RESIDENCE HALL MAKEOVER
Network Edition

Ruckus™ Simply Better Wireless.

WHITE PAPER

"MAKING COLLEGE A HOME-AWAY-FROM-HOME EXPERIENCE STARTS WITH WI-FI SOLUTIONS"

BAD WI-FI IS A BIGGER PROBLEM THAN YOU THINK

Millennials hitting campus today are a different animal than the students of the past. They've grown up as "digital natives." Smartphones, social media, oceans of information at their fingertips, instant contact with anyone, anywhere—this is the world they've always known.

Yes, these students are looking for digitally-enabled classrooms and learning, but those are almost beside the point. These students—and their parents—are choosing your institution to be their home, not just their school. And they expect a true "home-away-from-home" experience in residence halls. Which means an environment that supports constant connectivity as a basic feature of students' lives.

- 60% of people can't go without Wi-Fi access for more than a day.
- 43% said if they had to choose between Wi-Fi and chocolate, they'd go without chocolate.

*Broadcom Survey

To make all this possible, you're going to need Wi-Fi—strong, reliable, easily accessible Wi-Fi, available anywhere, anytime on any device. And if you haven't made delivering that a priority, you better believe that other institutions have. Across higher education, universities are engaging in a "lifestyle arms race" to recruit students, and great Wi-Fi is the key weapon in their arsenals.

What do the best institutions look like from a student's perspective? All of their devices connect "auto-magically." They can stream videos, FaceTime, download large files and more without slowdowns or disruptions. They have uninterrupted access, without constantly being prompted to re-enter credentials. And they can connect all of their devices—gaming consoles, smart watches, printers, Apple TVs—in seconds, without having to scroll through dozens of other people's devices or call the help desk. At premier universities, Wi-Fi is a basic utility, like the lights. It just works—wherever, whenever.

How does your institution stack up? What impression are you making to students, parents and prospective students visiting your campus? Keep in mind, this generation of digital natives does not suffer silently. If your Wi-Fi sucks, you're going to hear about it. So is your boss. Most likely, so is the rest of the world

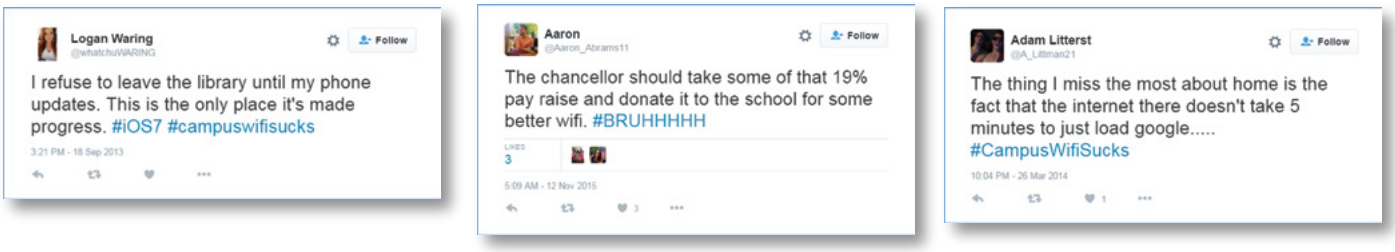

Figure - 01

Why is Wi-Fi so bad in most residence halls? And what can you do to not just make it better, but deliver the true home-away-from-home experience your students expect? Let's get some answers.

CHALLENGE #1: POORLY PERFORMING WI-FI

There are all sorts of issues with campus Wi-Fi—coverage, capacity, onboarding, security—but performance is at the top of the list. If the Wi-Fi isn't fast and reliable, nothing else matters. Here's what most students are dealing with today: Spotty coverage. Frequent dropouts. Choppy video playback and downloads that can take hours. What's going on? Here are the most common issues:

- **Weak signals between access points (APs) and devices:** Wi-Fi radio signals might be getting snuffed out by your building construction. You may have issues with AP placement or density. It might be new "Internet of Things" (IoT) devices with weak transmit power. It could even be problems with the orientation of mobile device antennas relative to APs. Sometimes it's all of the above.

> Did You Know: LEED-certified construction materials block RF signals.

