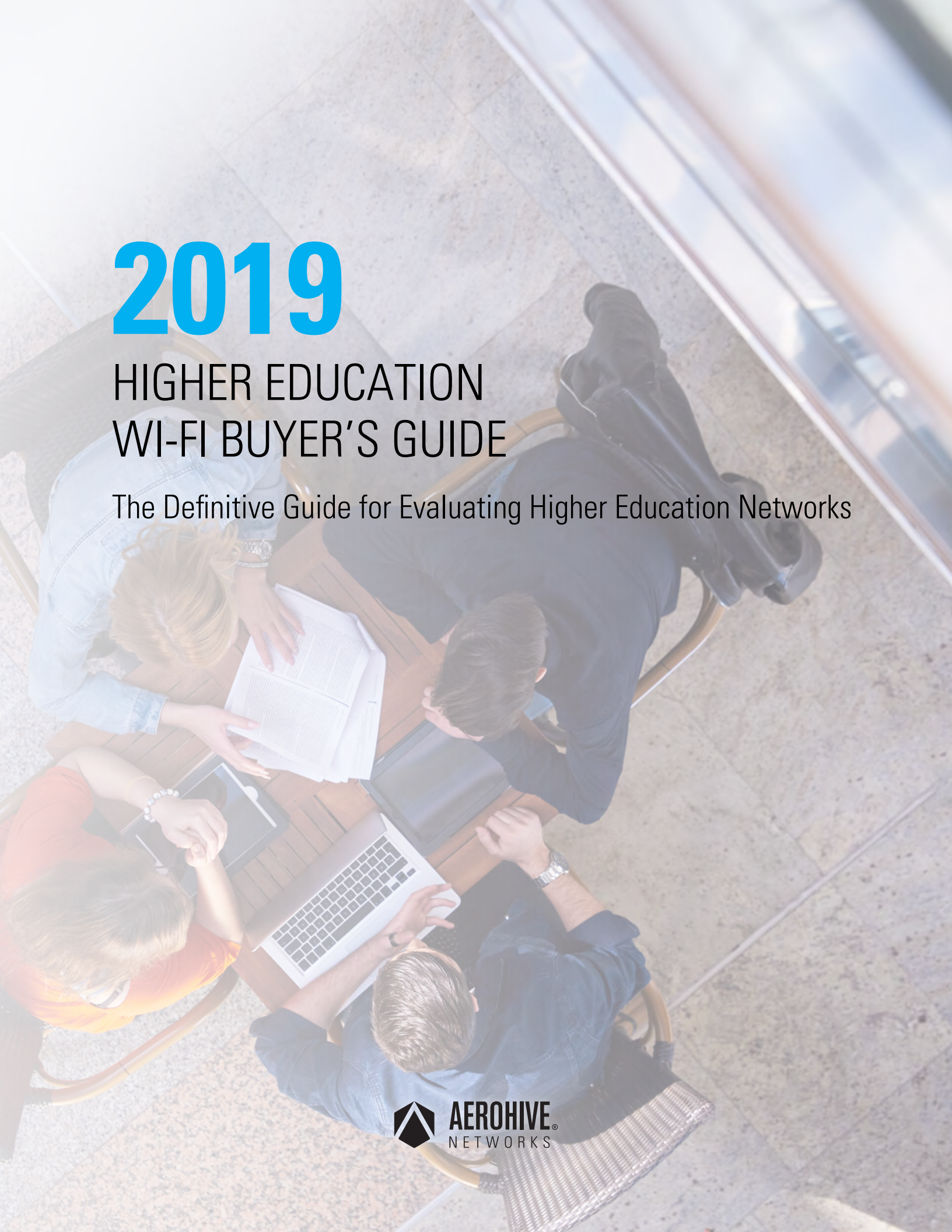


2019

HIGHER EDUCATION WI-FI BUYER'S GUIDE

The Definitive Guide for Evaluating Higher Education Networks

AEROHIVE® NETWORKS

2019 Higher Education Wi-Fi Buyer's Guide

2019 Higher Education Wi-Fi Buyer's Guide

What To Expect From This Guide

Educators are faced with unique problems when considering how best to implement their networking infrastructure. First, and perhaps most important, some higher educational facilities do not have dedicated in- house networking experts, which are considered foundational to most enterprises. This becomes even more problematic as educational institutions consider wireless LANs (WLANs). Wi-Fi–based networking is changing rapidly and continuously, and makes use of specialized terms, gear, and jargon that can be baffling. Each vendor has its own niche in the market and its own specialized terminology, adding to the confusion. And even if you can manage to catch up to the network side of Wi-Fi, you still have to try to keep up with innovations on the client side! This can result in constant dread that you have purchased gear that will not be scalable or manageable as your needs change.

While the learning curve in Wi-Fi can be steep, it is ultimately worthwhile. WLANs allow you to extend the benefits of connectivity throughout your institution, from the lecture hall to the courtyard. Professor collaboration and reach can be enhanced. Students can use the technology that suits them as a learning tool, not a distraction.

In this vendor-neutral guide, we will take you through some elements that you should consider when choosing Wi-Fi networking equipment. We will begin by considering the issues common to any WLAN deployment in the higher education market, including Wi-Fi standards and a forward look at the growth of Wi-Fi–enabled devices. We will then look at architectural and management considerations, and how these elements come together to create the overall solution.

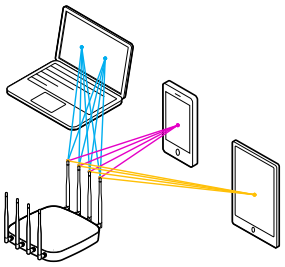
