

Five Common Wi-Fi Problems (With Simple Solutions!)

TABLE OF CONTENTS

- » Introduction
- » Wi-Fi Problem #1 Transmit power Mismatch
- » Wi-Fi Problem #2 Interfering Traffic
- » Wi-Fi Problem #3 Unconnected Guests
- » Wi-Fi Problem #4 Dead Zones
- » Wi-Fi Problem #5 Excessive Roaming

Every Wi-Fi deployment has problems. Sometimes vulnerabilities are worrisome and, on occasion, connecting can be a chore. But there is one Wi-Fi problem that is more prevalent than the rest: performance. No user like a slow or inconsistent wireless network, and no networking person likes to hear a user complain about a slow or inconsistent wireless network. Everybody knows this. But here's something a lot of people don't know: the solutions are often simple. (Not necessarily easy, but simple. Sometimes good Wi-Fi means bucking conventional wisdom or helping the people in charge unlearn outdated information. Those things definitely aren't easy.)



INTRODUCTION

Wi-Fi design guides and deployment best practices are plentiful, and those things can be helpful. The trouble is that if the Wi-Fi is already installed and running, then following design and deployment guides can lead to complicated solutions.

This paper looks at solutions a different way. The goal here is to keep solutions simple. Each and every problem listed in this paper has a simple solution. What's more, all of the problems are common, and all of the solutions are in WLAN infrastructure settings.

The tool used to uncover the source of common problems and to identify simple solutions is AirMagnet Wi-Fi Analyzer (WFA) from NetScout. WFA can technically be categorized as a wireless protocol analyzer (a tool that captures Wi-Fi traffic and displays information about the captured traffic). In reality, however, WFA is unique among wireless analyzers because of what it is designed to do. Most wireless protocol analyzers are designed to allow for deep dives into frame (sometimes referred to as "packet") traces. WFA, on the other hand, is designed for field work. It is a tool that dovetails with what this paper is all about: quickly identifying what's wrong so that it can be rectified.

Here, then, are five common Wi-Fi problems, each with an accompanying simple solution:

Wi-Fi Problem #1: Transmit Power Mismatch

Wi-Fi devices use the 802.11 standard (for smartphones, tablets and other consumer devices, typically it's the 802.11n or 802.11ac amendments to the 802.11 standard). 802.11 is a technology that allows wireless access to a LAN (or the Internet via a LAN, in most guest Wi-Fi scenarios).

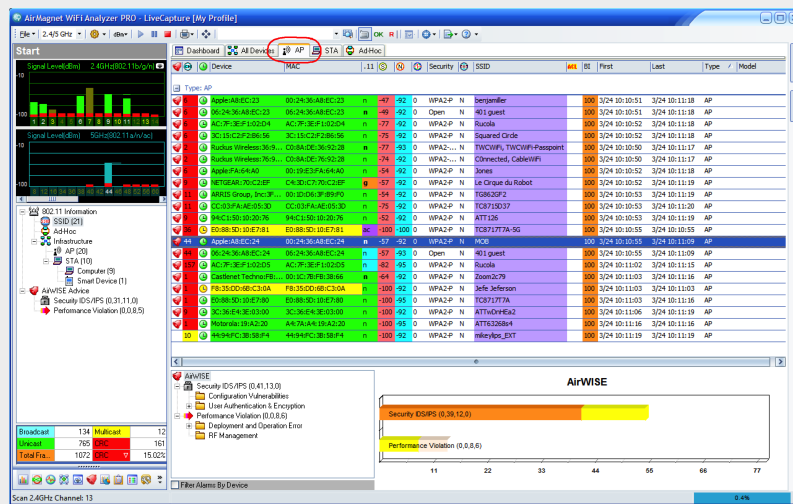
An essential requirement for 802.11 operability is for all devices to receive AND transmit. Just as a wired computer needs to be able to transmit to and receive from the routers and switches that make up a wired LAN, wireless APs and stations (smartphones, tablets, etc.) need to both transmit to and receive from each other in order for a wireless LAN to work.

The bad news is that a ton of wireless LANs are set up as if stations don't need to transmit. It happens during planning: the design for high density Wi-Fi often includes turning down the AP's transmit power regardless of whether or not supported stations have the ability to lower their transmit power. It happens before deployment: site surveyors walk around recording RECEIVED signal strength (typically in the form of received signal strength indicator[RSSI]) at the station, but not at the AP. It happens once the Wi-Fi is running: admins increase the AP's transmit power when smartphones suffer from poor performance, with no regard for the smartphone's transmit power. In too many cases, a two-way technology like Wi-Fi is handled as if it's in a one-way world.

