Utilisation de Wireshark sur un point d'accès sans fil Cisco Business pour l'analyse de paquets : Flux direct vers Wireshark

Objectif

Cet article explique comment effectuer une capture de paquets du trafic réseau à l'aide d'un point d'accès sans fil professionnel (WAP) Cisco et la diffuser directement à Wireshark.

Table des matières

Introduction et questions fréquentes

Les modifications de configuration, la surveillance et le dépannage sont souvent des problèmes auxquels un administrateur réseau doit faire face. Avoir un outil simple à utiliser est inestimable! L'objectif de cet article est d'être plus à l'aise avec les bases des captures de paquets et de savoir comment transmettre les paquets à Wireshark. Si vous n'êtes pas familier avec ce processus, répondez à quelques questions que vous avez peut-être déjà posées.

Tout d'abord, Wireshark est un analyseur de paquets gratuit pour quiconque cherche à dépanner son réseau. Wireshark fournit de nombreuses options pour la capture ainsi que le tri du trafic par plusieurs paramètres différents. Rendez-vous sur Wireshark pour plus de détails sur cette option open source.

Qu'est-ce qu'une capture de paquets ?

Une capture de paquets, également appelée fichier PCAP, est un outil qui peut être utile pour le dépannage. Il peut enregistrer chaque paquet envoyé entre les périphériques de votre réseau, en temps réel. La capture de paquets vous permet d'entrer dans les détails du trafic réseau, qui peut inclure tout, depuis la découverte de périphériques, les conversations de protocole et l'échec de l'authentification. Vous pouvez voir le chemin d'un flux de trafic spécifique et chaque interaction entre des périphériques sur des réseaux sélectionnés. Ces paquets peuvent être enregistrés pour une analyse plus approfondie si nécessaire. C'est comme une radiographie du fonctionnement interne du réseau via le transfert de paquets.

Quels types de paquets peuvent être capturés ?

Le périphérique WAP peut capturer les types de paquets suivants :

·paquets 802.11 reçus et transmis sans fil sur les interfaces radio. Les paquets capturés sur les interfaces radio incluent l'en-tête 802.11.

·paquets 802.3 reçus et transmis sur l'interface Ethernet.

·paquets 802.3 reçus et transmis sur les interfaces logiques internes, telles que les points d'accès virtuels (VAP) et les interfaces WDS (Wireless Distribution System).

Comment une capture de paquets peut-elle être effectuée sur un WAP ?

Deux méthodes de capture de paquets sont disponibles :

1. *Local Capture Method* - Les paquets capturés sont stockés dans un fichier sur le périphérique WAP. Le périphérique WAP peut transférer le fichier vers un serveur TFTP (Trivial File Transfer Protocol). Le fichier est formaté au format PCAP et peut être examiné à l'aide de Wireshark. Vous pouvez choisir *Enregistrer le fichier sur ce périphérique* pour sélectionner la méthode de capture locale.

Si vous préférez la méthode de capture locale, avec la dernière interface utilisateur Web, consultez Utilisation de Wireshark sur un WAP pour l'analyse de paquets : Télécharger le fichier.

Si vous préférez afficher un article qui utilise l'ancienne interface utilisateur graphique pour la méthode de capture locale, consultez Configurer la capture de paquets pour optimiser les performances sur un point d'accès sans fil.

2. *Remote Capture Method* - Les paquets capturés sont redirigés en temps réel vers un ordinateur externe exécutant Wireshark. Vous pouvez choisir *Stream to a Remote Host* pour sélectionner la méthode de capture distante. L'avantage de cette méthode est qu'il n'y a pas de limite au volume de paquets pouvant être capturés.

L'objectif de cet article est de diffuser vers un hôte distant, donc si c'est votre préférence, lisez sur !

Où puis-je diffuser le paquet ?

La fonctionnalité de capture de paquets sans fil permet de capturer et de stocker les paquets reçus et transmis par le périphérique WAP. Les paquets capturés peuvent ensuite être analysés par un analyseur de protocole réseau pour le dépannage ou l'optimisation des performances. De nombreuses applications tierces d'analyse de paquets sont disponibles en ligne. Dans cet article, nous nous concentrons sur Wireshark.

