Usando o Wireshark em um Cisco Business WAP para análise de pacotes: Transmitir diretamente para o Wireshark

Objetivo

Este artigo explica como executar uma captura de pacote de tráfego de rede usando um Cisco Business Wireless Access Point (WAP) e transmiti-lo diretamente para o Wireshark.

Table Of Contents

Introdução e perguntas frequentes

Alterações de configuração, monitoramento e solução de problemas são algo com que um administrador de rede precisa lidar com frequência. Ter uma ferramenta simples para usar é inestimável! O objetivo deste artigo é ficar mais confortável com os conceitos básicos das capturas de pacotes, bem como como enviar os pacotes para o Wireshark. Se você não está familiarizado com esse processo, responda a algumas perguntas que você talvez já tenha feito.

Primeiramente, o Wireshark é um analisador de pacotes gratuito para qualquer pessoa que deseje solucionar problemas de sua rede. O Wireshark fornece muitas opções para a captura, bem como para classificar o tráfego por vários parâmetros diferentes. Vá para o Wireshark para obter detalhes sobre esta opção de código aberto.

O que é uma captura de pacotes?

Uma captura de pacote, também conhecida como arquivo PCAP, é uma ferramenta que pode ser útil na solução de problemas. Ele pode gravar todos os pacotes enviados entre dispositivos na rede, em tempo real. A captura de pacotes permite que você descubra os detalhes do tráfego de rede, o que pode incluir tudo, desde descoberta de dispositivos, conversas de protocolo e autenticação com falha. Você pode ver o caminho do fluxo de tráfego específico e cada interação entre dispositivos em redes selecionadas. Esses pacotes podem ser salvos para análise adicional, conforme necessário. É como um raio-x do funcionamento interno da rede através da transferência de pacotes.

Que tipos de pacotes podem ser capturados?

O dispositivo WAP pode capturar os seguintes tipos de pacotes:

Pacotes 802.11 recebidos e transmitidos sem fio nas interfaces de rádio. Os pacotes capturados nas interfaces de rádio incluem o cabeçalho 802.11.

Pacotes 802.3 recebidos e transmitidos na interface Ethernet.

Pacotes 802.3 recebidos e transmitidos nas interfaces lógicas internas, como Pontos de Acesso Virtuais (VAPs - Virtual Access Points) e Interfaces do Sistema de Distribuição Wireless (WDS - Wireless Distribution System).

Quais são as maneiras pelas quais uma captura de pacotes pode ser feita em um WAP?

Há dois métodos disponíveis de captura de pacotes:

1. *Método de Captura Local* - Os pacotes capturados são armazenados em um arquivo no dispositivo WAP. O dispositivo WAP pode transferir o arquivo para um servidor TFTP (Trivial File Transfer Protocol). O arquivo é formatado no formato PCAP e pode ser examinado usando o Wireshark. Você pode escolher *Salvar arquivo neste dispositivo* para selecionar o método de captura local.

Se preferir o método de captura local, com a interface de usuário da Web (UI) mais recente, confira Usando o Wireshark em um WAP para Análise de pacote: Carregar arquivo.

Se preferir exibir um artigo que use a GUI mais antiga para o método de captura local, consulte Configurar Captura de Pacotes para Otimizar o Desempenho em um Ponto de Acesso Sem Fio.

2. *Método de Captura Remota* - Os pacotes capturados são redirecionados em tempo real para um computador externo que executa o Wireshark. Você pode escolher *Stream to a Remote Host* para selecionar o método de captura remota. A vantagem desse método é que não há limite para o volume de pacotes que podem ser capturados.

O foco deste artigo é transmitir para um host remoto, de modo que, se essa for sua preferência, leia!

Onde posso transmitir o pacote?

O recurso de captura de pacotes sem fio permite capturar e armazenar os pacotes recebidos e transmitidos pelo dispositivo WAP. Os pacotes capturados podem, então, ser analisados por um analisador de protocolo de rede para solução de problemas ou otimização de desempenho. Há muitos aplicativos de análise de pacotes de terceiros disponíveis on-line. Neste artigo, nos concentramos no Wireshark.

Alguns modelos de Cisco Business WAPs têm a capacidade de enviar pacotes em tempo real para o CloudShark, um site de decodificador e analisador de pacotes baseado na Web. É semelhante à Interface de Usuário (UI) do Wireshark para análise de pacotes que inclui muitas opções adicionadas com uma assinatura. Você pode escolher *Stream to CloudShark* para selecionar o método de captura remota. Para obter mais informações, clique nos seguintes links:

- CloudShark (o seu site oficial)
- Integração do CloudShark para análise de pacotes em um WAP125 ou WAP581

- Integração do CloudShark com WAP571 e WAP571E

Nem o Wireshark nem o CloudShark pertencem ou são suportados pela Cisco. Eles são incluídos apenas para fins de demonstração. Para obter suporte, entre em contato com o Wireshark ou o CloudShark.