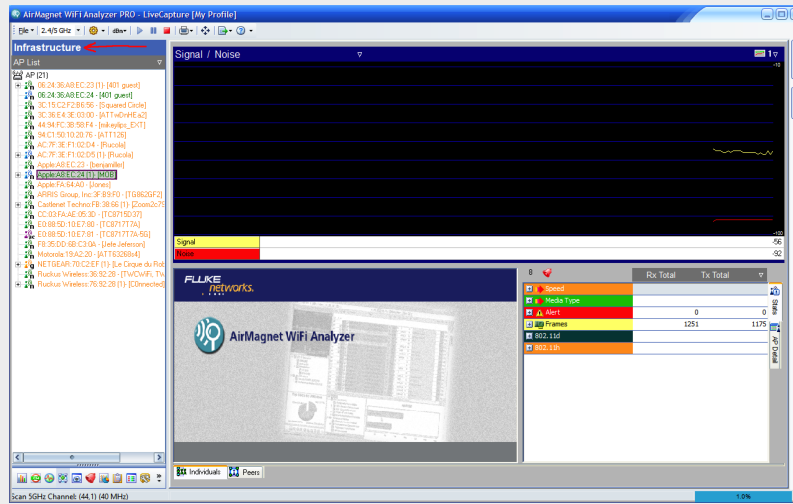


The good news is that AirMagnet Wi-Fi Analyzer can be used to check whether you have a transmit power mismatch. Just follow these steps:

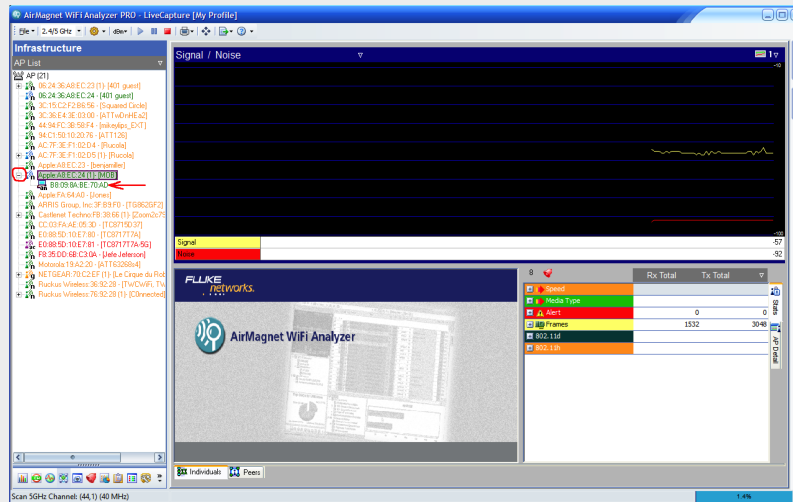
1. In the START screen of AirMagnet, find the AP that might have a transmit power mismatch. (Since there might be a lot of APs that are using the same SSID, the controller or management software that manages APs may have to be cross-referenced in order to find the relevant BSSID [AP's wireless MAC address].)