- **Interference:** Interference can be a huge factor in poorly performing Wi-Fi, and your airspace is getting more congested all the time. It could be co-channel or adjacent-channel interference from too many clients (or even APs) crowding the same RF spectrum. Or it could be spectral interference from microwaves, Bluetooth devices, or unmanaged Wi-Fi from neighbors or student-owned routers.
- **Too little capacity:** You're looking at a perfect storm of Wi-Fi usage. There are more devices per student, which means more devices per AP. Those devices have more powerful 5 GHz radios, spurring more high-bandwidth application usage—HD streaming video, online gaming, FaceTime—on more devices, more often. If your Wi-Fi infrastructure was designed for the needs of a few years ago, it's already behind the times.
- **Peak loads:** You've heard the old rumor about everyone in a hotel flushing at the same time and blowing out the pipes. That doesn't actually happen. But it can absolutely happen with your Wi-Fi. If everybody's streaming March Madness, everybody's getting sub-par quality. If everybody's downloading the new iOS update, they may be waiting hours for it to finish.

All of these variables can affect the throughput of a given connection, and create a singularly terrible Wi-Fi experience in residence halls and common areas. And remember, this isn't like having a slow connection at Starbucks, where students can just deal with the poor connectivity they expect from a public hotspot until they get home. This is their home! Your first priority is to make it feel like one. The expectation is clear; it's time for you to meet it.

CHALLENGE #2: WI-FI ACCESS IS A HASSLE

Move-in day! Students (and often their parents) arrive with all their belongings—including five to seven mobile devices each. They expect to be able to connect all those devices to the campus Wi-Fi right away. Are you ready? How do you know, when the summer has few users to test your network capacity or onboarding tools?

By the way, how are you securing all those devices? EDUCAUSE[1] ranks information security—protecting students and reducing the institution's exposure to the growing threat landscape—as the number one priority for higher education in 2016. But typically, more security means more complexity, more headaches and more time spent manually getting devices on the network—for both users and IT. Here are the common problems that make access such a hassle on campus:

- **Massive scale:** A few years ago, you could expect each student to have two or three wireless devices. Today, that's more than doubled. If you have 10,000 students, you're talking about 50-60,000 devices, all coming in and trying to get on the network, at once.
- **Headless devices:** Most students can figure out how to navigate a browser-based portal to connect their laptop or smartphone. What about their wireless printers, Fitbits, gaming consoles and Rokus? Traditionally, you'd have to authenticate each device's MAC address—a hassle for your students and a huge manual effort for your helpdesk. And these digital natives aren't just going to shrug and give up their PS4s. If they can't get their devices on your Wi-Fi, they'll go buy their own routers—creating new security and performance issues, and lots of new complexity.
- **Problems with passwords:** Attempting to enforce some level of security, many universities use password-based access methods (PEAP, TTLS). But these rarely translate to good experiences, either for students or IT. It's common to see millions of authentication requests hitting RADIUS servers every day. 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 her password, she has to manually reconnect all her devices (and hope she doesn't get locked out of her account).

1 Grajek, Susan. "Top 10 IT Issues, 2016: Divest, Reinvest, and Differentiate." EDUCAUSE.edu. http://er.educause.edu/articles/2016/1/top-10-it-issues-2016

> 40% of IT support desk volume is password-related problems.
> *Gartnerv

It all adds up to a massive headache for students and a nightmare for IT. Traditionally, many universities dealt with it by effectively throwing their hands up, and just providing open broadcast domains. This certainly makes life easier for IT—until they're cleaning up the aftermath of malware running wild on their network because nobody's connection is secure.

As an alternative, many universities now use PEAP/TTLS security, with online wikis or even an initial in-person IT "surge" to help everybody get online. But this still requires a huge IT effort. And not just on move-in day, but every time someone has a new password problem, headless device or eduroam issue.

The goal should be automated, self-service onboarding for all users and devices. But if you're going to do it with security, you're typically looking at a home-brewed solution that's neither robust nor well-supported, or an enterprise device management platform with high costs and complexity that's overkill for the problem you're trying to solve.

CHALLENGE #3: WHERE'S ALL MY STUFF?

