10 MYTHS ABOUT WI-FI

Higher Education

WHITE PAPER

EXECUTIVE SUMMARY

Students arriving on campus today have lived their entire lives as “digital natives.” Smartphones and social media providing information at their fingertips and instant contact with anyone, anywhere—this is the world they’ve always known. These students—and their parents—are often choosing your institution to be their home, not just their school. And they expect a true “home-away-from-home” experience, with constant connectivity in residence halls, classrooms, and across campus.

To make this possible, you’re going to need Wi-Fi—strong, reliable, easily accessible Wi-Fi, anywhere, anytime on any device. If you haven’t made delivering this a priority, you better believe that other institutions have. Across higher education, colleges and universities are engaging in a “lifestyle arms race” to recruit students, and great Wi-Fi is a key weapon in their arsenals. In a survey conducted for the State of RESNET Report 2016,
73 percent of Business and Housing Officers said that they consider “at home” quality network connections important to attract and retain on-campus students.

Keep in mind, this generation of digital natives does not suffer silently. Twitter, Instagram, and Snapchat are all wonderful tools for students to vent their frustrations about the state of your network. If your Wi-Fi stinks, you’re going to hear about it. So is your boss, and most likely, the rest of the world.

Unfortunately, Wi-Fi in campus network deployments has a 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 to provide a good user experience. Most complaints center around two basic issues:

- Performance: If the Wi-Fi isn’t fast and reliable, nothing else matters. Spotty coverage, frequent dropouts, choppy video playback, and down- loads that take hours—these are major concerns for students who are making your campus their home.
- Access hassles: Password reset requests, onboarding headless devices, and thousands of students hitting campus and attempting to get online all at once—it all adds up to a huge headache for students and a nightmare for Help Desk IT. That’s not even mentioning the need to secure all those devices and connections.

Your students come to campus expecting that all of their devices will connect easily. They want to get homework done and play videogames with super-fast download speeds. They have no patience to constantly be entering passwords or calling the helpdesk. They expect Wi-Fi that just works. Are you giving it to them?

WE HAVE IDENTIFIED 10 COMMON MYTHS ABOUT COLLEGE AND UNIVERSITY CAMPUS WI-FI DEPLOYMENTS. AVOID BUYING INTO THEM, AND THERE’S A MUCH BETTER CHANCE THAT YOUR CAMPUS WI-FI WILL WORK AS PROMISED, AND YOUR STUDENTS WILL CHOOSE TO COME AND STAY.

#1 THE AVERAGE COLLEGE STUDENT BRINGS THREE DEVICES TO CAMPUS.

Empty a student's bag, and you're likely to find a laptop and a smartphone. Many also carry a tablet or e-reader. Back in the residence hall, students may have hooked up a gaming console, wireless printer, Wi-Fi speakers, AppleTV, smart TV, Blu-Ray player and more. Add in wearable devices like smartwatches and fitness bands, and the notion that students are bringing just three devices to campus—which may have been true a few years ago—starts to look downright conservative.

According to a re:fuel Agency's 2015 College Explorer report, the average college student brings seven internet-connected devices to campus, and upgrades devices frequently.

All of these devices are Wi-Fi enabled, and they are all 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 expectations for 24/7 connectivity. If left un-managed, network costs soar, compliance is compromised, and critical applications become harder to assure.

#2 MORE ACCESS POINTS IN HIGH-DENSITY AREAS WILL ENSURE BETTER WIRELESS COVERAGE.

It's a common misconception in many areas of life—not just Wi-Fi—to think that throwing money at a problem will solve it. Just like having the highest payroll in baseball the last few years didn't buy the Dodgers a title, buying APs like they're going out of style won't necessarily translate to better performance. In fact, extravagant, over-deployed Wi-Fi networks consistently prove inferior to measured, incisive installations.

Why? Because adding APs to a Wi-Fi deployment can add capacity to a point, but add too many and they become counter-productive. When you over-deploy APs, you increase the likelihood of more than one AP communicating with the same device over the same channel—(a phenomenon known as co-channel interference) which degrades performance.