Dispositivos aplicáveis e versão de software

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

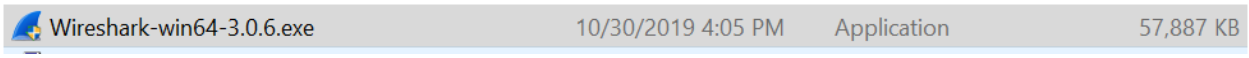
Download do Wireshark

Passo 1

Vá para o site do Wireshark. Selecione a versão apropriada. Clique em **Download**. Você verá o progresso do download na parte inferior esquerda da tela.

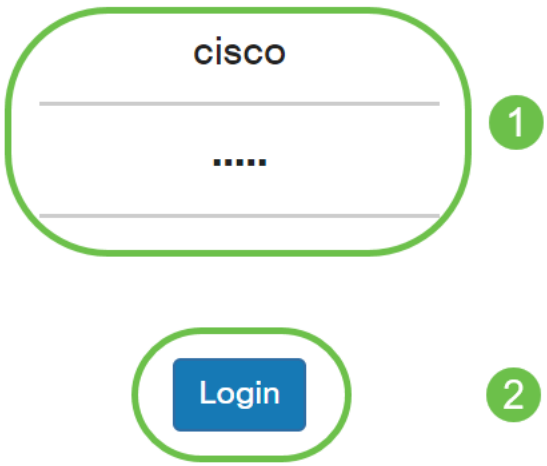
Passo 2

Vá para *Downloads* em seu computador e selecione o arquivo Wireshark para instalar seu aplicativo.



Faça login no WAP

No navegador da Web, insira o endereço IP do WAP. Digite suas credenciais. Se esta for a primeira vez que você acessa este dispositivo ou fez uma redefinição de fábrica, o nome de usuário e a senha padrão são *cisco*. Se precisar de instruções sobre como fazer login, siga as etapas do artigo Acesse o Utilitário baseado na Web do Ponto de acesso sem fio (WAP).



Explicação de captura de pacote remoto

O recurso Remote Packet Capture permite especificar uma porta remota como a porta de destino para capturas de pacotes. Este recurso funciona em conjunto com a ferramenta analisador de rede Wireshark para Windows. Um servidor de captura de pacotes é executado no dispositivo WAP e envia os pacotes capturados por meio de uma conexão TCP (Transmission Control Protocol) à ferramenta Wireshark.

Um computador com Microsoft Windows executando a ferramenta Wireshark permite exibir, registrar e analisar o tráfego capturado. O recurso de captura remota de pacotes é um recurso padrão da ferramenta Wireshark para Windows.

Embora a captura remota de pacotes não seja suportada pelo Linux, a ferramenta Wireshark funciona no Linux e os arquivos de captura já criados podem ser visualizados.

Quando o modo de captura remota está em uso, o dispositivo WAP não armazena dados capturados localmente em seu sistema de arquivos.

Se um firewall estiver instalado entre o computador instalado do Wireshark e o dispositivo WAP, o Wireshark deverá ter permissão para passar pela política de firewall do computador. O firewall também deve ser configurado para permitir que o computador Wireshark inicie uma conexão TCP com o dispositivo WAP.

Transmitir uma captura diretamente para o Wireshark

Para iniciar uma captura remota em um dispositivo WAP usando a opção *Stream to a Remote*

Host, siga as etapas listadas abaixo.

Passo 1

No WAP, navegue para **Troubleshoot > Packet Capture**.

Para o *método de captura de pacotes*:

1. Selecione **Stream to a Remote Host** no menu suspenso.
2. No campo *Remote Capture Port*, use a porta padrão de **2002** ou, se estiver usando uma porta diferente do padrão, insira o número de porta desejado usado para conectar o Wireshark ao dispositivo WAP. O intervalo de portas é de 1025 a 65530.
3. Há dois *Modos* para opções de captura de pacotes. Selecione o que é melhor para o seu cenário.

·*Todo o Tráfego Sem Fio* - Capture todos os pacotes sem fio no ar.

·*tráfego de/para este AP* - Capture o pacote enviado do AP ou do AP recebido.

