9 MYTHS ABOUT WI-FI IN K-12 EDUCATION

Ruckus
Simply Better Wireless.

Wi-Fi, it seems, is always growing. From the creation of the term "Wi-Fi" (which, according to the people who created it at the Wi-Fi Alliance, doesn't actually stand for anything) over a decade ago, it seems that Wi-Fi has perpetually been touted as a rapidly expanding technology.

Until a few years ago, however, schools were a Wi-Fi-free sanctuary. Many school districts lacked the budget for robust deployments, and many others avoided the technology for security or educational reasons (with the attention span of the average grade schooler not exactly being held in high regard even before smartphones became ubiquitous).

Today, Wi-Fi is a reality in many school districts. And if it's not a reality yet, it will be soon. No parent wants his child to be bullied for not being able to throw a baseball, even if it's only on the Home Run Derby application. Wi-Fi is the technology of choice for getting young people up to speed on educational fundamentals, world events and, in some cases, hitting the expert level in the Home Run Derby app. It's relatively inexpensive, universally supported in consumer devices and it works.

Or, at least, it can work.

Unfortunately, Wi-Fi in K-12 deployments has a little bit of a spotty reputation in some circles. Not to put too fine a point on it, but a lot of money has been spent by a lot of people on a lot of Wi-Fi networks that struggle with performance.

This paper aims to fix that. We have identified nine myths about K-12 Wi-Fi deployments, and if these myths are avoided, there is a much better chance that in-school Wi-Fi is going to work as promised. And even if your K-12 Wi-Fi network already avoids most of these myths, hopefully there will be something that will spark an idea that will get your Wi-Fi to its optimal state.

We appreciate you taking the time to read the paper. Now, let's dig into some common myths about Wi-Fi deployments in K-12 education environments.

#1 You need to upgrade your switches if you're going to upgrade your Wi-Fi

"My Wi-Fi is too fast." It sounds like a first-world problem, right? Like, "my parents are too rich," or "there's too many sunny days in Los Angeles." But, like the rich parents who spend all day at work or drought-stricken southern California, there are consequences to having too much of a good thing.

The consequence of 802.11ac Wave 2 Wi-Fi is that it might be too fast for the network's switches. That an AP supporting 600 Mbps over a 2.4 GHz channel and another 1.7 Gbps over a 5 GHz channel (1.733 Gbps, actually, but who's counting) will be too much for a 1 Gbps switch port. Or, so the myth goes.

In reality, switch speed almost never slows down Wi-Fi applications because Wi-Fi applications rarely put throughput stress on network links. Common Wi-Fi applications like email, web browsing, chatting and even on-demand video are bursty by nature. Bursty applications use the network the way a 4 x 100 meter relay team uses a running track. Packets — the network equivalent of the baton in a relay race — traverse each link in total before moving on to the next link. So, a fast Wi-Fi link is going to speed up the performance of bursty applications whether switch speeds are upgraded or not. The exception is large file transfers. Large file transfers treat the network more like a highway than a relay race. If a busy highway goes from three lanes to two lanes — the commuting equivalent of using 802.11ac Wave 2 Wi-Fi at full capacity with a gigabit wired infrastructure — then overall commute time slows. But think about it: does a typical K-12 Wi-Fi network primarily handle large file transfers, or does it primarily handle web browsing, on-demand video and other bursty applications? The latter is much more common.

There are other reasons why existing gigabit switch infrastructures can handle education 802.11ac Wave 2 Wi-Fi. Most Wi-Fi devices — including all smartphones, tablets, computers, and netbooks — use battery life conservation technologies that keep Wi-Fi speeds well below 1 Gbps. Wi-Fi environments are also more susceptible to collisions than wired networks, thus causing the vast majority of Wi-Fi channels to see throughput maximums fall well below 1 Gbps. Lastly, Ethernet is a full duplex technology while Wi-Fi is half duplex. That means that Ethernet can only become a "bottleneck" to Wi-Fi speeds if all of the Wi-Fi traffic goes in one direction. Modern Wi-Fi networks — especially in K-12 environments — handle significant amounts of uplink traffic, thus making worries about switch speeds a moot point.

While having fast wired speeds to go with increased Wi-Fi speeds is a fine idea, it's far from necessary. And in environments where most of the network access goes through Wi-Fi, upgrading wireless speeds gives schools more bang for their buck.

#2 One AP per classroom provides optimal performance

It is a common mistake in many areas of life — not just Wi-Fi — to think that throwing money at a problem will solve it. And just as the New York Yankees of the early 1990s had the richest player payroll in professional baseball with poor results to show for it, so too can extravagant Wi-Fi deployments prove inferior to measured, incisive installations.

