パケット分析のためのCisco Business WAPでのWiresharkの使用：Wiresharkに直接ストリーミング

目的

この記事では、Cisco Business Wireless Access Point(WAP)を使用してネットワークトラフィックのパケットキャプチャを実行し、Wiresharkに直接ストリーミングする方法について説明します。

目次

概要とFAQ

設定の変更、モニタリング、およびトラブルシューティングは、ネットワーク管理者が頻繁に対処する必要があります。簡単なツールを使用することは非常に貴重です！この記事の目的は、パケットキャプチャの基本と、パケットをWiresharkにストリーミングする方法について、さらに理解を深めることです。このプロセスに精通していない場合は、すでに質問に答えましょう。

まず最初に、Wiresharkは、ネットワークのトラブルシューティングを検討しているすべてのユーザに対する無料パケットアナライザです。Wiresharkには、キャプチャに関する多くのオプションが用意されており、複数の異なるパラメータでトラフィックをソートできます。このオープンソースオプションの詳細については、Wiresharkに進んでください。

パケットキャプチャとは何ですか。

パケットキャプチャ（PCAPファイルとも呼ばれる）は、トラブルシューティングに役立つツールです。ネットワーク内のデバイス間で送信されるすべてのパケットをリアルタイムで記録できます。パケットをキャプチャすると、ネットワークトラフィックの詳細を調べることができます。これには、デバイスの検出、プロトコルの会話、および認証の失敗などすべてが含まれます。特定のトラフィックフローのパスと、選択したネットワーク上のデバイス間のすべてのインタラクションを確認できます。これらのパケットは、必要に応じてさらに分析するために保存できます。これは、パケットの転送を介したネットワークの内部の動作のX線のようなものです。

どのような種類のパケットをキャプチャできますか。

WAPデバイスは、次のタイプのパケットをキャプチャできます。

・ 802.11パケットが無線インターフェイスで無線送受信される。無線インターフェイスでキャプチャされたパケットには、802.11ヘッダーが含まれます。

・ イーサネットインターフェイスで送受信される802.3パケット。

・ 仮想アクセスポイント(VAP)やWireless Distribution System(WDS)インターフェイスなどの内部論理インターフェイスで送受信される802.3パケット。

WAPでパケットキャプチャを実行する方法は何ですか。

パケットキャプチャには、次の2つの方法があります。

1. *ローカルキャプチャ方法*：キャプチャされたパケットは、WAPデバイス上のファイルに保存されます。WAPデバイスは、トリビアルファイル転送プロトコル(TFTP)サーバにファイルを転送できます。ファイルはPCAP形式でフォーマットされ、Wiresharkを使用して調べることができます。[*このデバイスにファイルを保存]を選択して、ローカルキャプチャ方式を*選択できます。

最新のWebユーザインターフェイス(UI)を備えたローカルキャプチャ方式を使用する場合は、パケット分析のWAPでWiresharkを使用してください。ファイルのアップロード。

ローカルキャプチャ方式に古いGUIを使用する記事を表示する場合は、「ワイヤレスアクセスポイントのパフォーマンスを最適化するためのパケットキャプチャの設定」を参照してください。

2. *リモートキャプチャ方法*：キャプチャされたパケットは、Wiresharkを実行している外部コンピュータにリアルタイムでリダイレクトされます。リモート・キャプチャ*方法を選択するには、[Stream to a Remote Host*]を選択できます。この方法の利点は、キャプチャできるパケットの量に制限がないことです。

この記事の焦点はリモートホストにストリーミングすることなので、それが好みの場合は読み込んでください！

パケットのストリーミングはどこで行えますか。

ワイヤレスパケットキャプチャ機能は、WAPデバイスで送受信されたパケットをキャプチャして保存することを可能にします。キャプチャされたパケットは、トラブルシューティングまたはパフォーマンス最適化のためにネットワークプロトコルアナライザで分析できます。オンラインで利用できるサードパーティ製パケットアナライザアプリケーションは数多くあります。この記事では、Wiresharkについて説明します。

Cisco Business WAPの一部のモデルでは、WebベースのパケットデコーダおよびアナライザサイトであるcloudSharkにリアルタイムでパケットを送信できます。これは、サブスクリプションを含む多くの追加オプションを含む、パケット分析のためのWiresharkユーザインターフェイス(UI)に似ています。[Stream to *CloudShark*]を選択して、*リモートキャプチャ方式を選択できます*。詳細については、次のリンクをクリックしてください。

- CloudShark（公式サイト）
- WAP125またはWAP581でのパケット分析用CloudSharkの統合
- CloudSharkとWAP571およびWAP571Eの統合

