Configuration of Packet Capture on WAP121 and WAP321 Access Point

Objective

Packet Capture is a feature of a network device that enables you to capture and store packets that are transmitted and received by the device. The captured packets can be analyzed by a network protocol analyzer to troubleshoot or optimize performance. The captured packet file can be downloaded via HTTP/HTTPS or TFTP. It can be shared and then further analyzed to understand the packet flow in the network.

The objective of this document is to explain how to configure packet capture and download the packet capture file on WAP121 and WAP321 Access Points (AP).

Applicable Devices

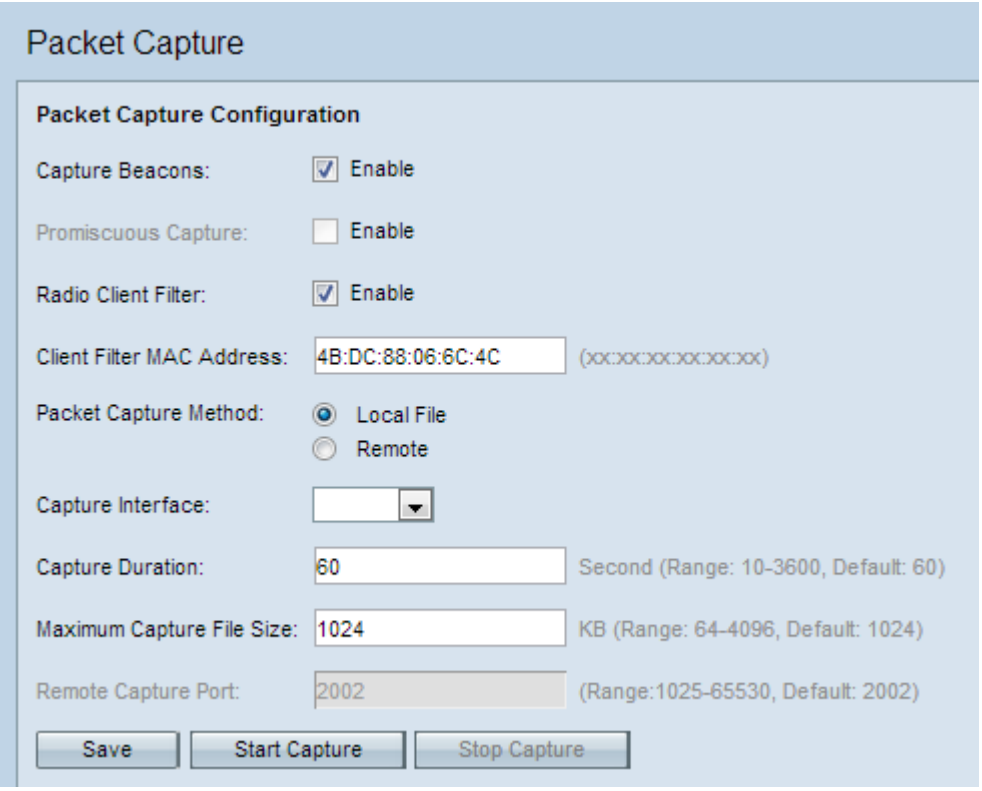
- WAP121
- WAP321

Software Version

- 1.0.3.4 (WAP121 and WAP321)

Configuration of Packet Capture

Step 1. Log in to the web configuration utility and choose **Administration > Packet Capture** . The *Packet Capture* page opens:



Step 2. Check the **Enable** check box of the *Capture Beacons* field. Beacon frames are transmitted periodically to announce the presence of a Wireless LAN network.

Step 3. Check one of the following check boxes beside one of the following fields to choose a particular capture option:

- Promiscuous Capture — This makes the wireless network interface card (NIC) capture all packets regardless whether it is meant for this device or not.

- Radio Client Filter — This makes the wireless NIC capture packets only from WLAN clients.

Note: Both Promiscuous Capture and Radio Client Filter cannot be enabled simultaneously.

Note: Skip Step 4 if you have chosen Promiscuous Capture mode.

