在思科企業WAP上使用Wireshark進行資料包分析：直接流式傳輸到Wireshark

目標

本文說明如何使用思科企業無線存取點(WAP)執行網路流量的封包擷取，並將其直接串流到Wireshark。

目錄

簡介和常見問題

配置更改、監控和故障排除是網路管理員必須經常解決的問題。擁有簡單的工具非常寶貴！本文的目標是更熟悉資料包捕獲的基礎知識，以及如何將資料包流傳輸到Wireshark。如果您不熟悉此過程，讓我們回答您可能已經遇到的一些問題。

首先，Wireshark是免費的包分析器，適合任何想要排除網路故障的人。Wireshark為捕獲提供了許多選項，並按幾個不同的引數對流量進行排序。請前往Wireshark，瞭解有關此開源選項的詳細資訊。

什麼是資料包捕獲？

資料包捕獲（也稱為PCAP檔案）是一種有助於進行故障排除的工具。它可以即時記錄網路中裝置之間傳送的每個資料包。通過捕獲資料包，您可以深入瞭解網路流量的詳細資訊，這些資訊可能包括裝置發現、協定對話和失敗身份驗證等所有內容。您可以看到特定流量的路徑以及選定網路上裝置之間的每次互動。可以根據需要儲存這些資料包以供進一步分析。它就像通過資料包傳輸來檢視網路內部運作情況的X光片。

可以捕獲哪些型別的資料包？

WAP裝置可以捕獲以下型別的資料包：

·通過無線電介面無線接收和傳輸的802.11資料包。在無線電介面上捕獲的資料包包括802.11報頭。

·在乙太網介面上接收和傳輸的802.3資料包。

·在內部邏輯介面(例如虛擬接入點(VAP)和無線分佈系統(WDS)介面)上接收和傳輸的802.3資料包。

在WAP上執行資料包捕獲的方式是什麼？

有兩種資料包捕獲方法可用：

1. *本地捕獲方法* — 捕獲的資料包儲存在WAP裝置上的檔案中。WAP裝置可將檔案傳輸到簡單式檔案傳輸協定(TFTP)伺服器。檔案採用PCAP格式，可以使用Wireshark檢查。您可以選擇*Save File on this Device*以選擇本地捕獲方法。

如果您更喜歡本地捕獲方法(使用最新的Web使用者介面(UI))，請檢視在WAP上使用Wireshark進行資料包分析：上傳檔案。

如果您更喜歡檢視使用舊版GUI進行本地捕獲方法的文章，請選中Configure Packet Capture to Optimize Performance on a Wireless Access Point。

2. *遠端捕獲方法* — 將捕獲的資料包即時重定向到運行Wireshark的外部電腦。您可以選擇*Stream to a Remote Host*以選擇遠端捕獲方法。此方法的優點是對可捕獲的資料包數量沒有限制。

本文的重點是「Stream to a Remote Host」，因此，如果這是您的首選項，請繼續閱讀！

可在何處傳輸資料包？

無線分組捕獲功能能夠捕獲和儲存由WAP裝置接收和傳輸的分組。捕獲的資料包隨後可由網路協定分析器進行分析，以進行故障排除或效能最佳化。許多第三方資料包分析器應用程式都可以線上使用。本文重點介紹Wireshark。

某些型號的Cisco Business WAP能夠將資料包即時傳送到基於Web的資料包解碼器和分析器站點CloudShark。它類似於用於資料包分析的Wireshark使用者介面(UI)，其中包括許多帶有訂閱的新增選項。您可以選擇*Stream to CloudShark*以選擇遠端捕獲方法。有關詳細資訊，請按一下以下連結：

- CloudShark(其官方網站)
- 在WAP125或WAP581上整合用於資料包分析的CloudShark
- CloudShark與WAP571和WAP571E整合