WiresharkもCloudSharkも、シスコが所有またはサポートしていません。これらはデモンストレ

ーション目的でのみ含まれています。サポートについては、Wiresharkまたは CloudSharkに問い合わせ。

該当するデバイスとソフトウェアバージョン

- WAP125バージョン1.0.2.0
- WAP150バージョン1.1.1.0
- WAP121バージョン1.0.6.8
- WAP361バージョン1.1.1.0
- WAP581バージョン1.0.2.0
- WAP571バージョン1.1.0.4
- WAP571Eバージョン1.1.0.4

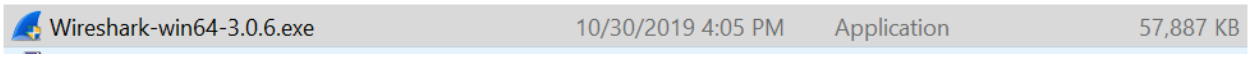
Wiresharkのダウンロード

手順 1

WiresharkのWebサイトに移動します。適切なバージョンを選択します。[Download] をクリックします。画面左下にダウンロードの進行状況が表示されます。

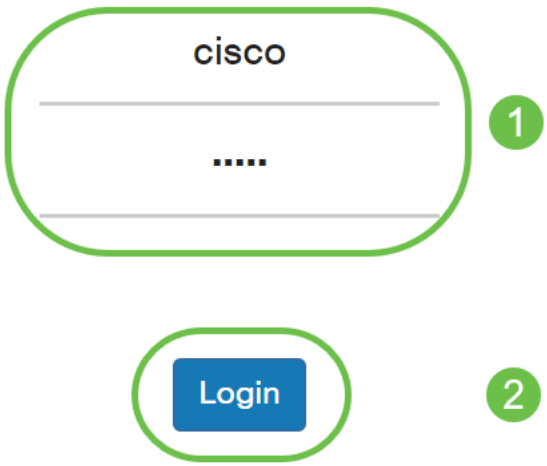
手順 2

コンピュータのダウンロードに移動し、Wiresharkファイルを選択してそのアプリケーションをインストールします。



WAPにログインします

Webブラウザで、WAPのIPアドレスを入力します。認証情報を入力してください。このデバイスに初めてアクセスした場合、または工場出荷時のリセットを行った場合、デフォルトのユーザ名とパスワードは*cisco*です。ログイン方法の説明が必要な場合は、Wireless Access Point (WAP)のWebベースのユーティリティへのアクセスに関する記事の手順に従ってください。



リモートパケットキャプチャの説明

リモートパケットキャプチャ機能を使用すると、パケットキャプチャの宛先ポートとしてリモートポートを指定できます。この機能は、Windows用のWiresharkネットワークアナライザツールと連携して動作します。パケットキャプチャサーバはWAPデバイス上で動作し、キャプチャされたパケットをTransmission Control Protocol(TCP)接続を介してWiresharkツールに送信します。

Wiresharkツールを実行しているMicrosoft Windowsコンピュータを使用すると、キャプチャされたトラフィックを表示、ログ記録、分析できます。リモートパケットキャプチャ機能は、Windows用Wiresharkツールの標準機能です。

リモートパケットキャプチャはLinuxではサポートされていませんが、WiresharkツールはLinuxで動作し、すでに作成されたキャプチャファイルを表示できます。

リモートキャプチャモードが使用されている場合、WAPデバイスはキャプチャされたデータをファイルシステムにローカルに保存しません。

Wiresharkがインストールされたコンピュータとデバイスの間にファイアウォールがインストールされている場合、Wiresharkがコンピュータのファイアウォールポリシーを通過できるようにする必要があります。また、WiresharkコンピュータがWAPデバイスへのTCP接続を開始できるようにファイアウォールを設定する必要があります。

キャプチャをWiresharkに直接ストリーミング

[*Stream to a Remote Host*]オプションを使用してWAPデバイスでリモートキャプチャを開始するには、次の手順に従います。

手順 1

WAPで、[Troubleshoot] > [**Packet Capture**]**に移動します。**

パケットキャプチャ方式の場合:

1. ドロップダウン**メニューから**[**Stream to a Remote Host**]を選択します。
2. [Remote Capture Port] フィールドで、デフォルトのポート**2002を使用します**。デフォルト以外のポートを使用している場合は、WiresharkをWAPデバイスに接続するために使用するポート番号を入力します。ポート範囲は1025 ~ 65530です。
3. パケットキャプチャのオプションには2つのモードがあります。シナリオに最適なものを選択します。