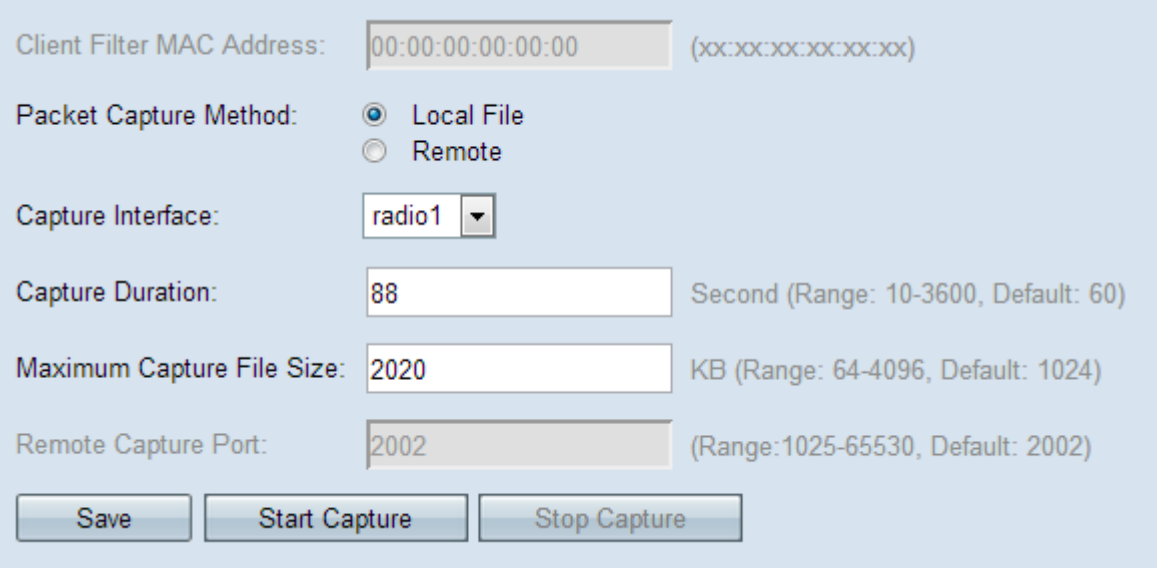
Step 4. If Radio Client Filter is enabled, enter the MAC address of the client filter in the *Client Filter MAC Address* field.

Step 5. Click one of the Packet Capture Method radio buttons.

- Local File — Stores the captured packets as a file on the AP device. The file is in pcap format and the AP can transfer file to a TFTP server. Skip Step 7 if you choose this.

- Remote — Redirects the captured packets in real time to an external computer that runs the network protocol analyzer tools. Skip Step 6 if you choose this.

Step 6. If Local File is chosen, configure these fields.



