Uso di Wireshark su Cisco Business WAP per l'analisi dei pacchetti: Streaming diretto a Wireshark

Obiettivo

In questo articolo viene spiegato come eseguire un'acquisizione di pacchetti del traffico di rete utilizzando un Cisco Business Wireless Access Point (WAP) e trasmetterli direttamente a Wireshark.

Sommario

Introduzione e domande frequenti

Le modifiche alla configurazione, il monitoraggio e la risoluzione dei problemi sono problemi che gli amministratori di rete devono affrontare spesso. Avere uno strumento semplice da usare è inestimabile! L'obiettivo di questo articolo è di acquisire familiarità con le nozioni di base sulle acquisizioni dei pacchetti e su come inviarli a Wireshark. Se non avete familiarità con questo processo, rispondete ad alcune domande che potreste già avere.

Per prima cosa, Wireshark è un analizzatore di pacchetti gratuito per chiunque voglia risolvere i problemi della rete. Wireshark fornisce molte opzioni per l'acquisizione e l'ordinamento del traffico in base a diversi parametri. Visitate Wireshark per i dettagli su questa opzione open-source.

Che cos'è l'acquisizione dei pacchetti?

L'acquisizione di un pacchetto, nota anche come file PCAP, è uno strumento che può essere utile nella risoluzione dei problemi. Può registrare in tempo reale ogni pacchetto inviato tra i dispositivi della rete. L'acquisizione dei pacchetti consente di analizzare i dettagli del traffico di rete, che può includere qualsiasi cosa, dall'individuazione dei dispositivi alle conversazioni di protocollo e all'autenticazione non riuscita. È possibile visualizzare il percorso di un flusso di traffico specifico e ogni interazione tra i dispositivi sulle reti selezionate. Questi pacchetti possono essere salvati per ulteriori analisi, se necessario. È come una radiografia del funzionamento interno della rete tramite il trasferimento di pacchetti.

Quali tipi di pacchetti è possibile acquisire?

Il dispositivo WAP può acquisire i seguenti tipi di pacchetti:

·pacchetti 802.11 ricevuti e trasmessi in modalità wireless sulle interfacce radio. I pacchetti acquisiti sulle interfacce radio includono l'intestazione 802.11.

·Pacchetti 802.3 ricevuti e trasmessi sull'interfaccia Ethernet.

·Pacchetti 802.3 ricevuti e trasmessi sulle interfacce logiche interne, come i VAP (Virtual Access Point) e le interfacce WDS (Wireless Distribution System).

In che modo è possibile acquisire un pacchetto su un WAP?

Sono disponibili due metodi di acquisizione dei pacchetti:

1. *Local Capture Method* - I pacchetti catturati vengono archiviati in un file sul dispositivo WAP. Il dispositivo WAP può trasferire il file in un server TFTP (Trivial File Transfer Protocol). Il file è formattato in formato PCAP e può essere esaminato utilizzando Wireshark. È possibile scegliere *Salva file sul dispositivo* per selezionare il metodo di acquisizione locale.

Se si preferisce il metodo di acquisizione locale, dotato della più recente interfaccia utente Web, utilizzare Wireshark su un WAP per l'analisi dei pacchetti: Carica file.

Se si preferisce visualizzare un articolo che utilizza la GUI precedente per il metodo di acquisizione locale, consultare Configurare l'acquisizione dei pacchetti per ottimizzare le prestazioni su un punto di accesso wireless.

2. *Metodo di acquisizione remota* - I pacchetti acquisiti vengono reindirizzati in tempo reale a un computer esterno che esegue Wireshark. È possibile scegliere *Trasmetti a host remoto* per selezionare il metodo di acquisizione remota. Il vantaggio di questo metodo è che non vi sono limiti al volume dei pacchetti che possono essere acquisiti.

Lo scopo di questo articolo è quello di trasmettere a un host remoto, quindi se questa è la vostra preferenza, leggere!

Dove posso inviare il pacchetto in streaming?

La funzione di acquisizione dei pacchetti wireless consente di acquisire e memorizzare i pacchetti ricevuti e trasmessi dal dispositivo WAP. I pacchetti acquisiti possono quindi essere analizzati da un analizzatore di protocolli di rete per la risoluzione dei problemi o l'ottimizzazione delle prestazioni. Sono disponibili online numerose applicazioni di analisi dei pacchetti di terze parti. In questo articolo, ci concentriamo su Wireshark.