・ *すべてのワイヤレストラフィック*：空中のすべてのワイヤレスパケットをキャプチャします。

・ *このAPとの間のトラフィック*:APまたは受信したAPから送信されたパケットをキャプチャします。

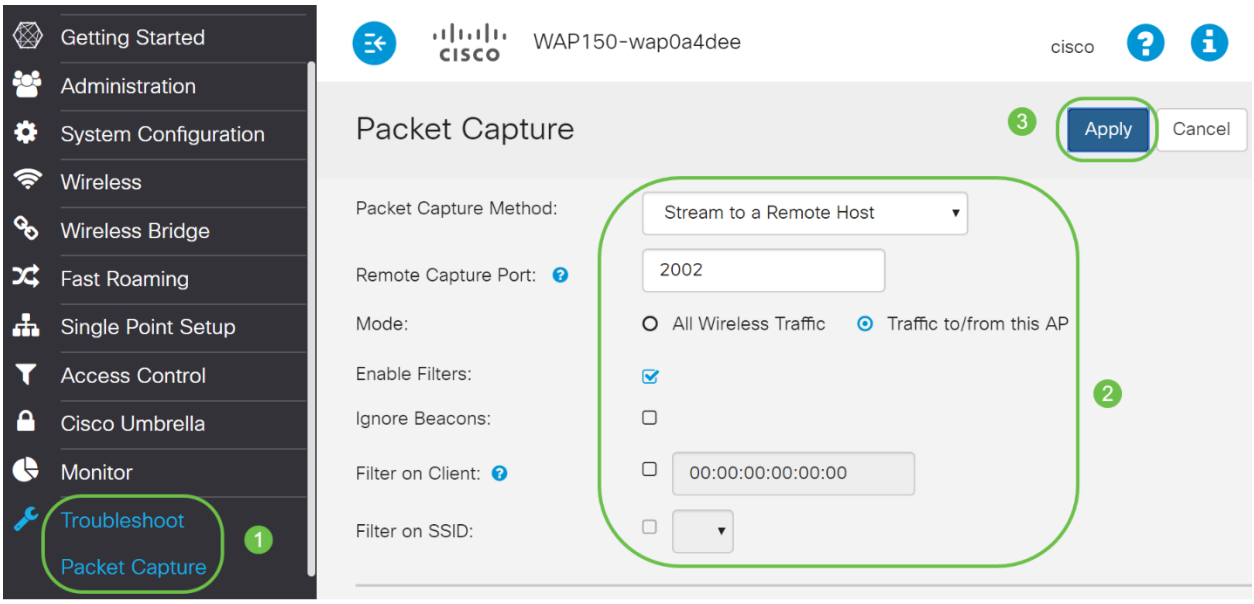
4. [Enable **Filters**]を**オンにします**。
5. 次のオプションから選択します。

・ *ビーコンを無視する*：無線で検出または送信された802.11ビーコンのキャプチャを有効または無効にします。ビーコンフレームは、ネットワークに関する情報を伝送するブロードキャストフレームです。ビーコンの目的は、既存の無線ネットワークをアドバタイズすることです。

・ *Filter on Client*：有効になったら、WLANクライアントフィルタのMACアドレスを指定します。クライアントフィルタがアクティブになるのは、802.11インターフェイスでキャプチャが実行された場合だけです。

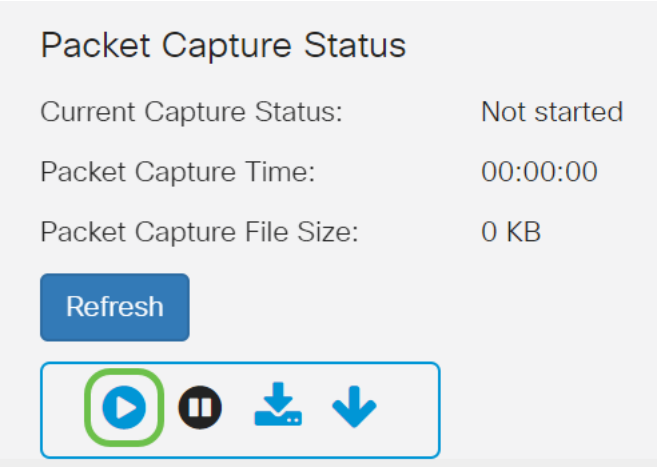
・ SSIDで*フィルター* – このオプションは、このStream to a Remote Hostオプションに対して*グレー表示*されます。