Certains modèles de WAP Cisco Business peuvent envoyer des paquets en temps réel à CloudShark, un décodeur de paquets basé sur le Web et un site d'analyse. Il est similaire à l'interface utilisateur de Wireshark pour l'analyse de paquets qui inclut de nombreuses options ajoutées avec un abonnement. Vous pouvez choisir *Stream to CloudShark* pour sélectionner la méthode de capture à distance. Pour plus d'informations, cliquez sur les liens suivants :

- CloudShark (leur site web officiel)
- Intégration de CloudShark pour l'analyse de paquets sur un WAP125 ou WAP581
- Intégration CloudShark avec WAP571 et WAP571E

Ni Wireshark ni CloudShark ne sont la propriété ou la prise en charge de Cisco. Ils sont inclus à des fins de démonstration uniquement. Pour obtenir de l'aide, contactez Wireshark ou CloudShark.

Périphériques et version logicielle applicables

- 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

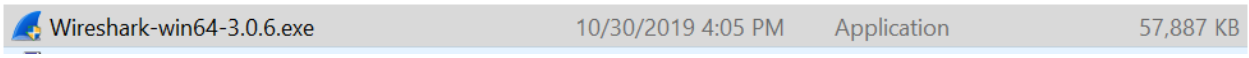
Télécharger Wireshark

Étape 1

Accédez au site Wireshark. Sélectionnez la version appropriée. Cliquez sur **Download**. Vous verrez la progression du téléchargement en bas à gauche de l'écran.

Étape 2

Accédez à *Téléchargements* sur votre ordinateur et sélectionnez le fichier Wireshark pour installer son application.



Se connecter au WAP

Dans votre navigateur Web, saisissez l'adresse IP du WAP. Entrez dans vos informations d'identification. Si vous accédez à ce périphérique pour la première fois ou si vous avez effectué une réinitialisation en usine, le nom d'utilisateur et le mot de passe par défaut sont *cisco*. Si vous avez besoin d'instructions pour vous connecter, vous pouvez suivre les étapes de l'article Accéder à l'utilitaire Web du point d'accès sans fil (WAP).

Explication de la capture de paquets à distance

La fonction de capture de paquets distante vous permet de spécifier un port distant comme port de destination pour les captures de paquets. Cette fonctionnalité fonctionne en conjonction avec l'outil d'analyse de réseau Wireshark pour Windows. Un serveur de capture de paquets s'exécute sur le périphérique WAP et envoie les paquets capturés via une connexion TCP (Transmission Control Protocol) à l'outil Wireshark.

Un ordinateur Microsoft Windows exécutant l'outil Wireshark vous permet d'afficher, de consigner et d'analyser le trafic capturé. La fonction de capture de paquets distante est une fonctionnalité standard de l'outil Wireshark pour Windows.

Bien que la capture de paquets distante ne soit pas prise en charge par Linux, l'outil Wireshark fonctionne sous Linux et les fichiers de capture déjà créés peuvent être affichés.

Lorsque le mode de capture à distance est utilisé, le périphérique WAP ne stocke aucune donnée capturée localement dans son système de fichiers.

Si un pare-feu est installé entre l'ordinateur Wireshark installé et le périphérique WAP, Wireshark doit être autorisé à passer par la stratégie de pare-feu de l'ordinateur. Le pare-feu doit également être configuré pour permettre à l'ordinateur Wireshark d'initier une connexion TCP au périphérique WAP.

Diffuser une capture directement vers Wireshark

Pour lancer une capture distante sur un périphérique WAP à l'aide de l'option *Stream to a Remote*

Host, procédez comme suit :

Étape 1

Sur le WAP, accédez à **Troubleshoot > Packet Capture**.

Pour la *méthode de capture de paquets* :

1. Sélectionnez **Stream to a Remote Host** dans le menu déroulant.
2. Dans le champ *Remote Capture Port*, utilisez le port par défaut **2002**, ou si vous utilisez un port autre que le port par défaut, saisissez le numéro de port souhaité utilisé pour connecter Wireshark au périphérique WAP. La plage de ports est comprise entre 1025 et 65530.
3. Il existe deux *modes* pour les options de capture de paquets. Sélectionnez ce qui convient le mieux à votre scénario.

·*Tout le trafic sans fil* - Capturez tous les paquets sans fil dans l'air.

·*Trafic vers/depuis ce point d'accès* - Capture le paquet envoyé par le point d'accès ou le point d'accès reçu.

