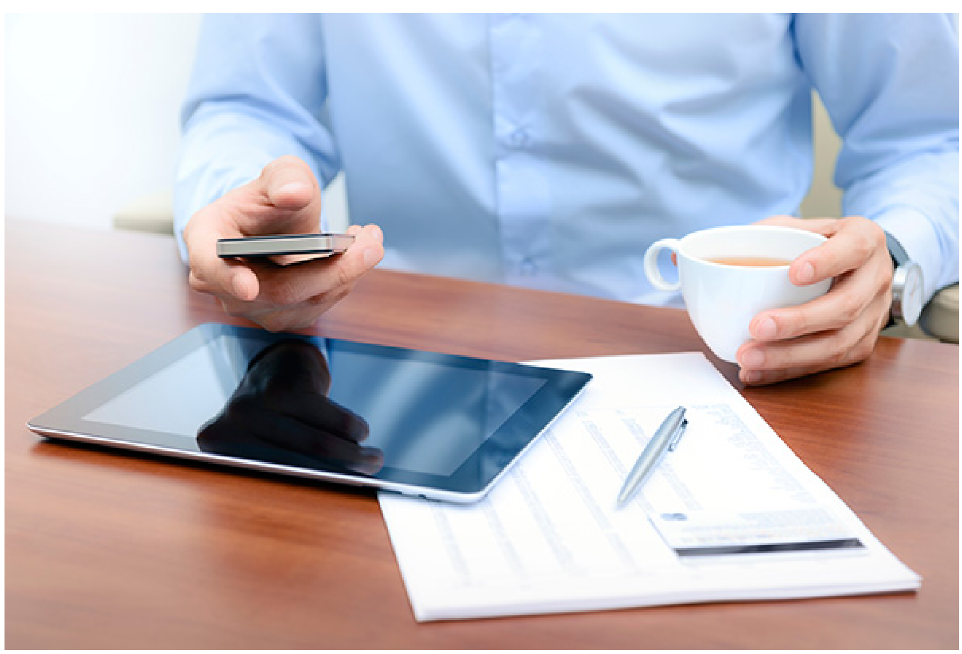
White Paper: BYOD Analysis using AirMagnet WiFi Analyzer

BYOD Analysis using AirMagnet WiFi Analyzer

This paper is designed to help networking people understand some of the key issues when supporting BYOD. The paper will cover important – and sometimes overlooked – aspects of supporting a variety of Wi-Fi devices, as well as specific solutions and strategies for BYOD support, including those offered by NetScout's wireless LAN analysis tool, AirMagnet WiFi Analyzer.

TABLE OF CONTENTS



Introduction

When a salesperson sells something, it's often a win-win. Both parties – buyer and seller – walk away happy. The person who likes mint chocolate chip ice cream enters the ice cream shop, sees his or her favorite flavor, and gleefully chooses. The buyer gets ice cream, the seller gets money and both parties leave satisfied. Salespeople get to enjoy win-win transactions all the time.

Networking professionals, on the other hand, are often faced with win-lose situations when working with users. Users often want something that makes life more difficult to networking folk. Users may want faster Internet access, but networking people understand the cost. Users may want unfettered access, but networking people need to keep it secure. And users may want to be able to use their own devices, but networking people know that BYOD (bring your own device) makes managing Wi-Fi more challenging.

In many cases it is fruitless to fight BYOD, because the users have already won. For many companies, once they see the benefits of BYOD — higher productivity, happier users, less expenditures on device acquisitions – having networking people who can support BYOD becomes essential.

If these services have already been deployed on the network and are performing poorly, these practices can also be used to optimize the network to improve service quality and user experience.