Wireshark和CloudShark均不歸思科所有或受思科支援。它們僅用於演示目的。如需支援，請聯絡Wireshark或CloudShark。

適用裝置和軟體版本

- 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

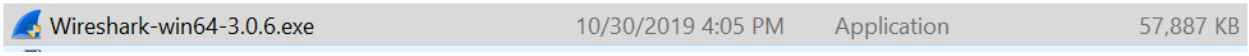
下載Wireshark

步驟1

訪問Wireshark網站。選擇適當的版本。按一下「Download」。您將在螢幕左下角看到下載進度。

步驟2

轉到*電腦上的Downloads*，然後選擇Wireshark檔案以安裝其應用程式。



登入到WAP

在Web瀏覽器中，輸入WAP的IP地址。輸入您的憑據。如果您是第一次訪問此裝置或進行了出廠重置，則預設使用者名稱和密碼為*cisco*。如果您需要有關如何登入的說明，可以按照無線接入點(WAP)文章訪問基於Web的實用程式中的步驟操作。

遠端資料包捕獲說明

使用遠端資料包捕獲功能，可以將遠端埠指定為資料包捕獲的目標埠。此功能與Windows版Wireshark網路分析工具配合使用。資料包捕獲伺服器在WAP裝置上運行，並通過傳輸控制協定(TCP)連線將捕獲的資料包傳送到Wireshark工具。

運行Wireshark工具的Microsoft Windows電腦允許您顯示、記錄和分析捕獲的流量。遠端資料包捕獲設施是Windows版Wireshark工具的一項標準功能。

雖然Linux不支援遠端資料包捕獲，但Wireshark工具在Linux下工作，可以檢視已建立的捕獲檔案。

當使用遠端捕獲模式時，WAP裝置不會在其檔案系統中本地儲存任何捕獲的資料。

如果在安裝的Wireshark電腦和WAP裝置之間安裝了防火牆，則必須允許Wireshark通過電腦的防火牆策略。防火牆也必須配置為允許Wireshark電腦啟動與WAP裝置的TCP連線。

直接將捕獲流式傳輸到Wireshark

要使用*Stream to a Remote Host*選項在WAP裝置上*啟動遠端捕獲*，請按照下列步驟操作。

步驟1

在WAP上，導航到**Troubleshoot > Packet Capture**。

對於封*包捕獲方法*:

1. 從下拉選單中選擇**Stream to a Remote Host**。
2. 在*Remote Capture Port*欄位中，使用預設埠**2002**，或者，如果您使用的是預設埠以外的埠，請輸入所需的埠號，用於將Wireshark連線到WAP裝置。埠範圍從1025到65530。
3. 封包擷取選項有兩個*模式*。選擇最適合您的方案。

