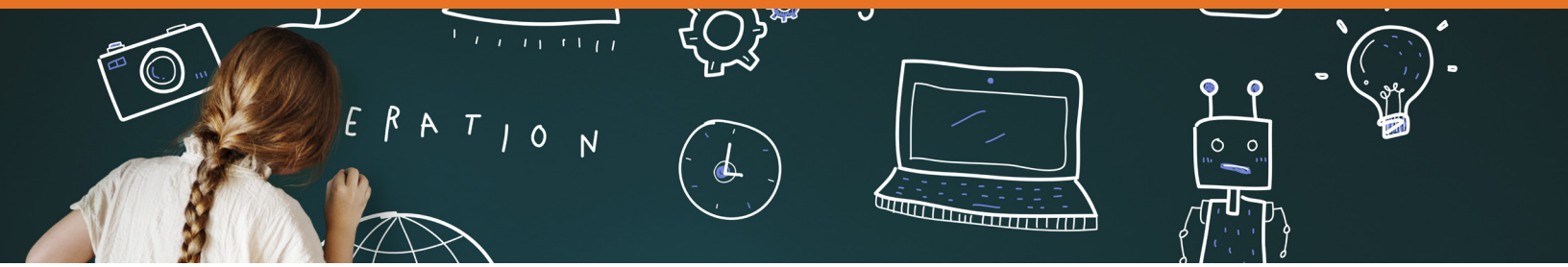
9 MYTHS ABOUT WI-FI

K-12 Education

WHITE PAPER



EXECUTIVE SUMMARY

Squint a little bit—and ignore the lack of color-coded pajamas—and the modern classroom might as well be Starfleet Academy (go watch Star Trek if you don't get the reference. It is great). Faculty and students tapping away at their touchscreens and interactive digital learning platforms. 4K video and collaboration connecting students to content and people everywhere in the world. Lighting, security cameras, thermostats, and a hundred other devices all networked together in smart classrooms and campuses.

Primary education is becoming a bold new frontier where no one has gone before. The growing use of Wi-Fi in public education is playing a big part in making this new frontier a reality. And while it's easy to get caught up in the sci-fi vision of tomorrow, school IT administrators face more mundane—and much more pressing—questions right now:

- How can I scale my Wi-Fi network to deliver uninterrupted access for 1:1 computing, digital curriculum and mobile learning—not to mention all the kids using Instagram and Spotify?
- How will my underlying wired network handle huge and growing bandwidth demands?
- How can I protect my students (and my school's reputation) when student data now lives everywhere?
- How can I position my infrastructure to evolve with what's coming down the road, without having to rip and replace it?

Look around the marketplace and media, and you can find proposed answers to these questions. Unfortunately, many of them aren't worth the pixels they're printed on. The reality is, despite many schools spending a lot of time and money trying to make smart choices about their Wi-Fi investments, many are still struggling with performance and security.

TO COMBAT THIS ISSUE, WE'VE IDENTIFIED NINE COMMON MYTHS ABOUT SCHOOL WI-FI DEPLOYMENTS. AVOID BUYING INTO THEM, AND YOUR SCHOOL AND DISTRICT WI-FI WILL EXCEED YOUR EXPECTATIONS.

#1

WANT TO BOOST YOUR WI-FI SPEEDS? YOU'LL NEED TO REPLACE YOUR WIRED SWITCHES.

Almost all fancy new classroom technologies—laptops, tablets, digital learning applications, online games and apps—now connect over the Wi-Fi network, and they're chewing up huge amounts of bandwidth. It's a good thing that new wireless technologies, like 802.11ac, can deliver big increases in throughput—you're going to need every bit of it. But that wireless traffic must go somewhere, and at the end of the day, it all lands back on your wired infrastructure. Consider that the future holds more devices in the classroom, more digital curriculum, and more IoT endpoints, and you might as well just accept that you're going to have to continuously rip and replace your wired network to keep up, right? Not exactly.

