White Paper: The Case for Portable Wi-Fi Analysis

In place of the table of contents, please have this brief lead in italicized at the top... This paper covers the essential aspects of portable Wi-Fi analysis: when it is needed, which types of activities can be done and the limitations that come with portable analysis.

INTRODUCTION

Think of your ideal wireless network. Keep it realistic, but also keep it optimistic. Keep what is truly necessary and avoid fantasies.

To begin with, let's define "ideal". "Ideal" could mean "ideal for the user" or "ideal for the admin". A user wants seamless connectivity; wake a device and it's on. Consistent access is also a must. Speeds should be at least 5 Mbps; fast enough to run typical enterprise applications. Essentially, these are the things that you probably want when you're using Wi-Fi at home.

Now, let's define an "ideal" wireless network from an admin's perspective. Admins like equipment that have defined capabilities. For example, if a vendor says that an AP can support up to fifty users, then it should support fifty users. Admins also want installations that are simple and repeatable. The network should be testable — throughput measurements should match real world performance. Once the network is set up, management should be managerial: centralized, with only rare excursions out of the NOC to fix infrastructure problems. Basically, admins like wireless networks that can be managed like wired networks.

In some ways, users and admins are looking for the same things: simple, predictable Wi-Fi. Unfortunately, the technology of wireless often causes the needs of wireless users and the desires of wireless admins to diverge. The most prominent area in which they diverge is troubleshooting & analysis. Wi-Fi uses radio frequency (RF) as its physical layer, and RF can vary depending on location; that makes troubleshooting & analysis something that needs to be done at the location of the problem. Admins may want troubleshooting to be centralized, but to give users good Wi-Fi, troubleshooting needs to be portable.

In Wi-Fi's defense, it is actually not that much different from Ethernet. In both Wi-Fi and Ethernet, disruptions at the physical layer of the network make consistent access impossible. What makes Wi-Fi tough is the fact that the Wi-Fi physical layer is air. Air changes when doors close, people move or even when someone takes a smartphone that is in their palm and puts it to their ear. It's like managing a wired network where data cables can become loose when people stand up at their desks. To troubleshoot a network like that, you'd need someone at the users' desks to ensure that cables are plugged in. For the wireless world, the equivalent is having a troubleshooting & analysis tool that you can carry to users' desks.

Portable network analysis is a new thing to a lot of folks, even admins with years of Wi-Fi experience. So, with this paper, we will attempt to cover essential aspects of portable Wi-Fi analysis: when it is needed, which types of activities can be done and limitations of portable analysis. Along the way, this paper will include some tips on using Netscout's best-in-class portable analyzer, AirMagnet WiFi Analyzer.

NETSCOUT

WHEN TO GO PORTABLE

Portable network analysis is an essential part of a wireless LAN troubleshooting and analysis toolkit, but it should be used judiciously. Portable analysis can be difficult and/or time consuming for the unprepared. Even relatively intuitive portable analyzers like AirMagnet WiFi Analyzer require a skilled professional, often one who has received formal training to understand all the nuances and features available. And being portable means have the wherewithal to get a laptop running AirMagnet WiFi Analyzer to the location that needs troubleshooting and/or analysis.

In general, portable analysis should be one of the last steps taken when tackling Wi-Fi problems. Step one should be verifying the settings configured on the user's device(s). Step two should be ensuring that the wireless LAN infrastructure has been set up according to sound RF principles. Once those two steps have been taken, step three should be to use a portable wireless analyzer.

Verifying that a user's device has proper Wi-Fi settings configured is often a simple task, but there are tips that some support professionals may find useful. In crowded Wi-Fi environments, removing/forgetting an existing Wi-Fi configuration and re-configuring the SSID manually (by typing the SSID rather than clicking or tapping on it) can make a Wi-Fi connection more consistent. Manual SSID configuration tricks the user’s device in to thinking that the SSID is hidden. When a consumer Wi-Fi device thinks that an SSID is hidden, the device will send a series of Probe Request messages in order to maintain the connection. Probe Request messages often allow consumer devices to stay aware of nearby Wi-Fi APs, even if the area is congested with neighboring Wi-Fi. Another device-based tip that may aid Wi-Fi troubleshooting and analysis is to utilize the Discovery feature (on users' devices. Discovery funtionality shows the current channel and BSSID (AP's wireless MAC address) of a device, thus removing some of the uncertainty that can be associated with troubleshooting Wi-Fi connectivity within a large infrastructure.