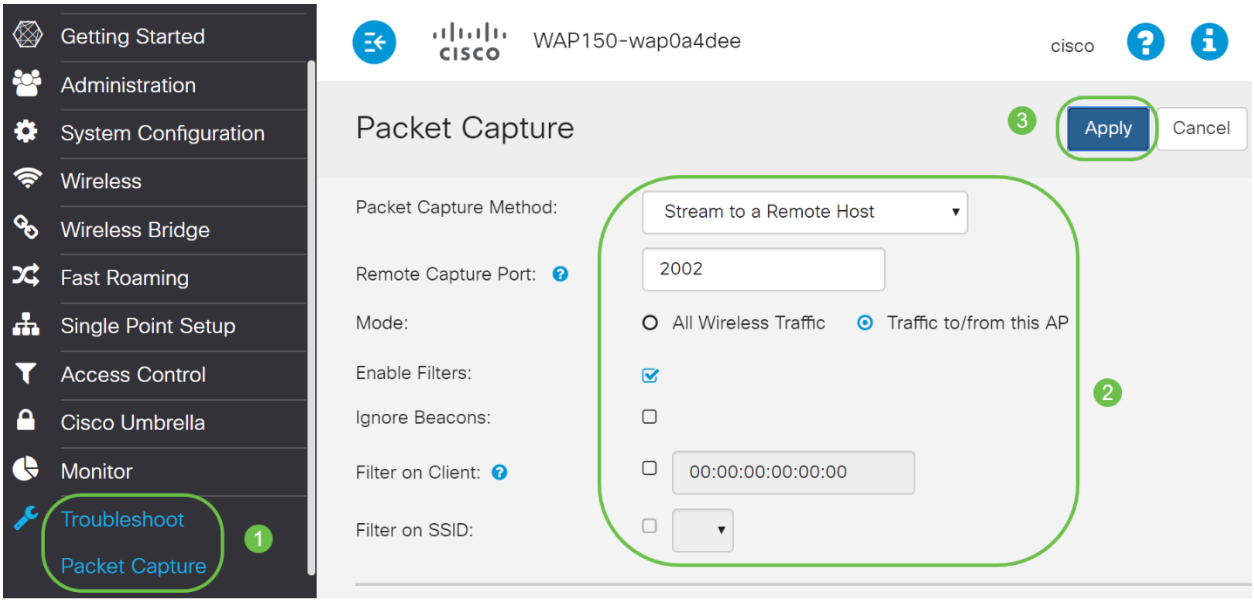
4. Cochez **Activer les filtres**.
5. Choisissez l'une des options suivantes :

·*Ignorer les balises* : activez ou désactivez la capture des balises 802.11 détectées ou transmises par la radio. Les trames de balise sont des trames de diffusion qui transportent des informations relatives à un réseau. L'objectif d'une balise est d'annoncer un réseau sans fil existant.

·*Filter on Client* - Une fois activée, spécifiez l'adresse MAC pour le filtre Client WLAN. Notez que le filtre Client est actif uniquement lorsqu'une capture est effectuée sur une interface 802.11.

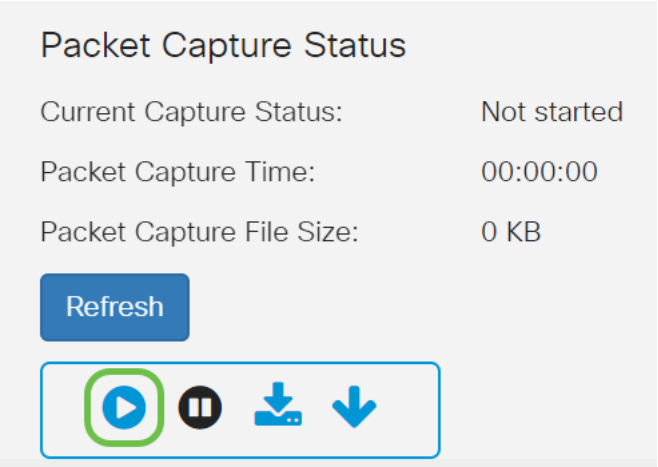
·*Filter on SSID* - Cette option sera grisée pour cette option *Stream to a Remote Host*.

6. Cliquez sur **Apply** pour enregistrer les paramètres.



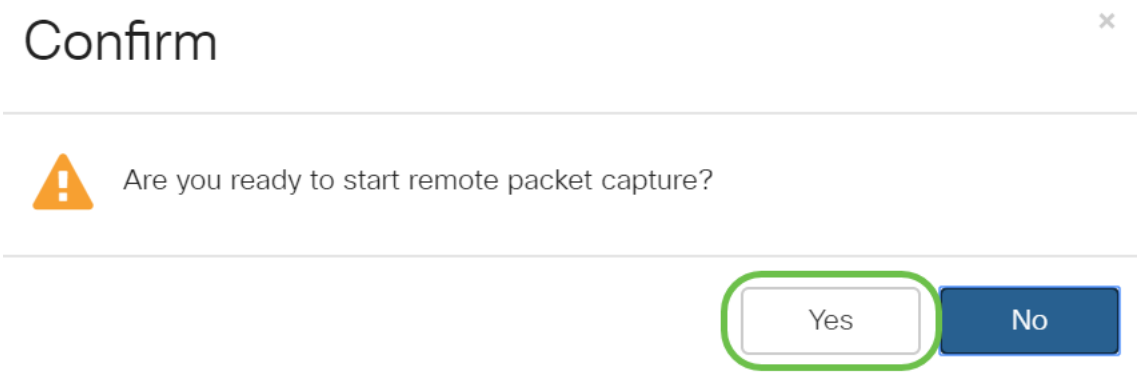
Étape 2

Cliquez sur l'icône **Start Capture**.