The quintessential example of excess in the world of Wi-Fi is to over-deploy APs. Adding APs to a Wi-Fi deployment can add capacity to a point, but there becomes a time when new APs become counter-productive.

APs see performance degradation due to over-deployment when more than one AP is covering the same channel to the same device. (Meaning, if someone takes his/her iPad and runs the scan function of the Airport Utility application [the scan function has to be enabled in the iOS Settings for the Airport Utility app, by the way] and sees more than one of the schools' APs operating on the same channel at a signal above -80 dBm). There are only three non-interfering channels available in North America when using the 2.4 GHz frequency band (which is the band that has the broadest support among consumer devices). When APs are installed in every classroom, it is a virtual certainty that smartphones, tablets and laptops will "see" more than one AP covering the same channel.

For some Wi-Fi installations in K-12 environments, APs are configured with low transmit power settings in order to give the allusion that an over-deployment has been avoided. Don't fall for this illusion. Wi-Fi is a two-way communication technology (meaning that smartphones, tablets and other Wi-Fi devices must transmit to APs, as well as receive), and thus decreasing AP transmit power fails to prevent channel congestion problems in environments with high concentrations of users.

Damage from the "One AP per classroom" myth can be avoided by commissioning a properly done site survey before choosing AP installation locations. There are times when one AP per classroom can work, but that isn't known without a proper site survey. Site surveys can be expensive and time-consuming, but a skilled integrator can produce a site survey that will save both time and money in the long run.

#3 APs need to be mounted inside classrooms

In some K-12 environments, there is a subtle conflict between personal health and Wi-Fi performance. People who have fears that radio waves cause health problems don't want to see APs anywhere near them. (As of this writing, there have been no audited, proper scientific studies proving that Wi-Fi exposes human beings to health problems. But, then again, there are no true scientific studies proving that Kanye West is the best rapper alive, and a ton of people believe in that. So, whadya gonna do?) People who want the best Wi-Fi performance want APs as close to them as possible.

Since performance tends to win out over hocus pocus when IT people make the decisions, the trend of installing APs in K-12 classrooms has become widespread. And that is great for performance. If teachers are fine with having APs five feet from their heads and if students' parents aren't worried that Wi-Fi is going to cause little Johnny to grow a third arm, then it makes sense to prioritize performance.

If, on the other hand, there are limitations on APs being placed in classrooms, then APs can be mounted in hallways without cause of unacceptable performance downgrades…in some cases. The key to hallway mounting is to have APs equipped with the right type of antenna. Internal omni-directional antennas — which is what most enterprise APs come equipped with might work. However, in cases where classrooms are large, walls are thick or insulation is blocking the Wi-Fi signal, then directional antennas might be needed for APs.

WARNING: Ruckus marketing content…

Ruckus Wireless offers a unique antenna system called BeamFlex that uses an array of antennas that dynamically creates directional antennas while at the same time supporting device connections in an omni-directional pattern. That means that APs mounted in hallways — out of sight and out of mind from

students and teachers — can transmit and receive a strong enough signal, even through classroom walls. It also means that external, directional antennas — which can add complexity and cost to AP mounting — are unneeded. The unique, patented BeamFlex antennas inside of Ruckus APs makes hallway mounting a viable option.

Admittedly, "APs need to be mounted inside classrooms" is less of a Wi-Fi myth and more of a Ruckus myth. If you decide to mount non-Ruckus APs in the hallways of an elementary school, don't go blaming this paper if Wi-Fi performance is inadequate.

#4 Wave 2 APs won't help without Wave 2 clients

Standards have always been a big deal in Wi-Fi, and the latest big deal is 802.11ac Wave 2. The 802.11ac standard was officially approved by the IEEE back in 2013, and 802.11ac APs and devices have been available going back even further than that. The problem is that — up until recently — everything was 802.11ac Wave 1. The technological explanation of 802.11ac Wave 1 can get a bit complicated, but essentially it is just 802.11n (the previous IEEE standard for Wi-Fi, which dates back to 2009) with a couple of enhancements for consumer Wi-Fi. (This is not to say that 802.11n and 802.11ac Wave 1 hardware is equivalent to one another. The chipsets for 802.11ac Wave 1 are more modern than the chipsets for 802.11n, and chipsets matter. In fact, the importance of having modern chipsets will be discussed in more detail shortly).