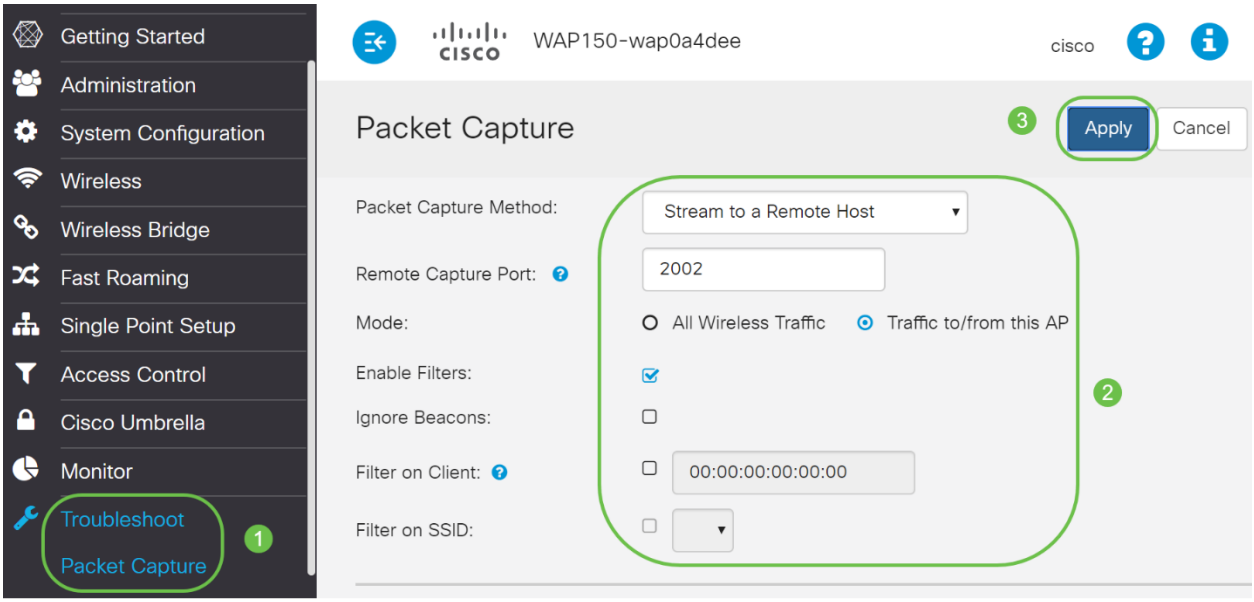
4. Marque **Ativar filtros**.
5. Escolha uma das seguintes opções:

·*Ignorar Beacons* - Ative ou desative a captura de beacons 802.11 detectados ou transmitidos pelo rádio. Os quadros beacon são quadros de broadcast que transportam informações sobre uma rede. A finalidade de um beacon é anunciar uma rede sem fio existente.

·*Filtro no Cliente* - Depois de ativado, especifique o endereço MAC para o filtro do Cliente WLAN. Observe que o filtro do cliente está ativo somente quando uma captura é executada em uma interface 802.11.

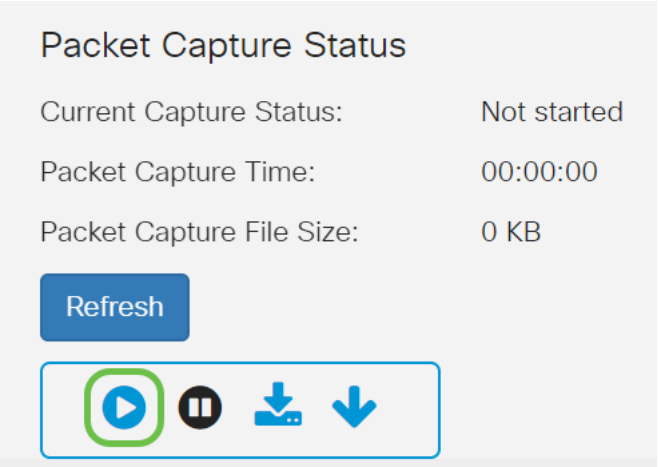
·*Filtro no SSID* - Esta opção ficará acinzentada para esta opção *Stream to a Remote Host*.

