

# 在思科业务WAP上使用Wireshark进行数据包分析： 直接流到Wireshark

## 目标

本文介绍如何使用思科业务无线接入点(WAP)执行网络流量的数据包捕获，并直接将其流传输到Wireshark。

## 目录

- [简介和常见问题](#)
- [什么是数据包捕获？](#)
- [可以捕获哪些类型的数据包？](#)
- [在WAP上执行数据包捕获的方式是什么？](#)
- [在哪里可以传输数据包？](#)
- [适用的设备和软件版本](#)
- [下载Wireshark](#)
- [登录WAP](#)
- [远程数据包捕获说明](#)
- [将捕获直接流到Wireshark](#)

## 简介和常见问题

配置更改、监控和故障排除是网络管理员必须经常处理的问题。使用简单的工具非常宝贵！本文的目标是更轻松地了解数据包捕获的基本信息，以及如何将数据包流传输到Wireshark。如果您不熟悉此流程，让我们回答您可能已经提出的一些问题。

首先，Wireshark是一款免费的数据包分析器，适用于任何想要排除网络故障的人。Wireshark提供了许多捕获选项，以及按多个不同参数对流量进行分类。转到[Wireshark](#)，了解此开源选项的详细信息。

## 什么是数据包捕获？

数据包捕获（也称为PCAP文件）是有助于排除故障的工具。它可以实时记录网络中设备之间发送的每个数据包。通过捕获数据包，您可以深入了解网络流量的详细信息，其中可能包括从设备发现、协议会话和失败的身份验证等所有内容。您可以看到特定流量的路径以及所选网络上设备之间的每次交互。可根据需要保存这些数据包以进行进一步分析。它就像通过数据包传输来检查网络内部运作的X光。

## 可以捕获哪些类型的数据包？

WAP设备可以捕获以下类型的数据包：

- 在无线电接口上无线接收和发送802.11个数据包。在无线电接口上捕获的数据包包括802.11报头。
- 在以太网接口上接收和传输的802.3数据包。
- 在内部逻辑接口(如虚拟接入点(VAP)和无线分布系统(WDS)接口)上接收和传输的802.3数据包。

## 在WAP上执行数据包捕获的方式是什么？

有两种数据包捕获方法可用：

1. **本地捕获方法** — 捕获的数据包存储在WAP设备上的文件中。WAP设备可以将文件传输到简单文件传输协议(TFTP)服务器。文件采用PCAP格式，可以使用Wireshark进行检查。可以选择“[在此设备上保存文件](#)”以选择本地捕获方法。

如果您更喜欢本地捕获方法(采用最新的Web用户界面(UI))，请选中[在WAP上使用Wireshark进行数据包分析：上载文件](#)。

如果您喜欢查看使用旧GUI进行本地捕获方法的文章，请选中[配置数据包捕获以优化无线接入点的性能](#)。

2. **远程捕获方法** — 捕获的数据包会实时重定向到运行Wireshark的外部计算机。可以选择 *Stream to a Remote Host* 以选择远程捕获方法。此方法的优点是，对可捕获的数据包数量没有限制。

本文的重点是“流到远程主机”，因此，如果这是您的偏好，请阅读！

## 在哪里可以传输数据包？

无线分组捕获功能可捕获和存储由WAP设备接收和传输的分组。然后，网络协议分析器可以分析捕获的数据包，以便进行故障排除或性能优化。有许多第三方数据包分析器应用程序可在线使用。在本文中，我们重点介绍Wireshark。

某些型号的思科企业WAP能够实时将数据包发送到CloudShark（基于Web的数据包解码器和分析器站点）。它类似于数据包分析的Wireshark用户界面(UI)，其中包括许多添加的订用选项。您可以选择 *Stream to CloudShark* 以选择远程捕获方法。有关详细信息，请点击以下链接：

- [CloudShark](#)（其官方网站）
- [在WAP125或WAP581上集成CloudShark以进行数据包分析](#)
- [与WAP571和WAP571E集成的CloudShark](#)

思科不拥有或支持Wireshark或CloudShark。仅用于演示目的。如需支持，请[联系Wireshark](#)或[CloudShark](#)。

## 适用的设备和软件版本

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

## 下载Wireshark

### 第 1 步

转到Wireshark[网站](#)。选择适当的版本。单击 **Download**。您将在屏幕左下角看到下载进度。

## 步骤 2

转到计算机上的“下载”并选择Wireshark文件以安装其应用程序。

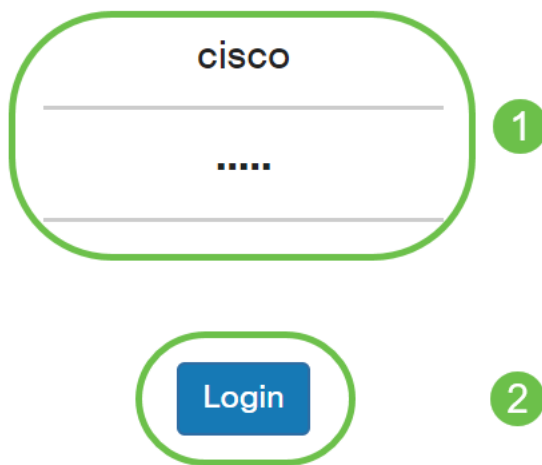
 Wireshark-win64-3.0.6.exe	10/30/2019 4:05 PM	Application	57,887 KB
--	--------------------	-------------	-----------