Alcuni modelli di Cisco Business WAP possono inviare pacchetti in tempo reale a CloudShark, un decoder di pacchetti e un sito di analisi basati sul Web. È simile all'interfaccia utente di Wireshark per l'analisi dei pacchetti, che include molte opzioni aggiunte con una sottoscrizione. È possibile scegliere *Stream to CloudShark* per selezionare il metodo di acquisizione remota. Per ulteriori informazioni, fare clic sui collegamenti seguenti:

- CloudShark (il loro sito ufficiale)
- Integrazione di CloudShark per l'analisi dei pacchetti su un WAP125 o WAP581
- Integrazione CloudShark con WAP571 e WAP571E

Né Wireshark né CloudShark sono posseduti o supportati da Cisco. Sono inclusi solo a scopo

dimostrativo. Per assistenza, contattare Wireshark o CloudShark.

Dispositivi e versione software interessati

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

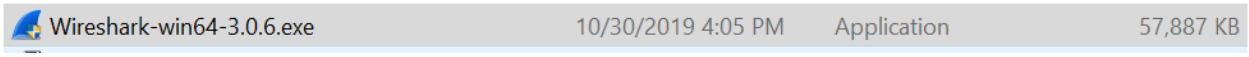
Scarica Wireshark

Passaggio 1

Visitate il sito Web Wireshark. Selezionare la versione appropriata. Fare clic su **Download (Scarica).** In basso a sinistra nella finestra viene visualizzato lo stato del download.

Passaggio 2

Andare su *Download* sul computer e selezionare il file Wireshark per installare la sua applicazione.



Accedere a WAP

Nel browser Web, immettere l'indirizzo IP del WAP. Immettere le credenziali. Se è la prima volta che accedi a questo dispositivo o hai eseguito una reimpostazione di fabbrica, il nome utente e la password predefiniti sono *cisco*. Per istruzioni su come eseguire l'accesso, seguire la procedura descritta nell'articolo Accesso all'utilità basata sul Web del punto di accesso wireless (WAP).

Spiegazione acquisizione pacchetti in remoto

La funzione di acquisizione remota dei pacchetti consente di specificare una porta remota come porta di destinazione per l'acquisizione dei pacchetti. Questa funzionalità viene utilizzata insieme allo strumento Wireshark network analyzer per Windows. Un server di acquisizione pacchetti viene eseguito sul dispositivo WAP e invia i pacchetti acquisiti tramite una connessione TCP (Transmission Control Protocol) allo strumento Wireshark.

Un computer con sistema operativo Microsoft Windows su cui è in esecuzione lo strumento Wireshark consente di visualizzare, registrare e analizzare il traffico acquisito. La funzione di acquisizione dei pacchetti remota è una funzionalità standard dello strumento Wireshark per Windows.

Anche se l'acquisizione remota dei pacchetti non è supportata da Linux, lo strumento Wireshark funziona su Linux ed è possibile visualizzare i file di acquisizione già creati.

Quando la modalità di cattura remota è in uso, il dispositivo WAP non memorizza alcun dato acquisito localmente nel proprio file system.

Se tra il computer installato Wireshark e il dispositivo WAP è installato un firewall, Wireshark deve poter passare attraverso i criteri firewall del computer. Il firewall deve inoltre essere configurato in modo da consentire al computer Wireshark di avviare una connessione TCP con il dispositivo WAP.

Trasmetti una cattura direttamente a Wireshark

Per avviare un'acquisizione remota su un dispositivo WAP utilizzando l'opzione *Stream to a Remote Host*, eseguire la procedura riportata di seguito.

Passaggio 1

Nel WAP, selezionare **Risoluzione dei problemi > Acquisizione pacchetti**.

Per il *metodo Packet Capture*:

1. Selezionare **Stream to a Remote Host** dal menu a discesa.
2. Nel campo *Remote Capture Port* (Porta di acquisizione remota), utilizzare la porta predefinita **2002** oppure, se si utilizza una porta diversa da quella predefinita, immettere il numero di porta desiderato per il collegamento di Wireshark al dispositivo WAP. L'intervallo di porte è compreso tra 1025 e 65530.
3. Le opzioni di acquisizione dei pacchetti sono disponibili in due *modalità*. Selezionare la soluzione migliore per lo scenario.

·*Tutto il traffico wireless* - Cattura tutti i pacchetti wireless in onda.

·*Traffico da/verso questo access point*: acquisizione del pacchetto inviato dall'access point o dall'access point ricevuto.