6.「適用」をクリックし、設定を保存します。



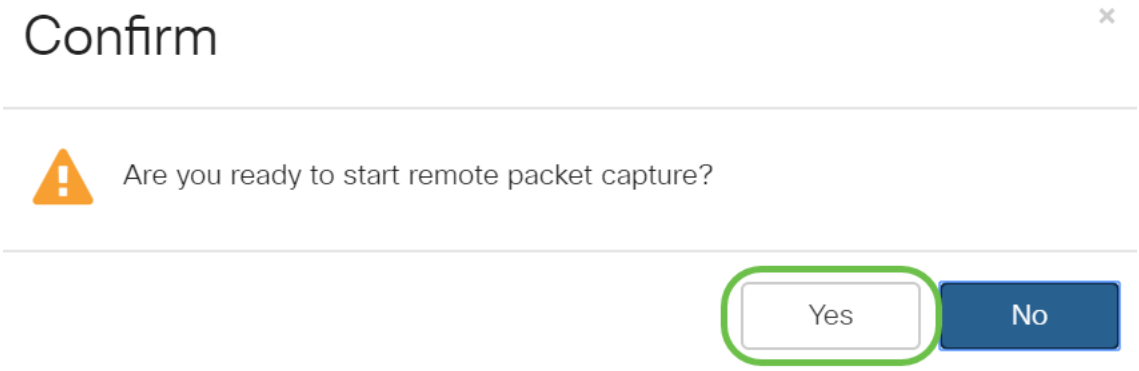
手順 2

キャプチャの開始アイコン**をクリック**します。



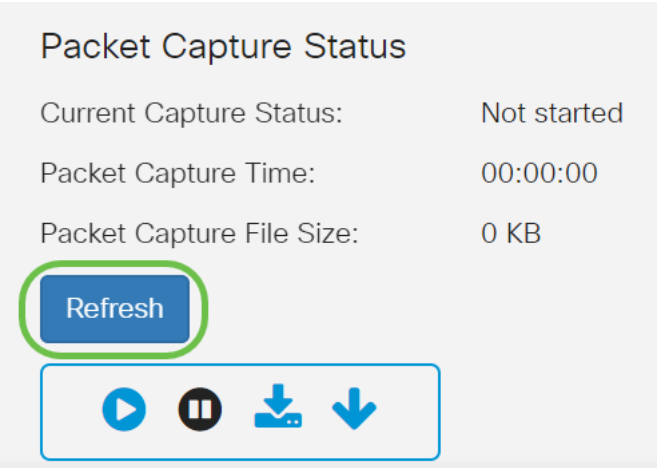
手順 3

確認ポップアップウィンドウが開きます。[Yes]をクリックし、キャプチャを開始します。



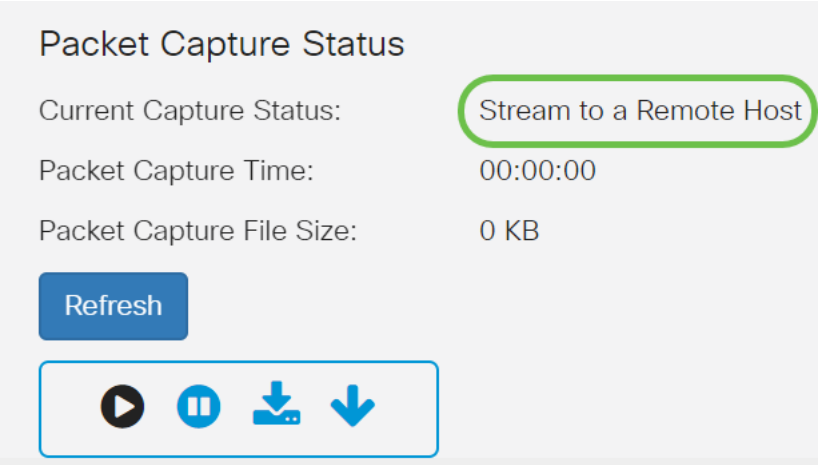
手順 4

[更新]ボタンをクリックして、現在のステータスを確認します。



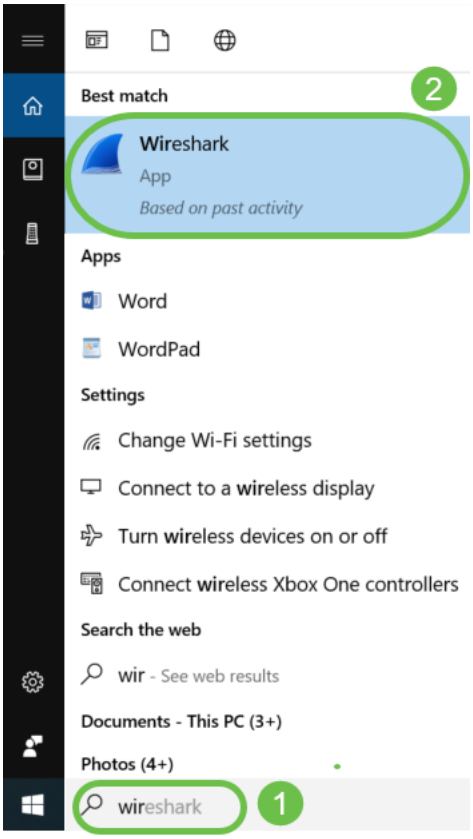
手順 5

これで、[Current Capture Status]が[*Stream to a Remote Host*]になることが確認できます。