802.11ac Wave 2 is now available, but only in access points. Most smartphones, tablets and laptops don't support 802.11ac Wave 2 right now, and it might be quite some time before some of them do. Apple, for example, is a company that is notorious for producing devices that adopt Wi-Fi standards late. While other device makers were producing 802.11ac Wave 1 smartphones by early 2013, Apple's first 802.11ac Wave 1 smartphone, the iPhone 6, wasn't released until late 2014. It is entirely possible, then, that 802.11ac Wave 2 devices may be unavailable until late 2015, with Apple waiting until 2016 to adopt Wave 2 in iPhones and iPads.

It is this lack of available Wave 2 devices that has caused this myth to propagate. "Without Wave 2 devices, it doesn't make sense to deploy Wave 2 APs," or so the thinking goes. But it is a half-truth. Yes, the benefits of Wave 2 will only be fully realized once Wave 2 devices are available. No, Wave 1 APs do not deliver the same performance as Wave 2 APs, even if the connected devices are all 802.11ac Wave 1 (or 802.11n, for that matter).

First, the negative: there aren't many 802.11 Wave 2 devices available on the market today. If Wave 2 APs are deployed in a high school, smartphones and tablets used by student and faculty will use the same maximum data rates that they would use if Wave 1 APs were deployed. Also, some devices may never use some of the more intense performance enhancing protocols because Transmit Beamforming (TxBF) and Multi-User Multiple Input, Multiple Output (MU-MIMO) may have side effects like more channel overhead or shorter device battery life.

It is disappointing that Wi-Fi technology is lagging in popular consumer devices, but just because smartphones and tablets are incapable of using all of the enhancements of 802.11ac Wave 2 doesn't mean that smartphones and tablets won't benefit from a Wave 2 upgrade. 802.11ac Wave 2 APs use a more modern chipset, which offers better receive sensitivity than Wave 1 APs. That means fewer pesky half-connections (those connections where the device shows that it's connected, but can't get consistent access to the network) and, ultimately, greater range. Wave 2 APs also have more antennas, which can improve

Wi-Fi conditions via enhanced receive diversity, even when connected devices support only 802.11ac Wave 1 or 802.11n. So, there are a few good reasons that Wave 2 APs are better than Wave 1 APs, even though full Wave 2 won't be realized until users' devices start supporting it.

#5

Keeping students' smartphones off the network improves Wi-Fi performance

There are two tiers to the argument that students' devices should be kept off K-12 Wi-Fi networks. Argument number one is that they use internet bandwidth. Argument two is that they don't support the high Wi-Fi speeds that are supported in the tablets and laptops that are often used for education.

The argument that student smartphones' use of internet bandwidth will have an effect on network performance is sound in some ways; flawed in others. The argument is sound because every elementary, middle and high school has a finite amount of internet bandwidth coming in and going out. If students get on their smartphones and use the school's Wi-Fi network for non-education activities, then that leaves less available internet bandwidth for education. The argument is flawed because the vast majority of internet traffic is bursty and because the total available bandwidth from the service provider is almost never used. Of course, at some point a school's internet connection could become truly saturated. But it would be a rare case, and it would also be a fixable problem (albeit at an additional cost paid to the Internet service provider).

The Wi-Fi side of the anti-smartphone argument is deceptive. Yes, smartphones do support lower maximum Wi-Fi speeds than tablets and laptops. Yes, low Wi-Fi speeds from one device can slow down a Wi-Fi channel for other devices. Yes, Wi-Fi is a technology that operates over a shared channel, meaning that when more devices use a channel, each individual device has less available access. All of that is true. All of that is also specious, because prohibiting students from connecting to a K-12 Wi-Fi network does not keep their devices off the Wi-Fi channel. Unconnected Wi-Fi devices use the Wi-Fi channel via a process called Probing (in some circles, Probing is also called Discovery or Active Scanning). Probing is an activity that allows devices to gather information about nearby APs. When a device is connected to a Wi-Fi network, it doesn't need to gather information about nearby APs because it already has an AP. (Unless the device is roaming, but that's another topic for another paper). When a device is unconnected to Wi-Fi, then it needs to know about the APs that are nearby.

The problem with Probing is that it can take up more Wi-Fi channel time than actual network data (and often does). Probe Request frames (a.k.a. "packets", except the word packet implies that a Network layer header is present and Probe Requests do not carry a Network layer header) are sent at extremely low rates (either 1, 2 or 6 Mbps, depending on the device and operating system), which means that Probe Request frames use up a disproportionately large amount of channel time. It is the exact scenario mentioned two paragraphs ago: low Wi-Fi speeds (in this case, from Probe Request frames) can slow down a Wi-Fi channel for all devices.

