9 MYTHS ABOUT WI-FI IN HIGHER 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 approved 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, universities were Wi-Fi-hot spots. Many institutions lacked the budget for robust deployments, and many others avoided the technology for security or educational reasons.

Today, Wi-Fi is a reality on most campuses. And if it’s not a reality yet, it will be soon. Parents want their children to feel like University living is a ‘home away from home’ whether that’s from pictures on the desk (or more likely screen savers) or having all their electronics available to them, to their favorite apps. Wi-Fi is the technology of choice for getting students 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 campus 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 campus Wi-Fi deployments, and if these myths are avoided, there is a much better chance that campus Wi-Fi is going to work as promised. And even if your Wi-Fi network already avoids most of these myths, hopefully there will be something that will spark an idea that will help you get your Wi-Fi to its optimal state.

Now, let’s dig into some common myths about Wi-Fi deployments in campus education environments.

#1 The average college student brings 3 devices to campus

Empty a student's bag, and you're likely to find a laptop and a smartphone. Many also carry a tablet. Back in their dorm rooms, students may have hooked up a gaming console, wireless printer, AppleTV, smart TV, Blue-ray player, e-reader or more. And with the increase in wearable devices, like smartwatches and fitness bands, the number of devices brought on campus increases.

According to a re:fuel Agency's 2014 College Explorer report, the average college student brings seven internet-connected devices to campus.

All these devices are Wi-Fi enabled. All of these devices are trying to connect to campus Wi-Fi access points (APs).

As more students connect to the network for a wider variety of purposes, from academic research in the lab to multi-player gaming in the residence hall, it's getting harder for IT teams to meet growing expectation for 24/7 connectivity. If left unmanaged, network costs soar, compliance is compromised, and critical applications become harder to assure.

#2 More access points in high density area will ensure better wireless coverage

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, or every dorm room, 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, 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 complex and time-consuming, but a skilled integrator can produce a site survey that will save you both time and money in the long run.

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.

#3 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 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 classrooms, 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.

WARNING: Ruckus marketing content…

One other consideration is future proofing. If your campus only upgrades the campus wireless network every 5 or so years, then deploying Wave 2 will support your campus users until you're next budgeted refresh. This same question came up during the 802.11n => 802.11ac transition, where 98% of client devices were not 802.11ac, yet institutions which invested in 802.11ac refreshed at that time were well positioned when the wave of new clients came. It's always nice when you can get ahead of student demands and avoid the complaints, right?

#4 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, faculty and administrators will have to be authenticated wirelessly. Hackers on 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 campus installations require WPA2.

Remember when a different nationwide department store chain was hacked because the HVAC repairman made a mistake? That ain't happenin', either. Modern campus 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 network security, as any addition to a network would. But the days of it being a weak link have long since passed. Or at least should. Deploying the secure wireless network is straight forward. Getting users to migrate from the open network to the secure network? A bit tricky. No one wants to deal with passwords, multiple logins, opening IT trouble tickets, etc.

WARNING: Ruckus marketing content…

One method recommended to avoid the problems with passwords is an automated certificate delivery system and public key infrastructure (PKI) solution, such as Ruckus Cloudpath.

- Minimizes IT involvement in configuring devices by enabling any user to configure and provision each of their devices, using the exact same steps for each device. This could relieve your IT staff of the burden of touching devices and allow you to accomplish more strategic IT objectives.
- Minimize IT time required to set up security by enabling your administrator to establish a single policy independent of device or OS type. Time required to set-up campus-wide security is dramatically reduced and would allow you to accomplish more strategic IT objectives.
- Minimize the re-securing of devices that were once secured by enrolling devices automatically to join and re-join your secure network until certificates expire. Your IT staff doesn't waste time doing the same thing for the same devices multiple times per year and would allow you to accomplish more strategic IT objectives. This starting to sound familiar?

#5 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 mythical 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.

#6 Increasing AP transmit power improves coverage

In the early days of Wi-Fi, back when 802.11g was ‘wicked fast,’ WLAN professionals would describe areas of coverage as ‘circles’ drawn around access points. If the circles did not overlap at all, that was a coverage gap. To close the gap, one would either move the APs closer together, reduce the minimum data rate, or increase the transmit power.

However, starting with the advent of 802.11n, things got pretty wonky (a technical term meaning ‘even stranger and harder to understand’). To overcome one of the fundamental challenges of RF, multipath reflections, the IEEE incorporated into the standard the means to tame this beast by leveraging constructive interference of multipath reflections. However, this led to coverage patterns which more closely resembled Rorschach ink blots than circles on a map. Increasing AP transmit power may increase coverage, but is not the same everywhere, since multipath characteristics are different in each environment local to each AP. That made coverage planning more complex, and site surveys crucial.

To truly understand our sixth myth, though, 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 makes 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.

#7 Password-based Wi-Fi networks are secure

As the Wi-Fi network has grown from a luxury to an expectation, the value of Wi-Fi connectivity has multiplied, leading to always-connected options like eduroam. Meanwhile, the number of devices and the types of devices are expanding, making it more difficult to establish a favorable first impression with students, faculty and guests.