In many universities, residence halls are moving towards apartment-like suites. And students expect to be able to live in them the way they do at home. That means being able to AirPlay video from their iPad over Wi-Fi, play multiplayer games with their friends down the hall (or around the world), connect to their personal printer without scrolling through dozens of networks and devices that have nothing to do with them. Here are the choices that students are typically looking at today:

- **Totally open:** Students arriving at the residence hall see a shared broadcast domain and common SSID, and are dumped into a single, huge VLAN segment. It's like they're sharing a virtual house with dozens or hundreds of other people, with all the hassles that implies. Every connected device can be seen, and potentially hacked. If a student down the hall is consuming tons of bandwidth, everyone else's connection suffers. And thousands of devices using chatty protocols like Bonjour can easily overwhelm the network.
- **Totally closed:** The common alternative is client isolation via per-client VLANs. Now, you're effectively telling everyone in the virtual house to go to their room and lock the door. If every device is on its own VLAN, students can't share anything. Communication among their devices, and with the rest of the world, is effectively cut off—not a good look for digital natives.

A true home-away-from-home approach would give every student his own secure virtual network. But conventional Layer-2 VLANs don't make it easy. Trying to create static VLANs ahead of time—without knowing who's coming or what they'll be connecting—is just not feasible. And conventional dynamic VLANs can't scale with tens of thousands of students.

YOU'VE GOT TO MAKE THIS BETTER

Your students—and their parents, who are often making the call—come to campus assuming that all of their devices will connect automatically. Like home, students want to see only their own stuff, and be able to get to it whenever. They want to work and play with wicked-fast download speeds. They have no patience for constantly entering passwords and making calls to the helpdesk.

They expect Wi-Fi that just works. Here's what they get:

- **Airplay doesn't work:** Dozens of AppleTVs and printers appear on user network settings, and scaling Apple's Bonjour protocol can create exponentially more traffic
- **Join which network?:** Dozens of SSIDS appear on Wi-Fi network settings
- **Moving my device drops the connection:** Orientation of mobile devices relative to access point antennas impacts throughput, and even connectivity if device drops below threshold RSSI
- **Neighbor Wi-Fi interference:** Consumer-grade home Wi-Fi routers deployed by students in a residence hall creates co-channel interference in an IT-provided Wi-Fi deployment. This is also true in urban settings where neighbor Wi-Fi could also interfere with, or even attempt to mitigate, your network
- **Netflix Buffering:** Insufficient bandwidth, improper wireless coverage and lack of QoS could result in poor video performance
- **Too many passwords!:** Users may have passwords for device access, network access and application access. Also, passwords may change periodically due to IT policy
- **How do I connect Xbox?:** Headless devices are often secured via IT help desk ticket to gain network access, low data rates enabled, and may require a firewall port change to enable MUD or group gaming

Go ahead and call Millennials spoiled. They're making your campus their home for the next several years of their lives. Does that sound like someplace you'd want to live?

SOLVING WI-FI PERFORMANCE

It's time to take some concrete steps to make this better. Start at the top of the list: Wi-Fi performance and reliability in residence halls. Here are three places to start.

Deploy 802.11ac Wave 2 with MU-MIMO

If you're still offering 802.11n wireless, it's time to upgrade. 802.11ac Wave 2 with multi-user MIMO (MU-MIMO) is a huge step up, on the level of the jump from 802.11g to 802.11n. The standard provides 160 MHz channel support, 256 QAM modulation and data rates up to 2.3 Gbps in the 5 GHz band. But this isn't just about bumping up peak data rates. Wave 2 MU-MIMO radically improves spectrum utilization, which makes Wi-Fi performance better for everybody, including non-Wave 2 clients.

Wi-Fi has traditionally been a half-duplex technology, where AP radios only talked to one device at a time. MU-MIMO allows radios to serve clients in groups, using up to four downlink spatial streams simultaneously. Take, for example, four devices communicating with an AP (three Wave 2 and one 802.11n). A traditional Wi-Fi radio would serve packets one client at a time, so each device gets served once every four cycles. A Wave 2 MU-MIMO AP serves all three Wave 2 clients at once, so all four devices are served every other cycle. You can now support much higher client density per AP. And even if you maintain the same overall capacity, your students get better performance because you're using your spectrum much more efficiently.