It's true that growing wireless traffic is putting pressure on schools' wired infrastructures. According to the 2016 Funds for Learning E-Rate Trends Report, 65 percent of school IT administrators expect their bandwidth demands to grow by 50 percent or more in the next three years, and a quarter of respondents expect demand to double in the same period. Considering schools typically update their wired infrastructure every six years, bandwidth demands could quadruple before the next refresh cycle.

It's easy to look at the numbers and think that there's no good way to close the gap. You could vastly over-provision your wired infrastructure to handle six years worth of escalating demand (because most schools have extra cash laying around for projects like that, right?). Or, you could just reassign yourself to overhauling the wired network every few years.

There's a better option. You don't have to spend more, just spend smarter. New switching platforms are built to be scalable, allowing for continuous bandwidth upgrades without a rip and replace.

WARNING: RUCKUS MARKETING CONTENT AHEAD...

The Ruckus ICX portfolio of simple, field-upgradeable switches is designed to support the most demanding networks—both today and in the future. Scale from 1 GbE ports to 10 GbE with a simple software upgrade. Go from 10 GbE to 40 GbE just by snapping a new module into the switch you already have deployed. You don't have to invest today for the capacity you don't yet need. Our ICX switches can evolve with your school—deploy once, and continue using the same Ruckus infrastructure for five, seven, or even 10 years without having to rip and replace.

#2

ONE AP PER CLASSROOM PROVIDES OPTIMAL PERFORMANCE.

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 access points (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, inclusive 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 classroom 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, it's a virtual certainty that your users' smartphones, tablets, and laptops will "see" more than one AP covering the same channel, leading to device interference. Picture driving to work, listening to your favorite song on your local radio station, when you hear another song cut in from a different radio station that's broadcasting over the same channel—it's the same kind of interference messing with your Wi-Fi connections.

For Wi-Fi installations in school environments, some 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 smartphones, 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 typical classroom), decreasing AP transmit power won't prevent co-channel interference.

Don't create new problems for yourself by buying into the "one AP per classroom" 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 school.

#3

CLOUD-MANAGED WI-FI MAKES IT SIMPLE TO DELIVER A GREAT WI-FI EXPERIENCE.

It's tempting to hear "cloud-managed wireless LAN" and assume that all of the complexities of a traditional wireless network magically go away. Just hand everything over to those wizards in the cloud, and your infrastructure will now work all day, every day, no matter what you throw at it. Unfortunately, that's not quite the case.

Here's the thing: cloud management does exactly what the name says: manage your Wi-Fi infrastructure. And it does a great job of it, but most of the problems that lead to poor wireless performance (slow connection speeds, dead spots, disconnects, and more) have nothing to do with management. A streamlined management interface won't eliminate sources of interference in your airspace, make your wireless signals travel more consistently through brick or concrete, or let you support more clients with the same infrastructure.

At the end of the day, your ability to deliver a great Wi-Fi experience comes down to the technology you use at the point where devices connect—in the APs on the wall or mounted on the ceiling. Managing those APs from the cloud can make life easier for onsite IT staff, but it doesn't make performance problems go away. Here's a dirty little secret: it can actually make them worse. That's because some cloud-managed Wi-Fi solutions, aiming to keep prices as low as possible, cut corners in their APs. They use off-the-shelf board designs from contract vendors and lowest-common-denominator antennas. No matter how much people might love the management software, it is still chained to sub-optimal AP technology. And unlike the cloud software, which can be updated at any time, once an AP is deployed, that's the antenna and RF ability you get for its years of service.

Fortunately, the newest generation of cloud-managed Wi-Fi solutions don't force you to make those tradeoffs. Some of the latest cloud Wi-Fi architectures and AP designs can provide the high performance and reliability you need, while allowing for simple deployment and management through the cloud. So, while the notion that cloud management will make all your problems go away really is a myth, it is indeed possible to have the best of both worlds. You can marry best-in-class AP performance with simple cloud-based management. And if you're considering moving to the cloud, you should demand nothing less.

WARNING: RUCKUS MARKETING CONTENT AHEAD...

