host

Packet Capture Time: 00:00:00

Packet Capture File Size: 0 KB

[Refresh](#)

▶
⏸
⬇
⬇

### Step 14

An *Alert* pop-up window will appear. Click **OK** to stop the remote capture.

## Alert ✕

---

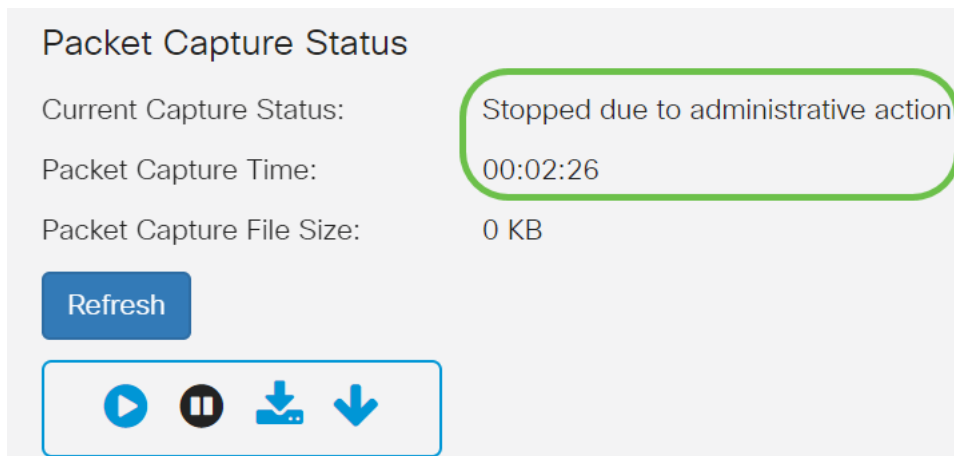
Stop packet capture.

OK

You may also stop the packet capture by clicking on the **Stop** button in Wireshark application.

## Step 15

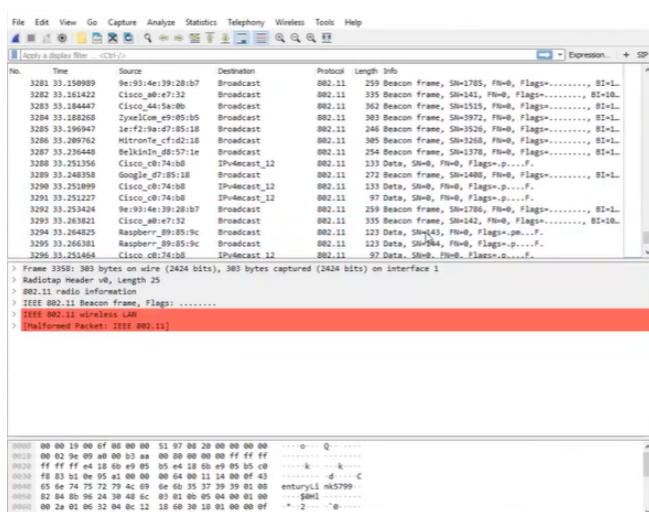
Now the *Current Capture Status* will be showing as *Stopped due to administrative action*, and *Packet Capture Time* will be reflecting to show the total capture duration.



The *Packet Capture File Size* will show as *0 KB*. In addition, file download options will not work in this scenario.

## Step 16

On Wireshark you can view your packet capture.



## Conclusion

You now have the skills to get a packet streamed directly to Wireshark and you can get to work analyzing it. Not sure where to go from here? There are plenty of videos and articles available online to explore. What you search for depends on the needs of your situation. You've got this!