Along the way, we will try to demystify the jargon and cut through the acronym soup. The goal of this guide is to help you to define what your organization really needs and wants from its Wi-Fi investment, and then help you to identify the gear that meets your requirements, without compromise. To that end, we've also included a few words on programs that may be helpful to you in the buying process.

Wi-Fi

Wi-Fi runs on two different low-power radio bands: the 2.4 GHz band and the higher-frequency 5 GHz band.

WLAN

A wireless local area network is a wireless computer network that links two or more devices using wireless communication within a limited area such as a home, school, computer laboratory, or office building.



MU-MIMO

(Multi-User Multiple Input Multiple Output)

Introduced in 11ac, MU-MIMO technology allows the simultaneous transmitting of multiple frames to different receivers at the same time on the same channel using multiple RF streams to provide greater efficiency. 11ax adds 8x8 and Uplink MU-MIMO services to provide significantly higher data throughput.

Basic Terminology

The **IEEE** (Institute of Electrical and Electronics Engineers), who write the 802.11 standards, is one of the names you will see most in any networking arena. They create and vet the standards, and, along with chipmakers and vendors, bring these standards to specifications and to the market. Another name to know is the **Wi-Fi Alliance**, a group that certifies that Wi-Fi gear will interoperate. Vendors are not required to be certified by the Wi-Fi Alliance, but you absolutely must make sure that any vendor you are considering has gone through that process, just to ensure that there are no surprises.

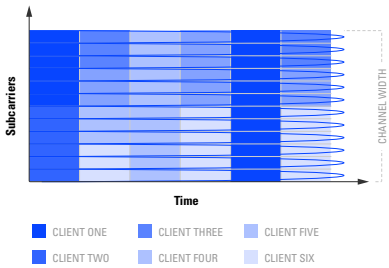
Over the past few years, wireless LANs have gone from isolated, convenience-oriented networks to the de facto access method in many organizations. This shift has happened hand in hand with the development of cost-effective mobile computing devices. Because the vast majority of these devices, including smartphones, laptops, and e-readers don't even have an Ethernet port for wired connectivity, Wi-Fi is mandatory for their use. With the explosion of mobile devices, Wi-Fi networking went mainstream.