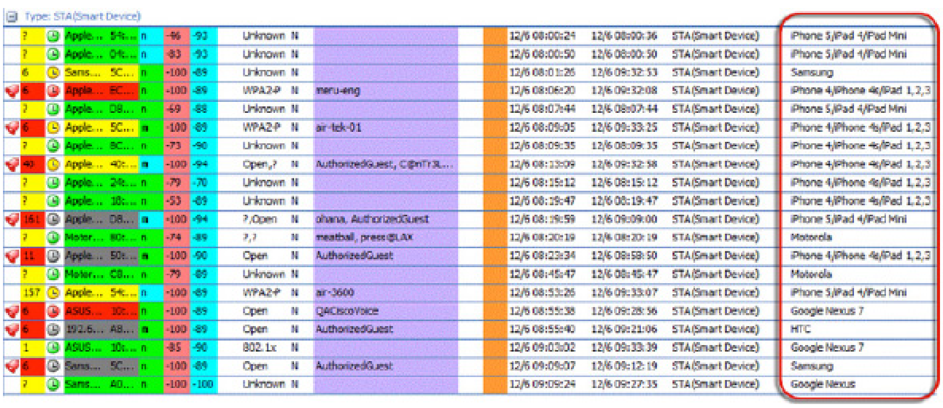
DIFFERENT DEVICES, DIFFERENT CAPABILITIES

The most important thing to keep in mind when supporting BYOD is that different Wi-Fi devices behave differently. All Wi-Fi devices support the 802.11 standard, but there are many variations allowed within that standard.

Differences between different Wi-Fi devices may include the following:

Standards support: 802.11ac is the most modern Wi-Fi standard, but an enterprise BYOD network is almost certain to have to support other standards. 802.11n, which made its debut in devices in 2007 and was officially approved by the institute of electrical and electronic engineers (IEEE) in 2009, is the most modern standard for Wi-Fi in the 2.4 GHz frequency band (which is the most common frequency band used by enterprise wireless LANs). The 802.11a and 802.11g standards, which were common in the mid-00's, may still be supported on wireless LANs that have non-traditional devices that are replaced less frequently than typical smartphones, tablets and laptops. The 802.11b standard, which dates back to the 1990's, may have to be supported in some cases, but is increasingly eschewed in modern enterprise Wi-Fi deployments.

AirMagnet WiFi Analyzer instantly detects and classifies smart phones and tablets that connect to the network. This capability allows users to authorize these devices, quickly troubleshoot and resolve issues caused by these devices as well as determine performance and security impact to the WLAN network.



Type: STA(Smart Device)

?	Apple...	54:...	n	-46	-93	Unknown	N		12/6 08:00:24	12/6 08:00:36	STA(Smart Device)	iPhone 5/iPad 4/iPad Mini
?	Apple...	04:...	n	-83	-93	Unknown	N		12/6 08:00:50	12/6 08:00:50	STA(Smart Device)	iPhone 5/iPad 4/iPad Mini
6	Sams...	5C...	n	-100	-89	Unknown	N		12/6 08:01:26	12/6 09:32:53	STA(Smart Device)	Samsung
6	Apple...	8C...	n	-100	-89	WPA2-P	N	meru-eng	12/6 08:06:20	12/6 09:32:08	STA(Smart Device)	iPhone 4/iPhone 4s/iPad 1,2,3
?	Apple...	D8...	n	-69	-88	Unknown	N		12/6 08:07:44	12/6 08:07:44	STA(Smart Device)	iPhone 5/iPad 4/iPad Mini
6	Apple...	5C...	a	-100	-89	WPA2-P	N	air-tek-01	12/6 08:09:05	12/6 09:33:25	STA(Smart Device)	iPhone 4/iPhone 4s/iPad 1,2,3
?	Apple...	8C...	n	-73	-90	Unknown	N		12/6 08:09:35	12/6 08:09:35	STA(Smart Device)	iPhone 4/iPhone 4s/iPad 1,2,3
40	Apple...	40:...	a	-100	-94	Open,?	N	AuthorizedGuest, C@nTr3L...	12/6 08:13:09	12/6 09:32:58	STA(Smart Device)	iPhone 4/iPhone 4s/iPad 1,2,3
?	Apple...	24:...	n	-79	-70	Unknown	N		12/6 08:15:12	12/6 08:15:12	STA(Smart Device)	iPhone 4/iPhone 4s/iPad 1,2,3
?	Apple...	18:...	n	-53	-89	Unknown	N		12/6 08:19:47	12/6 08:19:47	STA(Smart Device)	iPhone 4/iPhone 4s/iPad 1,2,3
161	Apple...	D8...	a	-100	-94	?,Open	N	ohana, AuthorizedGuest	12/6 08:19:59	12/6 09:09:00	STA(Smart Device)	iPhone 5/iPad 4/iPad Mini
?	Motor...	80:...	n	-74	-89	?,?	N	meatball, press@LAX	12/6 08:20:19	12/6 08:20:19	STA(Smart Device)	Motorola
11	Apple...	50:...	a	-100	-90	Open	N	AuthorizedGuest	12/6 08:23:34	12/6 08:58:50	STA(Smart Device)	iPhone 4/iPhone 4s/iPad 1,2,3
?	Motor...	C8...	n	-79	-89	Unknown	N		12/6 08:45:47	12/6 08:45:47	STA(Smart Device)	Motorola
157	Apple...	54:...	n	-100	-89	WPA2-P	N	air-3600	12/6 08:53:26	12/6 09:33:07	STA(Smart Device)	iPhone 5/iPad 4/iPad Mini
6	ASUS...	10:...	n	-100	-89	Open	N	QACiscoVoice	12/6 08:55:38	12/6 09:28:36	STA(Smart Device)	Google Nexus 7
6	192.6...	A8...	a	-100	-89	Open	N	AuthorizedGuest	12/6 08:55:40	12/6 09:21:06	STA(Smart Device)	HTC
1	ASUS...	10:...	n	-85	-90	802.1x	N		12/6 09:03:02	12/6 09:33:39	STA(Smart Device)	Google Nexus 7
6	Sams...	5C...	n	-100	-89	Open	N	AuthorizedGuest	12/6 09:09:07	12/6 09:12:19	STA(Smart Device)	Samsung
?	Sams...	A0...	n	-100	-100	Unknown	N		12/6 09:09:24	12/6 09:27:35	STA(Smart Device)	Google Nexus