·*所有無線流量* — 捕獲空中所有無線資料包。

·*傳入/傳出此AP的流量* — 捕獲從AP傳送的資料包或收到的AP。

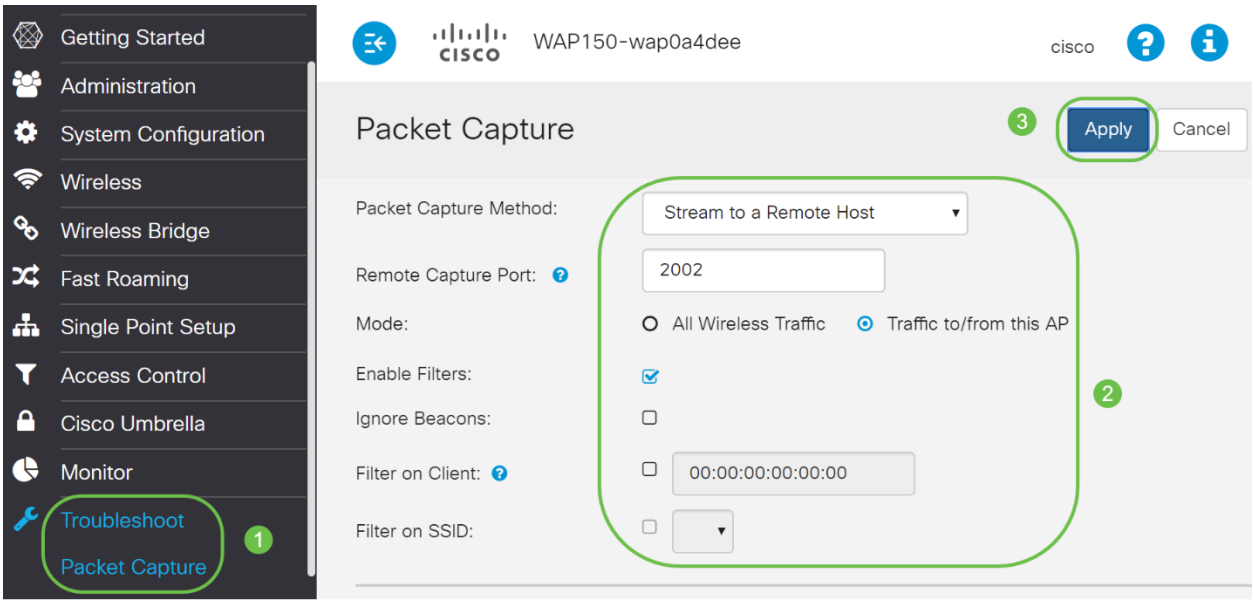
4. 勾選「**Enable Filters**」。
5. 從以下選項中選擇：

·*Ignore Beacons* — 啟用或停用對無線電偵測或傳輸的802.11信標進行擷取。信標幀是承載關於網路的資訊的廣播幀。信標的目的是通告現有的無線網路。

·*Filter on Client* — 啟用後，為WLAN Client過濾器指定MAC地址。請注意，僅當在802.11介面上執行捕獲時，客戶端過濾器才處於活動狀態。

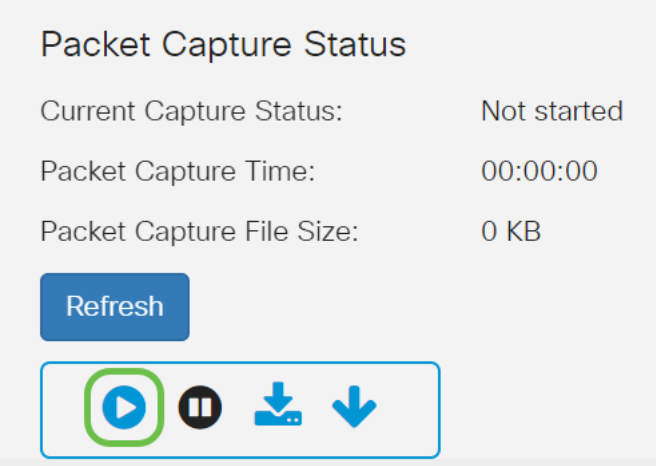
·*Filter on SSID* — 對於此*Stream to a Remote Host*選項，該選*項將呈灰色顯*示。