2. Double-click the AP in question. WFA will automatically navigate to the INFRASTRUCTURE screen of AirMagnet.

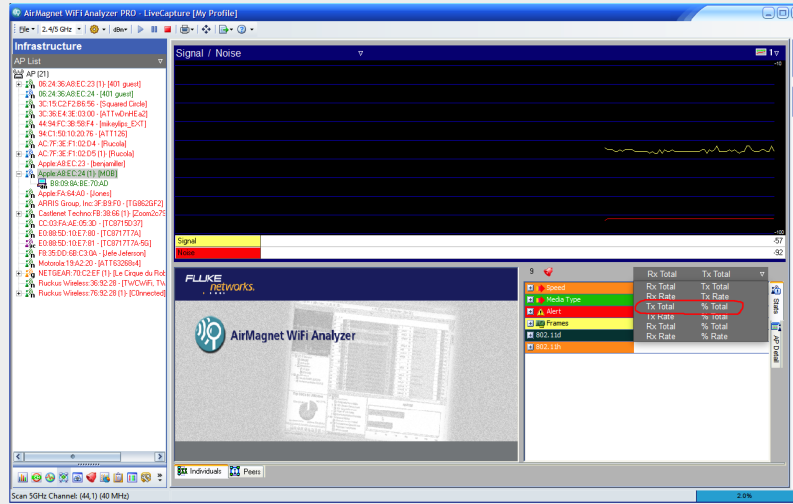


3. Click the [+] to the left of the AP in question. This expands a list of associated stations.

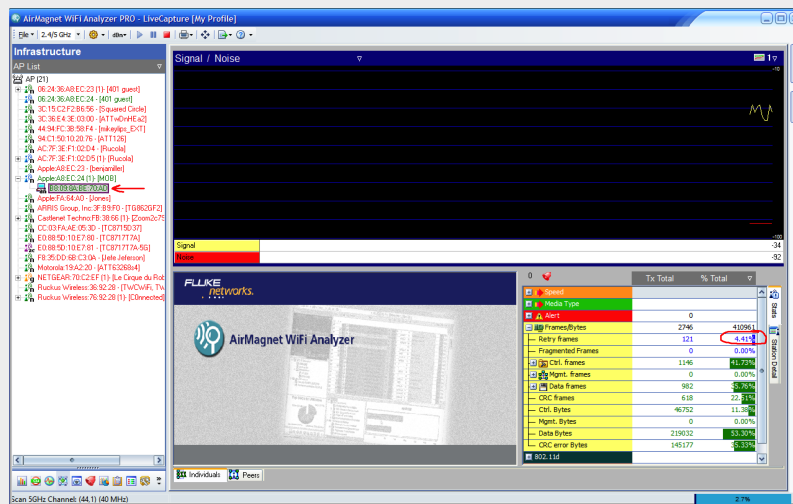


(As soon as an AP or station is clicked on in the Infrastructure screen, AirMagnet starts capturing ONLY on the channel of the AP or station. No need to manually change channels all the time when trouble-shooting a broad enterprise environment.)

4. In the lower right portion of the Infrastructure screen, a list of statistics is displayed. Above those statistics is a drop box that doesn't look like a normal drop box. Use that drop box to choose "Tx Total/% Total".

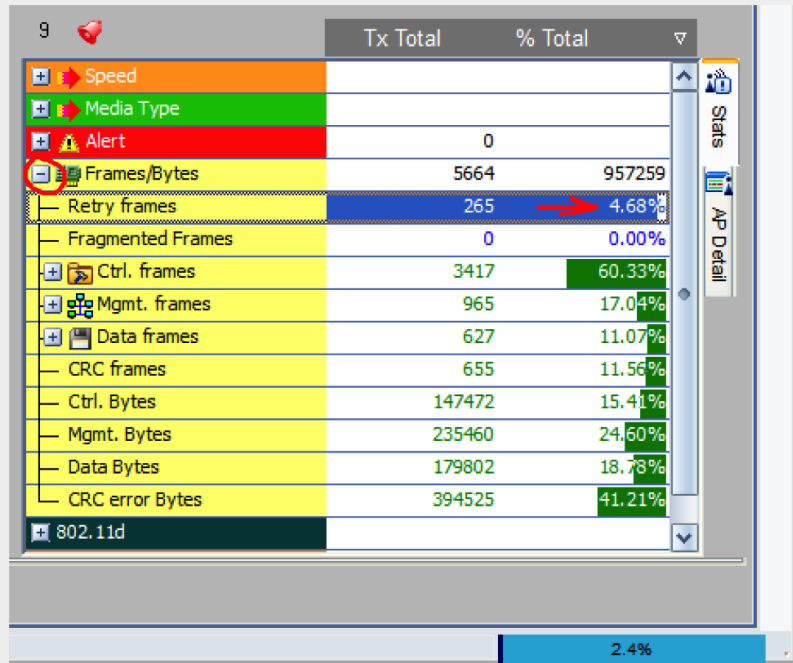


5. Now click the [-] to the left of "Frames/Bytes" in that same area. The Retry % for all traffic sent by your AP is now shown. Remember that percentage.



6. At this point, the Retry % values for different devices can be quickly viewed by clicking down the list of stations that are associated to the AP in question. While clicking through the list, pay attention to the Retry % statistic. Is it higher than the AP's Retry %? Lower? About the same?