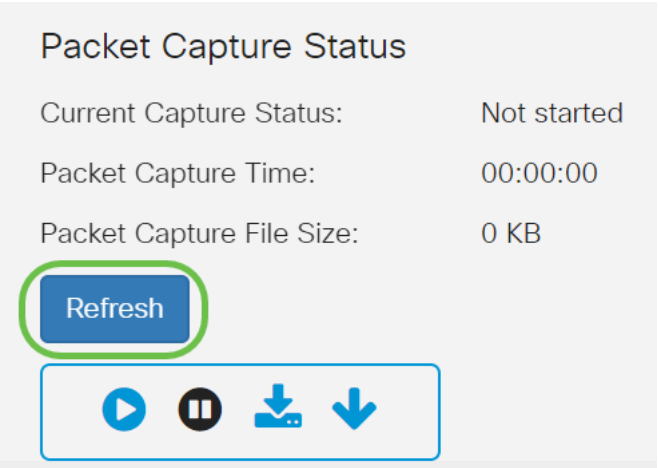
Étape 3

Une fenêtre contextuelle *Confirmer* s'ouvre. Cliquez sur **Oui** pour lancer la capture.



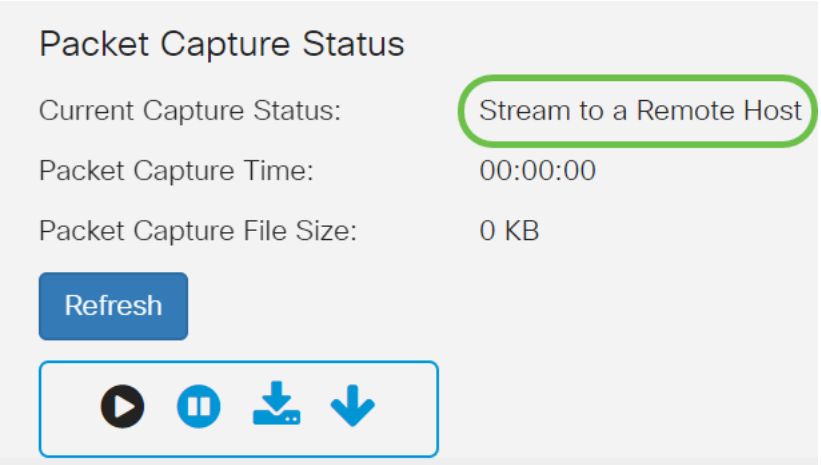
Étape 4

Cliquez sur le bouton **Actualiser** pour vérifier l'état actuel.



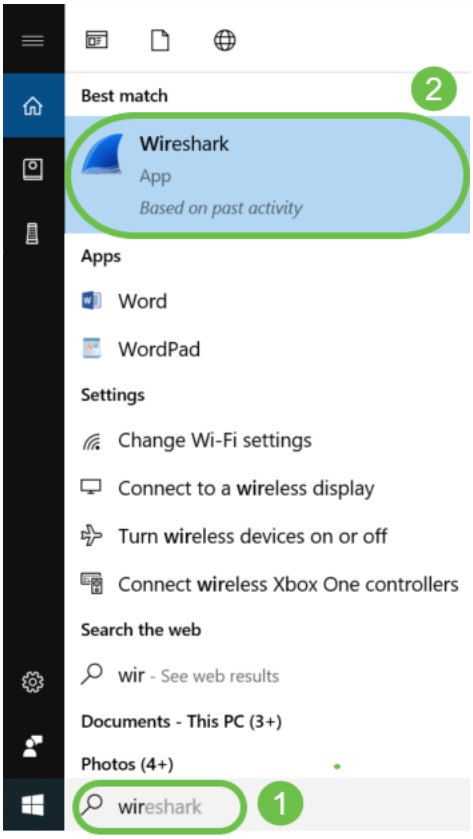
Étape 5

Vous pouvez maintenant voir que l'*état de capture actuel* sera *Stream to a Remote Host*.