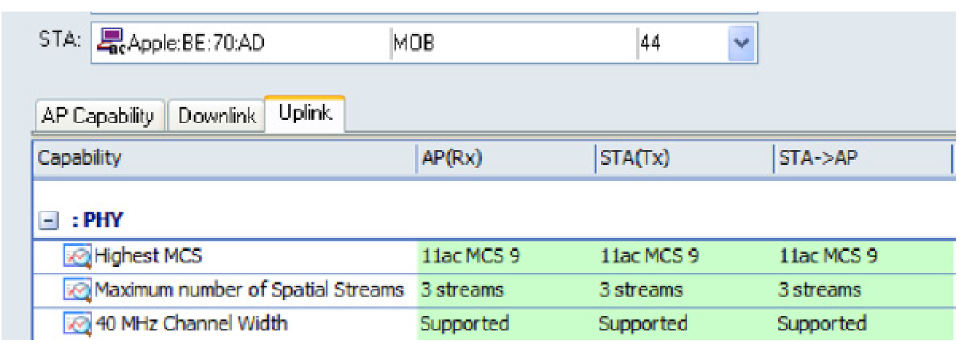
AirMagnet WiFi Analyzer can be a useful tool for identifying which standards are supported by different Wi-Fi devices in a BYOD environment. In the Infrastructure screen of Wi-Fi Analyzer, all devices are accompanied by a one or two letter sequence indicating which standard the device supports. WiFi Analyzer culls this information from management frames that are captured from Wi-Fi device transmissions.

MIMO support: Multiple-input, multiple-output (MIMO) antennas are antenna systems that allow devices to either use data rates that are two or three times higher or improve consistency and range. Device support for MIMO may be revealed in a device's data sheet, but in some cases a protocol analyzer, like AirMagnet WiFi Analyzer, may be required to identify a device's MIMO capabilities.

MIMO antenna systems can improve Wi-Fi connections in one of two ways: by improving data rates or by enhancing consistency and range. What MIMO technology does is it allows for two or three streams of data to be transmitted and received simultaneously. Essentially, the same frequencies are being re-used two or three times (at the exact same moment; MIMO isn't time-division) by two or three different antennas. One way that MIMO antenna systems can benefit Wi-Fi devices is by using If the data streams are unique, then data rates are doubled (when using two streams) or tripled (when using three streams. This is called spatial multiplexing. If the data streams are identical, then consistency and/or range may be improved. A number of MIMO-based technologies use identical data streams, including maximal ratio combining (MRC), space-time block coding (STBC) and transmit beamforming (TxBF).

The bottom line is that device support for MIMO is good for a wireless LAN. Either the device will use higher rates (thus improving the overall throughput capabilities of the wireless LAN) or the device will improve its range and/or efficiency. (Again, MIMO improves EITHER speed or range/consistency. MIMO cannot create data streams and identical data streams on the same device at the same time.)