If the Retry % for stations is higher than the Retry % for the AP that the stations are associated with, then the AP transmit power is almost certainly too high. If the opposite is true (meaning, if the Retry % for your stations is lower than the Retry % for your AP), then the AP transmit power is too low. Now head on into that controller or management software and fix it... that is, after you check to see if you have the next common problem:



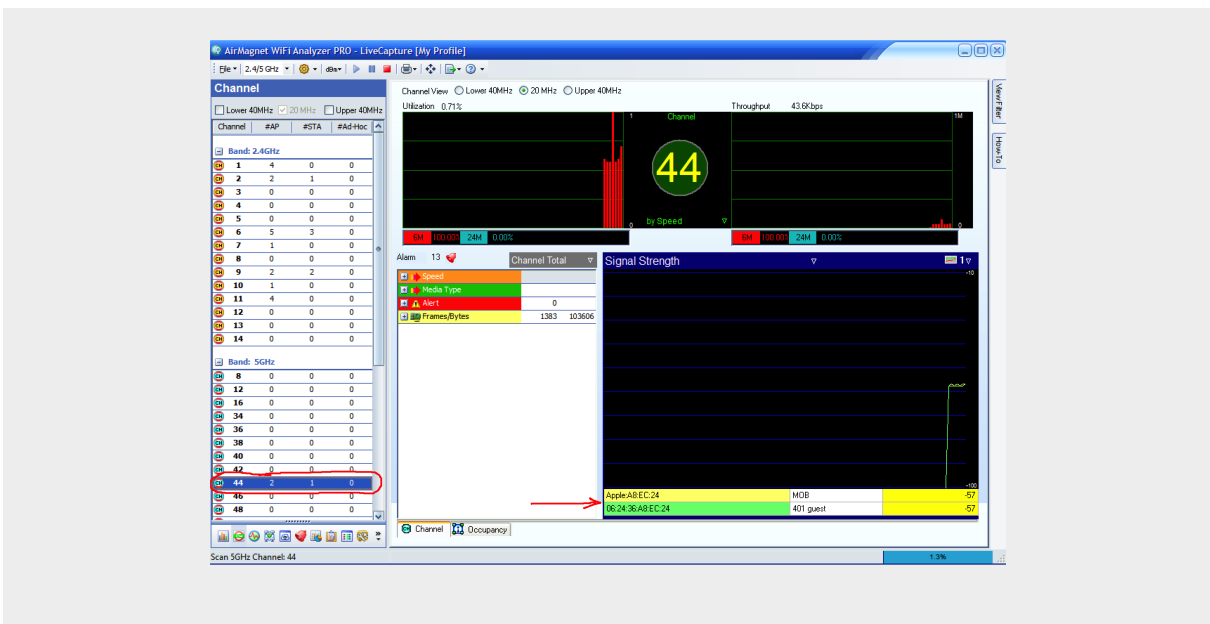
	Tx Total	% Total
Speed		
Media Type		
Alert	0	
Frames/Bytes	5664	957259
Retry frames	265	4.68%
Fragmented Frames	0	0.00%
Ctrl. frames	3417	60.33%
Mgmt. frames	965	17.04%
Data frames	627	11.07%
CRC frames	655	11.56%
Ctrl. Bytes	147472	15.41%
Mgmt. Bytes	235460	24.60%
Data Bytes	179802	18.78%
CRC error Bytes	394525	41.21%
802.11d		

Wi-Fi Problem #2: Interfering Traffic

On many WLAN controllers and management applications, the screen that allows you to change the AP's transmit power also allows you to change the AP's channel. And changing the AP's channel is a good solution for the second common WiFi problem: Interfering High Rate Traffic.

Enterprise WLAN infrastructure systems come equipped with protocols that allow APs to avoid interfering with each other. These auto-RF protocols can be a great time-saver during your setup and a good way to avoid unexpected interference problems after deployment. The problem is that auto-RF protocols aren't perfect. They have one fatal flaw: auto-RF protocols use information gathered by the AP. That means that when an auto-RF protocol is used to choose an AP's channel, it is designed to foster good air around the AP. Good air around the AP is nice, but good air around the station is more important. And sometimes a channel that is good around the AP isn't so good around the station.

To figure out whether the air around users' stations is congested, start by taking a computer running WFA to the location of problematic stations. Then look for indicators of channel congestion. The presence of nearby APs on the same channel or overlapping (meaning, less than four channel numbers apart in the 2.4GHz band) channels is a notable cause of congestion. Interfering APs are quickly identifiable in AirMagnet's CHANNEL screen in a way that is easy to see.