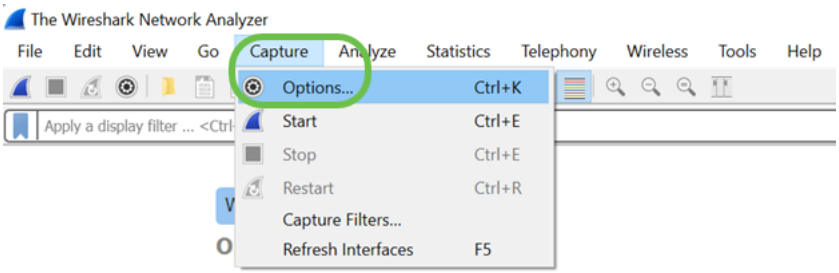
手順 6

Wiresharkはすでにダウンロードされているため、Microsoft Windowsの検索バーに**Wireshark**と入力し、**オプションとしてアプリケーションを選択することでアクセスできます。**



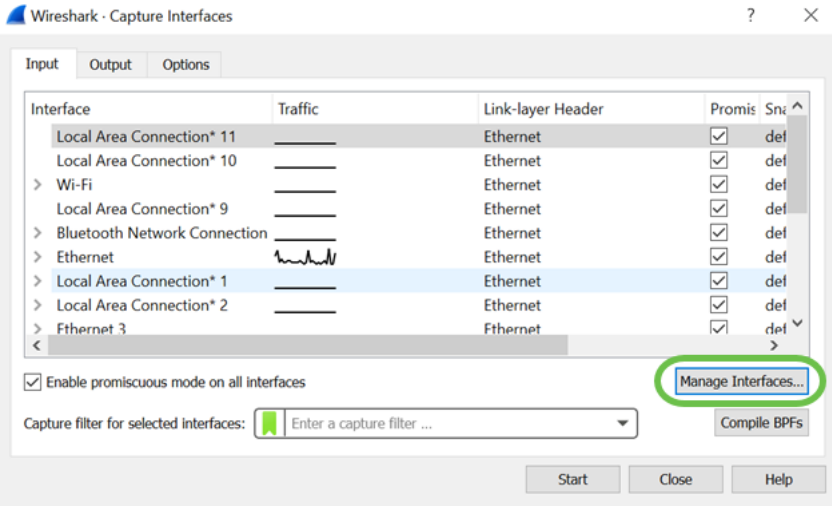
ステップ7

[Capture] > [Options...]に移動します。



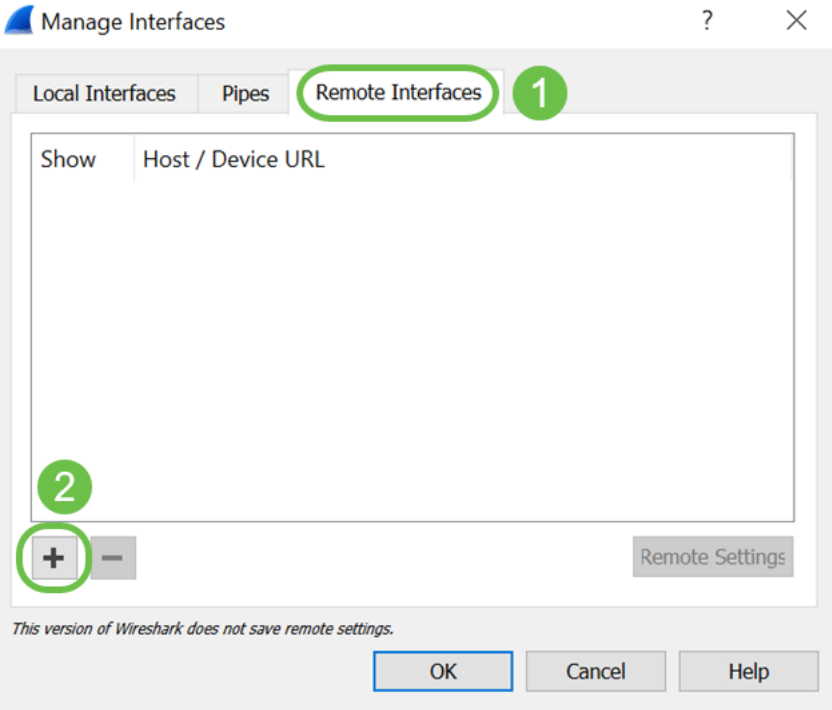
手順 8

新しいポップアップ[*Wireshark - Capture Interfaces*]ウィンドウで、[**Manage Interfaces**...]をクリックします。