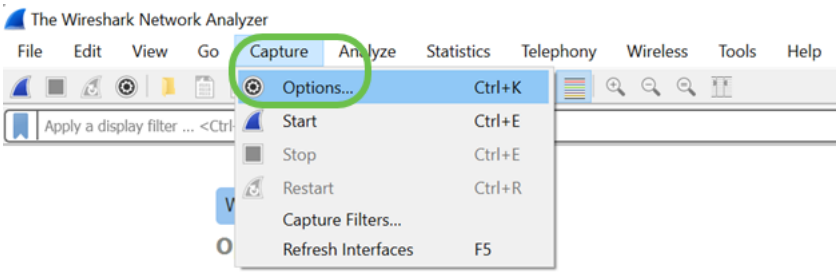
Étape 6

Étant donné que Wireshark a déjà été téléchargé, vous pouvez y accéder en tapant **Wireshark** dans la barre de recherche de Microsoft Windows et en sélectionnant l'application lorsqu'il s'agit d'une option.



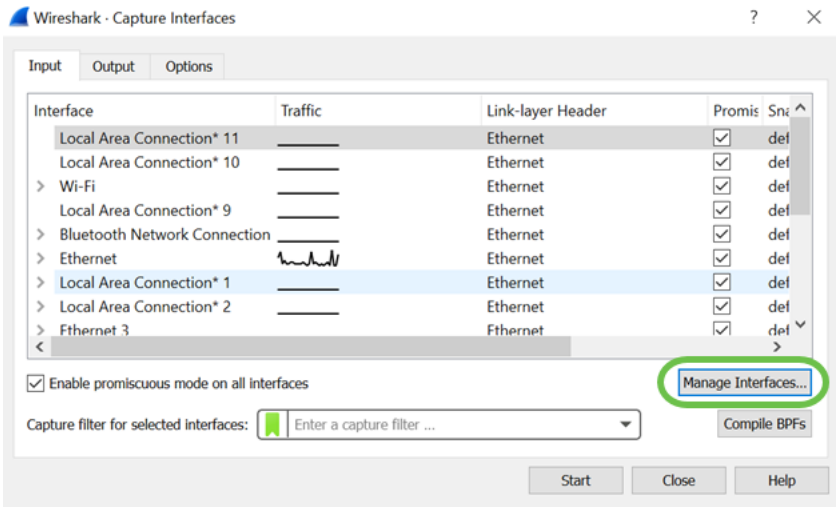
Étape 7

Accédez à **Capture > Options...**



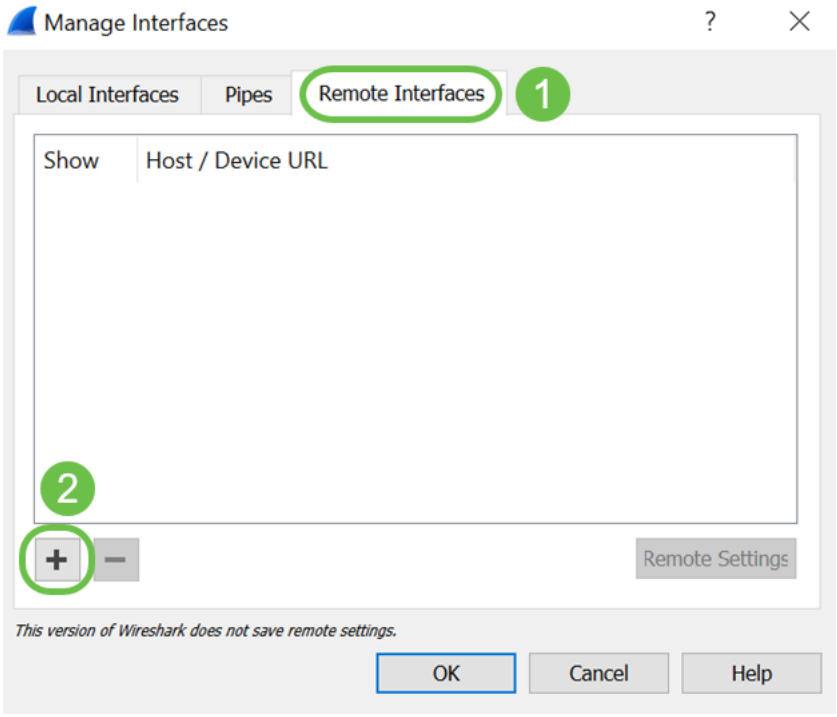
Étape 8

Dans la nouvelle fenêtre contextuelle *Wireshark - Interfaces de capture*, cliquez sur **Gérer les interfaces**...