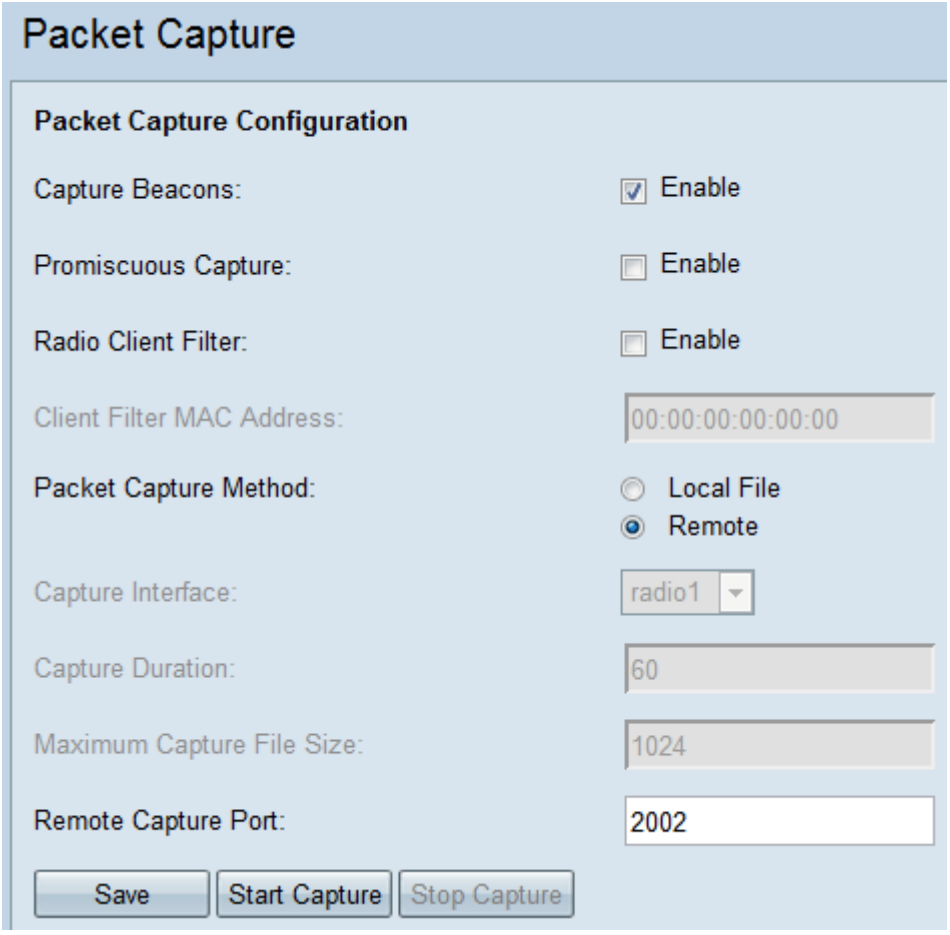
- Capture Interface — Choose the interface that the packets are to be captured from in the Capture Interface drop-down list. The drop-down list has the interfaces brtrunk, radio1, etho, and vap0.

- Capture Duration — Enter the capture duration in seconds. This can range from 10 to 3600 seconds.

- Maximum Capture File size — Enter the maximum capture file size (KB) ranges from 64 to 4096 KB.

Step 7. If Remote packet capture method is chosen, Enter the port number ranges from 1 to

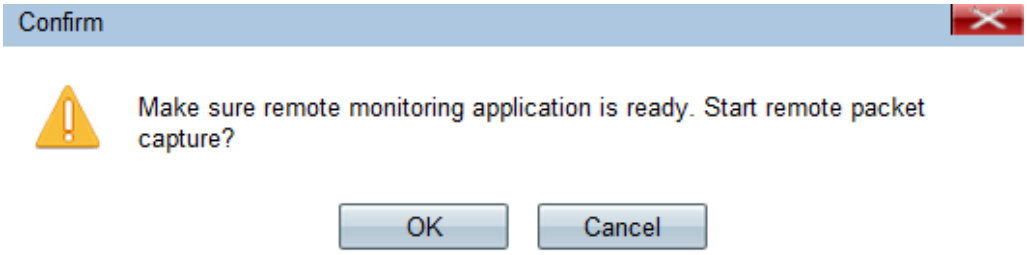
65530 in the Remote Capture Port field. The default is 2002.



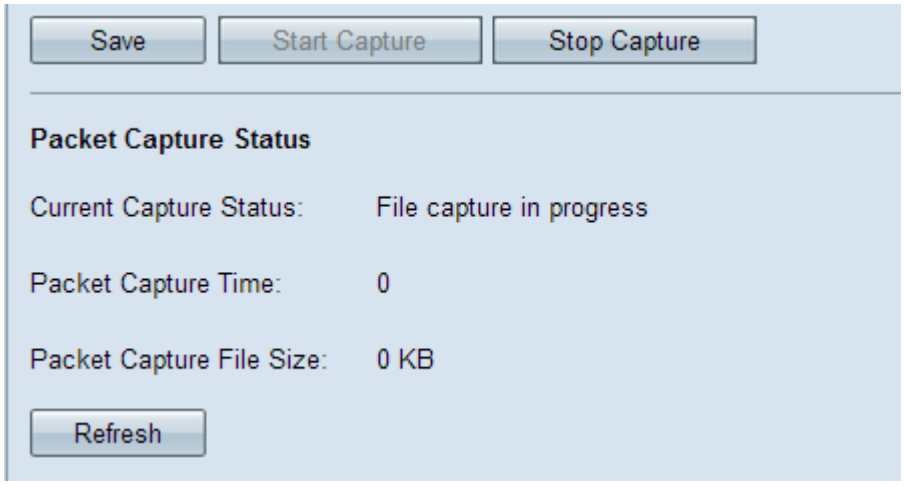
Step 8. Click **Save** to save the settings.