If users remain frustrated after device settings have been verified, then the wireless LAN infrastructure setup might need to be adjusted. Having a wireless LAN infrastructure designed and configured according to RF principles is the most reliable way to avoid the types of recurring problems that require portable Wi-Fi analysis. Good RF principles include configuring AP transmit power levels approximately equal to users' device transmit power levels (which are usually between 12 and 16 dBm for consumer devices like smartphones and tablets) and limiting the number of enabled APs so that each Wi-Fi channel shows no more than one AP covering any user's device. Additional infrastructure adjustments may be useful as well, but manually setting the APs’ transmit power and disabling excess APs is a great place to start.

Hopefully, once users' device settings have been verified and once infrastructure configurations have been adjusted, your Wi-Fi network will be ideal — or at least close enough to ideal. If it isn't, then it's time for portable Wi-Fi analysis. Also, in some cases, portable Wi-Fi analysis is a good idea even if users are getting good Wi-Fi. For example, you don't want to be satisfied that twenty users have good Wi-Fi if a space is designed to service eighty users. So, for both problem areas and areas that need proactive care, portable Wi-Fi analysis is helpful.

Ultimately, the decision to go portable should be governed by one question: am I missing something that I need to see? If Wi-Fi stinks near a shelf in a warehouse, then the shelf may be the problem. You need to see what's happening in the air near that shelf. If Wi-Fi goes bad when a university's lecture hall fills up, then students' devices may be affecting RF quality. You need to see what's happening in some of the locations where students are sitting.

Thus far, we've given you some broad strokes in identifying when portable analysis can be helpful. We also have some specific examples for you. What follows is a list of situations and activities that we have found portable analyzers useful for.

CAPTURING WHAT THE USER'S DEVICE SEES

Wireless captures can often be misleading because the capturing device may be seeing different Wi-Fi traffic than what users' devices see. If a wireless troubleshooting & analysis tool captures frames that fail to reach a user's device, that can lead to misguided analysis. If the reverse happens, and a troubleshooting & analysis tool misses capturing frames that are seen by a user's device, that can also lead to misguided analysis. But the reality is that a Wi-Fi capture is never going to be perfect. The changing nature of radio frequency and the differences between different devices' radios and antennas are always going to result in discrepancies between what is captured and what a user's device actually sees. So we just want to minimize those discrepancies. And a portable analysis tool is the best way to minimize discrepancies between capture and use.

Distributed wireless analysis systems, while increasingly popular, have a major limitation when it comes to capturing an accurate depiction of what a user's device is seeing. The sensors used in distributed capture systems have higher gain antennas than typical users' devices like smartphones, tablets and laptops. And there is a reason why sensors have high gain antennas: higher gain antennas reduce the number of frames that show as corrupt. Seeing low numbers of corrupt frames may give admins a warm and fuzzy feeling, but there is a price for the reduction in captured frame corruption: high gain antennas see too much stuff. Many of the frames captured by sensor antennas may not be received at all by actual users' devices (which have lower gain antennas). The end result is that a problem seen in a frame (packet) trace from a distributed sensor may not be a problem for the actual users' device, and vice versa.

AirMagnet WiFi Analyzer offers extra protection against capturing deceptive frame traces. Not only can AirMagnet WiFi Analyzer be run on a portable laptop that can be moved close to the location of the user's problem device, but AirMagnet WiFi Analyzer can be configured to only save and record frames that are captured above a set signal level. That way if, for example, a user's smartphone is equipped with a very low gain antenna (in fact, most modern smartphone antennas have a gain of less than 1 dBi), the slightly higher antenna gain of a AirMagnet WiFi Analyzer capture adapter can be accounted for.