## 登录WAP

在Web浏览器中，输入WAP的IP地址。输入您的凭证。如果这是您首次访问此设备或您执行了出厂重置，则默认用户名和密码为 *cisco*。如果需要有关如何登录的说明，可以按照[访问无线接入点 \(WAP\) 的基于Web的实用程序\(Access the Web-based Utility\)](#)一文中的步骤操作。



### Wireless Access Point



## 远程数据包捕获说明

远程数据包捕获功能使您能够指定远程端口作为数据包捕获的目标端口。此功能与Wireshark网络分析工具（适用于Windows）配合使用。数据包捕获服务器在WAP设备上运行，并通过传输控制协议 (TCP) 连接将捕获的数据包发送到Wireshark工具。

运行Wireshark工具的Microsoft Windows计算机允许您显示、记录和分析捕获的流量。远程数据包捕获设备是Wireshark工具的标准功能。

虽然Linux不支持远程数据包捕获，但Wireshark工具在Linux下工作，并且可以查看已创建的捕获文件。

当远程捕获模式正在使用时，WAP设备不会在其文件系统中本地存储任何捕获的数据。

如果在安装了Wireshark的计算机和WAP设备之间安装了防火墙，则必须允许Wireshark通过计算机的防火墙策略。还必须配置防火墙，以允许Wireshark计算机启动与WAP设备的TCP连接。

## 将捕获直接流到Wireshark

要使用“流到远程主机”选项在WAP设备上启动远程捕获，请执行以下步骤。

### 第 1 步

在WAP上，导航至Troubleshoot > Packet Capture。

对于数据包捕获方法：

1. 从下拉菜单中选择Stream to a Remote Host。
2. 在远程捕获端口字段中，使用默认端口2002，或者如果您使用的端口不是默认端口，请输入将Wireshark连接到WAP设备所需的端口号。端口范围为1025到65530。
3. 数据包捕获选项有两种模式。选择最适合您的场景的选项。

·所有无线流量 — 捕获空中的所有无线数据包。

·进出此AP的流量 — 捕获从AP或收到的AP发送的数据包。

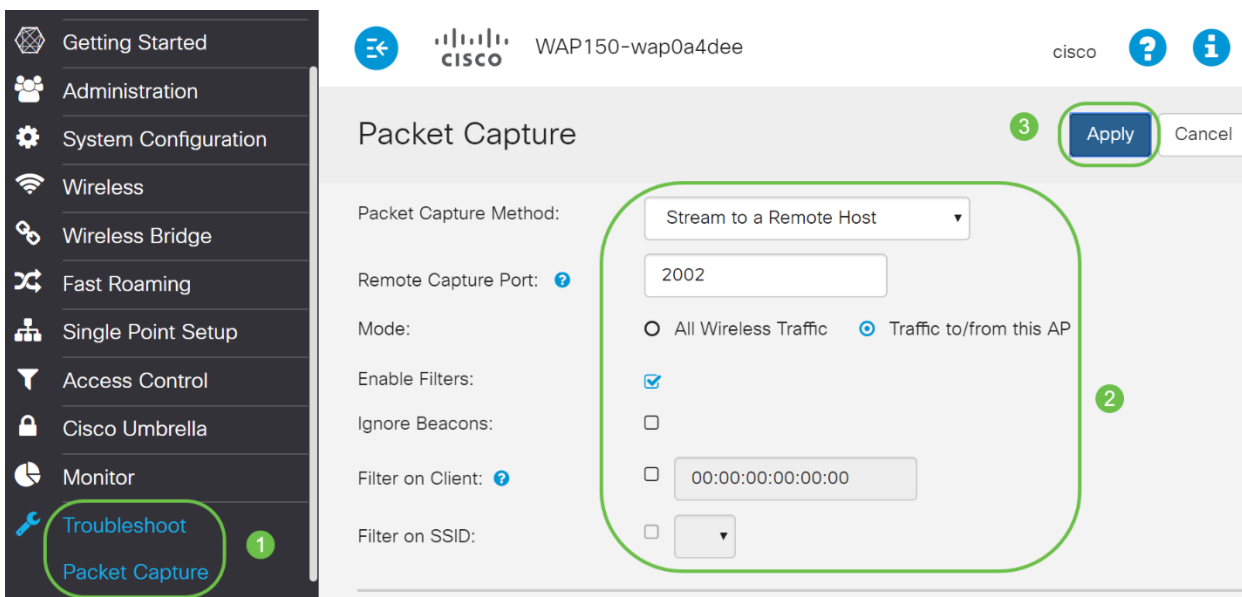
4. 选中启用过滤器。
5. 从下列选项中选择：

·忽略信标 — 启用或禁用捕获无线电检测或传输的802.11信标。信标帧是传送有关网络信息的广播帧。信标的目的是通告现有的无线网络。

·Filter on Client — 启用后，指定WLAN Client过滤器的MAC地址。请注意，仅当在802.11接口上执行捕获时，客户端过滤器才处于活动状态。