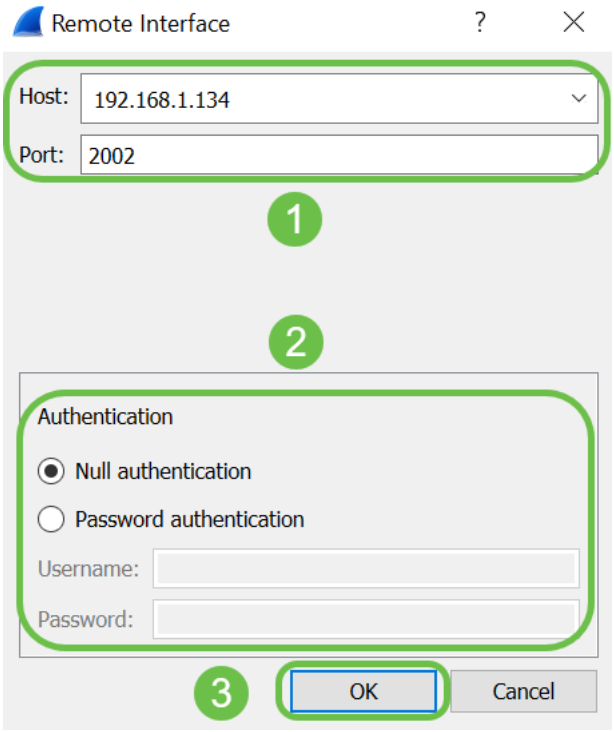
手順 9

新しい[インターフェイスの管理]ポップアップウィンドウで、[リモートインターフ**ェイス]に移動**し、プラスのアイコンをクリックして、**インターフ**ェイスを追加します。



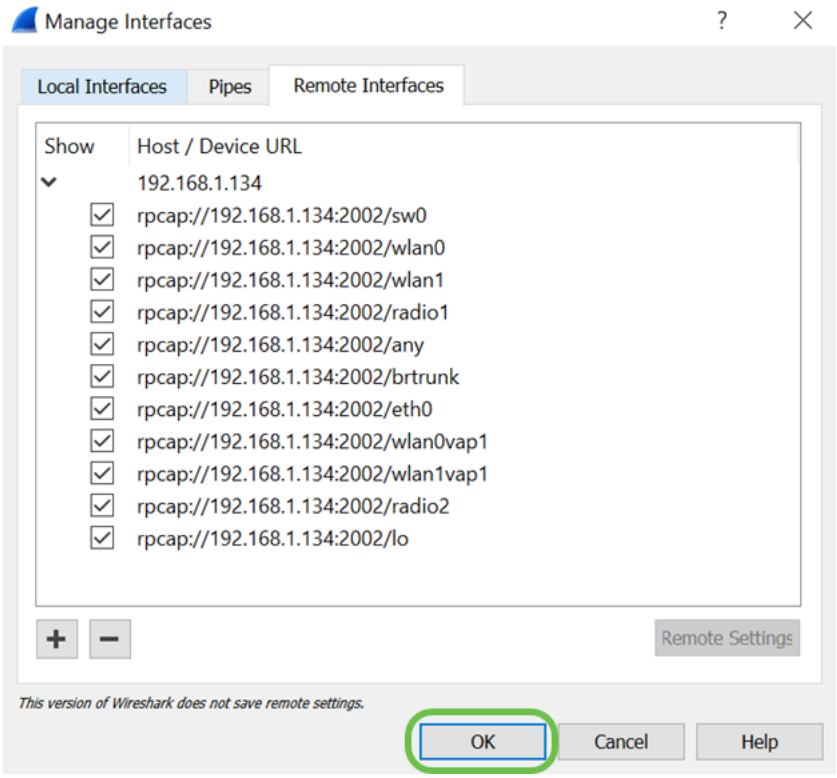
手順 10

新しいリモートインタフェースポップアップウィンドウで、Host:IPアドレスの詳細（リモートキャプチャを開始したWAPデバイスのIP）とポート：番号（リモートキャプチャ用にWAPで設定）この場合、WAPデバイスのIPは192.168.1.134です。設定に基づいて[*Null認証*]または[*パスワード認証*]オプションを選択することができます。パスワード認証を選択した場合は、ユーザ名とパスワードの詳細を*適宜*入力してください。[OK] をクリックします。