6. Clique em **Apply** para salvar as configurações.



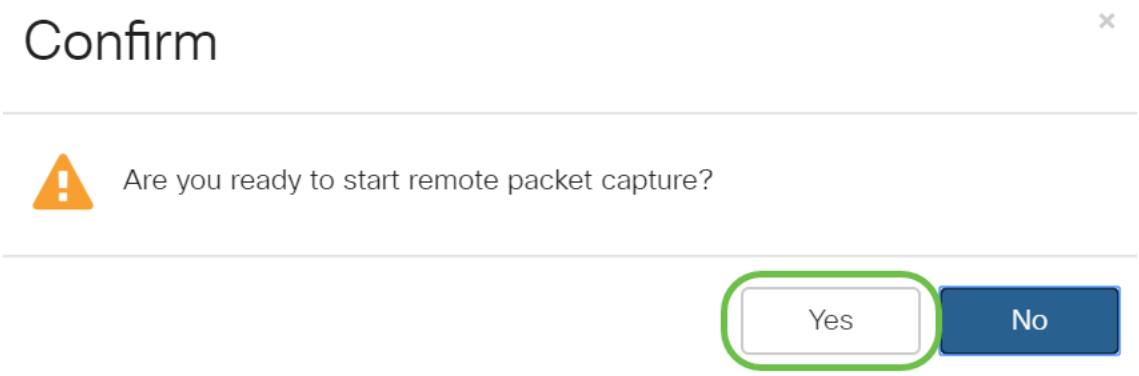
Passo 2

Clique no ícone **Iniciar captura**.



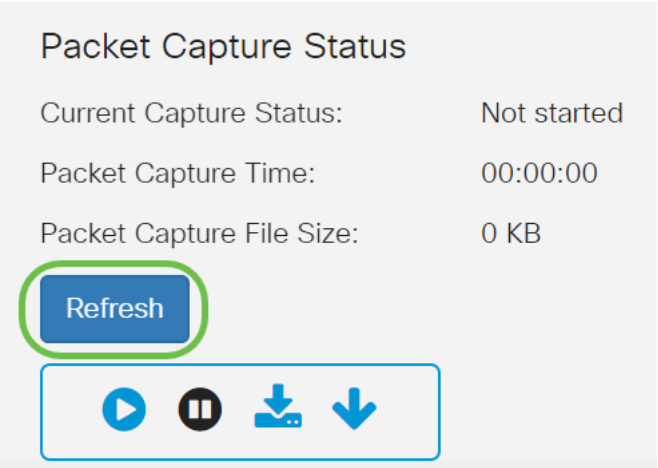
Etapa 3

Uma janela pop-up *confirm* será aberta. Clique em **Sim** para iniciar a captura.



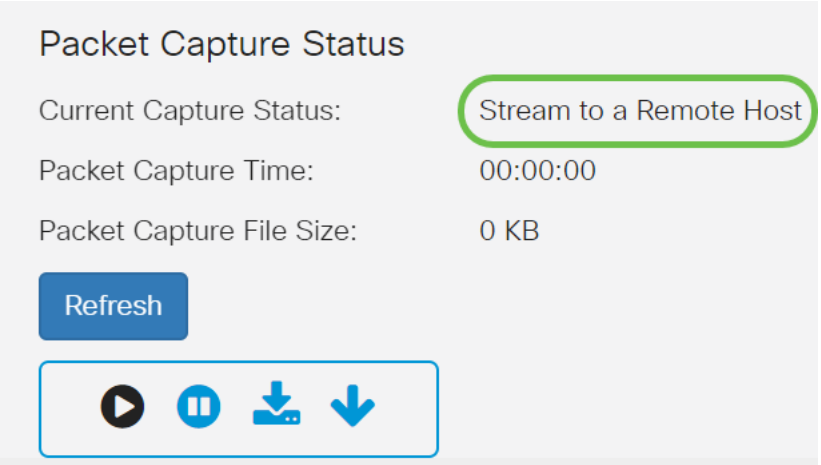
Passo 4

Clique no botão **Atualizar** para verificar o status atual.



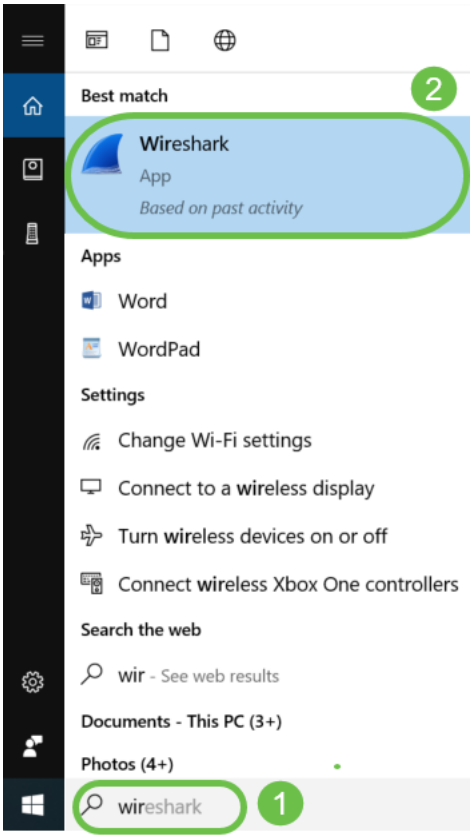
Etapa 5

Agora você pode ver que o *Status da Captura Atual* será *Fluxo para um Host Remoto*.