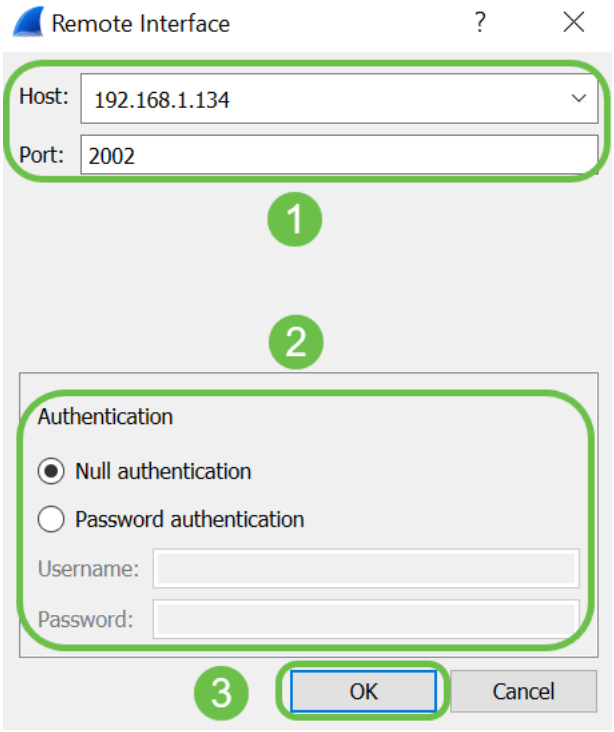
Étape 9

Dans la nouvelle fenêtre contextuelle *Gérer les interfaces*, accédez à **Interfaces distantes** et cliquez sur l'**icône plus** pour ajouter l'interface.



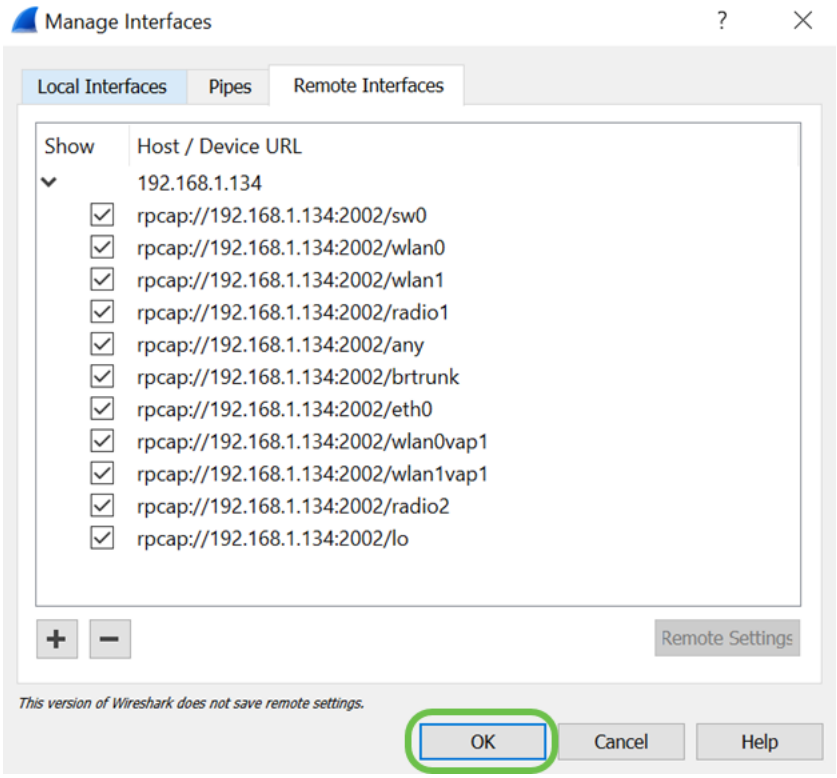
Étape 10

Dans la nouvelle fenêtre contextuelle *Interface distante*, saisissez l'*hôte :* Détails de l'adresse IP (l'adresse IP du périphérique WAP sur lequel vous avez démarré la capture distante) et *Port :* numéro (configuré sur WAP pour la capture à distance). Dans ce cas, l'adresse IP du périphérique WAP était 192.168.1.134. Vous pouvez sélectionner l'option *Authentification Null* ou *Authentification par mot de passe* en fonction de vos paramètres. Si vous sélectionnez Authentification par mot de passe, entrez le *nom d'utilisateur* et le *mot de passe* en conséquence. Click OK.