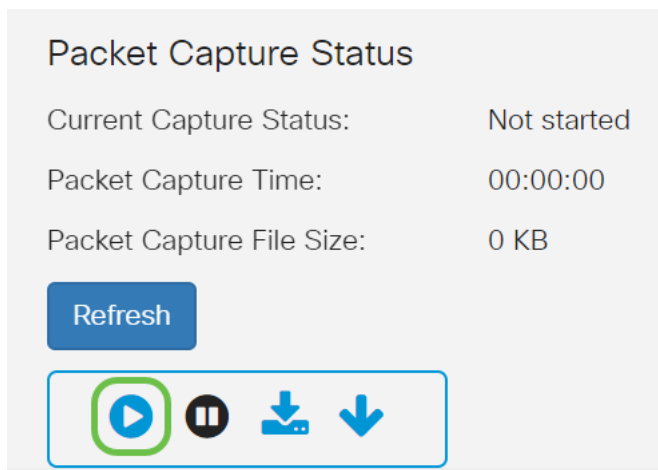
·按SSID过滤 — 此“流到远程主机”选项的此选项将灰显。

6.单击“应用”保存设置。



### 步骤 2

单击“开始捕获”图标。



Packet Capture Status

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

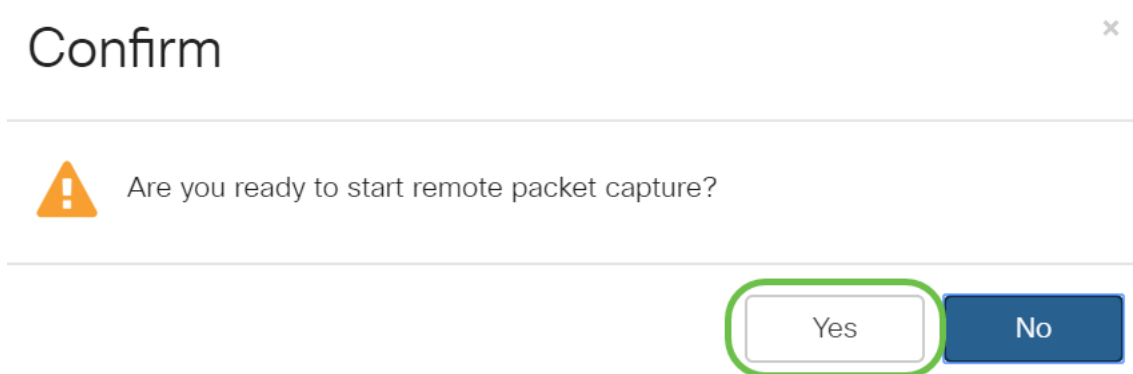
Refresh

▶ || ⬇️ ⬇️

Detailed description: This screenshot shows a 'Packet Capture Status' panel. It contains a table with three rows: 'Current Capture Status' (Not started), 'Packet Capture Time' (00:00:00), and 'Packet Capture File Size' (0 KB). Below the table is a blue 'Refresh' button. At the bottom, there is a toolbar with four icons: a play button (highlighted with a green circle), a pause button, a download icon, and another download icon.

### 步骤 3

将会打开确认弹出窗口。单击“是”开始捕获。



Confirm

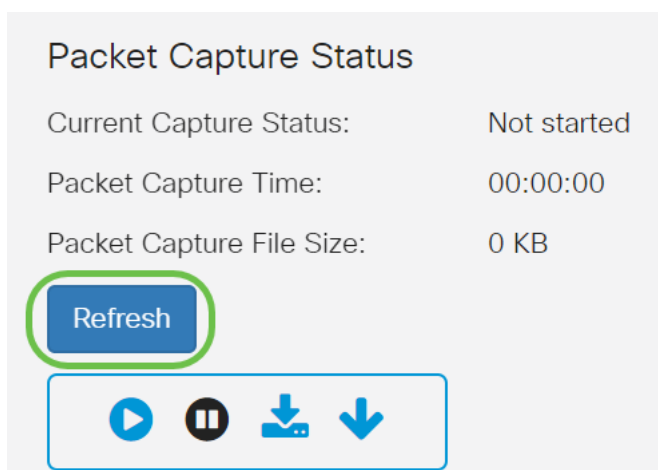
⚠️ Are you ready to start remote packet capture?