Solve Your Airspace Problems

Dealing with overcrowded airspace, environmental factors, channel and spectral interference is an enormously complex technical challenge. But it's the only way to give your students a strong, consistent connection. If you're looking to upgrade your infrastructure to 802.11ac Wave 2, here are some of the RF factors you should be considering:

- **Antenna design:** Conventional AP antennas radiate RF energy omni-directionally. Which is why there can be so much variation in a given user's throughput—and why adding more APs won't necessarily solve the problem if adjacent APs are stepping all over each other. Look for antennas that adapt radiation energy patterns for each user device to deliver additional gain (regardless of the device's antenna polarization), and employ excellent spatial separation to reduce co-channel interference.
- **Channel selection intelligence:** Enterprise-grade APs have the ability to constantly monitor RF channels within the 2.4 and 5 GHz bands, and algorithmically select channels to optimize throughput to client devices. But residence halls should be using channel selection technologies like those employed in contentious public venues and carrier Wi-Fi environments, which analyze capacity on all channels to switch to one that's actually better. Capacity-based channel selection optimizes the client experience.
- **Band steering:** The 2.4 GHz band is often more congested and susceptible to spectral interference due to it's limited channel reuse. Your Wi-Fi network should be able to identify dual-band clients and steer them towards the 5 GHz frequency whenever possible, improving performance for those clients, as well as for 2.4 GHz devices that can now operate in cleaner airspace with less contention.

Provide Per-Room Wi-Fi

The shift to the 5 GHz frequency band among newer Wi-Fi devices has big implications for your wireless architecture, and many residence halls haven't caught up. 5 GHz transmissions are stronger but don't propagate as far as 2.4 GHz. And the huge influx of smaller Wi-Fi devices on campus use smaller antennas and lower transmit power. So you want APs closer to clients. But the more APs you use, and the closer they are to each other, the more interference they could generate.

Given these issues, many universities are now implementing in-room AP designs. By putting APs closer to clients, you boost their received signal strength, while reducing interference by putting more attenuation (both distance and walls) between APs. When your in-room AP is also a managed Ethernet switch, it's now also much easier for students to connect a gaming console or smart TV. And you can use it to connect other services, like bulk IPTV, without having to pull new cabling—a huge cost savings.

Optimize the Network for IP Video

Video is the biggest Wi-Fi killer, both because it uses a ton of bandwidth and because small problems translate to seriously degraded experiences. The most important step you can take is to beef up your infrastructure with 802.11ac Wave 2 technology, and better AP antennas and architectures. These clear out the low-hanging issues clogging up your spectrum so you can use your capacity more efficiently.

At the application level, you should be looking at traffic inspection and Wi-Fi-optimized quality-of-service (QoS) mechanisms to prioritize video

traffic and alleviate choppy streams. This is particularly important if you're providing bulk IPTV service, where you'll want your Wi-Fi infrastructure to differentiate and manage IP multicast video frames separately from other traffic.

Ruckus Can Help

We offer a broad portfolio of indoor, outdoor and in-room APs that take full advantage of 802.11ac Wave 2. Our patented BeamFlex+ adaptive antennas with polarization diversity, along with breakthrough innovations in smart channel selection, roaming, multimedia QoS and more deliver strong, reliable connections in even the most contentious airspace.

SOLVING WI-FI ACCESS

Secure access doesn't have to be a pain for your students and a full-time job for IT. Here's how to make it easier.

Figure - 02

Use Certificate-Based Onboarding

The solution to the Wi-Fi access hassle been around for a long time: certificate-based Wi-Fi, in the form of WPA2-Enterprise with EAP-TLS. When you move to certificates, Wi-Fi access becomes:

- More secure: Certificate-based access uses the gold standard in encryption, WPA2-Enterprise with EAP-TLS, which is synonymous with network security and has never been hacked.
- Nonstop: With PEAP/TTLS, any password change becomes a major ordeal for students. With certificates, the certificate is the authentication key, and users can change passwords whenever they choose without interrupting access. They can register a device once and not worry about getting it on the network again until the certificate is set to expire, often for the rest of the year.
- Easier to manage: If a laptop gets infected with malware and needs be get booted off the network, that's traditionally meant revoking access for all that student's devices—or even an entire network segment. With certificates, you can revoke access to just that individual device, minimizing impact on the student experience as they still use their other devices.
- Eduroam-friendly: Password issues from your university's own students are a piece of cake compared to remotely based eduroam users. With certificates, you can securely connect them just as easily—along with any other guests that aren't defined in Active Directory or LDAP.