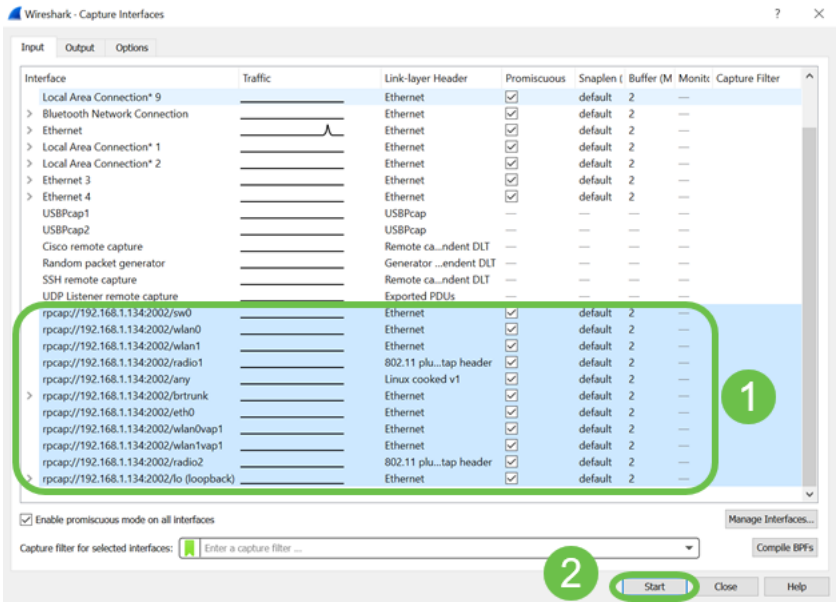
Étape 11

Sous l'onglet *Interfaces distantes*, vous pouvez voir toutes les interfaces du périphérique WAP distant. Il est possible que vous souhaitiez uniquement en désélectionner certaines pour réduire le volume des paquets capturés. Si vous voulez voir des paquets de balise, vous devez laisser les interfaces radio sélectionnées. Click OK.



Étape 12

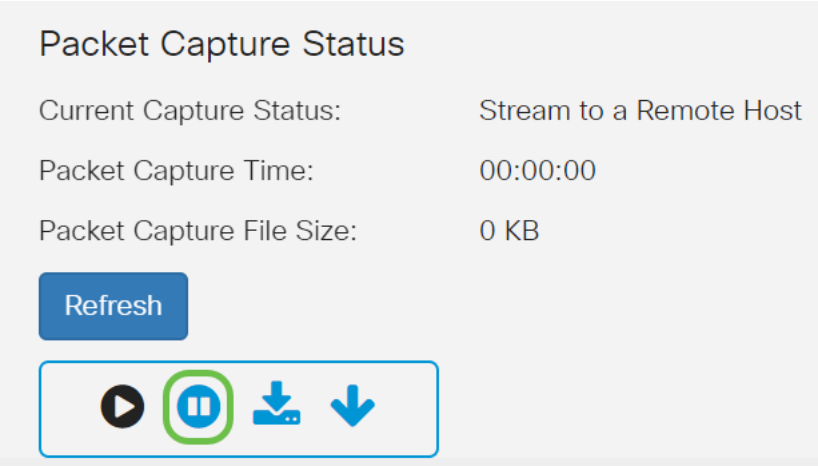
Les interfaces nouvellement ajoutées réfléchiront dans la fenêtre *Wireshark - Capture Interfaces*. **Sélectionnez** l'interface à surveiller et cliquez sur **Démarrer** pour afficher les paquets.



Si vous rencontrez des problèmes lorsque vous essayez d'afficher les paquets, cela signifie que le service *Remote Packet Capture Protocol* ne fonctionne pas sur votre système. Le service Remote Packet Capture Protocol doit d'abord être exécuté sur la plate-forme cible avant que Wireshark puisse s'y connecter. Pour plus d'informations, cliquez sur le lien *Remote Capture Interfaces* via Wireshark.