Yes No

Detailed description: This is a 'Confirm' dialog box. It has a title bar with a close button (x). Below the title bar is a warning icon (triangle with exclamation mark) and the text 'Are you ready to start remote packet capture?'. At the bottom, there are two buttons: 'Yes' (highlighted with a green circle) and 'No'.

### 步骤 4

单击“刷新”按钮以检查当前状态。



Packet Capture Status

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

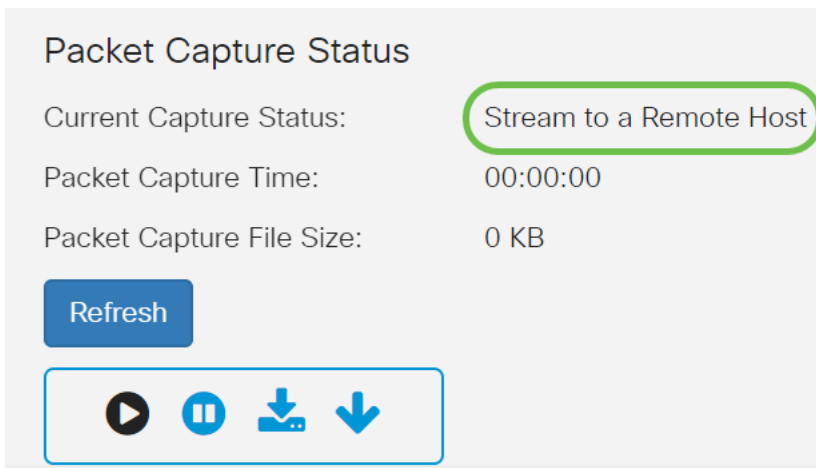
Refresh

▶ || ⬇️ ⬇️

Detailed description: This screenshot is similar to the first one, showing the 'Packet Capture Status' panel. The 'Refresh' button is now highlighted with a green circle. The status information remains the same: 'Not started', '00:00:00', and '0 KB'. The toolbar icons are also present.