A source of channel congestion that often gets overlooked is high rate traffic. High rate traffic is a beautiful thing for devices that are able to understand it. For APs and stations that are too far away to understand it, however, high rate traffic is essentially just noise. And as data rates climb, the effective range of high rates drops. This leads to a situation where the APs and stations close to a device transmitting Wi-Fi traffic at a high data rate, can demodulate ("hear", in simple terms) the traffic and avoid interfering, but APs and stations that are further away may not be able to demodulate successfully.

The tricky part about interference from high rate traffic is determining whether devices are seeing it as noise. WFA can assist in figuring that out, but it is more complicated than some of the other activities in this paper. To figure out whether high rate traffic is being viewed as noise, go to the INFRASTRUCTURE screen and click on an AP that you think might be interfering. (To be clear, the selected AP should not be the AP that is having problems, but a different AP that is using an interfering channel.) In the lower right area of the screen, expand Speed and Bytes. If a lot of high rate traffic is being captured, then high rate traffic is most likely not causing interference. If there is not a lot of high rate traffic being captured, then walk towards the AP that you think might be interfering. If the amount of high rate traffic being captured increases dramatically, then high rate traffic most likely is causing interference.

Whether the problem is a preponderance of nearby APs on the same channel (or an interfering channel) or the problem is high data rate traffic causing interference, the simple solution is to override your controller's auto-RF and manually select a new channel on one or more deployed AP.

Overriding auto-RF protocols can help a lot, but there is another cause of dirty air to be aware of that has nothing to do with channel or transmit power levels on the APs. And it is our third common problem:

Wi-Fi Problem #3: Unconnected Guests

It may seem counter-intuitive that a device outside of the network could cause a problem with the network. In wireless networks, however, that can be the case. That is because a Wi-Fi device never really leaves a wireless network. In wireless, the physical layer of the network is radio frequency. Both connected and unconnected Wi-Fi devices continue to transmit using radio frequency.

When guests connect to your Wi-Fi their devices go pretty easy on the wireless side of things. Guests tend to use bursty applications like web surfing, emailing and audio/video streaming. (Yes, even "real-time" video streaming services tend to be bursty when their traffic patterns are examined.) These applications will also typically use high data rates, thus taking up less channel time. Channel time is valuable, and less channel time taken up by guests means more channel time available for internal users (or other guests, for that matter).



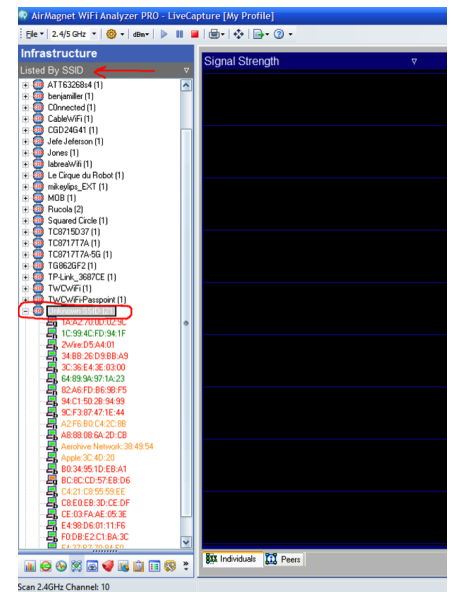
Unconnected guests are more of a problem because their devices typically take up a lot more channel time. Unconnected smartphones, tablets and computers Probe a lot. Probing is the process by which Wi-Fi devices look for networks in advance of connecting. If a device is connected, then it doesn't need to look (Probe) so much. If a device is unconnected, then it Probes perpetually. That becomes a problem because consumer devices Probe at low data rates. More channel time is used/wasted when the data rates are low. That's bad for your guests, internal users and everything else that's on your Wi-Fi.

AirMagnet can help you figure out if unconnected guests are causing a Probing problem. In the INFRASTRUCTURE screen, there is a list on the left hand side. If you change the drop box above that list to read "Listed By SSID", then you'll see a list of SSIDs in the area. Probing devices will show up in two places: under "Unknown SSID" and under SSIDs that have no AP listed (you'll have to click the [+] to the left of an SSID to see if there are no APs listed under it). The stations listed in those two places are unconnected. And if there are a lot of unconnected devices, then there is probably a Probing problem.

NETSCOUT.

(Don't go on a device-shaming binge after reading that last paragraph about unconnected smartphones causing performance problems. Networking folks have a bad rep in some circles for blaming users' devices when connectivity and performance problems arise. The reality is that good Wi-Fi can be had no matter what types of devices are used; even in large numbers. The wireless infrastructure just needs to be tailored to accommodate whatever devices are being used.)