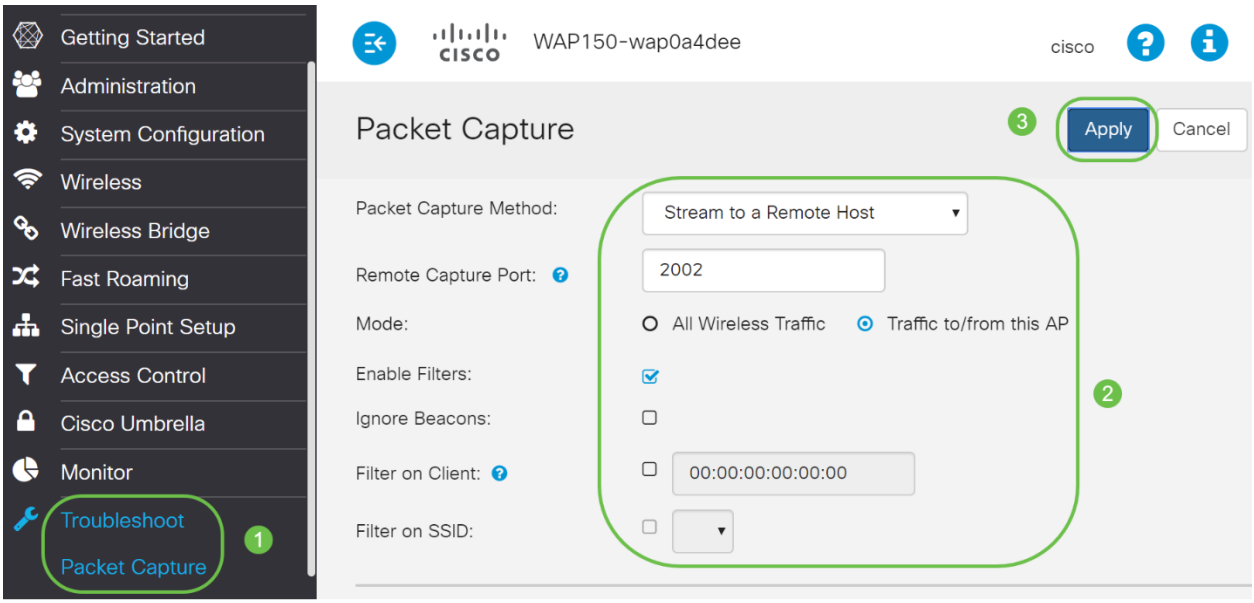
4. Selezionare **Abilita filtri**.
5. Scegliere una delle opzioni seguenti:

·*Ignora beacon* - Abilita o disabilita la cattura dei beacon 802.11 rilevati o trasmessi dalla radio. I frame beacon sono frame di trasmissione che contengono informazioni relative a una rete. Lo scopo di un beacon è quello di annunciare una rete wireless esistente.

·*Filtro sul client*: una volta abilitato, specificare l'indirizzo MAC per il filtro del client WLAN. Il filtro Client è attivo solo quando si esegue un'acquisizione su un'interfaccia 802.11.

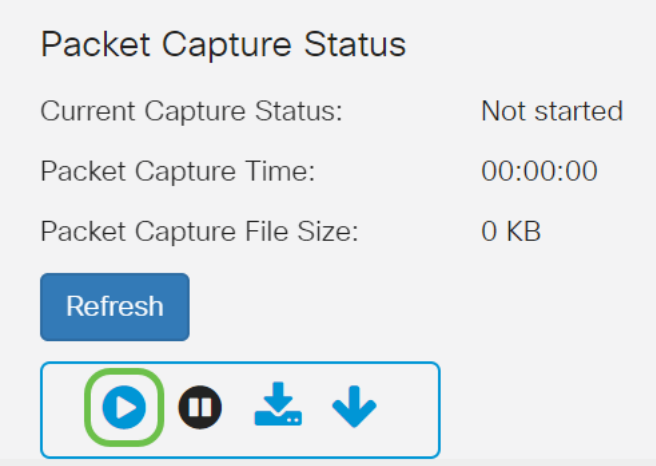
·*Filtro in base a SSID* - Questa opzione è disattivata per l'opzione *Stream to a Remote Host*.

