Step-by-Step: Handling RF Interference Challenges

TABLE OF CONTENTS

Introduction

Imagine a lecture hall that can hold four hundred students. Then imagine that the lecture hall has been tested for 5 Gbps aggregate throughput. Even at two and a half devices per student, that should be more than enough. Back-of-the-napkin math says that's at least 5 Mbps per device.

Now imagine that the students are in the lecture hall and the Wi-Fi stinks. “It’s slow,” they say. A peek at the controller shows under 100 Mbps for all the APs in that lecture hall, combined. How is that possible? How can 5 Gbps turn into 100 Mbps so quickly?

The answer is interference. Interference is the common cause of the all-too-common problem of tested wireless networks failing to perform to expectations.

Knowing that interference can cause Wi-Fi problems is the first step. That first step, however, is the easy part. Things get more difficult when things need to get more specific. Hard questions need to be answered: What is causing the interference? Can the interference be avoided? Will solving the present interference problem create new problems somewhere else? This paper aims to help in answering those questions.

AirMagnet WiFi Analyzer (“WiFi Analyzer”) and AirMagnet Spectrum XT (“Spectrum XT”) are outstanding tools for identifying the reason for interference problems. Spectrum XT is a spectrum analyzer. Spectrum analyzers capture radio frequency information, thus allowing all transmitters—both Wi-Fi and non-Wi-Fi—to be identified, analyzed and located. AirMagnet is a network analyzer. Network analyzers only capture 802.11/Wi-Fi transmissions, but network analyzers offer greater detail on the nature of those Wi-Fi transmissions. The detail available from a network analyzer—transmitting device, the intended receiver, the speed of the data and the Retry status (used to identify whether a wireless collision has occurred)—can be essential when interference is happening due to WiFi congestion.

Together, Spectrum XT and WiFi Analyzer can be used to identify interference sources in lecture halls—along with numerous other difficult Wi-Fi environments like healthcare, retail, manufacturing, etc.—and lead Wi-Fi professionals towards solutions to interference problems.

Here, then, is a step-by-step guide to using Spectrum XT and WiFi Analyzer to identify and resolve interference problems.

STEP ONE: Identify non-Wi-Fi interferers

It is best to start an analysis with non-Wi-Fi interferers because they can make good Wi-Fi impossible. If, for example, a hospital has a DECT phone system (DECT being a separate, non-Wi-Fi technology), it can kill Wi-Fi across the entire 2.4 GHz frequency band. (Modern versions of DECT use different frequencies than 2.4 GHz, but the problem could still exist around older DECT systems.) That is because DECT phones don't share. When a DECT phone needs to use wireless, it uses wireless. And many other wireless technologies—from Bluetooth to zigbee devices—work the same way: no sharing.