Imagine standing in a lecture hall running the wireless scan function on your iPad. Your device would see the AP in the room you're in, as well as the AP in the room(s) next door, all operating on the same channel at a signal above -80 dBm. For devices using the 2.4 GHz frequency band (the band with the broadest support among consumer devices), there are only three non-interfering channels available in North America. So, if you have APs installed in every classroom, or every dorm room, it's a virtual certainty that your users' smartphones, tablets and laptops will "see" more than one AP covering the same channel. Think about driving to work, listening to your favorite song on your local radio station, and hearing another song cut into it as you approach a different radio station that's broadcasting over the same channel—it's that same kind of interference messing with your Wi-Fi connections.

For some campus Wi-Fi installations, APs are configured with low transmit power settings in order to give the illusion that over-deployment has been avoided. Don't fall for this. Wi-Fi is a two-way communication technology (meaning that smart-phones, tablets and other Wi-Fi devices must transmit to APs, as well as receive). So, if you have a high concentration of users (like in a residence hall or lecture hall), decreasing AP transmit power won't prevent co-channel interference.

Don't create new problems for yourself by buying into the "one AP per room" myth. The best way to really get the best performance? Commission a properly done site survey before choosing AP installation locations. Site surveys can be expensive and time-consuming, but a skilled integrator will save you both time and money in the long run by helping you get the best coverage and capacity for your campus.

WARNING: RUCKUS MARKETING CONTENT...

Ruckus Wireless BeamFlex+ Technology is a unique antenna system that dynamically creates directional antennas while supporting device connections in an omni-directional pattern. This means that APs mounted in hallways—out of sight and out of mind from students and faculty—can transmit and receive a strong enough signal, even through classroom or dorm room walls. It also means that external, directional antennas—which can add complexity and cost to AP mounting—are unneeded. Having BeamFlex antennas inside of Ruckus APs even 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 recent top dog 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 even before 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 hard ware is equivalent. The chipsets for 802.11ac Wave 1 are more modern than the chipsets for 802.11n, and chipsets matter.

802.11 ac Wave 2 is now available, but it will be a while before it becomes the dominant Wi-Fi technology for users. Most APs now support 802.11ac Wave 2, and a growing number of new smartphones, tablets, and laptops do as well. But many still don't—including Apple devices, which are notorious for implementing new Wi-Fi standards late.

It is this lack of available Wave 2 devices that has caused this myth to propagate. "Without Wave 2 de-vices, 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 widely 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: 802.11 Wave 2 devices still make up a relatively small percentage of the wireless devices in use today. If you deploy Wave 2 APs in a residence hall, most smartphones and tablets used by students will still max out at the same data rates as if you'd deployed Wave 1 APs. Also, some devices may never use some of the new standard's more intense performance-enhancing protocols, like Transmit Beamforming (TxBF) and Multi-User Multiple Input, Multiple Output (MU-MIMO), because they can have side effects like more channel over head or shorter device battery life.

But here's the thing: just because a lot of your users' smart phones and tablets won't use all of the enhancements of 802.11ac Wave 2 doesn't mean that their devices won't benefit from a Wave 2 upgrade. 802.11ac Wave 2 APs use a more mod ern chipset, which offers better receive sensitivity than Wave 1 APs. This 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.

It's also worth noting that just having newer technology—even apart from the 802.11ac Wave 2—does provide value. Later-generation APs support newer connections, such as 2.5GbE ports, or USB for IoT dongles that let you add things like Bluetooth LTE location services or power peripherals (such as a video camera mounted on the same pole as the AP). Advances like these have nothing to do with 802.11ac Wave 2, but they're unlikely to be included on APs using previous-generation radio technologies. 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 more devices support it.

WARNING: RUCKUS MARKETING CONTENT...

One other consideration is future proofing. If your campus only upgrades the campus wireless network every five years or so, then deploying Wave 2 will support your campus users until your next budgeted refresh. This same question came up during the 802.11n => 802.11ac transition. At the time, 98 percent of client devices were not 802.11ac. But institutions that invested in 802.11ac refreshes 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 silly to argue that adding Wi-Fi has no effect on IT security. Students, faculty and administrators can be authenticated wirelessly. Hackers on premises can create "honeypots" to lure negligent users into vulnerable situations. Online "wardriving" sites can show nosy people the location of the school that students and teachers attend. None of those things make an IT person's job easier, and all of those things can cause embarrassment if a worst-case scenario happens.