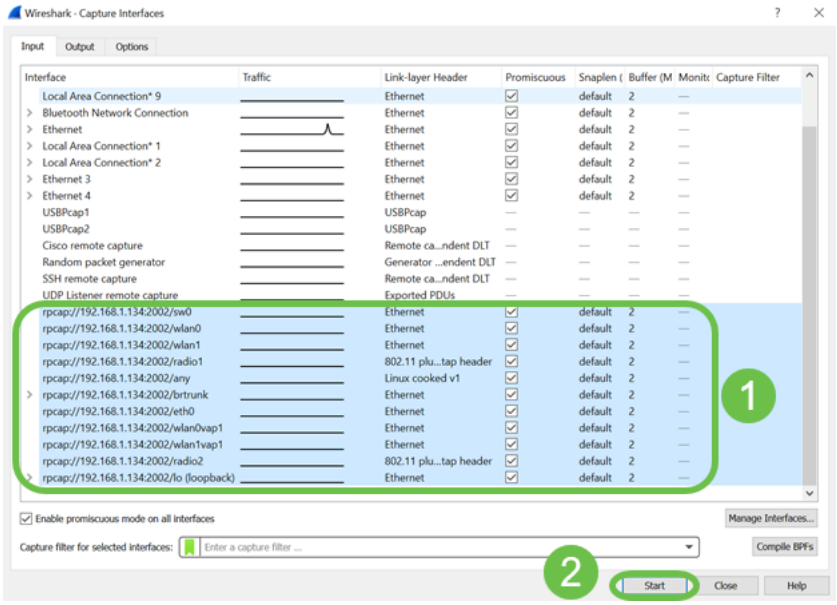
手順 11

[Remote Interfaces]タブで、リモートWAPデバイスのすべてのインターフェイスを確認できます。キャプチャされたパケットの量を減らすには、これらの一部を選択解除するだけです。ビーコンパケットを表示するには、無線インターフェイスを選択したままにします。[OK] をクリックします。



ステップ 12

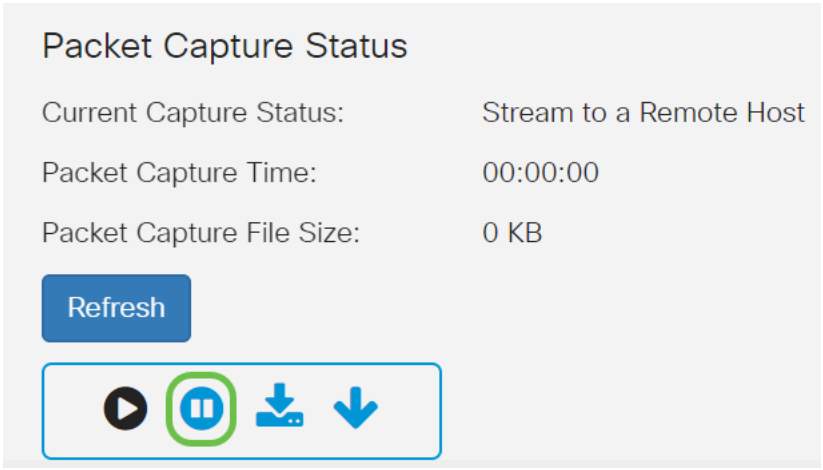
新しく追加されたインターフェイスは、[Wireshark - Capture Interfaces]ウィンドウに反映されます。**監視する**インタフェースを選択し、「開始」をクリック**してパケ**ットを表示します。



パケットを表示しようとしたときに問題が発生した場合は、*Remote Packet Capture Protocol*サービスがシステムで*動作*していないことを意味します。Wiresharkが接続する前に、Remote Packet Capture Protocol(RPCAP)サービスをターゲットプラットフォームで実行する必要があります。詳細については、[Remote *Capture Interfaces through Wireshark]リンクをク*リックしてください。