Wireless video camera

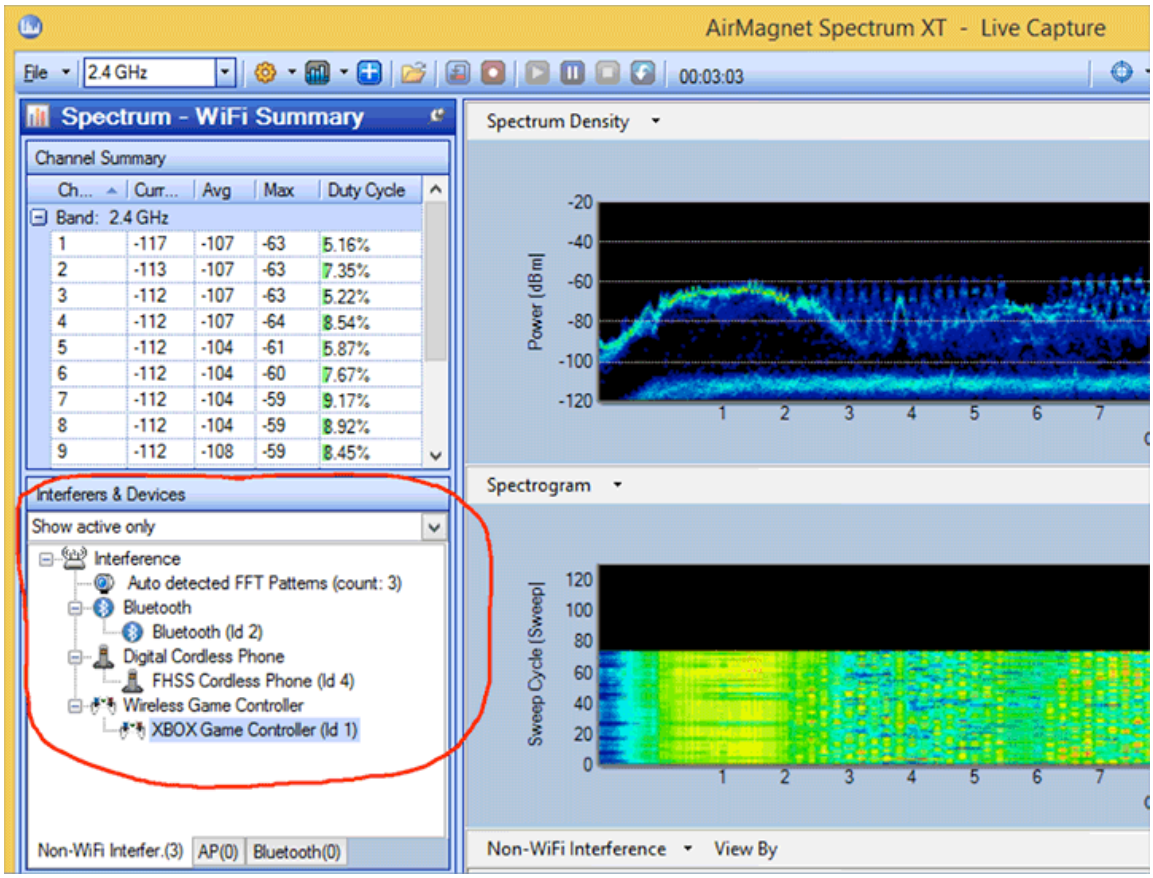
Microwave oven

Cordless phone

Wi-Fi interferers are almost always less harmful than non-Wi-Fi interferers because of 802.11 contention. 802.11 contention causes devices to listen and check the channel before transmitting. That checking and listening means that Wi-Fi devices tend to share channels tolerably with each other. In almost all cases, non-Wi-Fi devices do not share as well because they do not use contention.

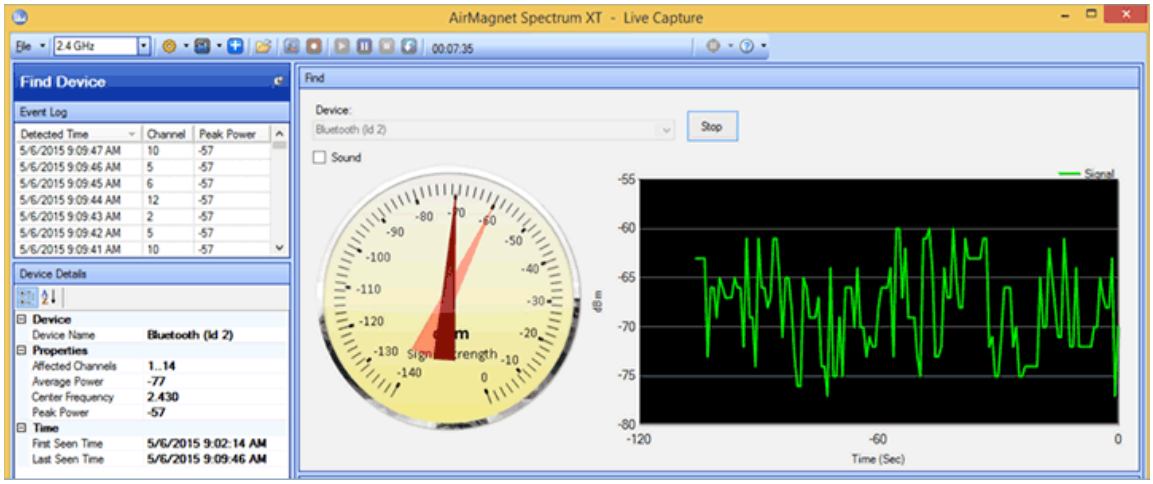
What, then, can be done about non-Wi-Fi interferers? The best bet is to identify them, locate them, try to determine their impact and then adjust accordingly. That is where Spectrum XT can help.