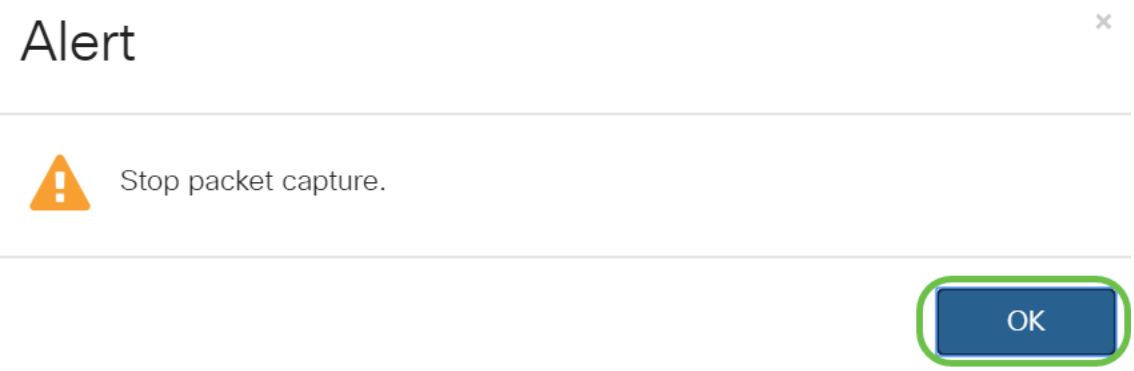
Étape 13

Sur le WAP, cliquez sur l'**icône Arrêter la capture** pour arrêter le processus de capture.



Étape 14

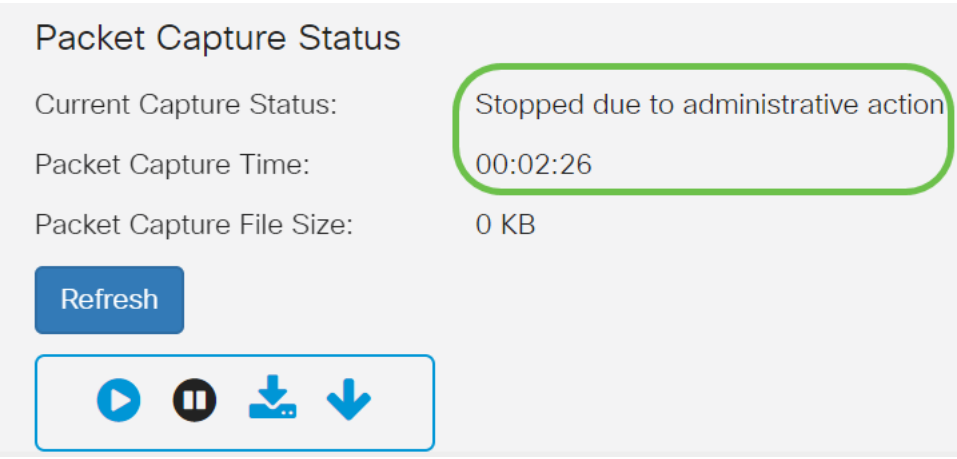
Une fenêtre contextuelle *Alerte* s'affiche. Cliquez sur **OK** pour arrêter la capture distante.



Vous pouvez également arrêter la capture de paquets en cliquant sur le bouton **Arrêter** dans l'application Wireshark.

Étape 15

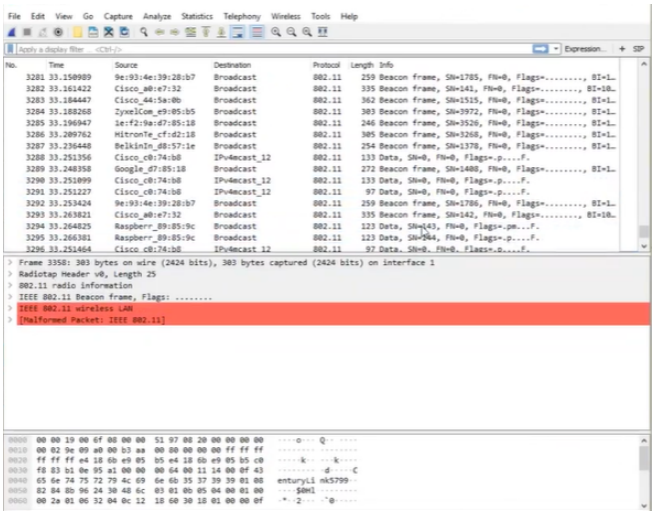
Maintenant, l'*état de capture actuel* sera affiché comme *arrêté en raison d'une action administrative*, et *le temps de capture de paquets* sera reflété pour afficher la durée totale de capture.



La *taille du fichier de capture de paquets* s'affiche comme *0 Ko*. En outre, les options de téléchargement de fichiers ne fonctionneront pas dans ce scénario.

Étape 16

Sur Wireshark, vous pouvez afficher votre capture de paquets.



Conclusion

Vous avez maintenant les compétences nécessaires pour transmettre un paquet directement à Wireshark et vous pouvez travailler à son analyse. Vous ne savez pas où aller ? Il y a beaucoup de vidéos et d'articles disponibles en ligne à explorer. Ce que vous recherchez dépend des besoins de votre situation. Vous avez ceci !