Wi-Fi runs on two different low-power radio bands: the 2.4 GHz band and the higher-frequency 5 GHz band. Many other non-Wi-Fi devices run on the 2.4 GHz band, including things like microwaves and older portable phones, so there is more interference there. The 2.4 GHz band also tends to extend farther than the higher-frequency 5 GHz band, making the interference more apparent in dense environments. The 5 GHz band has more channels available, and does not extend quite as far as the 2.4 GHz band, but some legacy clients may not support it.

The 802.11n standard introduced some important technological elements; including the concept of an antenna technology called **MIMO**, which stands for *Multiple In Multiple Out*. 802.11ac and 802.11ax further expand on this technical concept with support for **MU-MIMO**, which stands for *Multi-User-Multiple In Multiple Out*. MIMO allows multiple antennas in both the client device and the access point to communicate simultaneously, which dramatically boosts throughput. While the following few sentences may sound like technical mumbo jumbo, they will help you understand how to read an access point (AP) datasheet and some of the basic experiences that you might have while on a Wi-Fi connection.

When you look at AP datasheets, you will see a designation showing [X] x [Y] : Z. In the example shown here, the designation is 3x3:3. This means that the access point you are looking at has three transmit antennas and three receive antennas, which may be included inside the body of the AP. The last number, behind the colon, stands for spatial streams. Spatial streams enable the AP to split the outgoing signal into Z number of pieces, and send them at the same time; they can also send the same signal Z times simultaneously, for greater accuracy. In this datasheet example, the AP has three spatial streams. The most important thing to know about MIMO, however, is that the access point can only use the same number of antennas and spatial streams as the client device. Many client devices, such as smartphones, only support one receive antenna, one transmit antenna, and one spatial stream. This is because the use of multiple antennas takes up a lot of battery life. Therefore, you must take care to test any Wi-Fi deployment with identical clients in identical placement.

REMEMBER: Test for speed in your environment. It is not possible to reach the theoretical maximum output of a Wi-Fi device, although some vendors will actually cite those numbers as their throughput.



OFDMA

(Orthogonal Frequency Division Multiple Access)

Multi-user version of OFDM enabling concurrent AP communication (Uplink / Downlink) with multiple clients by assigning subsets of subcarriers, called Resource Units (RUs) to the individual clients. Based on client traffic needs, the AP can allocate the whole channel to only one user or may partition it to serve multiple users simultaneously.

802.11ax is Here

802.11ax is the latest IEEE standard, and it was designed to address some of today's biggest performance challenges – increasing capacity by up to 4x but more importantly improving efficiency to benefit both 2.4 GHz and 5 GHz bands in a variety of environments like office spaces, schools, colleges, and public Wi-Fi venues. 802.11ax is the latest generation Wi-Fi with both vendor access points and client devices available to support the standard and it will soon become the default for all environments.

802.11ax *(Wi-Fi 6)* completely changes the way Wi-Fi operates by not only providing a higher data rate (as did 802.11n & 802.11ac) but more importantly addresses the traditional inefficiencies of Wi-Fi; its limitation of only being able to communicate with a single client at a time. 802.11ax is the first technology to improve quality of service and user experience by allowing simultaneous multi-user communication to eliminate network congestion. 802.11ax was purpose built to serve clients and fix inefficiencies in the real world, with dozens of devices (or more) and access points in a given area.

It is also important to evaluate your wired infrastructure when new standards and capabilities are introduced. Access points are generally powered by the switch to which they are connected, using Power over Ethernet (PoE) or Power over Ethernet Plus (PoE+). Many 802.11ac and all 802.11ax access points run best when they use full PoE+. It's important, therefore, to consider your wired infrastructure when looking at wireless networking.

Which Access Point is for Me?

With both 802.11ac and 802.11ax access points available, which access point should you plan for?