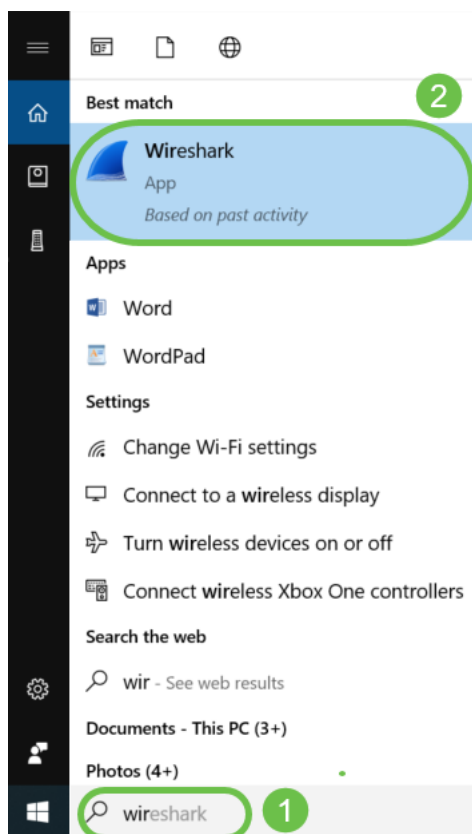
### 步骤 5

现在，您可以看到“当前捕获状态”将是“流到远程主机”。



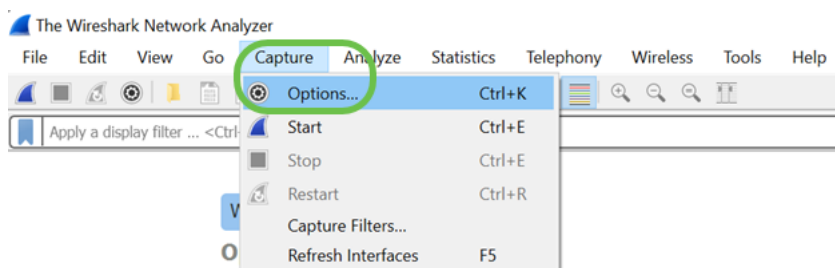
## 步骤 6

由于Wireshark已下载，因此可以在Microsoft Windows的搜索栏中键入**Wireshark**并在应用程序为选项时选择该应用程序来访问它。



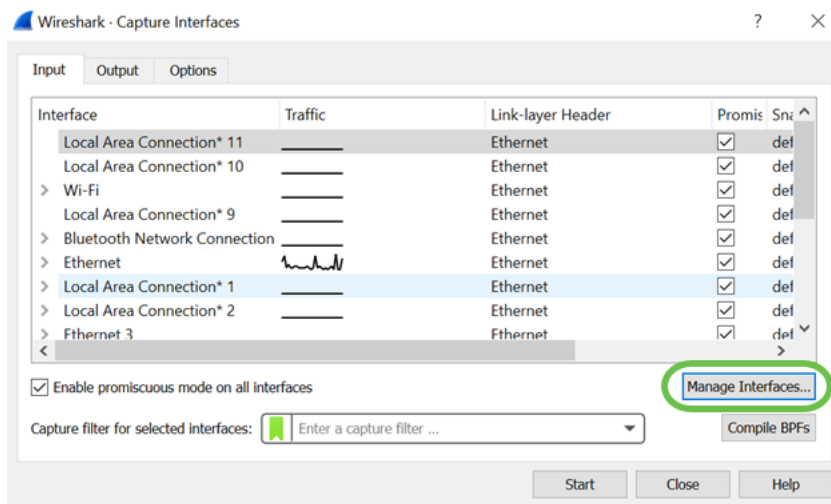
## 步骤 7

导航到**捕获>选项.....**



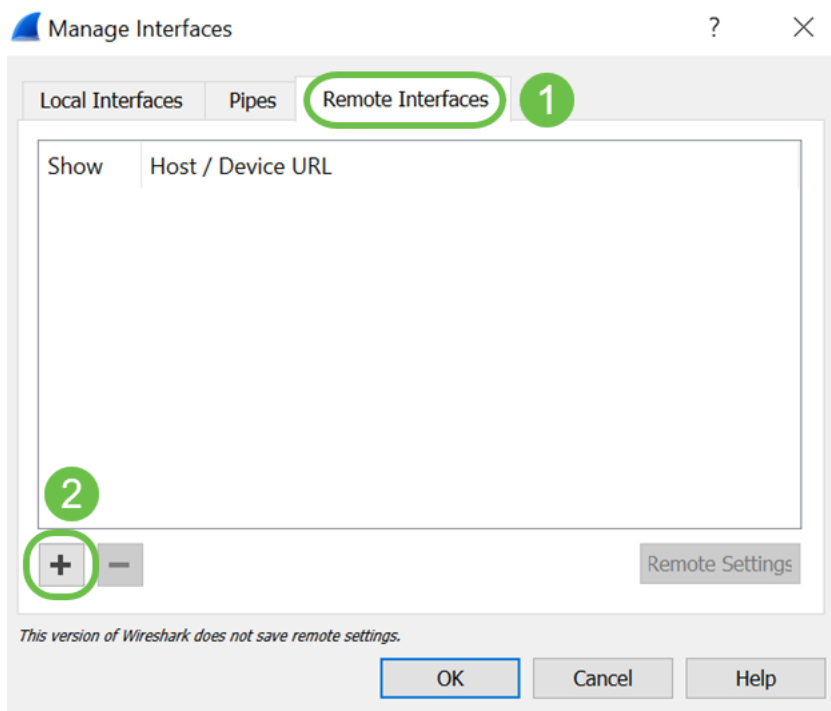
## 步骤 8

在新的弹出窗口Wireshark - *Capture Interfaces* ( 捕获接口 ) 窗口中 , 单击**Manage Interfaces...**