NETSCOUT

FIXING THE MISSED FRAME PROBLEM

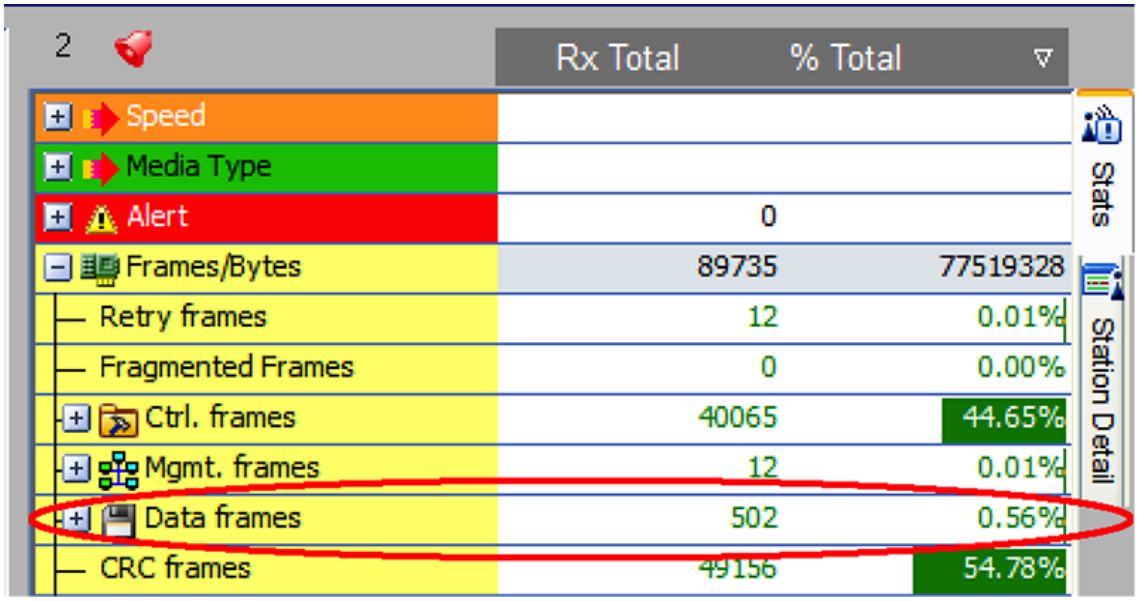
This next part is hard to admit. We love Wi-Fi analysis. We think that it makes Wi-Fi better for users, and at the end of the day that's what networking is all about. The problem is that Wi-Fi analyzers miss a lot of stuff. This isn't wired networking, where the physical properties of a switch port can be mirrored onto another port for capture and analysis. Mirroring the physical properties of RF is just plain impossible, and it leads to missed frames.

Compounding the missed frame problem is the fact that 802.11n and 802.11ac devices may use multiple-input, multiple-output (MIMO) technology. (Smartphones don't use MIMO, but many tablets, laptops and other larger Wi-FI devices do.) MIMO has been great for powering modern WiFi's improvements in speed and range. But MIMO also sometimes make it so that transmitted frames don’t get captured. It's just another physical variable that can make RF properties different between the analysis tool and the actual device.

Because of the inherent nature of RF, the missed frame problem cannot be completely eliminated. Both distributed and portable Wi-Fi analyzers are affected by it. But portable analyzers have the ability to minimize the missed frame problem, while distributed analyzers often do not.

Minimizing the missed frame problem involves two solutions: capturing nearby users' devices and adjusting capture antenna orientation. Both distributed and portable analyzers allow capture radios to be placed close to the user's device. For example, at least one large retail chain places distributed analysis sensors underneath the counters where employees typically use their Wi-Fi based point-of-sale devices. The limitation with sensors is that they cannot be re-orinented. Portable network analyzers can be tilted or turned. In many cases, tilting or turning the capture adapter on a portable Wi-Fi analyzer is enough to reliably capture MIMO-based frames.

If you're using AirMagnet WiFi Analyzer, you can use the Infrastructure or Channel screens to verify that missed frames are not a major problem. If you see a significant number of Control frames without the presence of at least 30% data frames (easily viewed under the "Frames" tree on either screen), then that likely means that the AirMagnet capture adapter is missing frames due to MIMO. (The use of wider channels, which includes 40 MHz 802.11n channels and 40 MHz or 80 MHz 802.11ac channels, may also cause some Wi-Fi capture adapters to miss frames.)