First: identify. The default start screen of Spectrum XT shows a list of interferers in the lower left area. More information (including which channels the interferers are using and how strong the received signal strength indicator (RSSI) from the interferer is), can be viewed by going to the bottom pane of Spectrum XT and choosing Spectrum Graphs -> Interferers. The same list of interferers will be displayed, but with additional detail.



STEP TWO: Locate non-Wi-Fi interferers

Once a non-Wi-Fi interferer has been identified, Spectrum XT can be used to find the interfering device's location. From the start screen of Spectrum XT, double-click any interferer that is shown in the lower left area, this will launch the Find tool. Once in the Find tool, click Start and a meter showing the received signal strength of the interference source will activate. With the Find tool started, the device running Spectrum XT can be carried around as a tracking device.



Once the device has been located, it can be dealt with according to the location's policies. Ideally an interfering device can be disabled, but that is not always possible. The 'Affected Channels' information in Spectrum XT can be used to make deployment adjustments for interferers in the environment that can't be turned off.

This is where the journey with Spectrum XT ends. Spectrum XT has lots of other useful graphs and features and there may be times when it can be valuable to explore those things. But this paper is focused on solving problems, and once we're confident that we understand our non-Wi-Fi interference, then the next step starts with using a tool that focuses on Wi-Fi issues: AirMagnet WiFi Analyzer.

STEP THREE: Identify Wi-Fi interferers

Once non-Wi-Fi interference sources have been handled, then nearby Wi-Fi devices should be analyzed. A network analyzer is necessary to properly analyze Wi-Fi activity, but WiFi Analyzer is more than just another network analyzer. AirMagnet has unique features like built in device filters, automatic channel adjustments and sortable statistics that can be viewed in a myriad of ways. In short, it'vs fair to say that AirMagnet WiFi Analyzer is the best network analyzer for analyzing interference from nearby Wi-Fi devices quickly.