Password-based (PEAP, TTLS) networks experience high rates of user disruption based on password changes. Disconnected devices try to connect back to the network as many as 30,000 authentication requests per day per student.

An average on 20% to 50% of all help desk calls are for requesting password resets. The solution to the persistent Wi-Fi challenges in higher education has been available for a long time. It's certificate-based Wi-Fi, in the form of WPA2-Enterprise with EAP-TLS.

Certificates eliminate passwords from Wi-Fi, meaning that passwords are neither cached on devices, nor transmitted on every connection attempt, and connectivity continues to function in spite of password changes. In essence, a device registered one time should continue to function throughout the year without disruption.

This means happier users and fewer support tickets.

WARNING: Ruckus marketing again…

When security is so simple, there's no reason to leave visitors to fend for themselves on unsecure Wi-Fi. Our Cloudpath Enrollment System (ES) makes it incredibly simple to extend secure Wi-Fi to visitors of all varieties. Cloudpath ES goes beyond traditional guest servers by onboarding guests onto WPA2-Enterprise wireless networks without IT involvement.

No more annoying web logins; no more concerns about unsecure wireless. Your visitor, your network, and your reputation are all protected.

Cloudpath ES offers a variety of traditional authentication and authorization options, including sponsorship and self-verification. Beyond the traditional functionality, Cloudpath ES adds an industry first, patented integration of secure Wi-Fi with external identity services, such as Google, Facebook, and LinkedIn.

#8 All Access Points are Created Equal

To many purchasing managers, Wi-Fi is just Wi-Fi. It's a utility and one access point is as good as the next. To those who have to field the complaints and troubleshoot issues, we know this is not true. Now, there is a half-truth here. All major brand enterprise APs are based on standard chipsets, many use OEM reference designs, and all follow the IEEE 802.11 standards and proven interoperable thanks to Wi-Fi alliance testing.

However, is there room to do more above and beyond the standards?

Let's consider a typical college or university campus, and the unique deployment challenges lurking.

Wi-Fi challenges are everywhere on campus

The campus grounds - Students and faculty increasingly use cloud applications, online data storage and BYOD with the latest and greatest devices. They expect full-bar coverage and capacity from campus Wi-Fi networks anywhere, anytime. To accomplish this may require point-to-point bridging, mesh networks, and robust outdoor AP hardware and mounting options.

The Stadium - Staying connected with friends, family and social media is part of the fan experience. APs designed for stadiums must support density, reduce interference, hardened for outdoors, and feature integrated sectorized antennae to help with channel planning and implementation.

Residence halls and dorms are a nesting ground for all the latest gadgets, embedded Wi-Fi consumer electronics such as smart TVs, wireless printers, and Blue-ray players. And now wearables like smart watches, fitness trackers and even glasses! To make Wi-Fi work here, in hardened cinder block construction, requires in-room wall plate APs to deliver Wi-Fi signals up close and personal to students and their devices.

WARNING: Ruckus marketing again…

Ruckus goes above and beyond – building on the 802.11 standards, our engineers optimize the board design, antenna design and even the industrial design based on how the AP will be used or where it will deployed. Not all access points are created equal. Each vendor's products are different than one another.

Of course budget will always play a factor but always going cheap doesn't make any sense. It's about matching the solution with your requirements.

#9 More broadband solves most problems

OK, to be fair, this isn't completely a myth. We all love more broadband, right? If your students see 100Mbps download speed on their iPad running a speed test, would they grab a screen shot and post it to Instagram, or Tweet it out? You bet.

That said, the most frequent and obvious problem for which IT is blamed for poor Wi-Fi is slow broadband connectivity. The fastest Wi-Fi networks on the planet that can now deliver local connection speeds at hundreds of megabits per second to devices, come to a crawl if there isn't enough distribution or backhaul to the Internet. Even a 100Mbps Internet connection is too slow when you have hundreds of students served by a handful of APs in a lecture hall struggling to make and keep connections and provide airtime fairness. This makes Wi-Fi appear slow or unreliable. Another major problem, not directly related to Wi-Fi, is simply wired network design. Switching, routing and higher layer functions such as DHCP and DNS systems not configured correctly to support the explosion of Wi-Fi network connections can wreak havoc on the network but still appears to be a Wi-Fi problem.

But for IT professionals, there is more to managing a wireless network and driving down complaints than purely delivering broadband. Often it all comes down to student experience, and avoiding those dreaded "#campuswifisucks" tweets which cause the Chancellor to embarrass the CIO, who blames the Director of IT, who assigns the Network Engineer to 'fix it'. The 'problem' could be related to onboarding and passwords, network storms from Bonjour or interference in the residence hall, insufficient capacity in the

lecture hall, insufficient coverage in the quad, and so on – all unrelated to the bandwidth provided.

Now that we have identified the nine myths about Campus 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

Ruckus®
Simply Better Wireless.
www.ruckuswireless.com