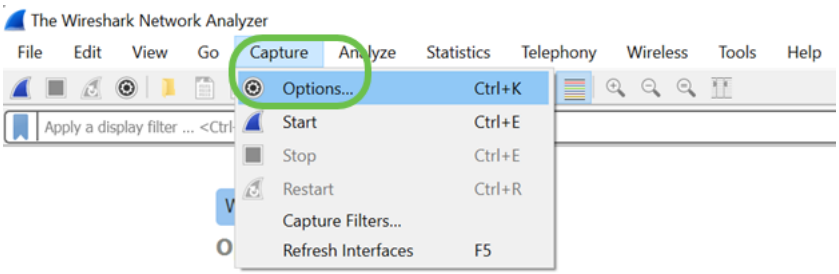
Etapa 6

Como o Wireshark já foi baixado, ele pode ser acessado digitando **Wireshark** na barra de pesquisa do Microsoft Windows e selecionando o aplicativo quando ele é uma opção.



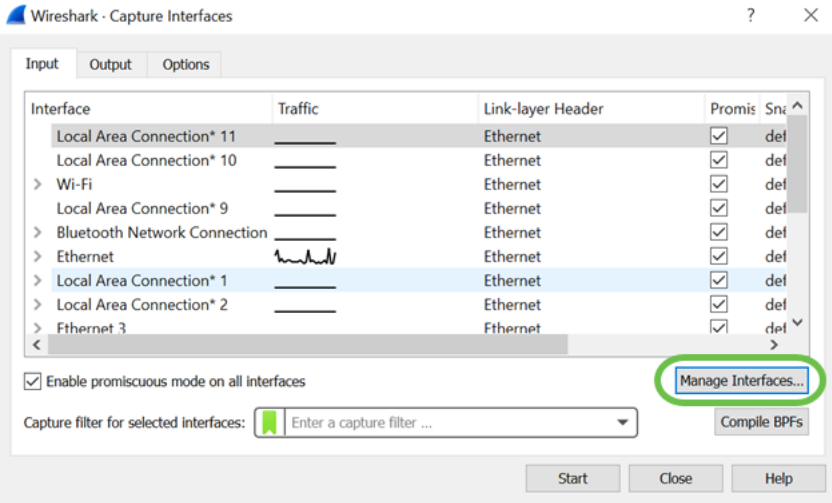
Etapa 7

Navegue até **Capture > Options...**



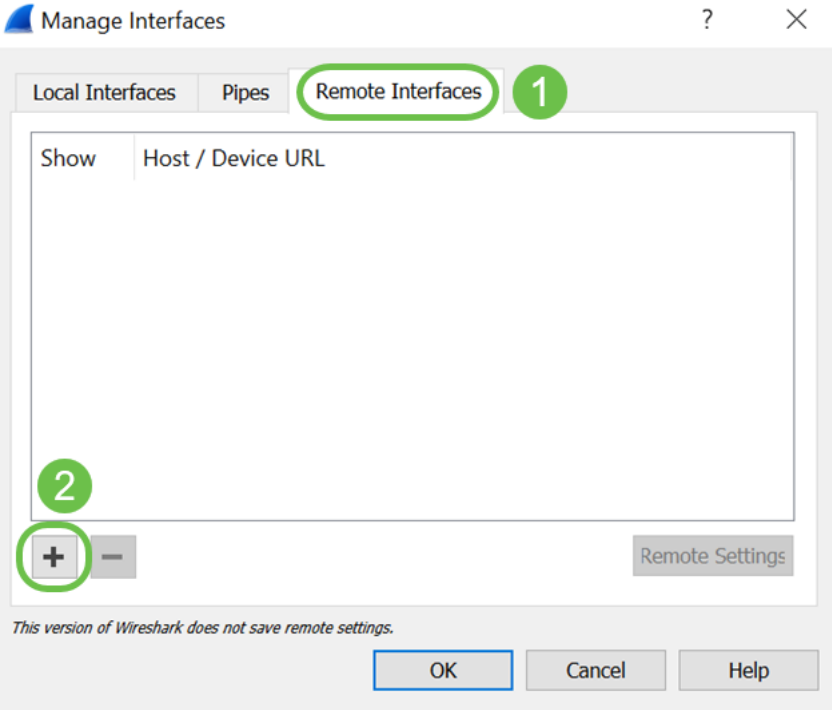
Passo 8

Na nova janela pop-up *Wireshark - Capture Interfaces*, clique em **Manage Interfaces**...