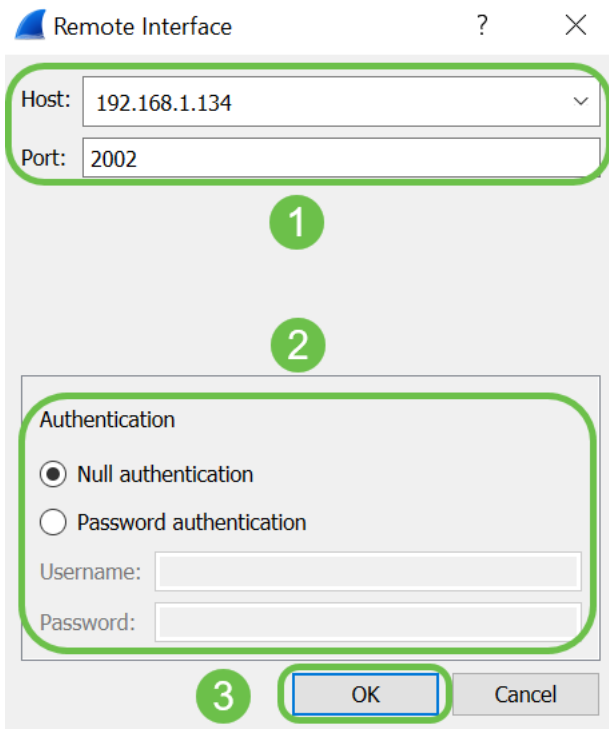
## 步骤 9

在新的“管理接口”弹出窗口中 , 导航至“远程接口” , 然后单击加号图标添加接口。



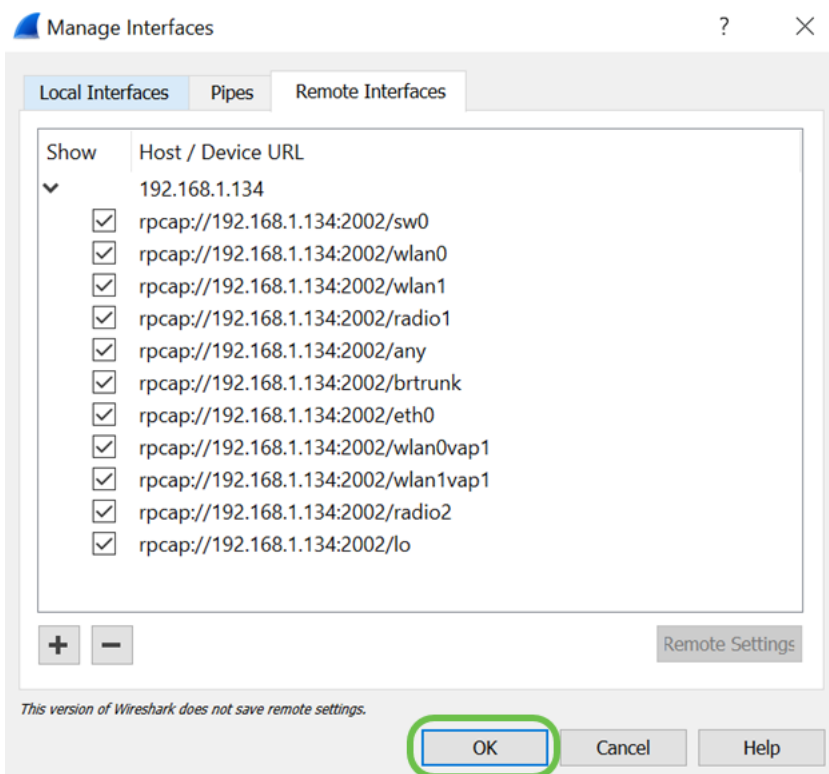
## 步骤 10

在新的“远程接口”弹出窗口中 , 输入主机 : IP地址详细信息 ( 已启动远程捕获的WAP设备IP ) 和端口 : 编号 ( 在WAP上配置以进行远程捕获 ) 。 在这种情况下 , WAP设备IP为192.168.1.134。您可以根据设置选择Null身份验证或Password身份验证选项。如果选择“密码身份验证” , 请相应地输入用户名和密码详细信息。Click OK.



## 步骤 11

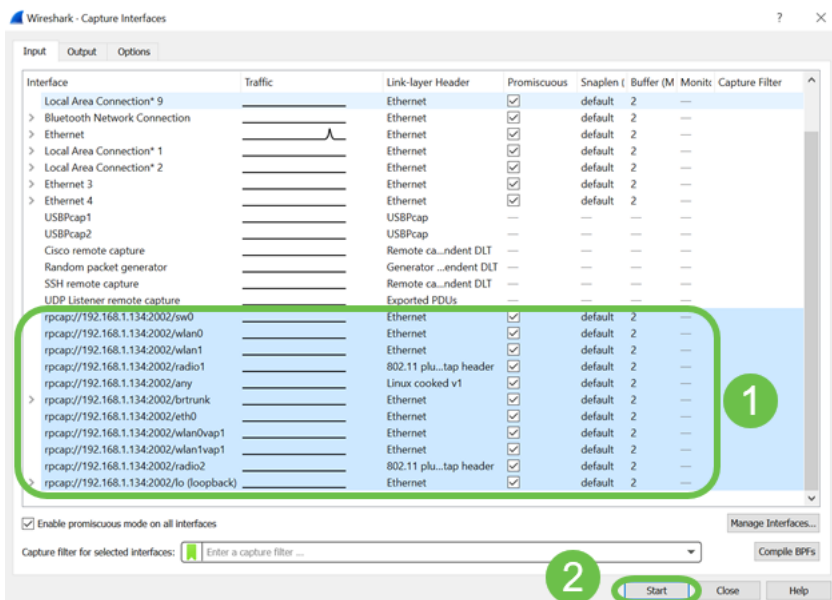
在 *Remote Interfaces* 选项卡下，您将能够看到远程WAP设备的所有接口。您可能只想取消选择其中一些，以减少捕获的数据包数量。如果要查看信标数据包，应将无线电接口保留为选中状态。Click OK.