6. Fare clic su **Applica** per salvare le impostazioni.



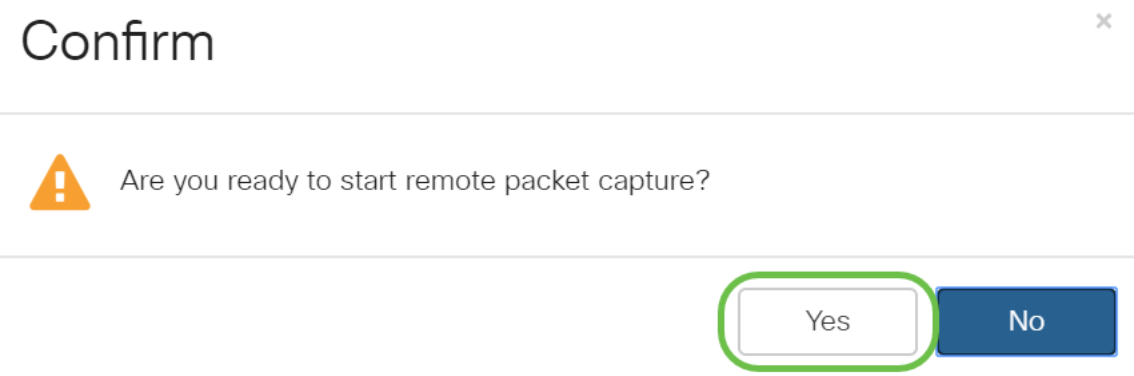
Passaggio 2

Fare clic sull'icona **Avvia acquisizione**.



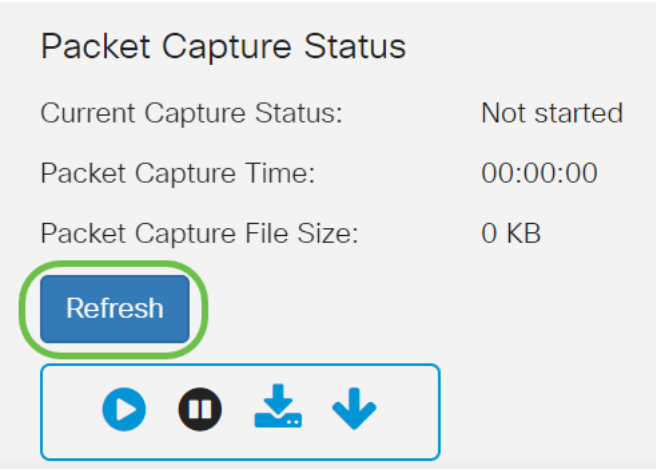
Passaggio 3

Viene visualizzata una finestra di *conferma*. Fare clic su **Yes** (Sì) per avviare la cattura.



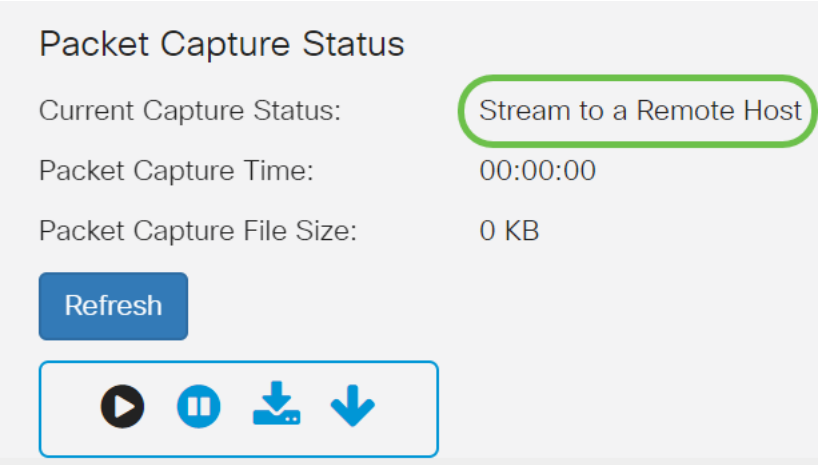
Passaggio 4

Fare clic sul pulsante **Refresh** per verificare lo stato corrente.



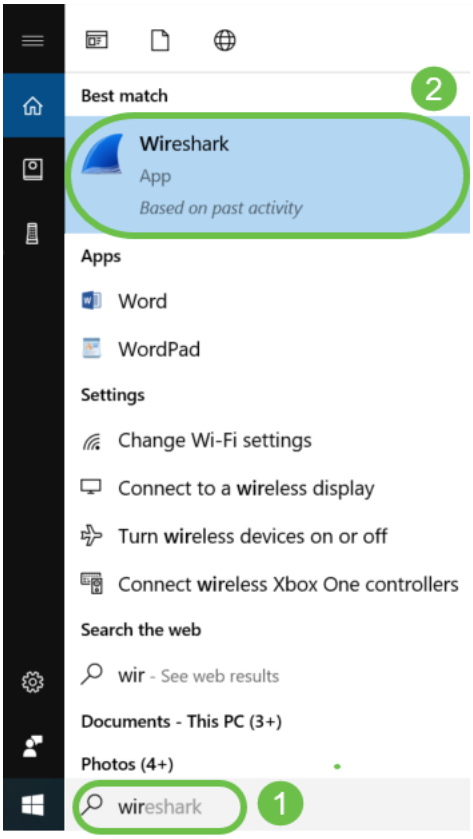
Passaggio 5

A questo punto è possibile visualizzare lo *stato di acquisizione corrente* come *flusso a un host remoto*.



