ekahau
WIRELESS DESIGN

Wireless in Higher Education - Top 8 Concerns

Colleges and Universities are frequently called out as their own vertical for good reason. While all WLAN environments do share some similarities, higher education absolutely brings its own bag of concerns to the Wi-Fi discussion. I'm currently a wireless network architect for a large private US university, and I also frequently interact with other schools on a number of network-related topics. I've been in this game for over 20 years, and the following is what I think anyone interested in this unique space should know, from the insider perspective. Don't expect to read about spatial streams and client device drivers in this article. There is a far bigger story here to tell.

1. Well-Defined Operational Policy Is a Must.

Whether the topic is identity management, WLAN encryption, guest access, or whether to allow IoT devices for campus business, solid policies drive solutions and system design. I'm talking CIO-endorsed words-on-paper policy about what is and isn't allowed and supported on campus, what security is required, who is allowed to do what, and what enforcement amounts to. Executive buy-in is a must. To run a large, complicated network environment without clear policies is an invitation to chaos that eventually manifests in network instability, and a lot of unhappy users as disorder and uncertainty sets in.

2. Bigtime BYOD/IoT.

Both bring-your-own-devices and oddball client things on the network have been fixtures of higher ed networks since long before they were given sexy marketing names. There's simply no end to what people want to put on the network. Whether you allow everything under the sun to connect or put technical limits in place (no .11b data rates, no Bonjour support, no self-installed routers, as examples) it has overlap with policy decisions, and also huge bearing on network designs. Expect requests for everything and anything, but be mindful of the technical and political ramifications of saying yes, or saying no, to each.

3. Not All Buildings Are Created Equal.

Many schools, like mine, are small cities unto themselves with hundreds of networked buildings. They also may be akin to international corporations- with satellite buildings or campuses in other cities or countries. You may have wireless work in a brand new building one day, and another that was built in the 1800s the following day. The differences in building construction will bear on your wireless designs and Wi-Fi behavior, whether cabling for access points is reasonable or a nightmare, and even if permits are required before you can alter the building. It's normal to have to drastically adjust your assumptions as you leave one building and enter the next for wireless work. You learn to keep an open mind here, and assume nothing when it comes to University buildings.

4. Budget Cycles Make You a Futurist.

It's not uncommon to expect at least some elements of today's network design to last 8-10 years into the future, in many cases. In those buildings where cabling costs are particularly expensive, you might well be looking at two or three access point refreshes with no practical option for changing mounting locations. While it's not easy designing that far out for this, experience and an open mind go a long way towards helping you build in flexibility that needs to last.

5. Swarm!

You never know what public space will get used for anything from a registration space to a pop-up conference area to a hackathon event setting. Far outside of auditoriums and meeting rooms, sometimes crowds can occur in the strangest of places for a few hours or a few days. You have to have something up your sleeve to provide more coverage or easier-than-normal access (with the Security Group's approval), whether it be adding an AP or two or using a conference-specific SSID. While the day to day goal of network stability and predictability is among the highest priority, you also have to be able to react and accommodate on the fly to large-scale events every now and then, sometimes with very little notice.

6. Compliance and Regulations Are Only Getting Stricter in Spots.

With so many different client demographics and support organizations on campus, there is definitely a regulatory undercurrent to many campus operations. It's not uncommon to have to comply with HIPPA requirements at the medical center, PCI at the bookstore, and even things as exotic as GPDR if you have European campuses. You may have to work with law enforcement at various levels, or provide regulation-driven security for intellectual property. All of this generally goes beyond your own policies, but you'll have to decide whether not using Wi-Fi at all in some applications is easier than tap-dancing through the regulatory minefield.

7. The Gift (Curse) of Good (Bad) Managers.

I've been fortunate throughout most of my higher education IT career to have really good bosses. When crazy network-related requests come knocking, I try to creatively accommodate if possible, or work the equation to something other than what was asked for that still meets the need. But when the zingers come- those requests that just can't be fulfilled- it helps to have tech-minded managers that will back you. I've heard horror stories from colleagues that weren't so fortunate… All it takes is one manager that gets starry-eyed by nonsensical vendor promises, makes arbitrary "YOU WILL DO THIS" decrees, or who decides that they know everything about everything for the entire operation to be thrown into disarray. Higher ed environments are targets for lots of vendors and solutions folks who see the world in their own ways as they seek your business, but having your own goals and approaches aligned with those in your chain of command helps to keep the wild and crazy at bay.

8. It's a Business, but the Devil is in the Details.

Whether a given school is public, private, or part of a bigger organization, every college and university is a business. In many cases, it's more like many smaller businesses under one umbrella heading. There are goals to meet, revenues to take in, and bills to pay, even for non-profits. There also happens to be different technical models for this business. In my environment, a central network team is responsible for policy, the shared network, core systems like DHCP and DNS, and all Internet connectivity. Other schools are decentralized, and units at those schools may have more freedom to do their own networking. (I chuckle when I see a vendor claiming some huge school as a customer, when frequently I know that it's only a small decentralized unit at that school who actually uses the product). I'm biased in that I believe the central model just runs smoother for all, and is an easier framework in which to control the networked chaos that often defines higher ed. But it's important to know that not all institutions approach their network needs the same way, and who you are dealing with when on campus.

As you can see, the higher education space is fraught with operational nuance. If you don't have at least a basic insight into how a given school functions, it gets easy to misjudge their networking needs. Perhaps nowhere is understanding "requirements" more important, and it's a fair statement that those requirements may be different even from one part of a single campus to another. There's absolutely no place I would rather work than at my university, but I frequently see how confounded vendors can be in trying to figure us out versus the last school they worked with. Just remember that the non-technical side of the story drives the operational needs of the technical side, and you'll understand why it's important to consider these eight concerns when it comes to higher education Wi-Fi.