If there is a Probing problem, then the solution is to get guests connected. Getting guests connected, however, often isn't simple. Guests have to know that there's Wi-Fi available, but even more than that, guests have to know which SSID to use and how to connect to it. If guests get re-directed web sessions (commonly called a Captive Portal), or some other methodology that requires customer interaction, evaluate what steps you can take to simplify and streamline this connectivity to reduce the number of unassociated clients in the environment. Numerous companies and other organizations have seen huge performance improvements after making the network connection experience simpler for guests...



Wi-Fi Problem #4: Dead Zones

The fourth common Wi-Fi problem is less common today than it used to be. What used to happen back when organizations were more cost-conscious about Wi-Fi installations is that number of installed APs about be fewer than were needed. Then the transmit power on APs would be set as high as possible (a mistake covered earlier in this paper) in order to "cover" the entire area that needed coverage. A nice-looking heatmap would be produced during the site survey, but once users connected to the Wi-Fi, they some would lack consistent network access.

An area where Wi-Fi devices can connect, but cannot consistently access the network is called a Dead Zone.



Wi-Fi professionals have gotten better about avoiding deployments where too few APs are installed. Most Wi-Fi folks have come to see installing APs as an investment rather than an expenditure. That's a good thing. Thus, there are far fewer installations with traditional, high-AP-transmit-power based Dead Zones.

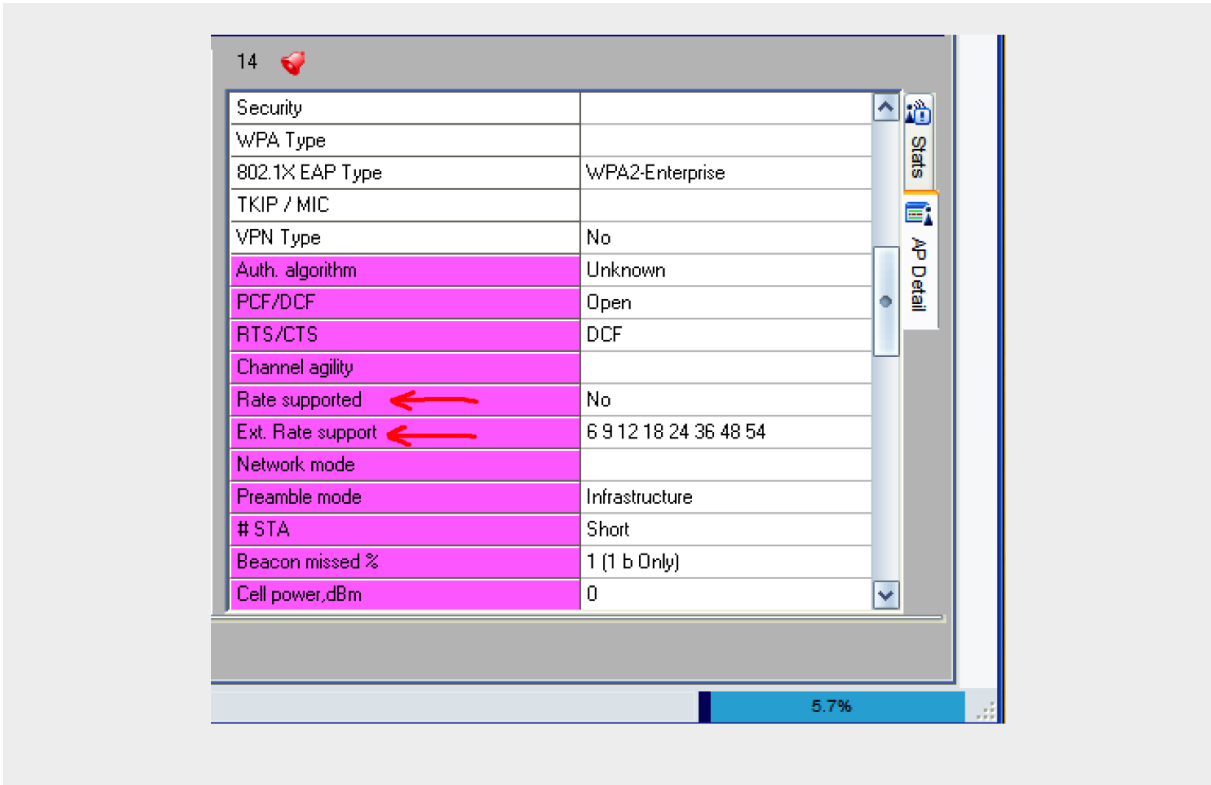
But Dead Zones still exist. And they exist because of a configuration tactic that can sometimes backfire: the disabling of low data rates.