Step 9. Click **Start Capture** to start the packet capture process.

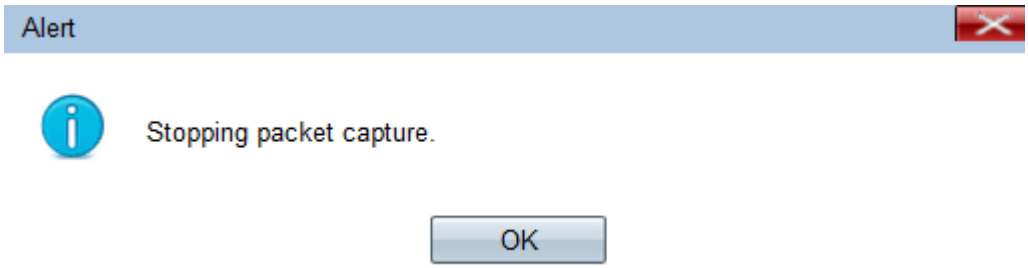
Step 10. The alert message appears. Click **OK** to continue the packet capture process.



Step 11. Click **Stop Capture** to stop the packet capture process. The Packet Capture Status area shows that capture is in progress.

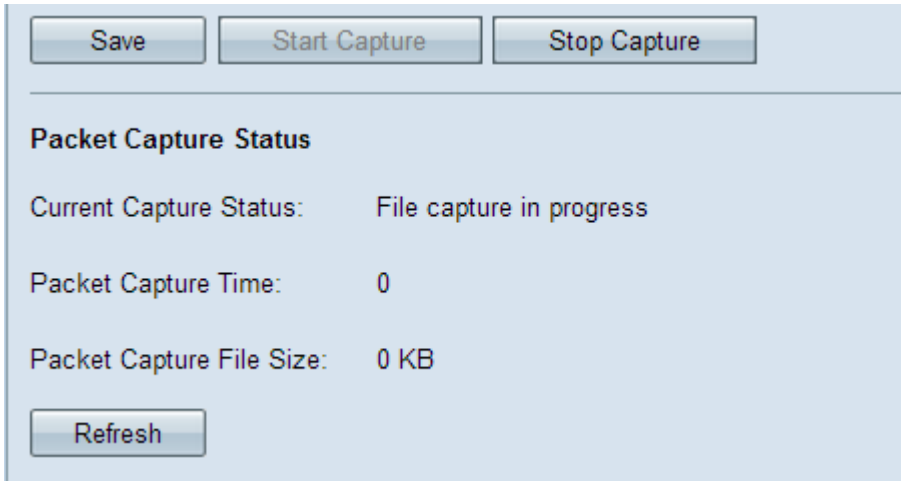


Step 12. The alert message appears. Click **OK** to stop the packet capture process.