AirMagnet WiFi Analyzer can be used to identify whether MIMO is supported, and boy is it simple. It also exemplifies one of the cardinal rules of using WiFi Analyzer: if you're looking at packets, then you're in the wrong place. When using other protocol a capture on the AP's channel would be required, followed by filtering to show only Probe Request frames and then opening the frame body of those Probe Requests to view the HT Capability information element. It can make the process of identifying devices' MIMO capabilities quite convoluted. WiFi Analyzer, on the other hand, allows MIMO capabilities to be viewed by simply right-clicking the device in the Infrastructure screen and selecting 802.11n/ac Efficiency. (Since WiFi Analyzer can detect whether devices are using 802.11n or 802.11ac, the actual wording will match whichever standard the device supports.) After selecting 802.11n/ac Efficiency, WiFi Analyzer will automatically switch to the WiFi Tools screen. The Efficiency tool will automatically have been selected and Uplink information will automatically be shown. The Uplink information indicates how many MIMO streak – if any – are supported by the selected Wi-Fi device.



Identifying spatial multiplexing support in Wi-Fi devices is important for managing expectations in a BYOD Wi-Fi environment. When devices support more spatial multiplexing streams, the overall performance capabilities of the Wi-Fi environment are increased because higher data rates are possible.

Data rates are sometimes misunderstood. Higher data rates do not necessarily guarantee devices more access to LAN resources or the Internet. Rather, higher data rates require that less RF channel time is used AFTER a device earns the right to transmit or receive data to/from the LAN or the Internet. That means that higher data rates are always a good thing for Wi-Fi. Even if an enterprise has strict restrictions on guest bandwidth (say, a 2 Mbps cap on Internet speeds), data rates should be kept as high as possible for all devices in order to prevent guests from slowing down LAN or Internet access for internal users.

Most Wi-Fi devices lack MIMO support, but many devices support it. Starting with the iPad Air, Apple tablets began supporting two-stream MIMO, which allows for data rates to double under clean RF channel conditions. Laptops and desktops have long supported MIMO, though support varies between two-stream, three-stream and possibly even a lack of MIMO support in some "netbook" laptops.

Diversity antennas: Diversity antennas improve the consistency and reliability of Wi-Fi by using multiple antennas to receive transmitted radio waves.

MIMO support and diversity antenna support often go hand-in-hand, but not always. Devices may support diversity antennas without supporting MIMO. Because MIMO uses multiple radio chains to transmit data simultaneously over a single RF channel, MIMO causes reduced battery life. Some larger devices, like tablets and "netbook" laptops, may support diversity antennas, but not MIMO.

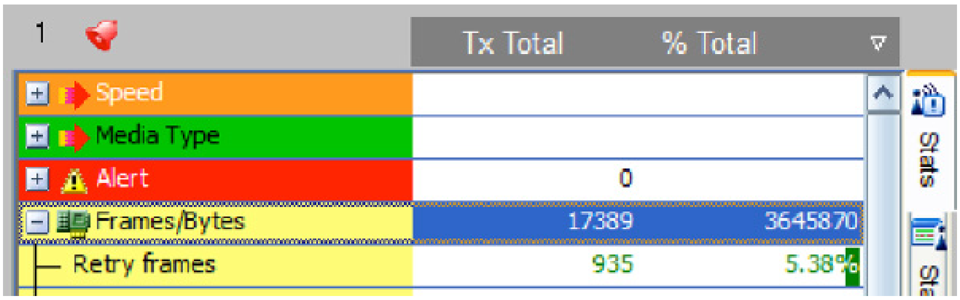
Smartphones, due to their relatively small size, typically do not support MIMO or diversity antennas. Both MIMO and diversity antennas require that antennas be placed a significant distance apart from each other within a device, and smartphones simply lack the space to make either multiple antenna technology work. (Though it should be noted that both antenna technology and smartphone technology often improve, so diversity antennas could become available in smartphones some day.)

Unfortunately, there is no requirement that Wi-Fi devices indicate whether diversity antennas are supported when transmitting frames. If MIMO is supported (see previous section), then diversity antennas will definitely be supported. If MIMO is not supported, then the Wi-Fi device vendor documentation would have to be consulted in order to verify support for diversity antennas.