## 步骤 12

现在，新添加的接口将反映在 *Wireshark - Capture Interfaces* 窗口中。选择要监控的接口，然后单击“开始”查看数据包。

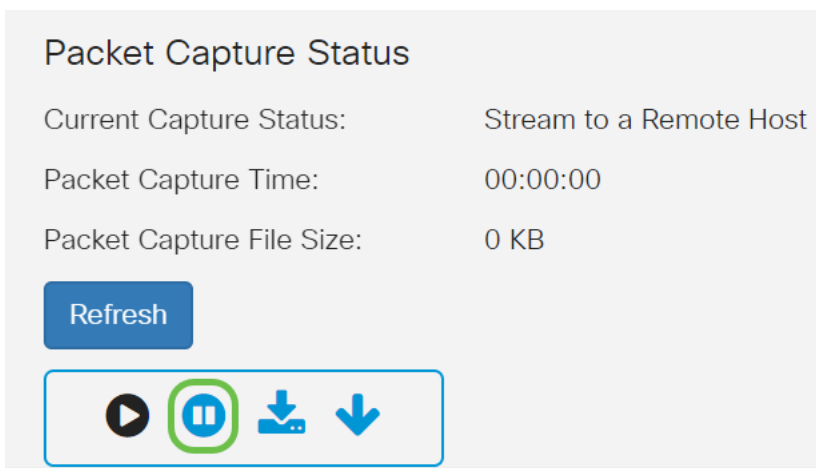




如果在尝试查看数据包时遇到问题，这意味着远程数据包捕获协议服务在您的系统上不工作。远程数据包捕获协议服务必须先要在目标平台上运行，Wireshark才能连接到它。有关详细信息，请单击通过Wireshark的[远程捕获](#)接口链接。