Packet Capture Status

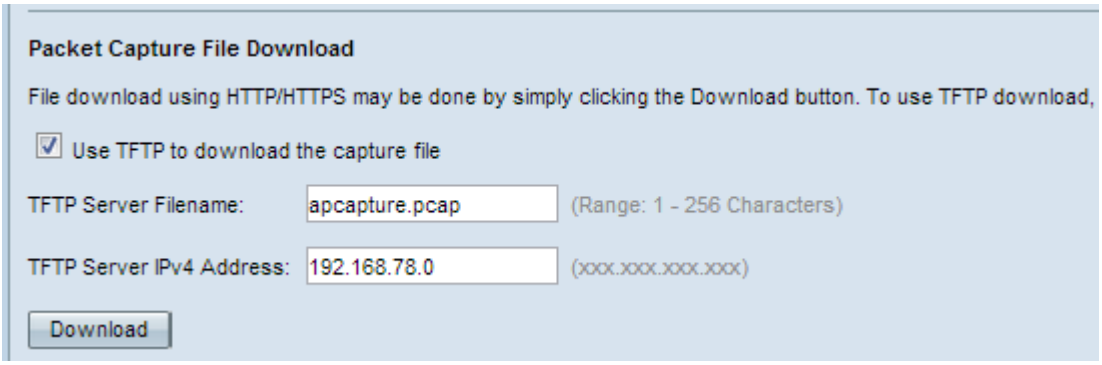
Step 1. The Packet Capture Status area contains the following information. Click **Refresh** to get the recent status.



- Current Capture Status — Displays the current packet capture status.
- Packet Capture Time — Displays the time for which the packets are captured.
- Packet Capture File Size — Displays the size of the packet captured file.

Packet Capture File Download

Step 1. (Optional) If the captured file has to be downloaded through a TFTP server, check the **Use TFTP to download the capture file** check box. The TFTP Server Filename field and the TFTP Server IPv4 Address fields activate.