6.按一下**Apply**儲存設定。



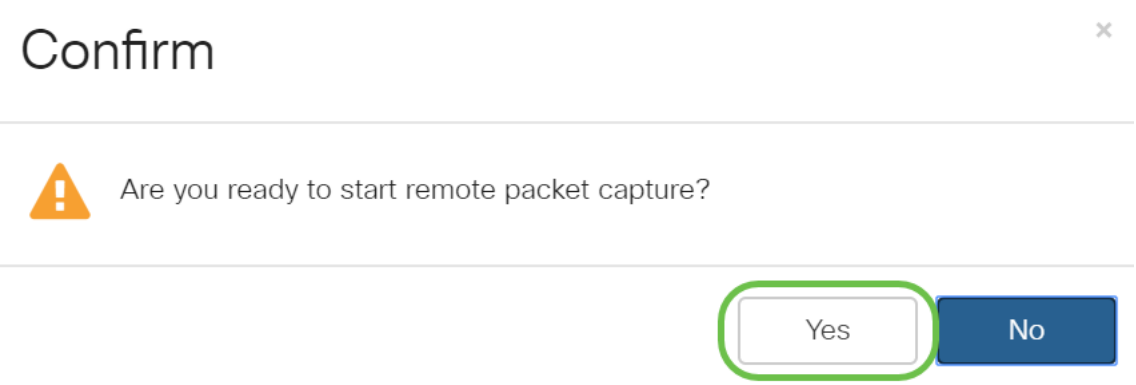
步驟2

按一下**Start Capture**圖標。



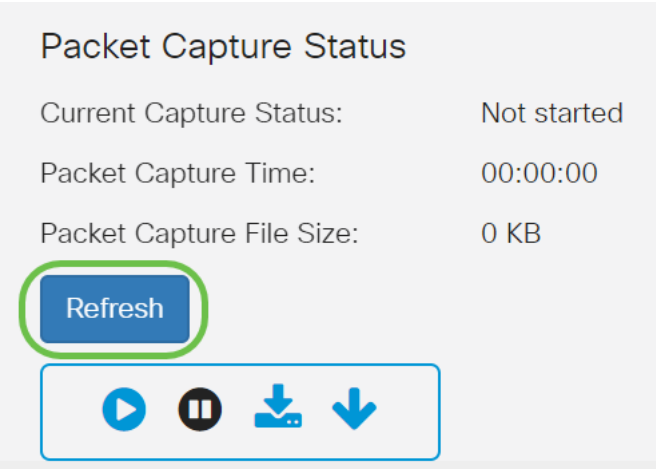
步驟3

將會開啟*confirm*彈出視窗。按一下**Yes**開始捕獲。



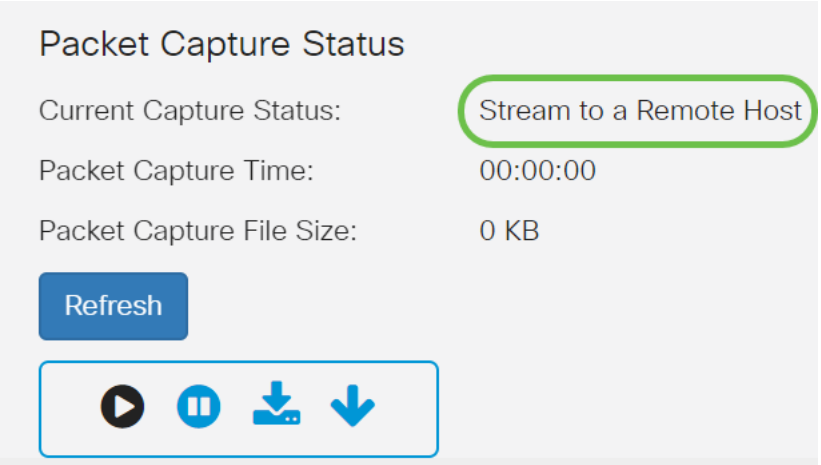
步驟4

按一下**Refresh**按鈕檢查當前狀態。



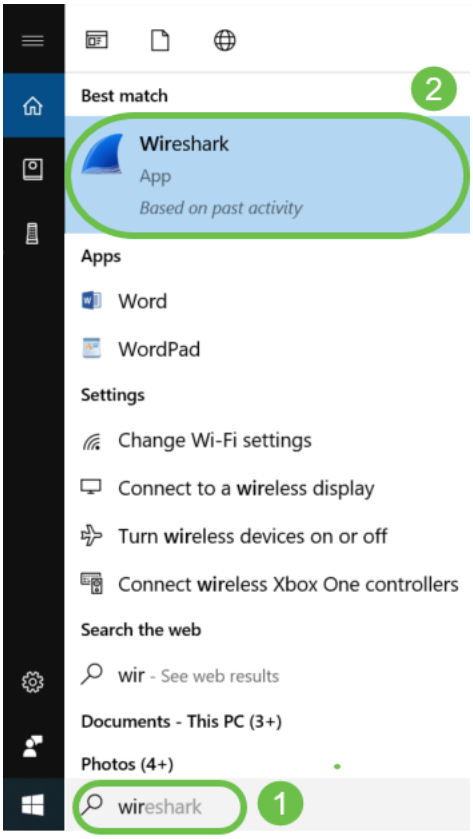
步驟5

現在您可以看到*Current Capture Status*將為*Stream to a Remote Host*。