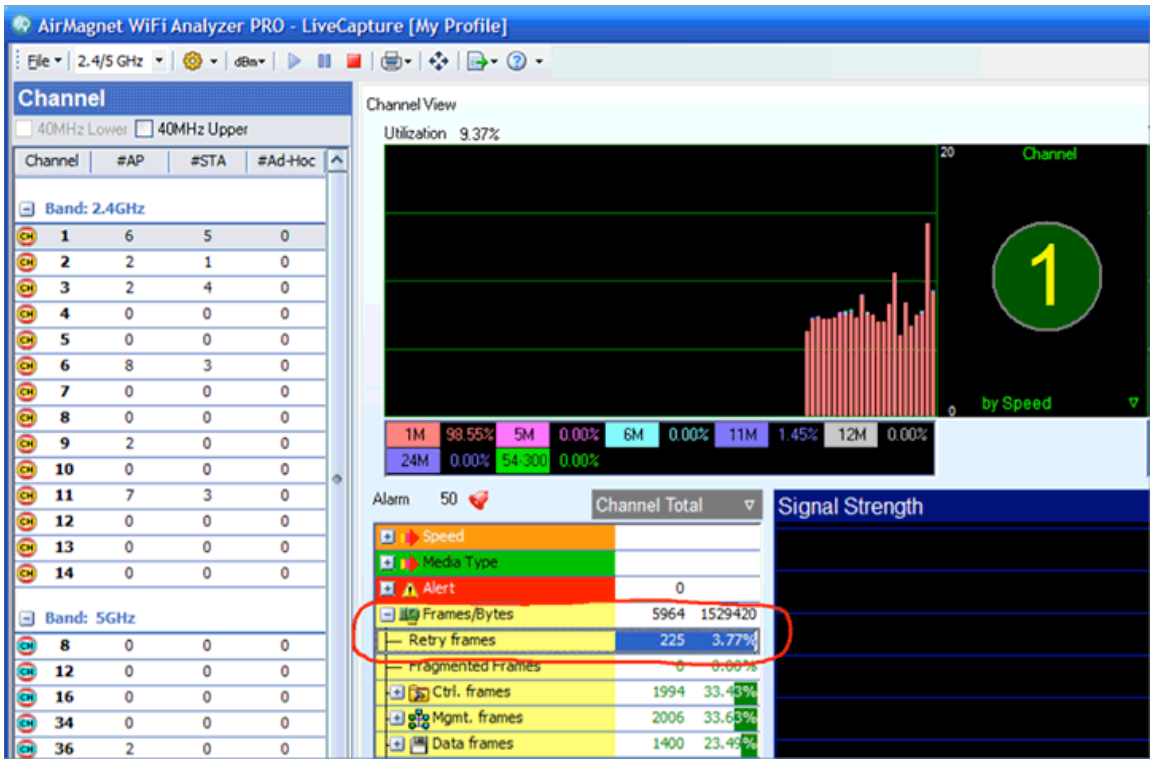
Before using WiFi Analyzer, one has to know what to look for. The overarching problem that results from Wi-Fi-based interference is wasted channel time. Wasted channel time can kill performance because channel time is the one resource that is limited. The number of packets on a wireless channel can increase: if there are fewer packet errors, then there can be more packets. The amount of data (bytes) on a channel can increase: if data rates improve, then more data can be accessed by each device. But one second is one second. If one second —or part of one second—is lost it cannot be recovered. When WiFi Analyzer is used to identify interference problems, the wasting of channel time should be the focus of the analysis.

There are several ways that time can be lost. Collisions cause the wireless channel to lose time because data that suffers a collision has to be sent again. That means that the initial transmission of data was a waste of time. Low speeds waste time as well. Data rates are measure by taking data and dividing it by time. If the data rate is lower, then that just means that it will take more time to send the same amount of data. Non-data traffic can also be a waste of time, if it is unnecessary.

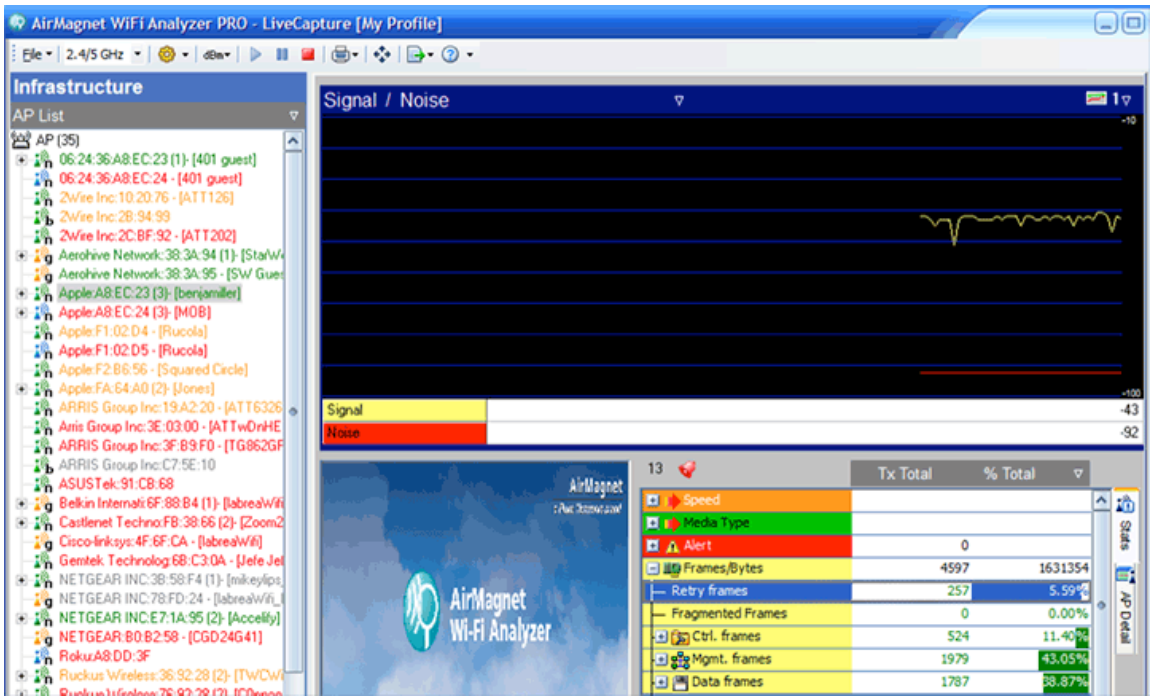
AirMagnet WiFi Analyzer can be used to identify all three of these big Wi-Fi time wasters.