Our cloud-managed Wi-Fi solutions use the same AP technology as our traditional wireless solutions that are managed on-premise—and deliver the same industry-leading performance. We bake groundbreaking Wi-Fi innovations into our APs that no one else can deliver. That includes our patented BeamFlex+ adaptive antenna system with polarization diversity, which dynamically reconfigures antenna patterns to provide the best possible connection with every client connecting to them. It also includes smart channel selection, roaming, multimedia QoS, and other Ruckus innovations to deliver the industry's strongest, most reliable connections in even the most contentious airspace.

#4

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 hardware is equivalent. The chipsets for 802.11ac Wave 1 are more modern than the chipsets for 802.11n, and chipsets matter).

802.11ac 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 high school, most smartphones and tablets used by students and faculty 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 overhead or shorter device battery life.

But here's the thing: just because a lot of your users' smartphones and tablets won't use all of the enhancements of 802.11ac Wave 2, it doesn't mean that their devices 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. 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 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.

#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 school Wi-Fi networks. First: they use Internet bandwidth. Second: they don't support the same high Wi-Fi speeds that tablets and laptops do, which are often used for education.

The argument that student smartphones' use of internet bandwidth will affect network performance is sound in some ways, and flawed in others. All elementary, middle and high schools have a finite amount of Internet bandwidth coming in and going out. If students use their smartphones on the school's Wi-Fi network for non-education activities, that leaves less available Internet bandwidth for education. Yet, the vast majority of Internet traffic is bursty, and therefore 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 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, but all of that is also specious. Prohibiting students from connecting to a 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). Devices use Probing to gather information about nearby APs. But, 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 search for APs that are nearby.

The problem with Probing is that it can—and often does—take up more Wi-Fi channel time than actual network data. Probe Request frames (a.k.a. "packets") 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. Therefore, 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 method for getting optimal performance out of school Wi-Fi is to allow students' and employees' personal devices to connect to the network. But what about security? Well, there is a myth about Wi-Fi security, too...

#6

WI-FI IS THE WEAKEST LINK IN SECURING STUDENT DATA PRIVACY.

Let's start with what's not a myth: protecting student data is a big challenge—and it gets even bigger the more schools embrace connected classrooms and personalized learning. With new devices, connections and applications comes a huge amount of student data that you're now responsible for, including identification numbers, addresses, test scores, disciplinary records, information about special needs, and assistance programs. That data is now practically everywhere, both at rest (in databases and servers) and on the fly (traversing connections between devices and networks, school sites, data centers and the cloud).

If that sounds like a big, scary security challenge, it is. Under federal law, school districts can be held liable for not taking reasonable measures to protect against a data breach. Even worse, schools that fail to secure student data risk seeing their names in the headlines. You too could see your face on the news, getting peppered with unpleasant questions about what went wrong and why you failed!

So yes, securing student data is a big deal. But let's get to the myth part: Wi-Fi is not the weak link in your security. Wi-Fi security is among the strongest mechanisms available today. If you're using WPA2 EAP-TLS encryption for all wireless traffic (and you should be), you're protecting your data with the gold standard in wireless security, using an encryption algorithm that's never been cracked. Therefore, you can rest assured that—as far as hackers pulling confidential data out of the air—your Wi-Fi is at least as strong, if not stronger, than your wired network.

That doesn't mean there aren't big challenges involved with securing all those new student and faculty devices. If you're still relying on MAC authentication and pre-shared keys—and if you're still using passwords as a major line of defense—you may be in for a world of hurt. MAC addresses can be easily spoofed. Pre-shared keys are… well… shared. And passwords rely on people not using the same password across all their devices and apps, not storing their passwords where others can see them, and not forgetting them. Unfortunately, people really are the weak link in your security. According to the Intel Security Report Grand Theft Data, nearly half of all school data breaches came from inside the organization, and half of those were accidental.

A great firewall isn't going to solve this problem. Strong encryption won't solve it either. What you need is a way to ensure that only authorized devices and users can access sensitive information in the first place. To do that, you should be using certificate-based access (instead of passwords) for all school- and student-owned (BYOD) devices. In addition, your certificate framework should be tied to sophisticated identity and policy management, so you can control who is able to access what at a granular level.