Your best answer may not be 802.11ac *or* 802.11ax, but whether you can use 802.11ac *and* 802.11ax. Like all IEEE standards, **802.11ac and 802.11ax are interoperable**, and the best AP deployment may well be a mixture of both. However, if you are looking to do a full refresh of your network, 802.11ax is the way to go so that you effectively future proof your network for the next three to five years.

Be wary of any vendor that makes a hard-and-fast recommendation without knowing about your layout, capacity plans, and your wired network. Regardless of the price point, your aim is to get an architecture in place that will meet your needs today and at least four years into the future.

A very good foundational question to ask any vendor, however, is whether their architecture allows you to mix 802.11ac and 802.11ax access points in the same deployment, and still get the best of both standards. You will also want to be sure that the deployment can easily be managed via the same interface, and that the same policies can be applied. Then consider what is required to move from an 802.11ac AP to an 802.11ax AP.

Getting a Wi-Fi Deployment that Works

A good Wi-Fi deployment looks like something out of science fiction; you simply put the access points up on the ceiling, and suddenly you are connected to the network through the air. It is vital to realize, however, that Wi-Fi is not magic; it's radio waves. And like radio waves, Wi-Fi is subject to interference. When Wi-Fi signals run into something, the result is not the scratchy signal you get from your car radio; the result is silence. That is because Wi-Fi works like a walkie-talkie in that the client and the AP can both transmit, but not at the exact same time. If a device runs in to interference, it will back off, wait for a certain amount of time, and then try to transmit again. The result is that your throughput can become very slow.

Many people are aware of the fact that Wi-Fi can be subject to interference, and they will try to get around the problem by deploying more access points. Ironically, that can often be the source of the problem. While it is well known that a concrete staircase interferes with Wi-Fi, it is less well understood that other Wi-Fi devices also create interference. So if access points are spaced very closely, they will actually interfere with each other!

This potential problem can become even worse if there is not some attention paid to the channels that the APs are running on. Wi-Fi signals are 20-22 MHz wide, and the channels overlap each other. For example, while there are eleven channels available in the 2.4 GHz band in the U.S., there are only three that don't share some spectrum. While you want coverage cells to overlap a bit so that mobile clients can roam, if the coverage cells' channels overlap (for example AP1 is on channel 1, and AP2 is on channel 2), there will be what is called adjacent channel interference. That is because both APs are trying to use channels that share a lot of that 22 MHz space; for example, channel 1 runs from 2401 to 2423 MHz, and channel 2 runs from 2404 to 2428 MHz. What you want is non-overlapping channels. This is particularly important in the 2.4 GHz band, where there are only three non-overlapping channels—in the U.S., that means channels 1, 6, and 11. As you can imagine, the more APs you stuff into a space, the harder it gets to ensure that there is no channel overlap.

Interference becomes a huge problem when you consider how many access points you will need for your deployment. The standard wisdom used to be to plan for each student to have a Wi-Fi device. Current projections suggest that you should plan for between three and five devices per student, given that you should expect the equipment you deploy today to last for at least four years. If you try to solve this issue with more access points (and without proper channel and power planning), you can make the problem much worse. The key is to put the right equipment in the right place.

Steps You Can Take to Avoid Interference Issues

- **Ensure that any vendor you are considering has a predictive analysis feature.** This feature allows you to input your building or campus layout, deploy imaginary access points, and visualize any potential interference issues. This analysis will also help you to determine how many access points you really require, and to easily justify that expense by showing a graphical layout.