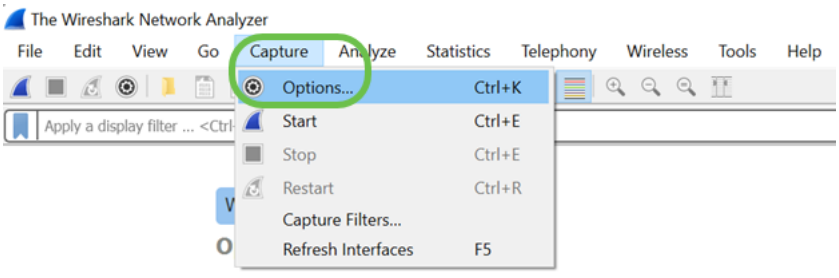
步驟6

由於Wireshark已經下載，因此可以通過在Microsoft Windows的搜尋欄中鍵入**Wireshark**並選擇應用程式作為選項來訪問它。



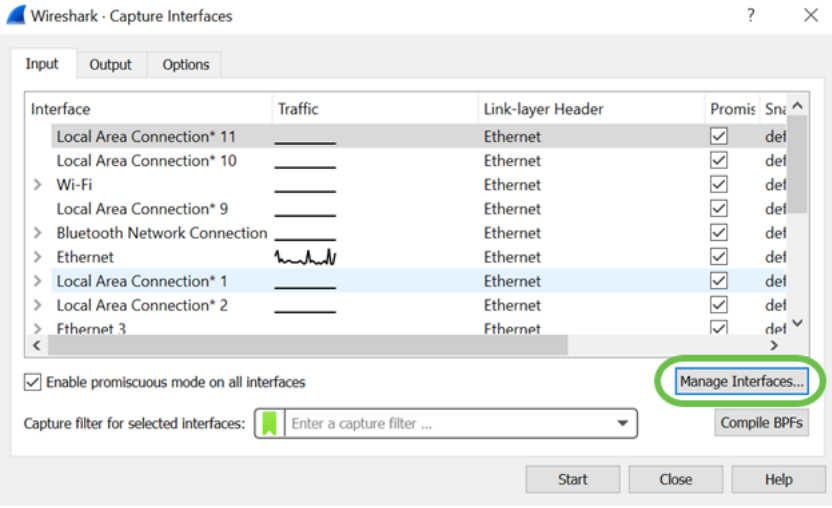
第7步

導航到**Capture > Options...**



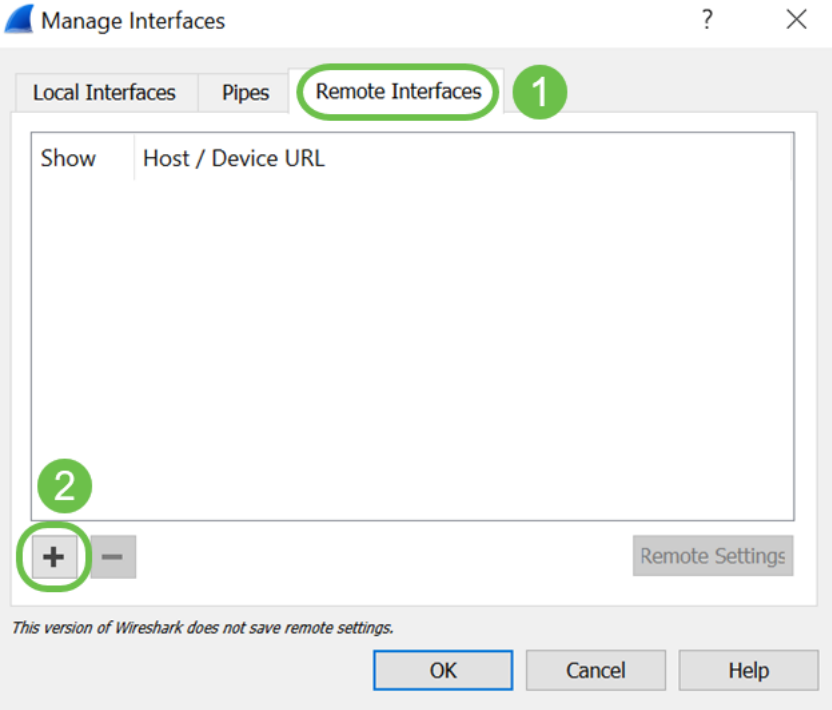
步驟8

在新的*Wireshark - Capture Interfaces*(*Wireshark - Capture Interfaces)彈出視窗*上，按一下**Manage Interfaces(管理介面)**。.