WARNING: RUCKUS MARKETING CONTENT AHEAD…

Ruckus Cloudpath Enrollment System (ES) software makes secure wireless connectivity simple for IT by providing self-service, certificate-based onboarding. It's a simple integrated solution that provides fast connectivity for students, staff, and guests using their own devices on-campus. At the same time, it improves security by automating the enforcement of the appropriate access policies for each user and device. Best of all, it is vendor neutral, working with any enterprise WLAN or wired switch you may have.

You can eliminate the risks and hassles of password-based security while automating access controls, use policies, authentication, and network privileges. Cloudpath ensures that both users and their devices can only access sensitive data if they meet stringent security requirements. You can automatically encrypt wireless traffic and track all users, devices, and policies in real-time to identify and address issues. And you can automate the provisioning of security certificates for Wi-Fi access and web authentication of all devices—including Chromebooks.

#7 UPGRADED POE IS NEEDED WHEN UPGRADING APS.

Let's begin with a non-myth (a.k.a., truth): With new standards come 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 tricky is when someone suggests you need to upgrade your wired switches to support newer Power over Ethernet (PoE) standards. It's 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 AHEAD…

Though upgrading to PoE Plus is unnecessary in many cases, 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 competitors scale back their APs to support fewer transmitters and receivers as power needs increase. For example, with high power PoE (802.3at), the AP may support 4x4:4 but with older PoE (802.3af) it will shut down two radios, reducing it to a 2x2:2 AP. With the Ruckus R710 (Wave 2 11ac), when PoE power is insufficient for full operation, the AP only shuts down the USB port and secondary Ethernet port. This conserves enough power to keep Wi-Fi speeds at maximum levels.

#8

INCREASING AN AP'S TRANSMIT POWER INCREASES COVERAGE.

To understand our eighth myth, 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 somewhere 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 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

MYTH #9: BAND-SELECTABLE AP RADIOS IMPROVE PERFORMANCE.

There are some things in life that make sense until they actually happen. Take the Run & Shoot offense—a mercifully deceased American football system created in the 1980s. The Run & Shoot was designed to play the game as fast as possible, with ample room for improvisation. The designers of the Run & Shoot found that statistically, football teams scored more often when they didn't use play-calling "huddles" that slow the game down. They 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, huddles were eliminated, and players were asked to improvise, rather than running pre-designed plays. And it worked beautifully... until it was tested at 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? Essentially, its designers focused on the positive and overlooked the negative. The Run & Shoot was effective at speeding the game up and making it more difficult for the opposition to predict plays. Unfortunately, speeding up the game reduced the amount of time defensive players had to rest, and using improvised plays didn't work so well when large, angry men from the opposing team were rushing the backfield and planting them on the turf.

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. Their proponents are focusing too much on positive potential, and overlooking the new problems they create. 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. 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 normally, 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 increases 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 percent to 16 percent, 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 percent retries when a single device is connected is going to mean an absolutely unusable Wi-Fi channel when dozens of devices connect, as commonly happens on classroom networks.

While the folks who created band-selectable AP radios deserve some amount of credit for trying new things, they also likely deserve as much scorn as the Run & Shoot progenitor Mouse Davis. His two seasons coordinating the Detroit Lion's offense produced two losing records, a 0 percent record of success. And, rest assured, 0 percent 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 of primary education 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 to upgrade, put the suppliers to the test. As the saying goes, "I'll believe it when I see it." Performance speaks volumes, and now with your new-found knowledge on these myths, you can make an informed decision by asking all the right questions. Use your Wi-Fi savvy for good by making smarter investments in infrastructure, protecting your students and helping them boldly go forth in a world of uninterrupted learning.

READY TO GET STARTED? WATCH OUR ON DEMAND WEBINAR TO LEARN HOW YOU CAN DESIGN A RUCKUS DIGITAL-READY CAMPUS, OR REQUEST A DEMO TO PERSONALLY SEE WHY RUCKUS IS THE PERFECT FIT FOR YOUR SCHOOL.

Ruckus Wireless, Inc. | 350 West Java Drive | Sunnyvale, CA 94089 USA | T: (650) 265-4200 | F: (408) 738-2065
ruckuswireless.com