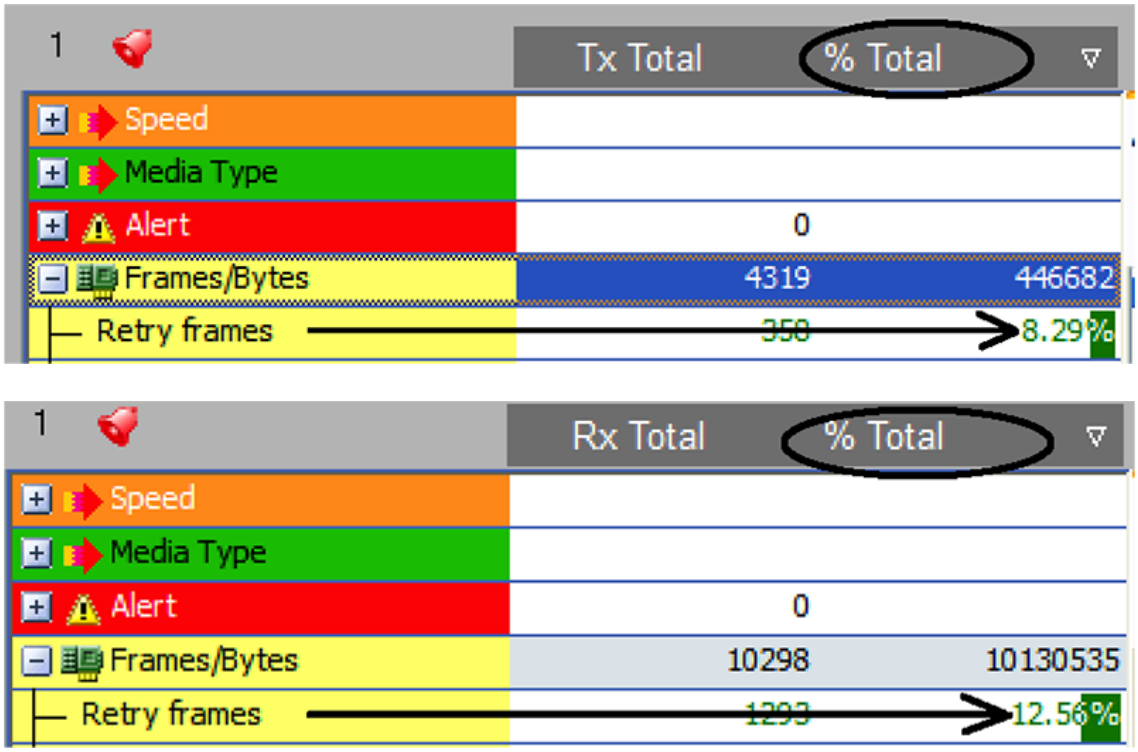
Moving the capture adapter, turning the capture adapter on its side or making other adjustments to the capture adapter's orientation often results in MIMO data that was once missing showing up in portable analyzer software.

The missing frame problem can also sometimes be solved by changing capture adapters. When a portable analysis tool like AirMagnet WiFi Analyzer is used, swapping capture adapters is often a simple process. A USB adapter can be exchanged for an ExpressCard adapter, or even a different model of USB adapter. When static sensors are used for wireless capture, a swapping of capture radio and antenna is usually impossible.