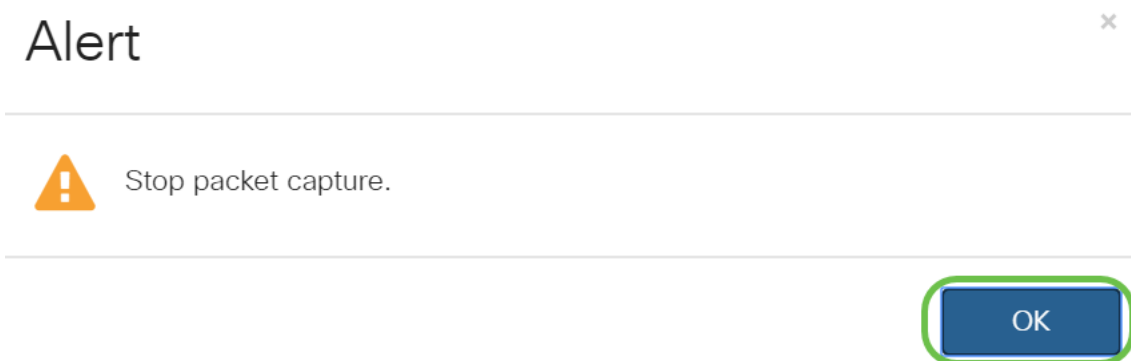
### 步骤 13

在WAP上，单击停止捕获图标以停止捕获过程。



### 步骤 14

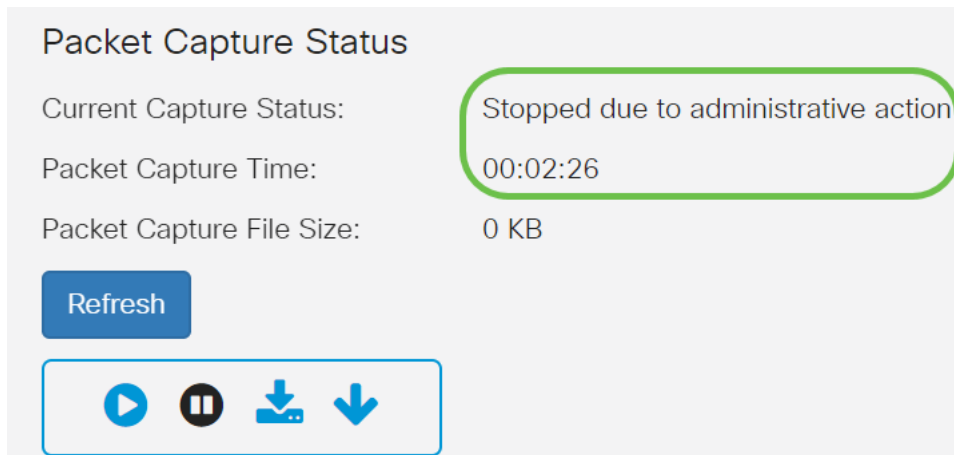
系统将显示一个警报弹出窗口。单击OK以停止远程捕获。



您也可以单击Wireshark应用程序中的“停止”按钮来停止数据包捕获。

## 步骤 15

现在，由于管理操作，当前捕获状态将显示为“已停止”，并且数据包捕获时间将反映为显示总捕获持续时间。



Packet Capture Status

Current Capture Status: Stopped due to administrative action

Packet Capture Time: 00:02:26

Packet Capture File Size: 0 KB

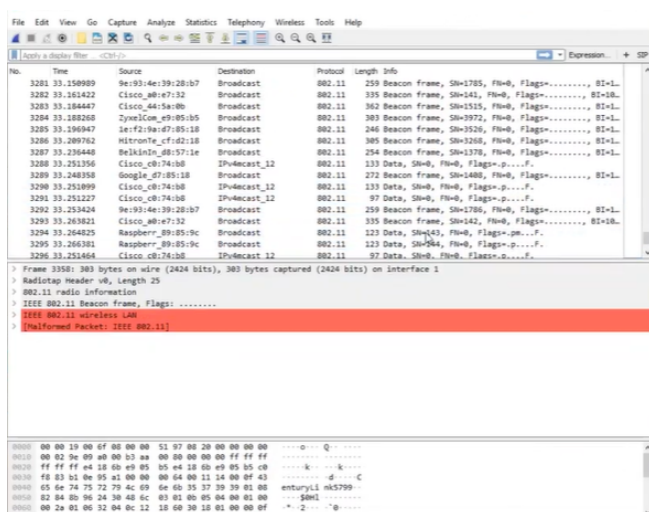
Refresh

▶ ⏸ ⬇ ⬇

数据包捕获文件大小将显示为 0 KB。此外，文件下载选项在此场景中不起作用。

## 步骤 16

在Wireshark上，您可以查看数据包捕获。



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <C3F>

No.	Time	Source	Destination	Protocol	Length	Info
3282	33.150900	Re:93:4e:39:28:b7	Broadcast	002.11	259	Beacon frame, SMI=725, FMI=0, Flags=....., BI=L
3282	33.151422	Cisco_0e:47:32	Broadcast	002.11	335	Beacon frame, SMI=441, FMI=0, Flags=....., BI=L
3283	33.184447	Cisco_4a:5a:8b	Broadcast	002.11	362	Beacon frame, SMI=515, FMI=0, Flags=....., BI=L
3284	33.188260	ZyexIca:e9:85:b5	Broadcast	002.11	383	Beacon frame, SMI=972, FMI=0, Flags=....., BI=L
3285	33.196947	Ie:72:8a:d7:85:18	Broadcast	002.11	244	Beacon frame, SMI=526, FMI=0, Flags=....., BI=L
3286	33.209762	MitronT:e:fd:2:18	Broadcast	002.11	385	Beacon frame, SMI=326, FMI=0, Flags=....., BI=L
3287	33.236448	BelkinT:e:08:57:1e	Broadcast	002.11	254	Beacon frame, SMI=378, FMI=0, Flags=....., BI=L
3288	33.251356	Cisco_c8:74:b8	IPv4cast_12	002.11	133	Data, SMI=0, FMI=0, Flags=p....f
3289	33.248358	Google_07:85:18	Broadcast	002.11	272	Beacon frame, SMI=480, FMI=0, Flags=....., BI=L
3290	33.251899	Cisco_c8:74:b8	IPv4cast_12	002.11	133	Data, SMI=0, FMI=0, Flags=p....f
3291	33.251227	Cisco_c8:74:b8	IPv4cast_12	002.11	97	Data, SMI=0, FMI=0, Flags=p....f
3292	33.253424	Re:93:4e:39:28:b7	Broadcast	002.11	259	Beacon frame, SMI=726, FMI=0, Flags=....., BI=L
3293	33.263821	Cisco_0e:47:32	Broadcast	002.11	335	Beacon frame, SMI=442, FMI=0, Flags=....., BI=L
3294	33.264825	Raspber:89:85:9c	Broadcast	002.11	123	Data, SMI=43, FMI=0, Flags=gm...f
3295	33.266381	Raspber:89:85:9c	Broadcast	002.11	123	Data, SMI=44, FMI=0, Flags=gm...f
3296	33.251464	Cisco_c8:74:b8	IPv4cast_12	002.11	97	Data, SMI=0, FMI=0, Flags=p....f

> Frame 3358: 383 bytes on wire (2424 bits), 383 bytes captured (2424 bits) on interface 1

- > Radiotap Header v0, Length 25
- > 802.11 radio information
- > IEEE 802.11 Beacon frame, Flags: .....
- > IEEE 802.11 wireless LAN
- > [Unformatted Packet: IEEE 802.11]

0000 00 00 19 00 ef 00 00 00 51 97 00 20 00 00 00 00 .....Q.....  
0010 00 02 0e 09 00 00 b3 aa 00 00 00 00 ff ff ff .....<.....<  
0020 ff ff ff 44 18 00 05 b5 e4 18 00 09 00 55 c8 .....<.....C  
0030 f8 83 b1 0e 95 a1 00 00 00 64 00 11 14 00 0f 43 .....d.....<  
0040 05 6e 74 75 72 79 4c 09 6e 66 35 37 39 39 01 00 enturyLi nks799...<  
0050 82 84 80 8e 24 30 48 5c 03 03 00 05 04 00 01 00 .....<.....<  
0060 00 2a 01 06 32 04 0c 12 18 60 38 18 01 00 00 0f .....2.....<

## 结论

现在，您具备了将数据包直接流式传输到Wireshark的技能，并且可以开始分析数据包。不确定该从哪里去哪里？有大量视频和文章可供在线浏览。您搜索的内容取决于您的情况需求。你有这个！