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

Have you seen stories in the past about department stores being hacked via the Wi-Fi? That isn't happening today. Those hackers cracked WEP, and modern campus installations require WPA2 Enterprise.

Remember when another nationwide department store chain was hacked because the HVAC repairman made a mistake?

That isn't happening again either. Modern campus installations use separate VLANs for guest access, thus keeping vendors, repairmen, and others away from sensitive internal data.

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. Deploying a secure wireless network is straightforward. But getting users to migrate from the open network to the secure network? A bit tricky.

WARNING: RUCKUS MARKETING CONTENT...

One method for avoiding the password problem is an automated certificate delivery system and public key infrastructure (PKI) solution, such as Ruckus Wireless Cloudpath software. Solutions like these:

- Minimize 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 all those student 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, allowing you to accomplish more strategic IT objectives.
- Minimize the re-securing of devices one they've been 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, allowing you to accomplish more strategic IT objectives. This starting to sound familiar?

#5

IF YOU'RE ADDING OR UPGRADING APS, YOU'RE GOING TO NEED MORE SWITCHES.

Wireless traffic has to go somewhere and at the end of the day, it all lands back on your wired infrastructure. Wireless APs connect back to ports on an Ethernet switch, so if you're adding more APs, you'll need more ports. If there are no available ports on your existing switches, then yes, you'll need to buy more switches. However, if you do have enough available ports, then adding APs or upgrading (and replacing) existing APs doesn't necessarily mean you also have to add or upgrade your wired switches. The question is whether your current switching infrastructure will provide adequate performance.

The performance of a network—and this is true of any network—is a function of its weakest link. You need to figure out where the potential bottlenecks are. Even the best designed wireless network won't deliver stellar Wi-Fi performance if the underlying switch infrastructure can't get the data to and from your broadband Internet connection quickly and efficiently. Ideally, you should balance your network so that each component of the network delivers comparable performance.

Here are a few things to consider when deciding whether to purchase more switches or upgrade existing switches:

Downlink port speeds: This is the connection between the wireless APs and the switch. You'll want switch ports that support the maximum connection speed of the ports on the AP. Connecting a 1GbE port on an AP to a 100M port on a switch will work, but it will limit the amount of data that can be transferred—effectively slowing down the AP. Alternatively, you can invest in switch ports that support higher speeds than the AP and they'll work fine, but they won't provide any incremental performance gains. You'll just be paying for more than you need.

Uplink (or "backbone") speeds: Many existing switches are connected upstream, to an aggregation switch or core router, at 1GbE. That was fine with 802.11g or even 802.11n, but the newer 802.11ac APs can transmit 1 Gbps, or more, each. If you're going to connect 10+ APs to a single switch, then combined they could be transferring 10 Gbps or more. If the switch uplink speed is only 1 Gbps, you could be looking at significant delays when there is a lot of activity on the Wi-Fi network. Most organizations today are upgrading their switch networks to 10GbE and, given the rapid growth in Wi-Fi usage, many are leap-frogging directly to 40GbE. Consider how many APs will be connected to the switches and what peak Wi-Fi loads you're likely to see.

You should also think about oversubscription of the switch. If all the ports on the switch are being used, can the switch transmit all that data upstream? If not, then it's oversubscribed, and there may be some network delays. Consider how much data is likely to be pushed through the switch, and if there are delays during those times when everything is running at peak, how big of a deal will that be?

PoE/PoE+ power: These days, most wireless access points deployed on campuses draw Power over Ethernet (PoE) connections rather than from dedicated power supplies. Some APs can run on PoE (15.4 Watts) and others require PoE+ (30 Watts). Most PoE switches today support both standards. The question is, how many ports are on the switch that can support PoE or PoE+, and the switch's total PoE budget. If you plan to connect 48 APs that require PoE+ to a switch, then all 48 ports on that switch will need to support PoE+, or in other words, provide a total PoE budget of 1440 Watts (48 ports x 30 Watts).