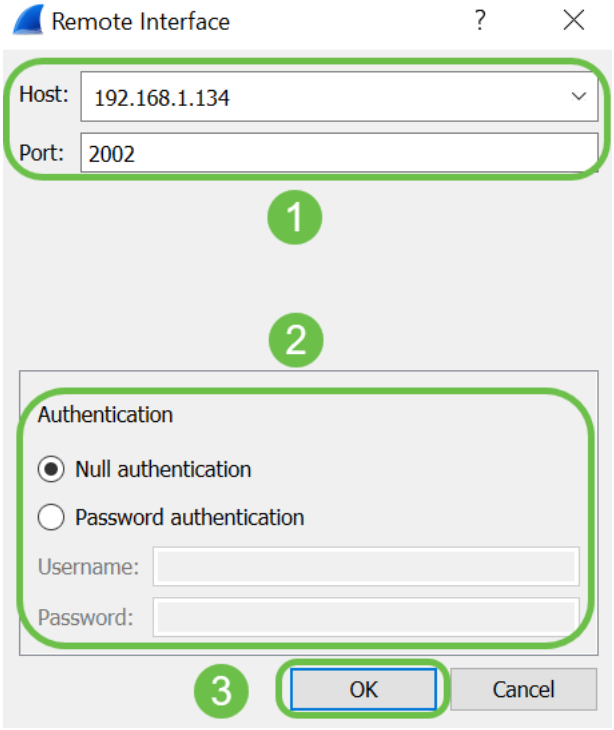
步驟9

在新的*Manage Interfaces*彈出視窗中，導航到**Remote Interfaces**，然後按一下**plus圖示**新增介面。



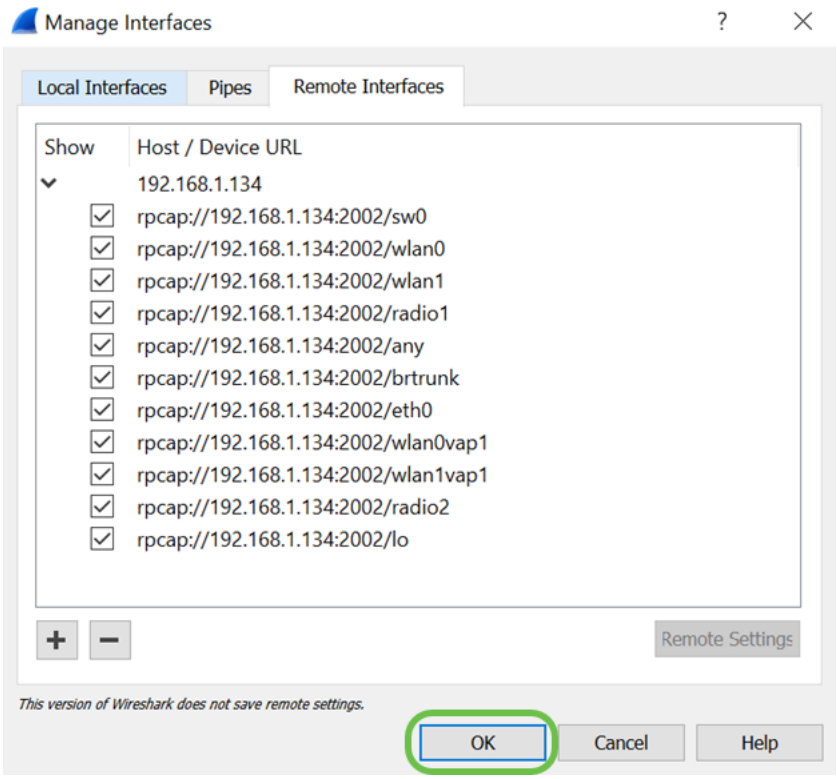
步驟10

在新的*Remote Interface*彈出視窗中，輸入*Host:*IP地址詳細資訊（已啟動遠端捕獲的WAP裝置IP）和*埠：*編號（在WAP上配置用於遠端捕獲）。 在這種情況下，WAP裝置IP為192.168.1.134。您可以根據設定選擇*Null authentication*或*Password authentication*選項。如果您選擇「密碼身份驗證」，請相應地輸入*使用者名稱*和*密碼*詳細資訊。按一下「**OK**」（確定）。