In most cases, one component of getting optimal performance out of a K-12 Wi-Fi network is to allow students' and employees' personal devices to connect, but what about security? Well, there is a myth about K-12 Wi-Fi security, too…

#6 Wi-Fi is the weakest link in your IT security

It would be a bit silly to argue that adding Wi-Fi has no effect on IT security. It does. Students, teachers and administrators will have to be authenticated wirelessly. Hackers on school premises could create honeypots to lure negligent users into vulnerable situations. Online wardriving sites allow nosy people to learn the location of the school that students and teachers attend. None of those things makes an IT person's job easier, and all of those things could cause embarrassment if a worst case scenario happens.

Let's be honest, though: the days of realistic, serious network attacks originating via the Wi-Fi link are over. Wi-Fi security is now strong, standardized and widely available.

Remember the story of the nationwide department store chain being hacked via Wi-Fi? Ain't happenin' today. Those hackers cracked WEP, and modern K-12 installations require WPA2.

Remember when a different nationwide department store chain was hacked because the HVAC repairmen made a mistake? That ain't happenin', either. Modern K-12 installations use separate VLANs for guest access, thus keeping vendors, repairmen and others away from sensitive internal data.

And the list goes on: Passwords aren't flying through the air, because every certified Wi-Fi device (since 2006, which is a year BEFORE the very first iPhone was announced) must support AES encryption. Bogus APs can't attract internal users because modern Wi-Fi devices won't roam unless APs are using identical WPA2 credentials.
Rogue APs are no longer a threat because wired ports are no longer left open. And so on, and so forth.

Wi-Fi is going to have an effect on K-12 network security, as any addition to a network would. But the days of it being a weak link have long since passed.

#7 Upgraded PoE is needed when upgrading APs

Let's begin with a non-myth (a.k.a. truth): With new standards, comes greater power requirements. When 802.11a became popular, dual-radio APs began being used. The additional radio required more power. When the 802.11n standard added MIMO, multiple radio chains became commonplace, thus increasing AP power requirements again. When 802.11ac Wave 1 made three-stream MIMO commonplace, it led to APs needing even more power. Now 802.11ac Wave 2 is here, and its support of four MIMO streams (and possibly up to eight streams in the future) has increased AP power needs again.

Where things get myth-ical is when switch upgrades are suggested in order to support newer PoE standards. It is true that the newer 802.3at (PoE Plus) supports an extra 12W of delivered power per port (25W, to be exact), but APs can still function when connected to switch ports that only support the older 802.3af (PoE) standard (which supports 12.95W of delivered power).

WARNING: Ruckus marketing content…

Though upgrading to PoE Plus is unnecessary in many cases, it is true that schools with a high concentration of desktops and laptops may see Wi-Fi speeds reduced when APs connect to switch ports that only support original PoE. Laptops and desktops may support 3-stream MIMO, and most enterprise APs reduce their available MIMO streams when the AP is short of power.

Ruckus does things differently (and better, in the case of PoE). Many competitive APs reduce their APs

to support fewer transmitters and receivers. For example, with high power PoE (802.3at), it may support 4x4:4 but with older PoE (802.3af) it will shut down two radios and will reduce it to a 2x2:2 AP. The Ruckus R710 (Wave 2 11ac) only shuts down the USB port and secondary Ethernet port when PoE power is insufficient for full operation, thus conserving enough power to keep Wi-Fi speeds at maximum levels.

#8 Increasing APs' transmit power increases coverage

To understand our eighth myth, the term "coverage" must first be defined. There are three possibilities, and we'll let you decide which one should mean "coverage":

1. "Coverage" means that devices can see the Wi-Fi network.
2. "Coverage" means that devices can see and connect to the Wi-Fi network.
3. "Coverage" means that devices can see, connect to and consistently access the Wi-Fi network.

OK, we lied. We're not going to let you decide. "Coverage" is number three.

Wi-Fi "coverage" simply isn't coverage unless devices can consistently access the Wi-Fi network. And, while increasing APs transmit power making it more likely that APs will be able to consistently SEND data to devices, it does absolutely nothing to make it more likely that APs will be able to RECEIVE data from devices. That's because increasing AP transmit power does not increase device transmit power. And without an increase in both AP and device transmit power, true coverage (using our third definition) is not going to be improved. (In fact, some devices actually REDUCE their transmit power when connected to a more powerful AP, thus creating worse coverage. The device may see a super strong signal and naturally reduce their transmit power in an attempt to prolong battery life).