Beyond these considerations, a big challenge is anticipating how these requirements will change and grow over time. How well will the switch infrastructure support your requirements over the life of the switches—typically 5 to 7, or perhaps up to 10, years? How easily can this network expand to support more APs, future wireless standards, higher application network demands, etc.? Can the existing switches be upgraded (e.g., can you upgrade the uplinks from 1G to 10G or 40G without having to replace the entire switch)?

WARNING: RUCKUS MARKETING CONTENT...

Ruckus ICX switches deliver high performance (i.e., non-blocking, no oversubscription) and high PoE budget options, including support for PoE+ on all ports, and the latest Power-over-HDBaseT (90 Watts) standard. They also include future-proofing features such as uplinks that are software upgradable from 1G-to-10G, advanced stacking of up to 12 switches, and Campus Fabric capabilities that allow you to manage different ICX product families, up to 1700+ access ports, as a single domain (i.e., one IP address). Our customers know that the network they've purchase from us will easily grow and expand to meet their future network requirements for 7–10 years.

#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 APs. If the circles did not overlap, 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 constructive interference of multipath reflections into the standard. However, this led to coverage patterns which more closely resembled Rorschach ink blots than circles on a map. In this new world, increasing AP transmit power can increase coverage, but that doesn't hold true everywhere, since multipath characteristics are different in each environment, local to each AP. All of this has 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 choices—we'll let you decide which one is correct:

1. Coverage = devices can see the Wi-Fi network.

2. Coverage = devices can see and connect to the Wi-Fi network.

3. Coverage = devices can see, connect to and consistently access the Wi-Fi network.

OK, we lied. We're not going to let you decide. The correct definition of coverage is number three.

Wi-Fi "coverage" simply isn't coverage unless devices can consistently access the Wi-Fi network. And, while increasing an AP's transmit power makes it more likely to consistently send data to devices, it does absolutely nothing to make it more likely to receive data from devices. That's because increasing AP transmit power does not increase device transmit power. And without an increase in both, true coverage won't 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 its transmit power in an attempt to prolong battery life.

WARNING: RUCKUS MARKETING AGAIN...

Having APs with a higher transmit power than devices' transmit 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 some-where in the 14 to 17 dBm range, Ruckus APs thrive with AP transmit power set as high as 19 or 20 dBm.

Don't ask us how we gave our APs so much better receive sensitivity—that's part of our 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 listeners, ever.

#7

YOU SHOULD EXPECT ONBOARDING AND PASSWORD PROBLEMS TO MAKE UP HALF OF YOUR HELPDESK CALLS—AND THERE'S NOT MUCH YOU CAN DO ABOUT IT.

For digital natives—and really, for anybody—the best network in the world will go unused if it's a hassle to find, access, and connect to. Unfortunately, that's often the case on campus.

Take move-in day: thousands of students arriving on campus, bringing tens of thousands of devices. They expect to connect them all to the campus Wi-Fi right away. That includes their "headless" devices—wireless printers, Fitbits, gaming consoles, etc. Are you ready for the onslaught?

By the way, how are you securing all those devices? Many universities today rely on password-based access (using PEAP or TTLS), but these rarely translate to good experiences for students or IT. Students may be forced to re-enter credentials every time they disconnect from and reconnect to the network, multiple times per day. And every time a student resets their password, they have to manually reconnect all their devices (and hope they doesn't get locked out of their account). When we talk to colleges and universities, they tell us that 40, 50, in some cases 60 percent of their helpdesk calls are about pass- word-related issues.

It's no surprise that many universities have thrown up their hands. They've resigned themselves to the idea that onboarding is just going to be a massive headache on move-in day, requiring a huge, hands-on IT surge. And they assume that the avalanche of trouble tickets associated with passwords—forgotten passwords, insecure passwords, account lock-outs, and constantly having to re-enter credentials—just comes with the territory.