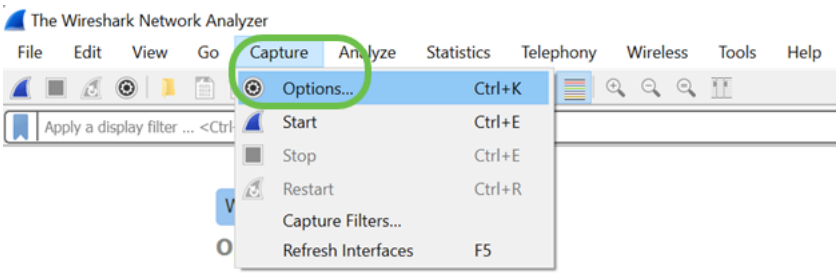
Passaggio 6

Poiché Wireshark è già stato scaricato, è possibile accedervi digitando **Wireshark** nella barra di ricerca di Microsoft Windows e selezionando l'applicazione quando è disponibile.



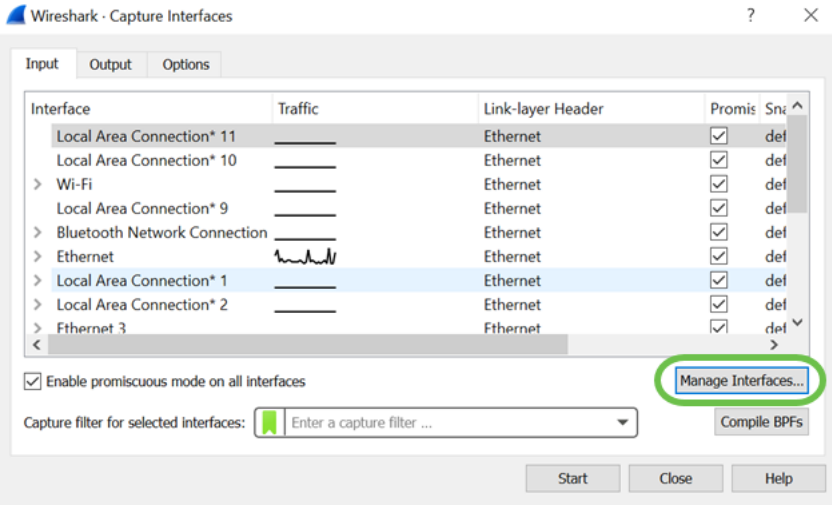
Passaggio 7

Passare a **Acquisizione > Opzioni...**



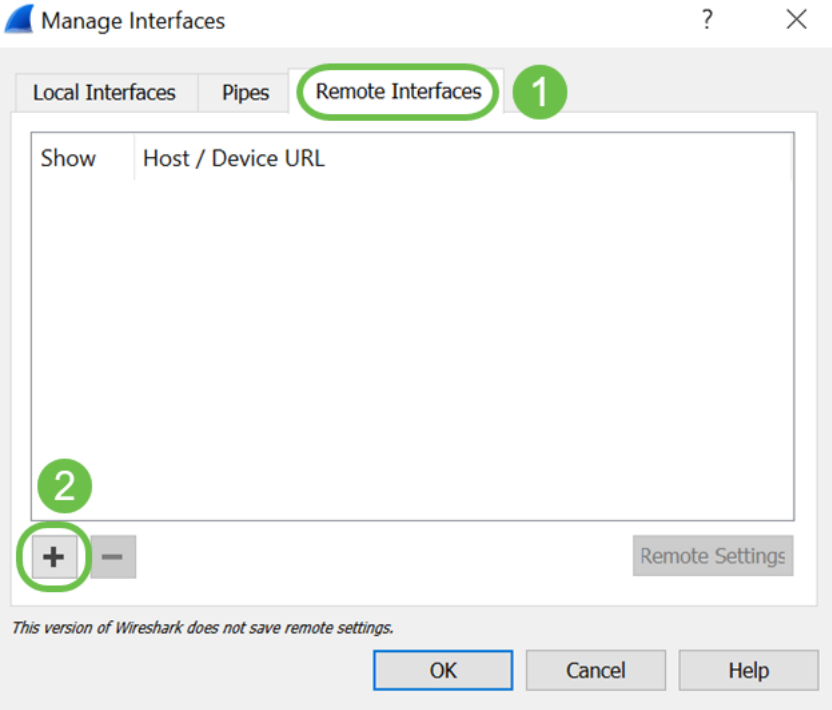
Passaggio 8

Nella nuova finestra popup *Wireshark - Capture Interfaces*, fare clic su **Manage Interfaces**...