Employ Simple or Sophisticated User Policy

One of the biggest reasons passwords fail as secure access is that they get reused and shared across multiple devices and users. Certificates, on the other hand, are unique to each device. Which means you can apply different policies to different devices, even when they're all associated with the same student. You gain more granular control over how devices are accessing your network and what they do when they're on.

Policies don't just have to govern what a student can access on a given device, they can also apply to the experience itself. For example, you can set bandwidth limits for devices using specific applications, so that every student has the bandwidth they need, and nobody's hogging capacity and degrading other students' performance.

Use Simple, Self-Service Onboarding

If you want people to actually use your security, it has to be simple. Fortunately, you don't have to build out your own DIY certificate infrastructure and try to explain to students how to use it. Modern certificate-based onboarding platforms are fully automated and self-service. Users just log onto the campus portal with their credentials for a one-time setup process. They see a simple, custom-branded, 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 effectively a managed device. But the student didn't have to have IT touch it, and all the complexity is under the covers. All students know is that they can get their devices on the network in a few seconds, one time, after which their devices connect automatically, with no login prompts.

You don't have to limit automated self-service to your campus geography either. You can use "pre-boarding"—sending incoming students a link to the portal as part of a welcome (or welcome back) packet. They can onboard their devices from home, on their own time, and they'll automatically connect when the student arrives on campus. No more wrestling with technology on move-in day, making their lives (and IT's) a lot easier.

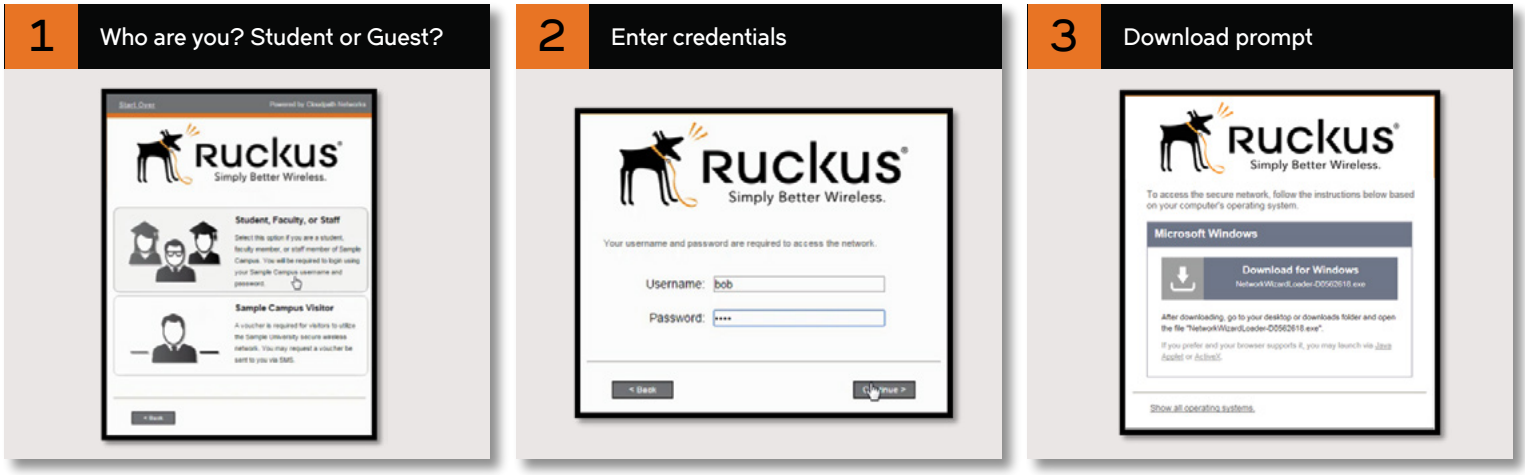

Figure - 03

Ruckus Can Help

Ruckus' CloudPath Enrollment System (ES) provides secure, self-service certificate-based onboarding for higher ed. It's a simple, plug-and-play 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.