First: Collisions. A collision is a failed Wi-Fi data transmission. The way a Wi-Fi collision can be identified in a network analyzer such as WiFi Analyzer is by looking for data marked as a Retry. The 802.11 standard (the standard that Wi-Fi is built on) specifies that if data is sent and an acknowledgment is not received (thus indicating that a collision happened), then the device or AP that sent the data must mark the retransmitted data as a Retry. This means that the percentage of Retry data is equal to the percentage of data transmissions that suffer collisions.

WiFi Analyzer not only identifies Retry data, but it allows Retry statistics to be gathered quickly and simply. To see the percentage of collisions over an entire channel, go to the CHANNEL screen of AirMagnet and open the little area in the middle of the screen labeled “Frames/Bytes”.

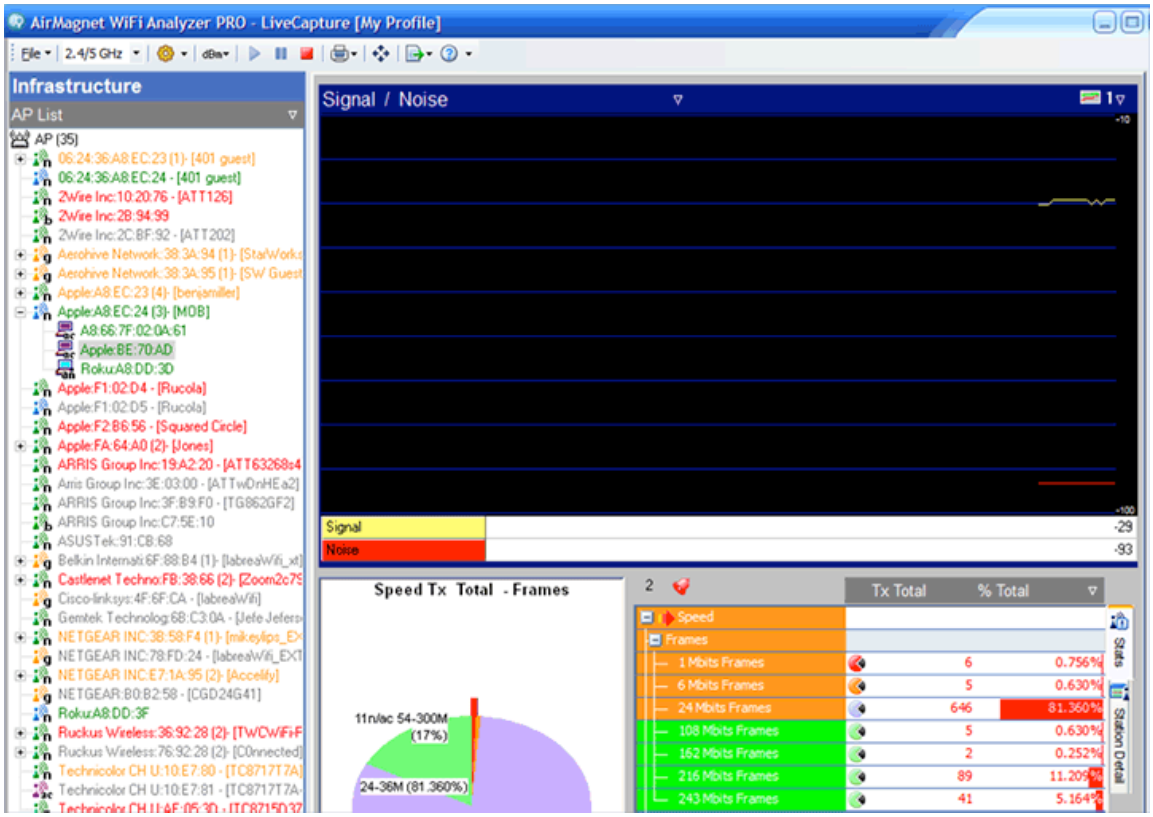


If the percentage of collisions relating to a single AP is required, that can be found in the INFRASTRUCTURE screen. After going to the Infrastructure screen, click on an AP on the left hand side and then open up “Frames” or “Frames/Bytes” in the lower right Stats window. Retry statistics for stations can be seen from that same Stats window. WiFi Analyzer allows the user to simply click on any station or AP listed on the left menu of the Infrastructure screen to immediately see statistics for that device.



In order to put collision statistics to good use, one has to know what is considered a high Retry percentage. A good place to start is at 8% for ordinary Wi-Fi and 20% for difficult Wi-Fi (high density of users, lots of mobility or significant amounts of non-Wi-Fi interference). Once Retry percentages climb above those numbers, it is usually a good idea to set aside some time and investigate why so many retransmissions are happening.

The second big time-waster is low data rates (often called “speeds”). Data rates can be seen in the same general areas that Retry percentages can be seen. The only difference is that in order to see which data rates are being used, the “Speed” tree needs to be expanded after clicking on an AP or station device in the Infrastructure screen.