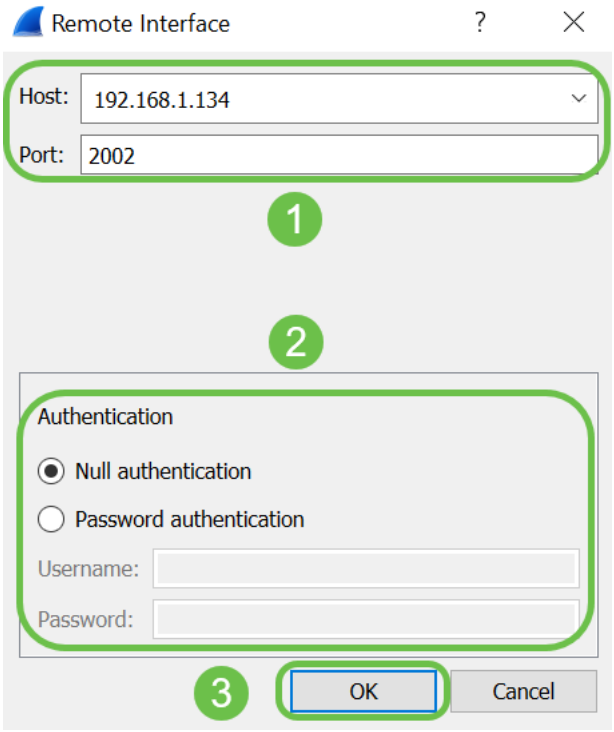
Passaggio 9

Nella nuova finestra popup *Gestisci interfacce*, passare a **Interfacce remote** e fare clic sull'**icona più** per aggiungere l'interfaccia.



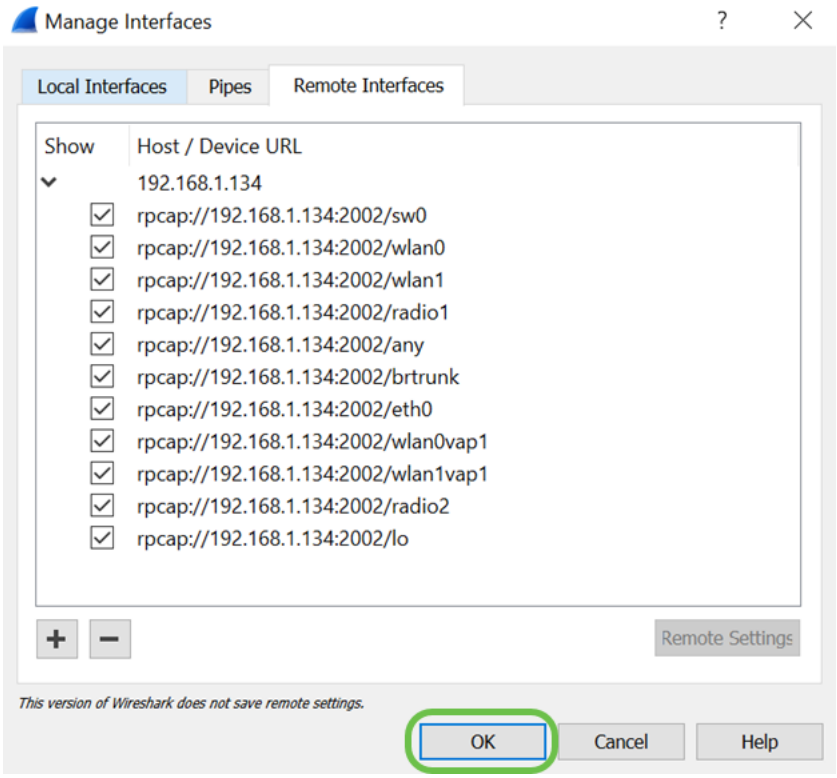
Passaggio 10

Nella finestra popup della nuova *interfaccia remota*, immettere il comando *Host:* Dettagli indirizzo IP (indirizzo IP del dispositivo WAP da cui è stata avviata l'acquisizione remota) e *Porta:* numero (configurato su WAP per l'acquisizione remota). In questo caso, l'indirizzo IP del dispositivo WAP è 192.168.1.134. È possibile selezionare l'opzione di *autenticazione Null* o *Autenticazione password* in base alle impostazioni specificate. Se si seleziona Autenticazione password, immettere il *Nome utente* e la *Password*. Fare clic su **OK**.