NETSCOUT

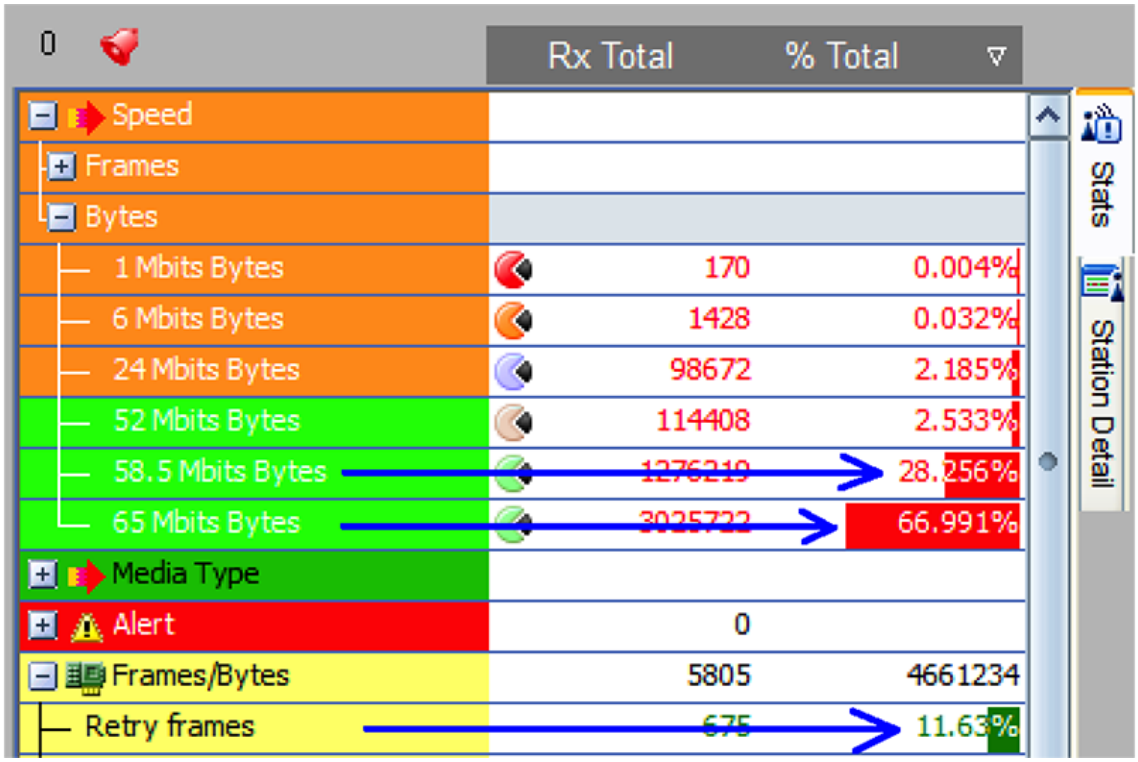
IDENTIFYING THE BEST CHANNEL

While the most problematic of Wi-Fi deployments may require new APs, different antennas or changes to AP installation locations, most enterprise Wi-Fi deployments can be adequately improved simply by optimizing existing APs' RF settings. Optimization of RF settings involves three tasks: disabling excess AP radios, configuring AP transmit power so that it approximately matches users devices' transmit power and choosing the best channel. Discovery (a.k.a. Scanner) applications are best for identifying which AP radios should be disabled, and any Wi-Fi analyzer - distributed or portable - can be used to figure out which transmit power setting is best.



Channel selection is the one optimization activity that requires a portable Wi-Fi analyzer. Enterprise Wi-Fi networks have protocols that are designed to optimize RF settings automatically, but those protocols fail for the same reason that portable analyzers succeed: location. Automatic RF configuration protocols glean data captured by APs, which are static devices. To know the best channel a portable device must capture from the locations where users need to connect. Capturing from users' locations results in more accurate information being used when choosing RF settings.

There are a number of metrics that can be used to determine which channel is best for an AP, but two stand out: retry % and data rates. When APs and users' devices use high data rates and show low retry percentages, then that means that the channel is being used efficiently. Those two statistics, along with the number of existing neighbor APs and stations on the channel and the amount of Management traffic on the channel, are relevant indicators of which channel is likely to work best for users' needs.



The most important thing to remember about identifying the best AP channel setting is that analysis should be done at the location where users connect, not at the location where APs are mounted. While it is less than ideal to have a channel be congested nearby an AP, it is far worse to have a channel be congested nearby a user's device. User's devices can always choose a different AP to associate to if the RF around a single AP is poor. If, however, the Wi-Fi is failing at a user's desk, cubicle or office, then there may be no recourse. Either the user will have to move to a new location or the user will get bad Wi-Fi. Therefore, when choosing the best channel for installed APs, always analyze the RF environment at the location where users are expecting to use the wireless LAN.

OVERLOOKED, UNDERVALUED

In many cases, the last thing a wireless administrator wants to do is go portable. That is understandable. Portable Wi-Fi analysis takes up an admin's most precious resource: time. But portable analysis is an essential weapon in a wireless professional's arsenal. The ability to go to the location of users, adjust the capture orientation if frames go missing and produce recommendations that are tailored to solving the problems of real world environments and devices is something that there is just no substitute for.