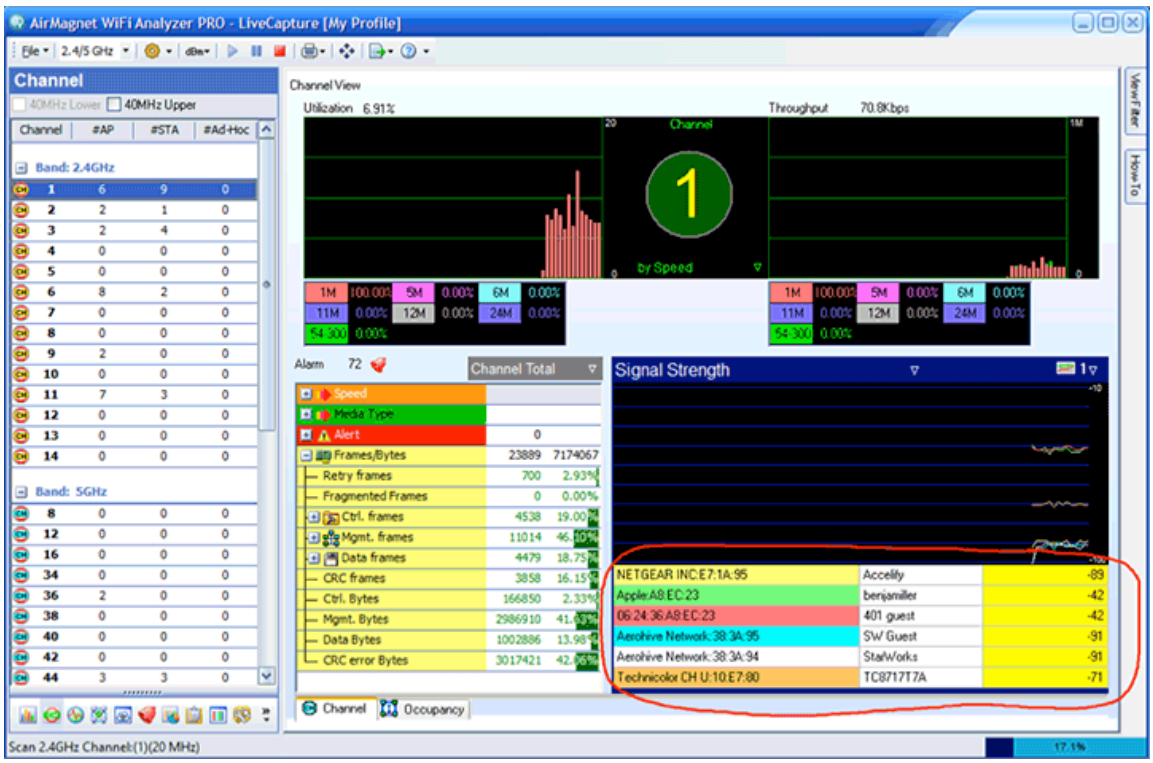


Determining whether low data rates are a fixable problem can take time and careful analysis. Devices and APs—especially 802.11n/ac devices and APs—routinely use data rates well below their stated maximum rates, even if interference is not significant. In other words, an office worker with an 802.11ac smartphone (maximum rate on a 40 MHz-wide channel: 200 Mbps) connected to an 802.11ac AP might routinely use data rates below 150 Mbps, even if the RF environment is great. 802.11ac (and, to a lesser extent, 802.11n) includes a lot of technologies that are rarely available during typical enterprise