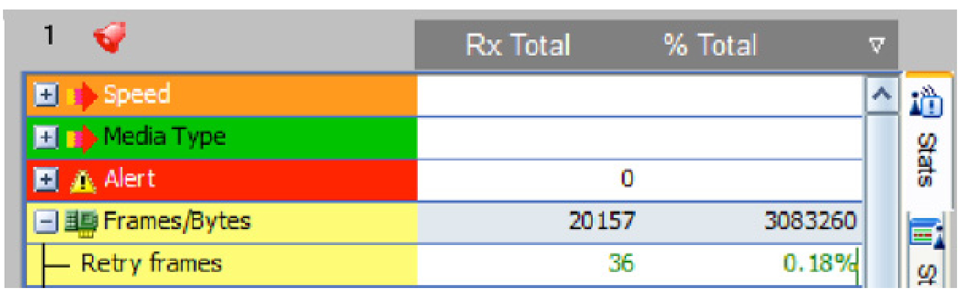
Transmit power: Wi-Fi usually works best when APs use the same transmit power as the devices that connect to them. The problem is that different models of smartphones, tablets and laptops often have differing transmit power levels.

Matching the transmit power of an AP with its associated Wi-Fi device works best because Wi-Fi is a two-way method of communication. For every web page that is downloaded, a Wi-Fi device must send an HTTP request to the AP. While there are many applications that create more downlink traffic than uplink traffic, Wi-Fi still tends to work best when transmit power matches because matching transmit power tends to minimize the number of retransmitted data frames. Retransmitted data frames can be very damaging to a Wi-Fi channel because every retransmitted frame creates wasted channel time, which ultimately limits the availability of the Wi-Fi channel for all APs and stations.

AirMagnet WiFi Analyzer can be used to identify whether AP transmit power is approximately equal to the transmit power of a Wi-Fi device, like a smartphone tablet or laptop. To test whether transmit power matches, start by using an application on a Wi-Fi device. Then go into Wi-Fi analyzer and navigate to the Infrastructure screen. Once in the Infrastructure screen, click on the AP that the Wi-Fi device is connected to in order to begin capturing on the channel that the AP and device are using. To the left of the AP, there will be a [+] icon. Click the [+] icon and then click on the Wi-Fi device that is running the application. At this point, Wi-Fi Analyzer will be showing only statistics that are related to the Wi-Fi device that has been selected. With the Wi-Fi device selected, look in the lower right corner of the Infrastructure screen to view statistics. Change the dropbox labeled “Rx Total/Tx Total” to “Tx Total/% Total” in order to view traffic transmitted from the Wi-Fi device, by percentages. Then open the Frames category to view the percentage of Retry frames.



Once the percentage of transmitted Retry frames has been recorded, change the dropbox to “Rx Total/% Total” and record the percentage of received Retry frames.



If the Retry percentages match, then the transmit power of the AP is approximately equal to the transmit power of the Wi-Fi device. If the received Retry percentage is higher, then the AP transmit power is too low and if the transmitted Retry percentage is higher, then the AP transmit power is higher than the Wi-Fi device’s transmit power.

Adjusting AP transmit power to match Wi-Fi device transmit power can be especially difficult in a BOYD environment because a number of different Wi-Fi devices may need to be supported. In situations where it is impractical to test each Wi-Fi device’s transmit power, choosing an AP transmit power between 12 dBm and 15 dBm is a good place to start.

Probing behavior: When devices are unconnected to a Wi-Fi network, they send Probe Request frames as a way to search for nearby APs.

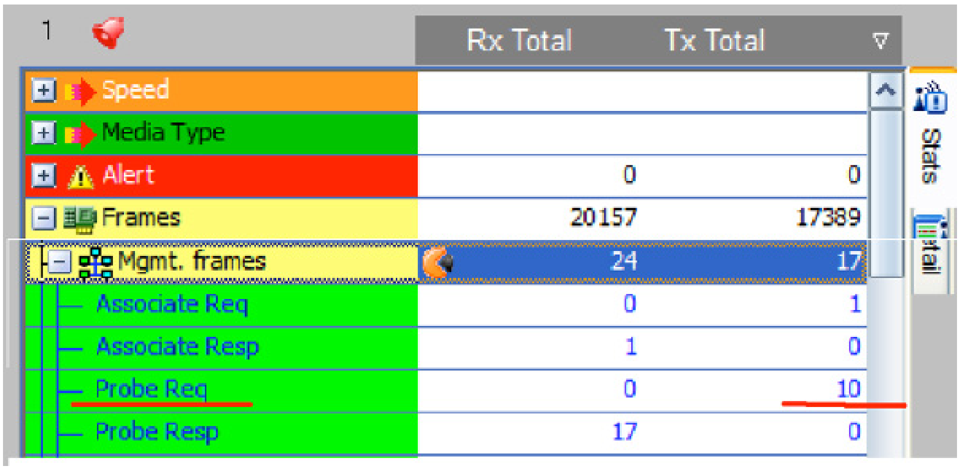
The problem with probing is that some devices send so many probe request frames when unconnected to Wi-Fi, that the device ends up using MORE Wi-Fi channel bandwidth when its unconnected than when it’s connected.