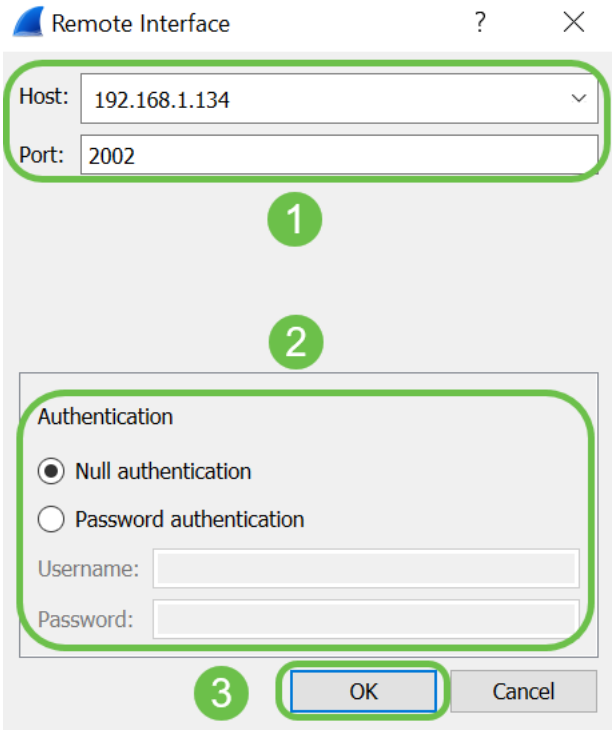
Passo 9

Na nova janela pop-up *Gerenciar interfaces*, navegue até **Interfaces remotas** e clique no **ícone de mais** para adicionar a interface.



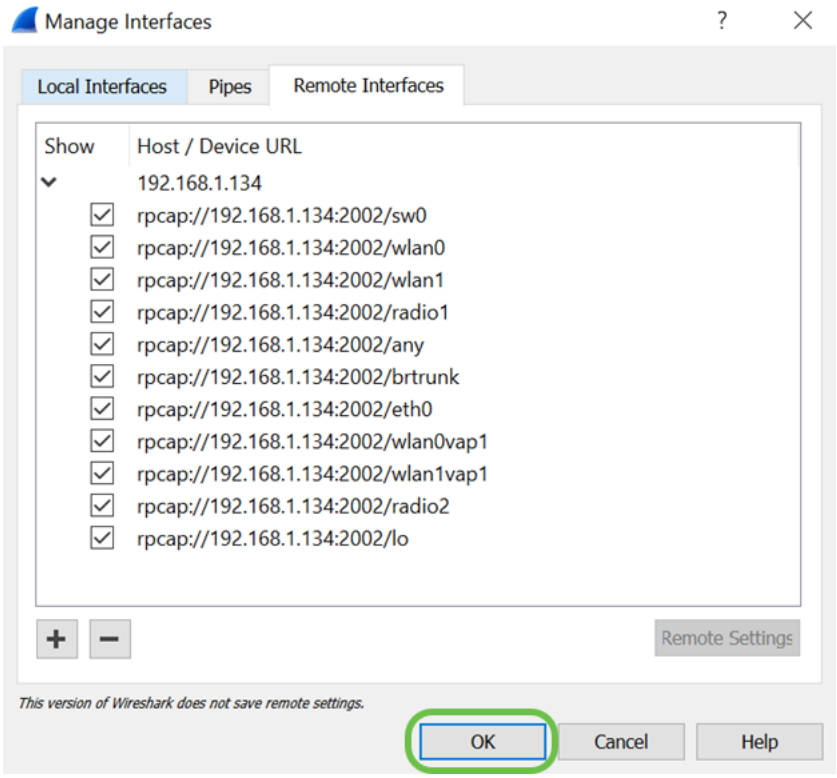
Passo 10

Na nova janela pop-up *Interface remota*, digite o *Host:* Detalhes do endereço IP (o IP do dispositivo WAP onde você iniciou a captura remota) e *Porta:* número (configurado no WAP para captura remota). Nesse caso, o IP do dispositivo WAP era 192.168.1.134. Você pode selecionar a opção *Null authentication* ou *Password authentication* com base em suas configurações. Se você selecionar, Autenticação de senha, insira os detalhes *do nome de usuário* e da *senha* de acordo. Click **OK**.