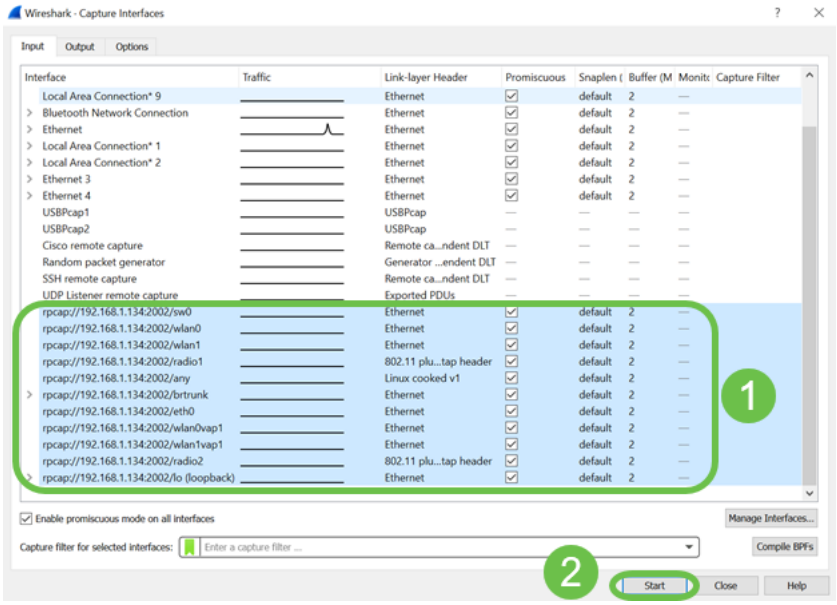
Passaggio 11

Nella scheda *Interfacce remote* è possibile visualizzare tutte le interfacce del dispositivo WAP remoto. È possibile deselezionare solo alcune di queste opzioni per ridurre il volume dei pacchetti acquisiti. Se si desidera visualizzare i pacchetti beacon, lasciare selezionate le interfacce radio. Fare clic su **OK**.



Passaggio 12

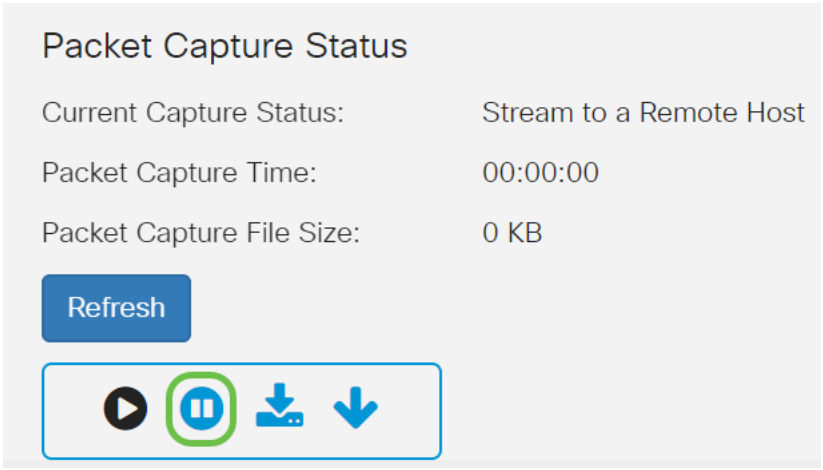
Le nuove interfacce verranno visualizzate nella finestra *Wireshark - Capture Interfaces*. **Selezionare** l'interfaccia che si desidera monitorare e fare clic su **Start** per visualizzare i pacchetti.



Se si verificano problemi durante il tentativo di visualizzare i pacchetti, significa che il servizio *Remote Packet Capture Protocol* non funziona nel sistema. Il servizio Remote Packet Capture Protocol deve essere in esecuzione sulla piattaforma di destinazione prima che Wireshark possa connettersi a tale piattaforma. Per ulteriori informazioni, fare clic sul collegamento *Interfacce di acquisizione remota* tramite Wireshark.