PROVIDING PERSONAL STUDENT NETWORKS

At home, setting up a network is no problem. You buy a wireless router, set up DHCP and network address translation, and you're good. All your devices can now talk to each other in their own secure silo. Creating those private silos over a common network can be a lot more complicated. How do you balance the need for sharing with the need for security and privacy for each student? How do you enable students to roam between locations without losing access to their stuff?

These are thorny questions, but if you're going to give students anything resembling their at-home experience, you need to answer them. That's why Personal Student Networks have become an essential concept in campus bulk Wi-Fi. Here's what you should be thinking about to deliver them.

Provide Better Experiences with Per-User Device Policy

Certificate-based onboarding provides the framework for uniquely identifying and applying policy to devices, and correlating multiple devices with one user within a personal VLAN. Modern Personal Student Network solutions integrate with and build on your certificate-based access platform. They allow multiple users to log onto the same SSID, recognize all the devices associated with each user, and dynamically generate personal VLANs from a shared resource pool.

For students, it's as simple as logging into a web portal and authenticating. A personal SSID pops up in their room, and they can now connect all their devices the same way they would at home, without IT doing a thing. Each student now has a personalized, home-like network experience. All of their devices are easily connected and accessible, but no two are alike. Each device is treated individually via policy management, and the network and application experience is optimized for that specific device.

For IT, taking this Layer-2 approach has advantages over an application-level approach, as it avoids the complexity of having to set up and maintain the multitude of configuration options possible. This approach also solves the headless device problem, because now students can get their printers, fitness trackers, gaming consoles and streaming media players connected in seconds—without remote MAC authentications or manual white lists. These platforms integrate headless devices with your back-end certificate framework, automatically correlating them with the right student and applying the right policy. And they use Dynamic Pre-Shared Key (DPSK) encryption to keep them protected.

This is a huge load off of IT's shoulders and a major quality-of-life improvement for students. Wi-Fi now "just works" like it does at home. And in some ways, better than home, because students can now access their devices from anywhere on campus. If they're in Bio lab and realize they forgot to print out a paper for English Lit that afternoon, they can hit print right where they are, and swing by the residence hall to pick it up on the way to class. If they have network-attached storage with hundreds of TV shows and movies, they can now stream them from the quad. And they don't have to scroll through dozens of strange choices to get to their device. All they see on their network is their own stuff.

Deploy Gateway Devices Closer to Clients

One of the bigger challenges of implementing Personal Student Networks is trying to control the broadcast domain, and preventing broadcast traffic from killing your network. VLAN isolation is supposed to make life easier. The last thing you want is thousands of new chatty devices constantly pinging and sending Bonjour traffic over your campus switching fabric.

Your personal network architecture should position access routers at the edge, as close to your users as possible, ideally with built-in Bonjour gateways. You want students to be able to see their iPad on their personal LAN and be able to AirPlay movies on their TV. But all that broadcast traffic should stay within that domain, instead of proliferating out over the WAN and sucking up everyone else's bandwidth.

RUCKUS CAN HELP

Ruckus works with industry-leading partners in personal networks, who provide solutions that tightly integrate with Ruckus Wi-Fi infrastructure and CloudPath ES. Using standards-based APIs, they can programmatically control the Wi-Fi system to make home-like personal networks simple, secure and self-service.

GET STARTED

At universities everywhere, the lifestyle arms race is intensifying, the residence hall is becoming the new battlefield, and Wi-Fi is becoming a critical weapon. Among the digital native generation you're competing for, and their parents who are paying the bills, Wi-Fi isn't an amenity. It's an essential feature of students' everyday lives. And if your residence hall Wi-Fi sucks, you're losing that competition, losing you reputation as a cutting-edge institution, maybe even losing your job.

It doesn't have to be that way. By taking the right steps now, you can solve your Wi-Fi reliability problems. You can make access simple and automated. And you can make your campus a true home-away-from-home for your students.

Fast connections from anywhere, no matter which device students are using, what they're doing with it or how they're holding it. Five bars of coverage in residence hall rooms, hallways and outdoor spaces. Thousands of devices onboarded in seconds, connected from the moment students arrive. And personal networks that just work, giving students access to their stuff—and only their stuff—from anywhere on campus.

You can make all this happen. Ruckus can help. Find out how.

Start Learning More Right Now

https://www.ruckuswireless.com/solutions/higher-education

Ruckus™
Simply Better Wireless.

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