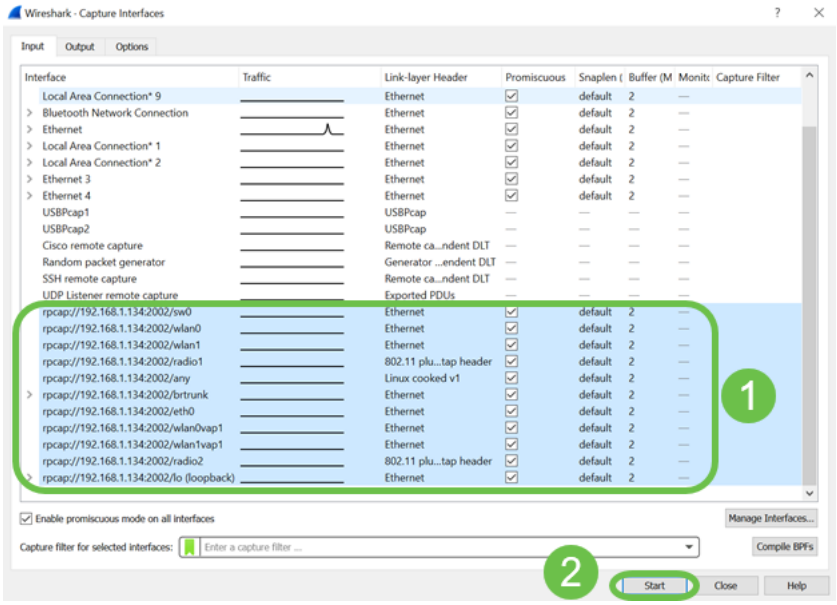
Passo 11

Na guia *Interfaces remotas*, você poderá ver todas as interfaces do dispositivo WAP remoto. Talvez você queira apenas desmarcar alguns desses para reduzir o volume de pacotes capturados. Você deixaria as interfaces de rádio selecionadas se quisesse ver pacotes de beacon. Click **OK**.



Etapa 12

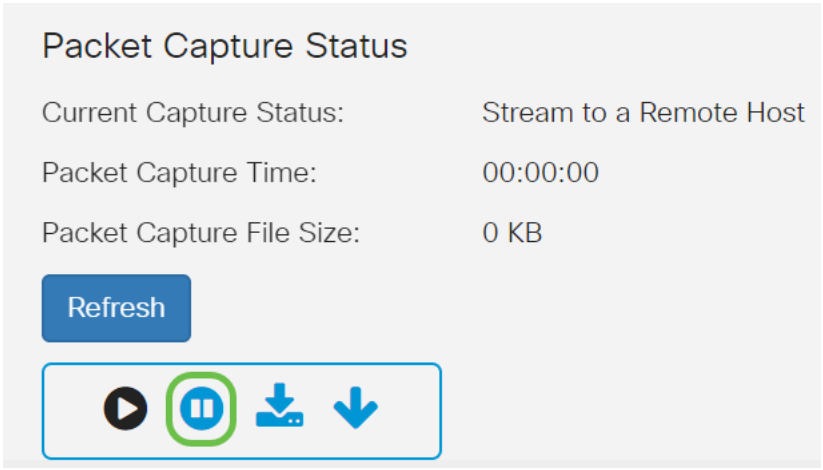
Agora, as interfaces recém-adicionadas refletirão na janela *Wireshark - Capture Interfaces*. **Selecione** a interface que deseja monitorar e clique em **Iniciar** para visualizar os pacotes.



Se você encontrar problemas ao tentar visualizar os pacotes, isso significa que o serviço *Remote Packet Capture Protocol* não está funcionando no sistema. O serviço Remote Packet Capture Protocol deve ser executado primeiro na plataforma de destino antes que o Wireshark possa se conectar a ele. Para obter mais informações, clique no link *Remote Capture Interfaces* através do Wireshark.