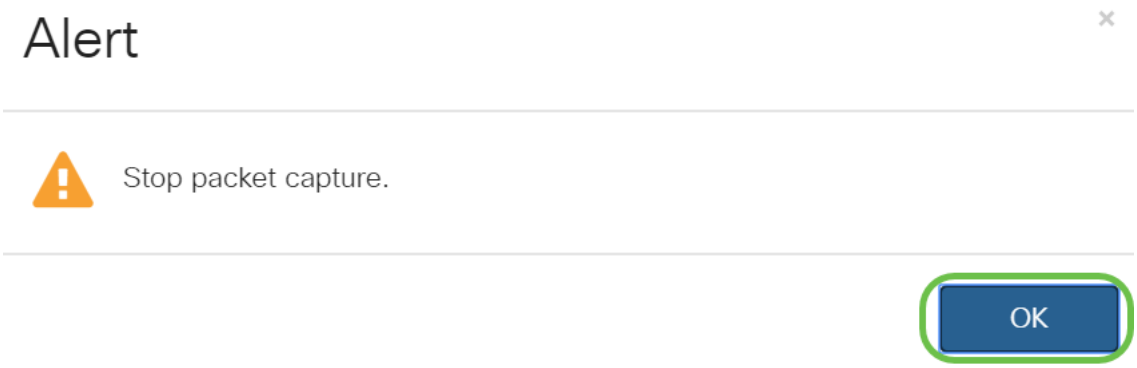
Passaggio 13

In WAP, fare clic sull'**icona Interrompi acquisizione** per interrompere il processo di acquisizione.



Passaggio 14

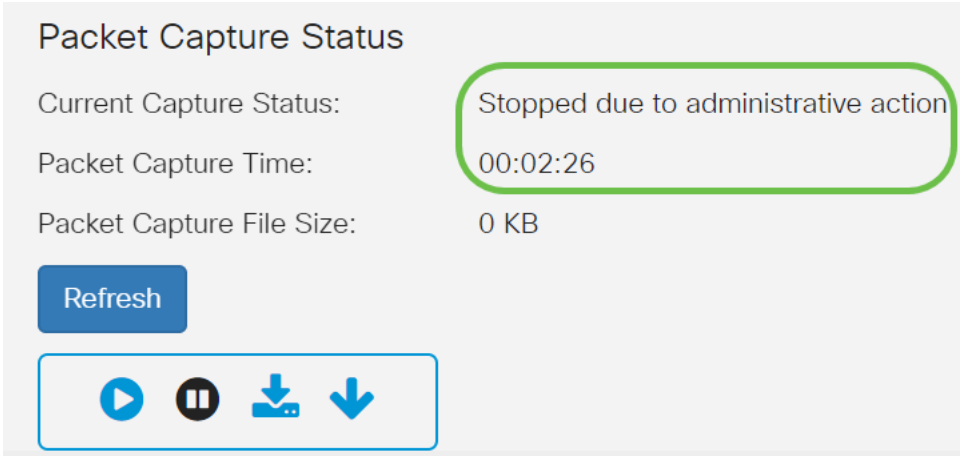
Verrà visualizzata una finestra popup di *avviso*. Fare clic su **OK** per interrompere la cattura remota.



È inoltre possibile interrompere la cattura del pacchetto facendo clic sul pulsante **Stop** nell'applicazione Wireshark.

Passaggio 15

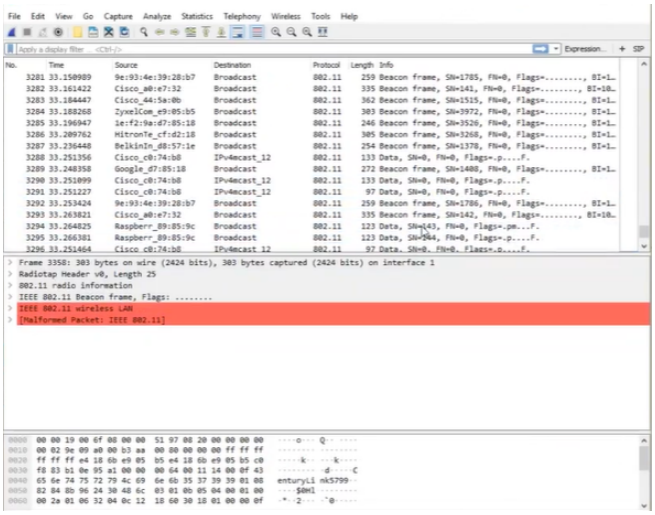
A questo punto, *lo Stato acquisizione corrente* verrà visualizzato come *Arrestato a causa di un'azione amministrativa*, mentre il *Tempo di acquisizione pacchetto* verrà visualizzato per indicare la durata totale dell'acquisizione.



Le *dimensioni del file di acquisizione pacchetto* saranno *0 KB*. Inoltre, le opzioni di download dei file non funzioneranno in questo scenario.

Passaggio 16

Su Wireshark è possibile visualizzare la cattura del pacchetto.



Conclusioni

Ora avete le abilità per far passare un pacchetto direttamente a Wireshark e potete iniziare ad analizzarlo. Non sai dove andare da qui? Ci sono moltissimi video e articoli disponibili online da esplorare. Ciò che cercate dipende dalle esigenze della vostra situazione. Ce l'avete!