Luckily, colleges and universities don't have to throw in the towel, this myth is just that—a myth. Wi-Fi access doesn't have to be a pain for your students and a full-time job for IT. Follow these three steps to make things a lot easier:

- Use certificate-based access: The solution to hassle-free Wi-Fi access has been around for a long time: certificate-based Wi-Fi. Certificate-based access uses the gold standard in encryption, WPA2-Enterprise with EAP-TLS, which is synonymous with strong network security and has never been hacked. At the same time, when you use certificates as the authentication key, you eliminate most of the problems associated with passwords. Users can change passwords when- ever they choose without interrupting access. They can register a device once and not worry about it getting kicked off the network until the certificate is set to expire, often not until the next year.
- Use simple, self-service onboarding: Modern certificate-based onboarding platforms are fully automated and self-service. Users can just log onto the campus portal with their credentials for a one-time setup process. They see a simple, web-based wizard to join the secure campus network from practically any device or OS—on their own, 24/7/365. Their device installs a small package that configures and connects it to the right secure SSID—with no middle man and no call to the helpdesk. That device is now online, IT didn't have to touch it, and it only took a few seconds. After this one time set up, devices will connect automatically, with no login prompts.
- Use "pre-boarding": You don't have to limit automated self-service to your campus geography. You can use "pre-boarding", a feature that lets you send incoming students a link to the portal as part of a welcome packet, before they have ever stepped foot on campus. Incoming students can onboard their devices from home, on their own time, and they'll automatically connect when the student arrives on campus. Instant access without the hassles on move-in day—making their lives (and IT's) a lot easier.

WARNING: RUCKUS MARKETING AGAIN...

Ruckus Wireless Cloudpath Enrollment System (ES) software provides secure, self-service certificate-based onboarding for higher education. It's a simple, integrated solution designed specifically for busy BYOD environments like campuses. It delivers the right capabilities and security, with policy management for wired and wireless clients, and is vendor-agnostic so will work with your existing infrastructure.

#8

ALL ACCESS POINTS ARE CREATED EQUAL.

To many purchasing managers, there persists this notion that Wi-Fi APs are just a commodity. Wi-Fi is just Wi-Fi, the thinking goes. All products are based on the same OEM board designs, designed to a common standard of interoperability, and the same across vendors. It may be tempting to believe that Wi-Fi is just a utility these days, and one AP is as good as another. But if you're the one who has to field the complaints and troubleshoot issues, you know this just isn't true.

All major brand enterprise APs use standard chipsets and OEM reference designs, follow the IEEE 802.11 standards, and offer proven interoperability thanks to Wi-Fi Alliance testing. But there's a lot of room to go above and beyond the standards, and not every AP vendor takes that next step.

Unfortunately, some AP vendors offer "cheap" APs that look great on a bill of materials but often perform poorly. Using off-the-shelf OEM board designs and basic AP antennas with no RF performance optimization allows vendors to sell APs at bargain-basement prices. If your vendor is offering "too good to be true" pricing on your APs, that's a red flag that you may be looking at a lower-performing, off-the-shelf design.

Fortunately, that's not the only option. By using a highly optimized board design and antenna innovation, high-performing APs can deliver 6dB stronger signal and 9dB less noise from an RF perspective, resulting in superior performance as measured scientifically by signal-to-noise ratio (SNR). Luckily, you don't have to pore over stats on a data sheet to see this improved performance. Test out a standard OEM board design AP vs a performance-optimized AP in your own environment, and compare download speeds versus distance to mobile clients. You'll see the difference pretty quickly.

When evaluating APs, you should also consider the unique deployment challenges lurking in the diverse environments of a typical college or university. 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 Wi-Fi networks anywhere, anytime. To accomplish this, networks 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 now part of the fan experience. APs designed for stadiums must support high density, reduce interference, be hardened for the outdoors and feature integrated sectored antennae to help with channel planning and implementation.
- Residence halls and dorms: Guests and residents today have all the latest gadgets—smartphones, tablets, laptops, and embedded Wi-Fi consumer electronics such as smart TVs, wireless printers, and even smart watches and other wearables. To make Wi-Fi work in these locations, with hardened cinder block construction, it requires in-room wall plate APs to deliver Wi-Fi signals up close and personal to users and their devices.

WARNING: RUCKUS MARKETING AGAIN...

Not all access points are created equal. Ruckus APs go well above and beyond basic 802.11 standards, using optimized board, antenna, and industrial designs based on how the AP will be used or where it will be deployed. Of course, budget will be a factor, but going cheap doesn't always make sense. It's about implementing a solution that will actually meet the requirements it was deployed for.

