Evaluating Wireless Packet Capture Methods

There are many different ways to capture packets for wireless LAN analysis. Some methods are standalone, while others require multiple devices and resources. Each of these solutions has pros and cons, with no single solution being perfect in every situation.

Why does this matter? Because when it comes to WLAN packet capture, it can be difficult to know if you’re getting the right data. With wired packet capture it’s far easier to know if the capture is going well, but with WLAN you often won’t know. Ultimately, the quality of the analysis will depend upon the quality of the data being captured, so it pays to be aware of each method, and apply the right one in order to capture the data that you need.

Wireless packet capture generally falls into one of three categories:

- **Portable** — using a laptop directly in the area where packet capture is being conducted
- **Remote** — the capture takes place at a separate (often distant) location
- **Distributed** — the capture and analysis are both done remotely, somewhere across the network

Here are some pros and cons of the most popular wireless capture methods:

1. **(Portable) Direct-connected 802.11n/802.11ac USB adapters**
   - **Pros:** With this method it’s possible to attach multiple USB adapters to a single laptop, creating a self-contained, fully portable system that can capture multiple channels simultaneously. This approach is relatively inexpensive.
   - **Cons:** On the downside, this method is highly dependent on the USB adapters, so an 802.11n adapter cannot see 802.11ac traffic. This solution is limited to 2-stream 802.11ac at most. In addition, the WLAN packet capture needs to be done at the point of the problem. Also, WLAN adapters aren’t normally designed for packet capture and they’re becoming the dinosaurs of the industry.

2. **(Portable) AP direct-connected to analyzer**
   - **Pros:** You can direct-connect an AP to your analyzer, giving you up to 4-stream 802.11ac packet capture while providing the best reception possible in a capture device.
   - **Cons:** It can be very difficult to power the AP. This solution often lacks vendor support to put the AP into sniffer or promiscuous mode, and you can only capture one channel at a time.

3. **(Portable) MacBook/MacBook Air**
   - **Pros:** MacBooks have a built-in utility that puts the laptop into sniffer mode. It offers 3-stream 802.11 capabilities in a simple, very reliable package.
   - **Cons:** This is a single-channel solution, and it’s a ‘blind’ capture of packets, meaning that you cannot see the results live. Packets needs to be exported and viewed in an analyzer later.

4. **(Portable) MacBook with TCPDump and Omnipeek®**
   - **Pros:** This is a very portable way to capture packets and have real-time data analysis with the full 3-stream 802.11ac capabilities of the MacBook. It has limitations, but if you have already narrowed down the source of an issue, this method can be a very useful.
   - **Cons:** This is a single channel solution that can be difficult to configure. You also need to consider that bandwidth is limited to ~30 Mbps total capture.
5. (Remote) Remote Capture “Assistants”
   **PROS:** One of the biggest advantages is that you don’t need to be physically present. It also allows for multiple channels simultaneously, and the remote user is responsible for the capture.
   **CONS:** On the downside, you need supported adapters, and there’s no real-time feedback. The files still need to be moved in order to be analyzed, and this method isn’t always as user-friendly as others, depending on the implementation.

6. (Remote) 802.11n/802.11ac adapter attached to a network USB hub
   **PROS:** With this method, the you can be hundreds of feet or hundreds of miles away. Network USB hubs are relatively inexpensive, and you can capture multiple channels using multiple adapters.
   **CONS:** This technique requires a wired network connection, and offers a maximum of 2-stream 802.11ac. You should also be aware that network USB hubs are becoming harder to find in the market.

7. (Remote) General TCPDump
   **PROS:** This is a good solution that is very well supported, but it has only limited performance so is best used when other methods aren’t available.
   **CONS:** This is a single channel solution with low (~30 Mbps) performance. Wireless adapter support can prove challenging, and the packets need to be sent over the network.

8. (Remote) Remote Pcap
   **PROS:** Like other remote solutions, the fact that you don’t need to be on site is a plus. Multiple channels can be captured (if available), and it offers real-time feedback.
   **CONS:** You need to be aware that this solution is not well supported. It also relies on the network to transport captured packets, and has bandwidth limitations of ~100 Mbps (which is considerably higher than a TCPDump).

9. (Distributed) AP connected to WLAN capture appliance
   **PROS:** Using an AP in promiscuous mode gives you the highest throughput possible, offering solid performance for capture and analysis 24/7 in a single box.
   **CONS:** Some of the limitations of this solution include that it is rackable, but not portable. There is also significant cost involved in the appliance and the APs, and the network loses an AP if one is not specifically dedicated to sniffer mode.

10. (Distributed) Capture Engine with USB WLAN adapters
    **PROS:** This software-based solution also offers 24x7 WLAN analysis and troubleshooting. It also enables analysis of multiple channels.
    **CONS:** This solution is limited by the adapter capability, the hardware running the Capture Engine, and it offers moderate analysis ~1 Gbps.

11. (Distributed) Capture Engine using APs
    **PROS:** Like APs connected to a capture appliance, this software-based solution using an AP(s) gives 24x7 WLAN analysis and troubleshooting of multiple channels.
    **CONS:** This is a software-only solution that requires an access point to be put into sniffer mode. It also delivers only moderate analysis at up to ~1 Gbps.