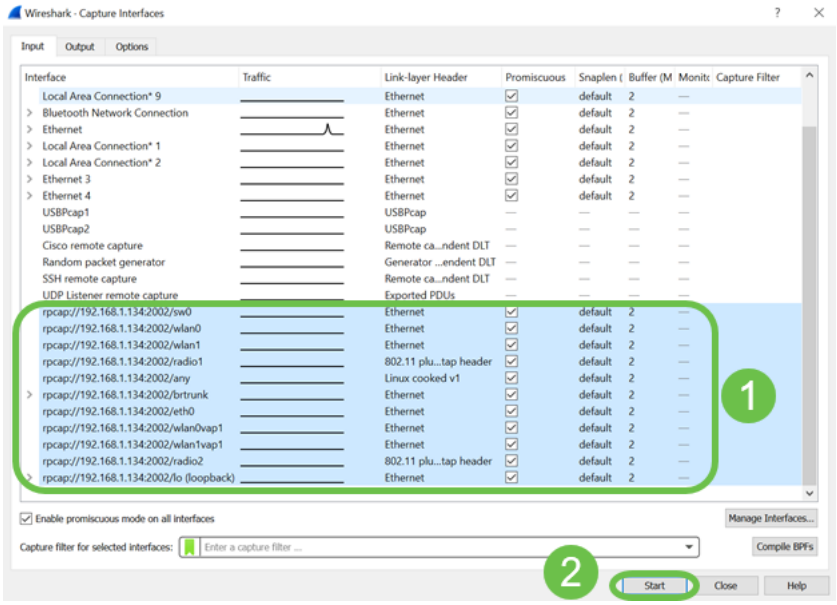
步驟11

在*Remote Interfaces*頁籤下，您將可以看到遠端WAP裝置的所有介面。您可能希望僅取消選擇其中的某些選項以降低捕獲的資料包量。如果要檢視信標資料包，請將無線電介面保持為選中狀態。按一下「**OK**」（確定）。



步驟12

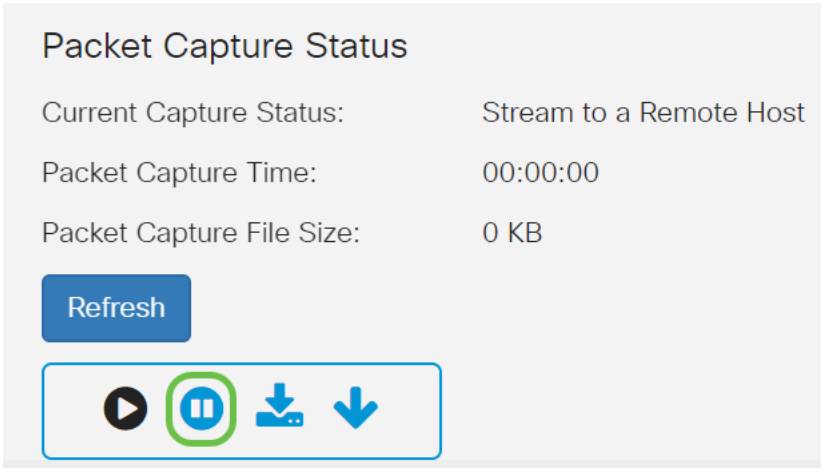
現在，新增的介面將反映在*Wireshark - Capture Interfaces窗*口上。**選擇**要監控的介面，然後按一下**Start**以檢視資料包。



如果您在嘗試檢視資料包時遇到問題，則表示*遠端資料包捕獲協定*服務未在您的系統上運行。遠端資料包捕獲協定服務必須先在目標平台上運行，Wireshark才能連線到該服務。有關詳細資訊，請通過Wireshark按一下*Remote Capture Interfaces*連結。