#9

MORE BROADBAND SOLVES MOST PROBLEMS.

OK, to be fair, this isn't completely a myth. We would all love more broadband, right? If your students see 100Mbps download speeds 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 that causes students to complain about poor Wi-Fi (and blame IT) is slow broadband connectivity. Yet in many cases, the Wi-Fi really isn't the problem. The fastest Wi-Fi networks on the planet, which 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 that are 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. Yet this will still appear 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. Let's avoid those dreaded "#campuswifisucks" tweets that cause the Chancellor and CIO to be so embarrassed that they blame the Director of IT, who then 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.

#10 THERE ARE NO GOOD OPTIONS TO IMPROVE CELLULAR COVERAGE IN BUILDINGS.

One of the most pernicious problems on college and university campuses is poor cellular coverage in buildings and residence halls. Even if the Wi-Fi is great, if students can't get reliable mobile voice calls, e911, SMS texting, etc., they're not going to be happy. Of course, the fact that students in a residence hall can't connect to Verizon isn't your fault. But that won't prevent them from Tweeting out "This campus sucks! I'm paying all this money and I can't even use my phone." Which is why nearly 60 percent of university Building and Housing Officers, according to the State of RESNET Report 2016, are looking for ways to give students more bars of cell coverage in buildings. And looking... And looking...

You could build your own cell towers, but that's very expensive and takes years of planning. You could ask cellular carriers to build new towers for you (good luck with that). You could try small cells, but the complexity and limitations of the technology have caused most universities to decide it's not worth the hassle. Many universities are now looking at distributed antenna systems (DAS) to try to fix the problem, but since DAS was originally designed for large, high-end venues, it is really expensive and complex to deploy. Even if you bite the bullet and deploy DAS anyway, you end up with coverage for just one mobile carrier.

So technically, it isn't a myth that there's no good way to improve in-building cellular coverage. But very soon, it will be.

The FCC recently allocated 150 MHz of radio spectrum in the 3.5 GHz band to support Citizens Broadband Radio Service (CBRS)—a new shared LTE broadband technology that's open to everyone. When CBRS solutions hit the market, universities will be able to add vendor-neutral cellular coverage as easy as snapping an LTE module into supporting Wi-Fi APs. They'll be able to provide five bars of LTE roaming wherever they have Wi-Fi, connecting users to any mobile carrier that's in the CBRS Alliance. Schools will also be able to set this up on their own, without the complex and expensive professional services engagement with mobile carriers.

Note that all of these benefits are described in future tense. That's because, while CBRS is real, and vendors are developing CBRS solutions for Wi-Fi APs, handheld devices that can support CBRS aren't on the market yet. But they're coming—the first are slated to appear in late 2017, with many new devices expected to support CBRS in 2018 (just like 802.11ac devices first trickled to campus initially, then exploded on the scene).

So yes, if you want to improve in-building cellular coverage right now, you still might be stuck. But look at it this way: if you're currently budgeting for a DAS system (typically hundreds of thousands of dollars), your project won't actually go live until right about the time that CBRS goes mainstream. Why make that huge capital investment when a better, much less expensive option is right around the corner? By putting off your in-building cellular project by a year, you could save enough to refresh your entire Wi-Fi infrastructure.

Now that we've identified the myths of campus Wi-Fi deployments, you can get your Wi-Fi to its optimal state. You are no longer in the dark on how to secure your Wi-Fi and get the most out of it without breaking the bank. When looking for that upgrade, put the suppliers to the test.

Like the saying goes, "I'll believe it when I see it." Performance speaks volumes, and now with your newfound knowledge on these myths, you can make an informed decision by asking all the right questions. Future-proof your network and provide the new generation of digital native students with instant access to a world without walls.

READY TO GET STARTED? WATCH OUR ON DEMAND WEBINAR TO LEARN MORE ABOUT HOW CAMPUS NETWORKS CAN ATTRACT AND RETAIN STUDENTS, OR REQUEST A DEMO TO PERSONALLY SEE WHY RUCKUS IS THE PERFECT FIT FOR YOUR CAMPUS.

RUCKUS™ an ARRIS company

350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckusnetworks.com