WARNING: Ruckus marketing again…

Having APs with a higher transmit power than devices transmitting power, can improve coverage in one scenario: if the receive sensitivity of the AP is better than the receive sensitivity of the device. Ruckus just so happens to have the best receive sensitivity in the Wi-Fi business. So, while most vendors' Wi-Fi implementations work best with AP transmit power set somewhere in the 14 to 17 dBm range, Ruckus APs thrive with AP transmit power set as high as 19 or 20 dBm.

And don't ask us how we gave our APs a better receive sensitivity. That's part of the secret sauce. But, proving it is quite simple. Test a Ruckus AP versus the competition. You'll be able to connect and transfer data farther away with the Ruckus AP because of how well it can hear. We are like the best listener. Ever.

#9 Band-selectable AP radios improve performance

There are some things in life that make a whole lot of sense until they actually happen. The Run & Shoot offense — a mercifully deceased American football system created in the 1980s — was one of those. The Run & Shoot was designed to play the game as fast as possible, and with as much room for improvisation as possible. The designers of the Run & Shoot found that, statistically, football teams scored more often without using play-calling "huddles" that slow the game down. Run & Shoot designers also found that pre-designed plays could sometimes be predicted by the opposition, thus nullifying their effectiveness. (Players of early football video games became aware of this to great effect.) Thus, the designers of the Run & Shoot eliminated huddles and asked players to improvise,

rather than running pre-designed plays. And it worked beautifully.....until it was tested on the professional level. The Run & Shoot lasted only a couple of seasons in the NFL before its proponents were relegated to the lower levels of American football.

What went wrong with the Run & Shoot, you ask? Essentially, it's designers focused on the positive and overlooked the negative. The Run & Shoot was, in fact, effective at speeding the game up and making it more difficult for the opposition to predict plays. Unfortunately, speeding up the game backfired by reducing the amount of time that defensive players were allowed to rest. And using improvised plays backfired because improvisation naturally creates less precision than something that is pre-designed. At the elite level, that precision was essential for success.

The same essential flaw that sent the Run & Shoot to an early grave is present in the modern day Wi-Fi trend of band-selectable AP radios. Some APs now have one radio statically set to the 5 GHz frequency band, while the second radio can be set to either the 2.4 GHz or the 5 GHz band. And these band-selectable AP radios were designed by people who suffer from the same short-sightedness as the designers of the Run & Shoot suffered from: they are focusing too much on the positive and overlooking the negative.

The idea behind the band selectable AP is that since almost all devices support 5 GHz, why not just have more 5 GHz APs? On the surface that makes sense. But, there is more to the story. The positive of a band-selectable AP radio is that more channels can be used. Whereas, a small area covered by five traditional APs would only be able to take advantage of eight unique channels (channels 1, 6 and 11 in the 2.4 GHz band, with five unique channels being used in the 5 GHz band), an installation of five band-selectable APs would allow ten channels to be used. Two of the APs could have both radios set to the 5 GHz band, while the other three APs could have a traditional configuration with one radio each in the 2.4 GHz and 5 GHz bands. That sounds good, right? Ten channels instead of eight.

The negative of band-selectable AP radios is that interference becomes massive when two AP radios use the same frequency inside the same AP. A recent independent test of another vendor's band-selectable AP showed that single-device retries increased from 3% to 16% and throughput was almost cut in half when switching the band-selectable AP radio from 2.4 GHz to 5 GHz. Anyone who's done in-depth Wi-Fi troubleshooting will tell you that 16% retries when a single device is connected is going to mean an absolutely unusable W-Fi channel when dozens of devices connect, as commonly happens on K-12 networks.

While the folks who created band-selectable AP radios deserve some amount of credit for trying new things, they also probably deserve as much scorn as long time fans of the Detroit Lions have for Run & Shoot progenitor Mouse Davis. His two seasons coordinating the team's offense produced two losing records, a 0% record of success. And, rest assured, 0% of the schools with band-selectable AP radios will function optimally when a high density of users attempt to access the Wi-Fi simultaneously.

Now that we have identified the nine myths about K-12 Wi-Fi deployments, you can get your Wi-Fi to its optimal state. No longer are you in the dark on how to get the most out of your Wi-Fi without breaking the bank. When looking for that upgrade, put the suppliers to the test just like the saying goes, "I'll believe it when I see it." Performance speaks volumes and now with your new found knowledge on the myths, you can make an informed decision by asking all the right questions. Future-proof your network and provide this generation of kids instant access to a world without walls.

Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089 USA
(650) 265-4200 Ph \ (408) 738-2065 Fx