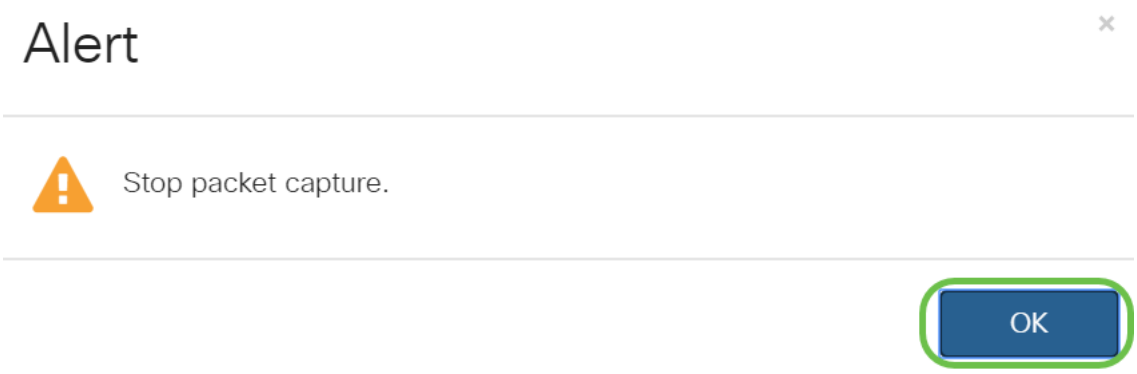
步驟13

在WAP上，按一下**Stop Capture**圖示以停止捕獲進程。



步驟14

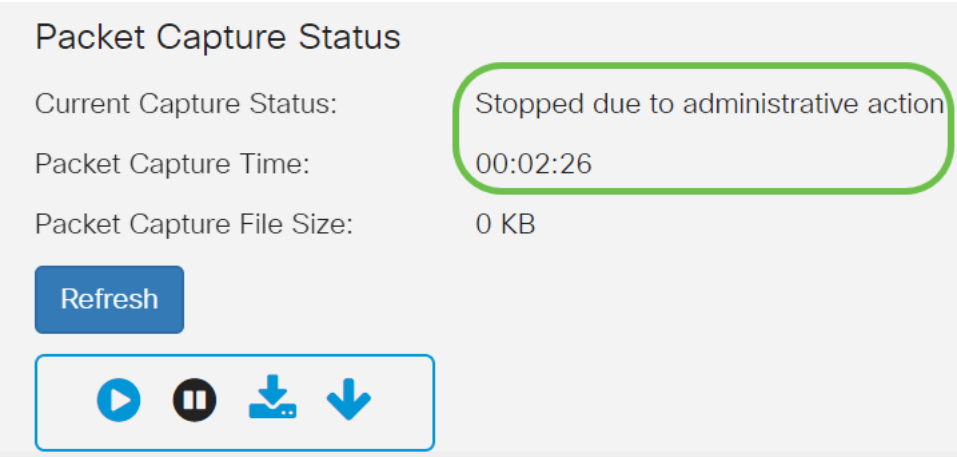
系統將顯示*Alert*彈出視窗。按一下**OK**停止遠端捕獲。



您也可以按一下Wireshark應用程式中的**Stop**按鈕來停止資料包捕獲。

步驟15

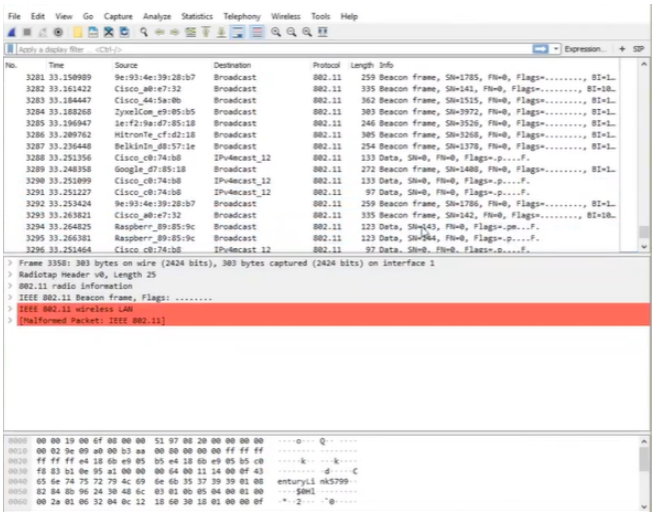
現在，*Current Capture Status*將顯示為*Stopped due to administration action*，並且*Packet Capture Time*將反映顯示總捕獲持續時間。



*Packet Capture File Size*將顯示為*0 KB*。此外，檔案下載選項在此案例中無法使用。

步驟16

在Wireshark上，可以檢視資料包捕獲。



結論

現在，您已經掌握了將資料包直接傳輸到Wireshark的技能，並且您可以開始分析該資料包。不知道從這裡往哪裡走？網上有大量的影片和文章可供探索。您搜尋的內容取決於您的具體情況。你有這個！