usage, even in areas where interference is minimal. For that reason, analyzing data rates to determine interference problems is a task that usually requires some experience.

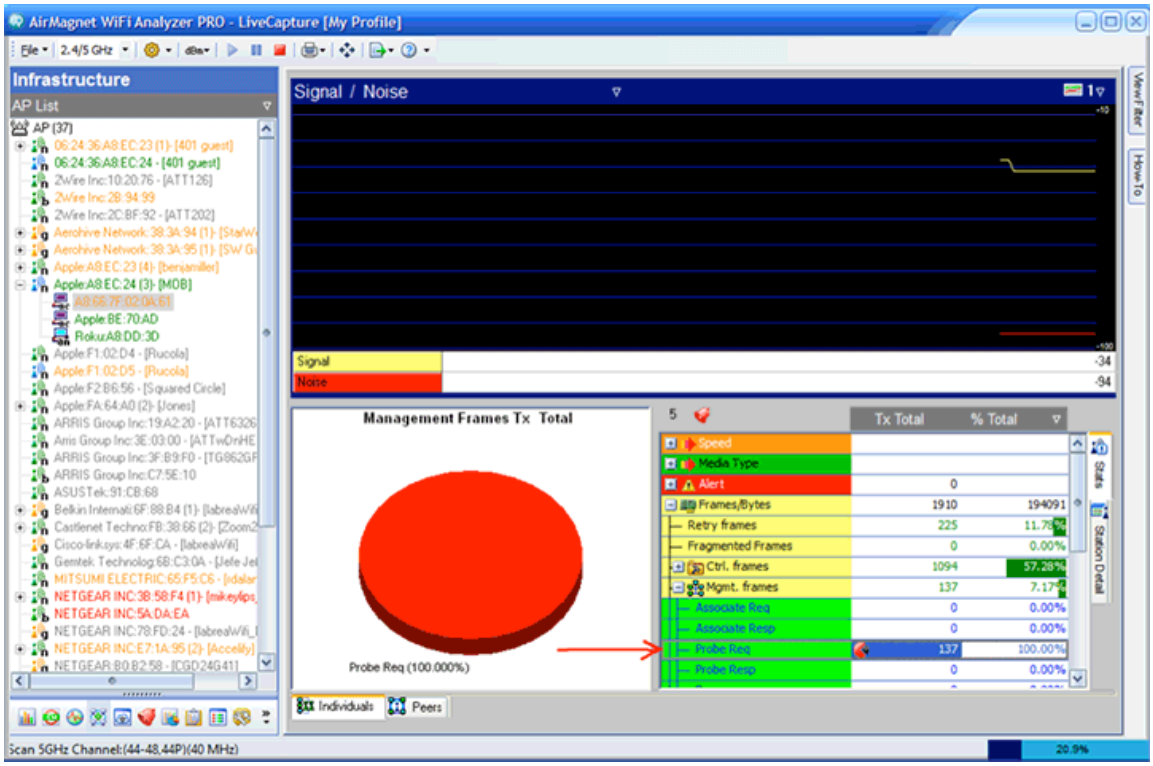
Thirdly (and lastly), non-data traffic can be the cause of a Wi-Fi channel losing time. There are lots of different types of non-data traffic, but most of them aren't worth going into because they're mandatory for 802.11 operation. APs and stations have to exchange a number of types of non-data traffic to be able to stay connected, detect collisions and all sorts of other necessities for a wireless network to function.