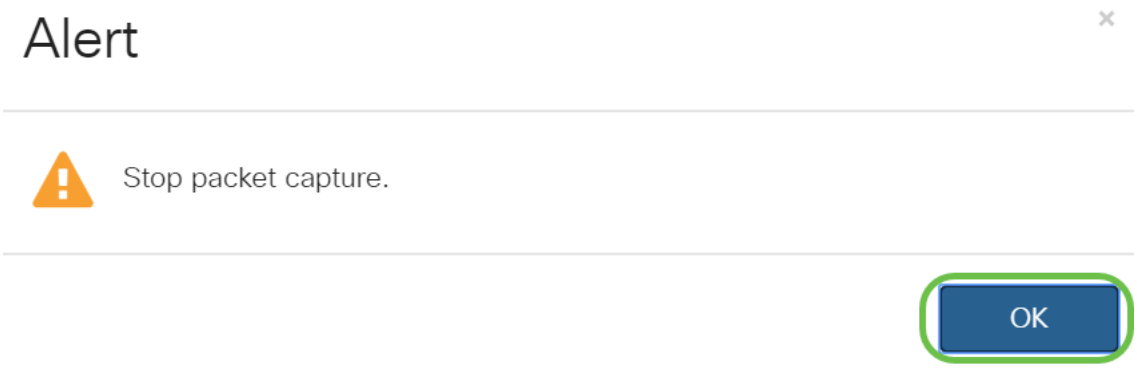
Passo 13

No WAP, clique no **ícone Stop Capture (Parar captura)** para interromper o processo de captura.



Passo 14

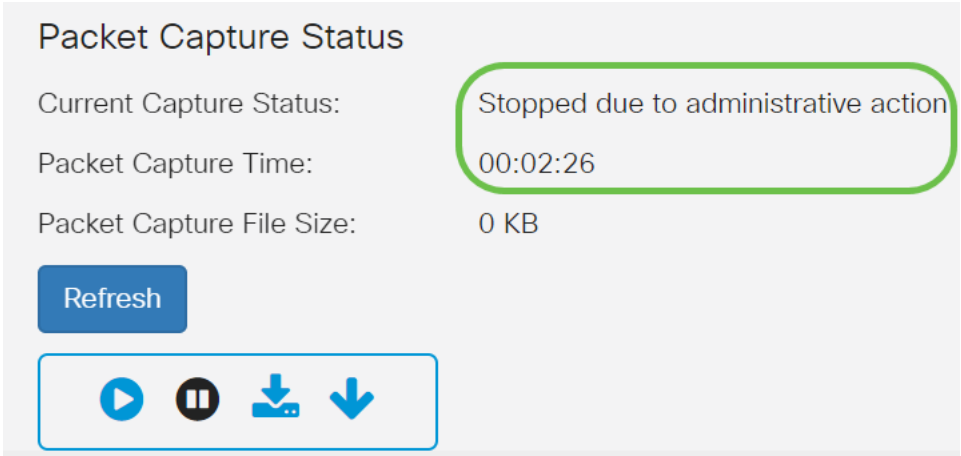
Uma janela pop-up *Alerta* será exibida. Clique em **OK** para interromper a captura remota.



Você também pode interromper a captura de pacotes clicando no botão **Stop (Parar)** no aplicativo Wireshark.

Etapa 15

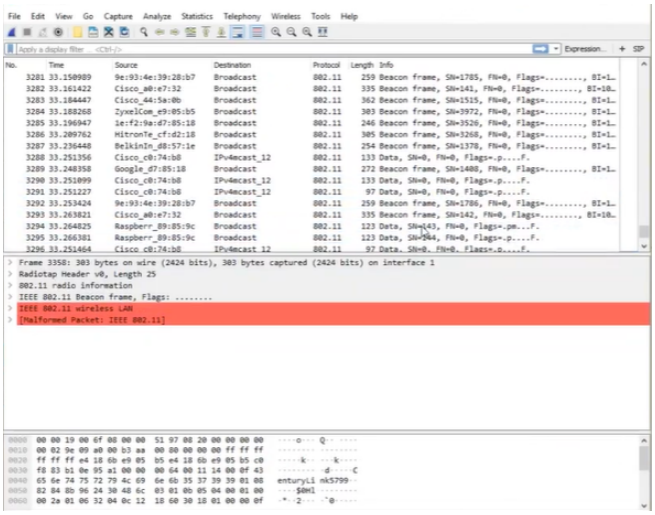
Agora, o *Status da Captura Atual* será exibido como *Parado devido à ação administrativa*, e o *Tempo de Captura de Pacotes* será refletido para mostrar a duração total da captura.



O *tamanho do arquivo de captura de pacote* aparecerá como *0 KB*. Além disso, as opções de download de arquivos não funcionarão neste cenário.

Passo 16

No Wireshark, você pode visualizar sua captura de pacotes.



Conclusão

Agora você tem as habilidades para transmitir um pacote diretamente ao Wireshark e pode trabalhar analisando-o. Não sabe aonde ir daqui? Há muitos vídeos e artigos disponíveis online para explorar. O que você procura depende das necessidades da sua situação. Você tem isso!