Disabling low data rates is designed to improve overall Wi-Fi performance. The theory makes sense: low rate traffic allows less data over the channel in a given amount of time. (Data rates are calculated by measuring data [megabits or gigabits, typically] divided by time [per second]. That means that a low data rate packet is using up more time.)

The problem with disabling low data rates is that it can create a Dead Zone for certain stations. Some types of devices will stay connected to an AP even if the data rate it needs to use is unavailable. That is because many device's association algorithms use signal strength as the primary metric when choosing an AP. If a device sees a great signal strength from an AP, it may stay connected (one of the symptoms of a Dead Zone) while being unable to send and/or receive data (the other symptom of a Dead Zone).

The simple fix for a modern Dead Zone is to re-enable low data rates on your APs. That, however, is risky. If there really isn't a Dead Zone, then allowing low rates could drag down Wi-Fi performance for no good reason.

AirMagnet Wi-Fi Analyzer can be used to identify whether devices are suffering from Dead Zones due to APs having low rates disabled. Here are the steps: Get into the INFRASTRUCTURE screen and click on the AP that has possible Dead Zone'd stations connected. In the lower right corner, click the AP Detail tab and then scroll down until the list of Basic Rates and Supported Rates is visible. Take note of those. Then go back over on the left hand side and click on the MAC address of the station that is having a problem. Go over to the lower right again and this time click on the Stats tab. Now expand the Speed areas and see if the problem station is transmitting a lot of traffic using data rates that were not listed as Basic or Supported rates on the AP. If it is, then the Dead Zone is probably being caused by the AP having low rates disabled. Once the APs' low rates are re-enabled, users should experience a stable, Dead Zone-free wireless LAN...



...unless there are too many APs. Because that can lead to our fifth and final problem:

Wi-Fi Problem #5: Excessive Roaming

Wi-Fi stations, not APs, decide when roaming will occur. And how they decide is up to the vendor's implementation. A Wi-Fi network could have ten different types of devices connected, and all ten might have different parameters for initiating a roam. (Though there is one consistency across different device types as it pertains to roaming: All devices engage in Probing when they are ready to roam. So, go back to the section about UNCONNECTED GUESTS if a quick recall about devices' Probing behavior is needed.)



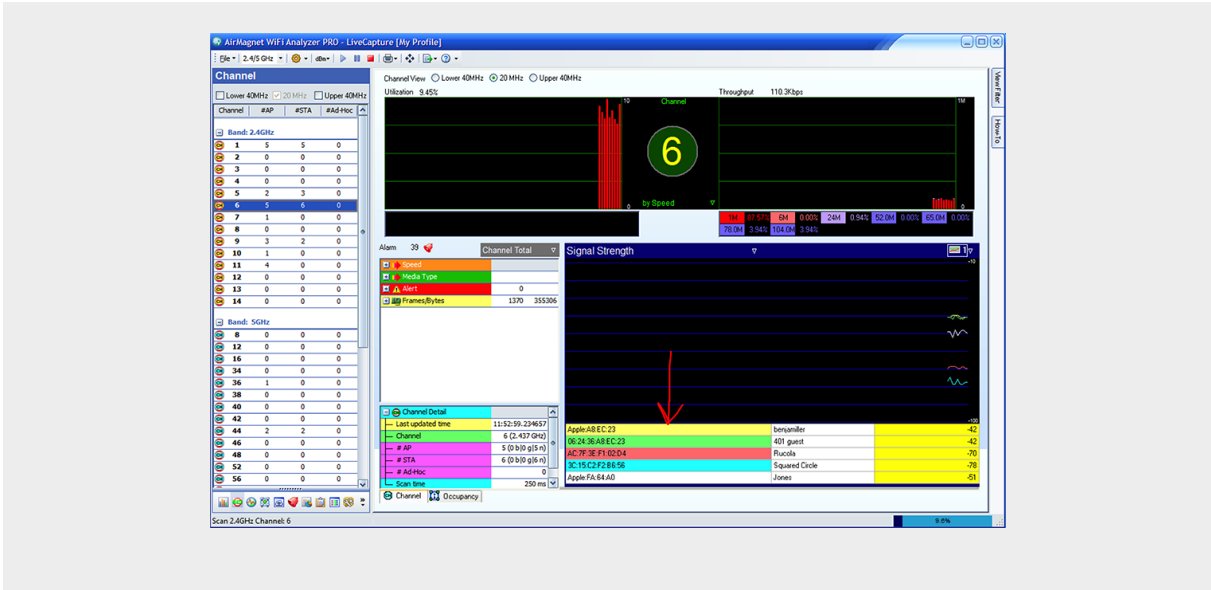
Excessive roaming can be a problem because devices might spend so much time roaming between APs that they might have very little time to access the network. What typically causes excessive roaming is either too many or too few APs. Having too many APs causes congestion, which can result in stations viewing their channel as unstable. Having too few APs can cause stations to have a low RSSI (received signal strength indicator), which results in your stations trying over and over again to connect to a better AP.