There are, however, two types of non-data traffic that can sometimes be reduced: Beacons and Probes. Beacons are used by APs to let stations know that a Wi-Fi network is available. The problem is that each Wi-Fi network needs its own set of Beacons. If there are two SSIDs (one guest and one internal), then Beacons will typically take up between 2% and 5% of the available time on a channel. But if the number of SSIDs expands to eight (possibly by having unique SSIDs for different vendors or different groups of internal users), then Beacons will typically take up between 8% and 20% of channel time. That's a big difference. And the problem gets exacerbated if more than one AP is covering the same channel. If a given enterprise tablet can see three APs on channel 11 and all three of those APs are using eight SSIDs, then that makes for 24 sets of Beacons on the channel. That's 24% to 60% of your channel time that is being used for Beacons instead of for Data.

The place to identify an excess of Beacon traffic is in the CHANNEL screen of WiFi Analyzer. Whenever a channel number is selected, the Channel screen shows how many APs and how many SSIDs in the lower right corner. Use that information to identify whether Beacons are using up channel time that would be better spent on data.



Probes are the other type of non-data frame that can waste channel time. Probing is initiated by stations, so that means that the INFRASTRUCTURE screen of WiFi Analyzer is the place to identify whether they are causing a problem. Simply click on a station on the left side of the Infrastructure screen, and then look at the Stats box in the lower right corner. In the Stats box, expand “Frames” or “Frames/Bytes” and then expand “Mgmt frames”. The number of Probe Request frames sent by the selected station will then be displayed. If the number of Probes keeps increasing, then that device might be taking channel time for Probes that could better be used for data. If there is a Probing problem, try making sure that the station in question has a stable Wi-Fi connection. Modern Wi-Fi devices (smartphones, tablets, laptops, etc.) do very little probing if their Wi-Fi connection has stable access to the Internet.



Handling Wi-Fi interferers has some similarity to handling non-Wi-Fi interferers, but there are also big differences. It is always best to start by identifying and locating the interferer. After a Wi-Fi interferer is identified and located, the problem can often be minimized or eliminated by adjusting the wireless LAN infrastructure. Disabling AP radios, adding new APs in different locations, manually configuring AP channel numbers and setting AP transmit power to levels similar to those of client devices are all activities that can improve an infrastructure of APs and controllers. In contrast, non-Wi-Fi interferers often need to be disabled or avoided in order to get the Wi-Fi working.

Following these steps using AirMagnet Spectrum XT and AirMagnet WiFi Analyzer creates an excellent chance of preventing Wi-Fi interference from becoming a lasting problem. Using a spectrum analyzer and a network analyzer can take some getting used to, but it sure beats blind exercises in trial-and-error. Once you get used to using these tools, you may even be surprised at how fast formerly difficult interference problems get identified and resolved.