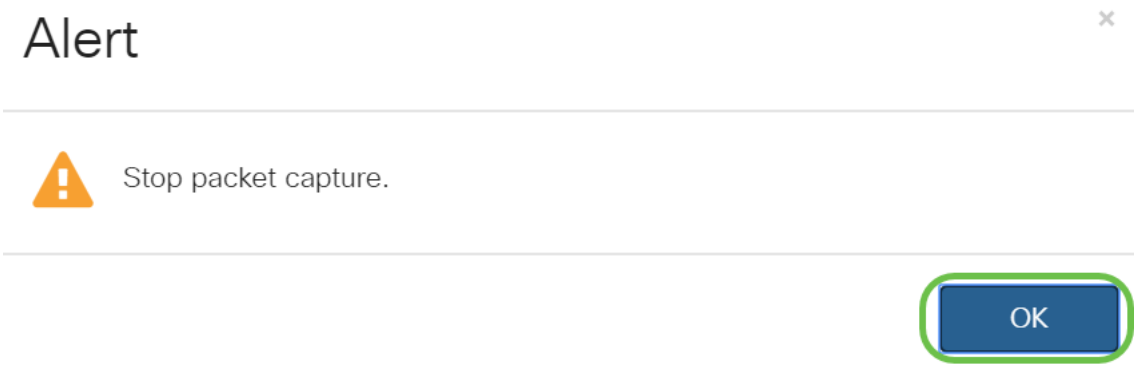
手順 13

WAPで、[Stop Capture]アイコンをクリックして、**キャプチャ**プロセスを停止します。



ステップ 14

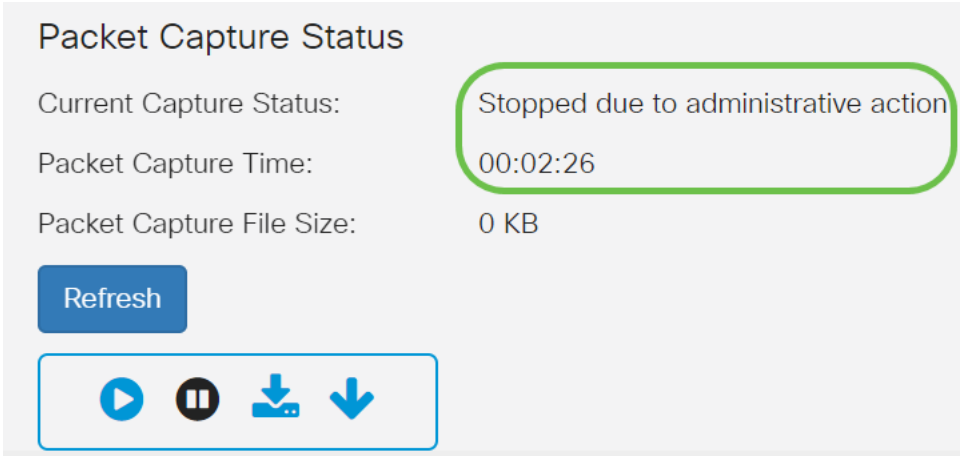
[Alert]ポップアップアップウィンドウが表示されます。「**OK**」を**クリック**して、リモート・キャプチャを停止します。



また、Wiresharkアプリケーションの[Stop]ボタンをクリックして、パケットキャプチャを**停止する**こともできます。

ステップ 15

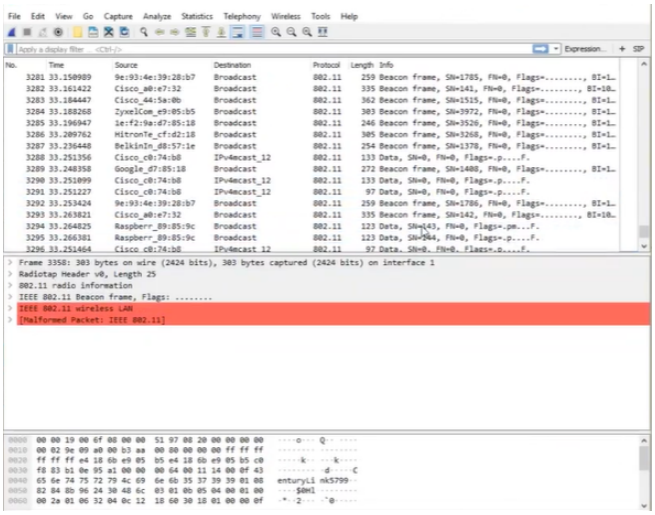
現在のキャプチャステータスは、管理アクションが原因で*[Stopped]と表示され*、[*Packet Capture Time*]はキャプチャの合計時間を示す内容になります。



パケットキャプチャファイルのサイズは*0 KBと表示されます*。また、このシナリオでは、ファイルのダウンロードオプションは機能しません。

ステップ 16

Wiresharkでは、パケットキャプチャを表示できます。



結論

これで、Wiresharkに直接ストリーミングされるパケットを取得するスキルが身に付き、それを分析する作業を行うことができます。ここからどこに行けばいいのか分からないのか？オンラインで閲覧できる動画や記事は多数あります。検索する内容は、状況のニーズによって異なります。これだ！