- **If at all possible, do a site survey.** It is compelling to believe some vendors who tell you that predictive analysis is sufficient to ensure a good Wi-Fi deployment, but, once again, remember that predictive analysis is theoretical. A full-blown site survey features a trained professional walking your site pre-deployment and looking at what is really going on in the radio frequency (RF) spectrum. You may easily get a surprise—your smartboard is transmitting, as are your new door locks. The microwave in the break room is leaking through the wall. And you may also have other Wi-Fi devices running; it's not uncommon to discover pre-existing Wi-Fi gear or even products installed before any of the 802.11 standards were officially ratified hiding in older buildings! While a complete site survey could be unattainable, there are many interim steps, some of which you can run yourself, which will help you to see the real picture from an RF point of view.

- **Keep your pre-deployment results and retest after deployment.** These records will put you far ahead of the game if/when you need to troubleshoot.

Above: A predictive survey is an important component of a thorough Wi-Fi deployment.

VENDOR-SPECIFIC ARCHITECTURAL CONSIDERATIONS

One of the primary differences between WLAN architectures is where and how the system is controlled. Broadly speaking, some vendors are controller-based and some focus on distributed intelligence, and are considered to be controller-less. The reality can be more complex, as you'll see below.

When Wi-Fi was first introduced in the late 1990s, access points were standalone, isolated pools of connectivity, mostly designed to provide access to the Internet. In the early part of 2000, it became obvious that Wi-Fi must be somehow joined to the wired network. At that point, however, the processing power required for access points to handle networking decisions independently was overly expensive. The result was a centralized controller, in which access points were distributed throughout a facility and backhauled to one or more controllers. The controller was then connected to the wired network.

Complex decisions like firewalling, access control, authentication, roaming, and more were handled by the controller. This required traffic to travel from the AP to the controller and back, but at the time this lag was not a significant barrier to adoption. Management and control were centralized, and Wi-Fi joined the network.

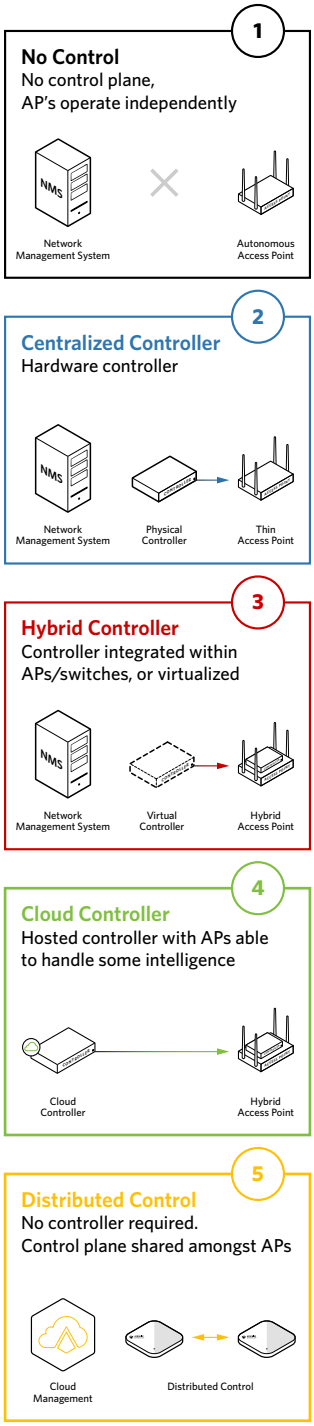
Centralized controllers were not without their drawbacks, however. Because of the nature of their connection, each controller model was "capped" at a certain number of access points. This did not seem like a limitation until it was time to purchase the AP that was "one too many," at which point an expensive new controller also had to be purchased. The controllers themselves became a single point of failure, requiring the purchase of redundant controllers in areas where Wi-Fi was considered mission critical. This centralized controller architecture is still in existence, although the need for it has disappeared.

Over the last decade, the cost of processing power has fallen sharply, largely due to the advent of affordable, powerful mobile clients. Some WLAN vendors that originated at this point in the continuum built their products from the ground up on highly capable processing power that had become economically available to all. These vendors were able to build a networking system that did not require a centralized controller to function. In this model, access points were able to communicate with each other in a fashion similar to the way routers communicate on the Internet: control became distributed.