Repeat: Sometimes it is WORSE for Wi-Fi performance to have devices that are NOT connected to the Wi-Fi network.

It seems counter-intuitive that an unconnected device could affect performance more than a connected device, but that’s how Wi-Fi probing works. When Wi-Fi devices are connected, they only send probe request frames if they have initiated the roaming process. When Wi-Fi devices are unconnected, they send probe requests all the time because the device is looking for a Wi-Fi connection all the time. And the accumulated Wi-Fi channel time taken up by probe requests can often be greater than the accumulated Wi-Fi channel time taken up by network data.

Probing behavior is especially difficult to deal with in an enterprise Wi-Fi environment because it varies by device and operating system. The only way to really know whether a Wi-Fi device’s probing behavior will cause harm to a Wi-Fi environment is to test it. And even testing for probing behavior is an inexact science.

Testing a Wi-Fi device for probing can be done in WiFi analyzer using the Infrastructure screen. Once in the Infrastructure screen, the Wi-Fi device must be selected on the left side of the screen. After the Wi-Fi device has been selected, the Wi-Fi device must be disconnected from any Wi-Fi networks, but must have its Wi-Fi radio turned on. (In iOS and Android devices, that means to "Forget" Wi-Fi networks.) After the Wi-Fi device has been selected, the number of Probe Request frames can be viewed in the Stats area in the lower right corner of the Infrastructure screen. Probe Request stats are shown under Frames, and then under Mgmt Frames.



1	Rx Total	Tx Total
Speed		
Media Type		
Alert	0	0
Frames	20157	17389
Mgmt. frames	24	17
Associate Req	0	1
Associate Resp	1	0
Probe Req	0	10
Probe Resp	17	0

It is possible that a given Wi-Fi device will have identical probing behavior on all Wi-Fi channels, but that is not guaranteed. If more information about probing behavior is needed, the Decodes screen of AirMagnet can be used. In the Decodes screen, a Probe Request filter can be created and applied to any Wi-Fi channel. Testing probing behavior on every single Wi-Fi channel is a time-consuming and monotonous process, but it may be necessary in extreme cases where probing Wi-Fi devices are causing the wireless LAN to become unusable.

Roaming behavior: There is good news and bad news about roaming behavior.

The bad news about roaming behavior is that it is one of the most difficult parts of supporting a BYOD environment. Not only do different devices roam differently, but sometimes a single Wi-Fi device will change its roaming behavior because a different application is running, because there are too many APs nearby or because the motion sensor within the device detects movement. Roaming behavior is really hard to predict.

The good news about roaming behavior is that testing for it is very similar to testing for probing behavior because probing is the first step of roaming. What was written previously about using AirMagnet WiFi Analyzer to test for probing behavior also applies when testing for roaming behavior. The only difference is that the Wi-Fi device that is being tested will have to be physically moved away from its associated AP in order to trigger the probing behavior that begins the roaming process. In modern Wi-Fi devices, received signal strength indicator (RSSI) triggers the roaming process, so pay attention to the RSSI reading on the Wi-Fi device while moving it as part of a roaming test.

Once the signal strength at which a device starts Probing has been determined, then the infrastructure may be designed or adjusted to support device roaming. Most Wi-Fi devices roam well with an 8 dB cell overlap. That means that if a device initiates Probing at -72 dBm, the device is likely to roam smoothly if the device sees a different AP giving an RSSI of at least -64 dBm.

One last note about supporting roaming in a BYOD environment is to expect the unexpected. A Wi-Fi device that starts probing at -72 dBm in a lab may start probing at a different RSSI once it is being used in the field. Supporting roaming is one of the more difficult parts of managing a BYOD environment because device behavior can be unpredictable. So, plan on using WiFi Analyzer more than once to understand how different devices handle roaming.

Conclusion

This paper has covered a number of ways in which Wi-Fi devices vary, but there may be other variations that crop up as wireless LANs continue to evolve. It is hard to predict the future accurately, but one thing seems certain: different Wi-Fi device will continue to be different. It has always been that way, and makers of Wi-Fi devices have shown no signs of gravitating towards uniform behavior. For that reason, it can be useful to take some time and analyze the different behaviors of Wi-Fi devices, so that they can be better supported in a BYOD environment.