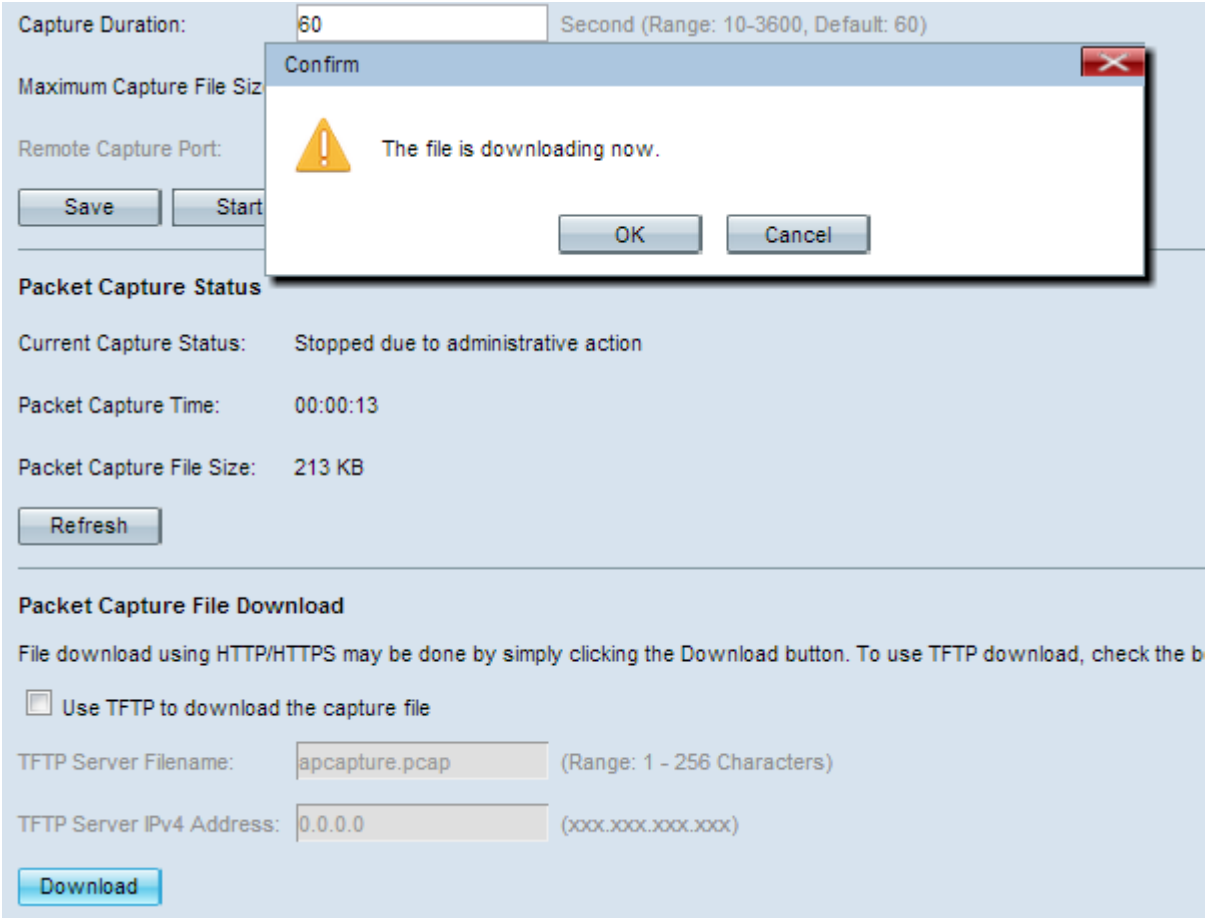


Timesaver: If you do not check the check box in Step 1, skip to Step 4.

Step 2. Enter the file name in pcap format in the TFTP Server Filename field.

Step 3. Enter the IPv4 address of the TFTP server in the TFTP Server IPv4 Address field.

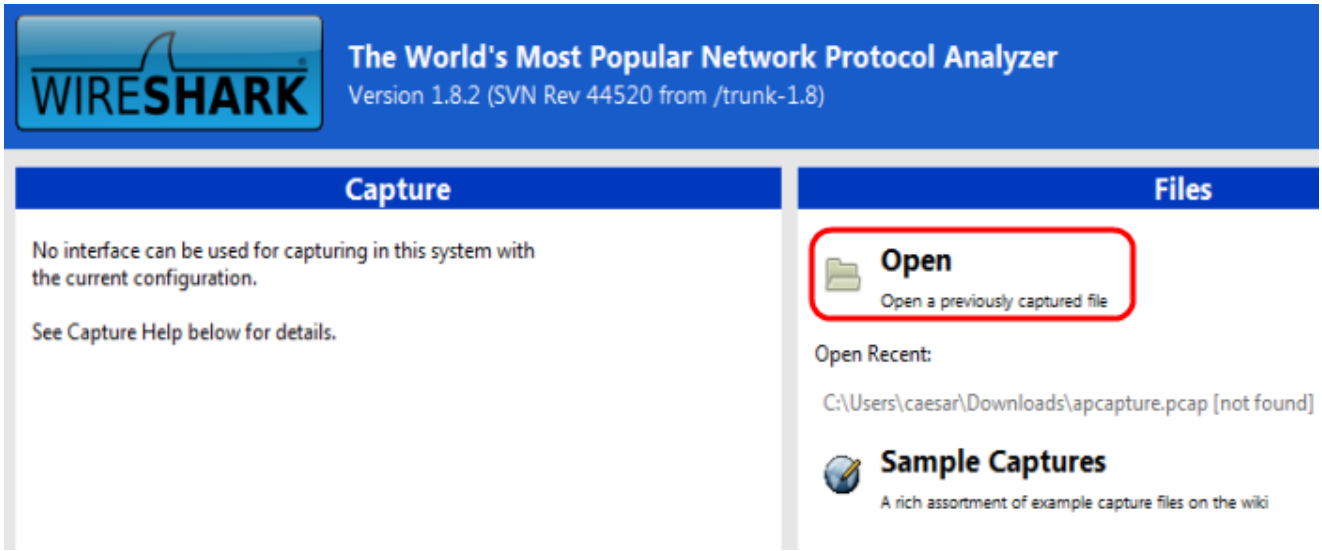
Step 4. Click **Download**. If you did not choose TFTP the file is downloaded with HTTP/HTTPS, a window appears to inform you that the download is in process. Click **OK**.



Note: You can use the Wireshark software, which is open source, to interpret and understand the information obtained from packet capture.

View Captured Packet in Wireshark

Step 1. Launch the Wireshark Software.



Step 2. Click **Open** in the File section to browse and select capture file from your PC.

Step 3. Locate file on PC.

Step 4. Open to view captured file.