The problem of having too few APs does not have a simple solution. It would be easy to say that mounting a new AP near by the location of the excessive roaming will solve the problem, but seasoned Wi-Fi folks know better. Adding a new AP could mess up the whole RF design, and result in network admins playing Wi-Fi Whack-A-Mole. (Whack-A-Mole is the old arcade game where a foam hammer is used to smash little toy mole-looking creatures as they pop up from various holes. Whenever one mole would get whacked, another would pop up. Then the process gets repeated over and over. Playing Wi-Fi Whack-A-Mole involves mounting new APs, thus ruining the performance of a different AP. Then another AP gets added in the new location of the AP that is newly problematic, thus repeating the process over and over.) If the problem is too few APs, then a more robust analysis and/or survey could be needed in order to identify a lasting solution to the problem.

If the problem is too many APs, however, then there is a simple solution: turn off some AP radios. Turn them into intrusion sensors, spectrum analyzers, capture radios or whatever else might be useful. But just make sure that enough of them get turned off so that no more than one AP per channel has a significant signal in any given area.

The first step in solving a problem with excessive roaming is to verify that such a problem exists. AirMagnet makes it simple. Go to the INFRASTRUCTURE screen and click on the MAC address of the station that has an inconsistent connection. In the lower right hand corner, you will see the statistics for that station's traffic. Now expand "Frames/Bytes" and expand "Mgmt frames". The type of Management frames you're looking for are Reassociation Request and Reassociation Response. Those frames only get captured if a device is roaming. If the station you're analyzing is stationary, but still shows more than two of those frames, then your device is roaming more than it should be.

Once excessive roaming has been confirmed as a problem, AirMagnet can be used to see whether more than one AP is covering a given area. Take AirMagnet Wi-Fi Analyzer to the area where excessive roaming was happening and go to the CHANNEL screen. On the left hand side the channel can be selected. For each channel selected, look in the lower right and see whether there is more than one AP covering that channel at high signal strength. If there is, then that may be the reason that stations are roaming excessively. After walking to different trouble areas and checking for excess APs, it may become clear that some AP radios should be disabled. After excess AP radios get disabled the excessive roaming problem for wireless LANs that are over-deployed with APs often goes away.



(At this point it should be mentioned that NetScout has another great tool for diagnosing over-deployed AP situations: AirMagnet Survey. With AirMagnet Survey a floor plan can be uploaded prior to walking around areas where excessive roaming is happening. After surveying, a color-coded map is created, with the option to display how many APs are covering a given area at high signal strength.)

There it is: five common Wi-Fi problems and five simple solutions to those problems. With AirMagnet Wi-Fi Analyzer, users are powered with:

- Real-time accurate, independent and reliable analysis of 802.11a/b/g/n and ac wireless networks without missing any traffic
- A highly portable wireless network analyzer that travels to the source of the wireless network troubleshooting problems enabling faster and accurate fault-finding without any AP downtime
- A dedicated Wi-Fi troubleshooting solution guaranteeing any wireless network fault detection as compared to "time-slicing monitoring functionality" built inside the wireless network infrastructure
- The ability to reduce IT costs, simplify workload and minimize user complaints by obtaining instant answers to ANY wireless network connectivity, performance, roaming, interference and security issues using the AirWISE intelligence engine
- An unique active toolset to isolate and troubleshoot Wi-Fi connectivity and performance issues
- The Ability to strengthen your wireless network security by detecting and eliminating any wireless network threats and vulnerabilities
- Auditor-ready Wi-Fi Security compliance reporting for multiple verticals including wireless PCI compliance, SOX, ISO and many more
- Tools to troubleshoot BYOD induced performance and wireless network security issues