Management remained centralized, resulting in a much more cost-effective model that was easy to scale and equally easy to manage. These two architectures—centralized controller-based and distributed controller-less - form the extremes in control for WLANs. As the distributed controller-less architectures gained popularity, several leading controller-based vendors created or purchased their own controller-less WLAN offering, while continuing to sell their controller-based products. The controller-based model has come under increasing fire in recent years due to several issues, including:

- **Mobile clients move.** A client may go from one access point's coverage area to that of another, sometimes crossing Layer 3 boundaries and into another subnet as it does so. As the client crosses into another subnet, its signal will be received by an AP that does not share the client's IP addressing sequence. Any delay or jitter, which can happen when traffic has to transit the network to the controller and back, can become problematic, especially for sensitive transmissions like voice or video.

- **802.11ac and 802.11ax.** As APs become capable of much greater speed and efficiency, the amount of traffic that would have to be backhauled to the controller becomes increasingly untenable. If you architect a network to forward data to a central control point, as it is in the controller-based model, there is no way to balance multiple gigabits-per-second of data across multiple controllers. In addition, some vendors require a controller upgrade to support 802.11ac or 802.11ax.



Above: Wi-Fi Architecture has changed dramatically over the past two decades.

Considering Both Architectures

If a company offers both controller and controller-less architectures, ask:

- Why? If the controller-based design is considered the right path for larger or more complex deployments, what elements, specifically, would contribute to the decision to deploy both styles? What elements of your Wi-Fi requirements would enable you to opt for the less costly controller-less models, and at what point does the vendor say that you need to reconfigure your entire architecture to controller-based?

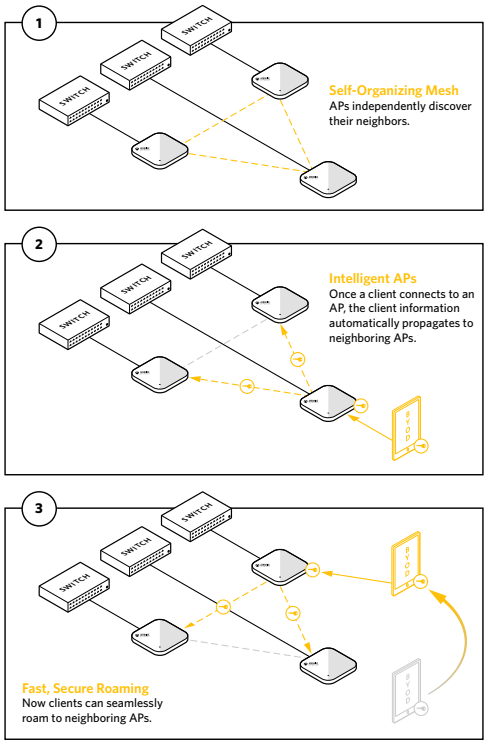
- Do the controller-based and controller-less models communicate with one another as one?
- If you deploy a distributed, controller-less WLAN in most settings and a controller-based WLAN in your central office, can you push a single policy or update throughout all of the WLANs?
- If you want to move a controller-less deployment to a controller-based one, what specific elements are required, such as re-architecture, policy reconfig, licenses, and new hardware— including the controller(s)?

Some controller-based companies offer a "hybrid" approach, called distributed forwarding, in which local traffic is forwarded between access points, but major control functions are still handled at the controller. In that case, ask:

- What features are not available locally? Some can include policy enforcement, client authentication, deep packet inspection, or quality of service (QoS)

If the company offers only a distributed controller-less architecture, ask:

- How does your architecture handle control functions?
- Is control functionality centralized anywhere, including in the cloud? If yes, what happens if that control point becomes unavailable?
- How does it handle roaming, including Layer 3 roaming?



Above: Self-Organized Access Points create a hassle-free network that allows devices to roam quickly and securely.

HANDLING BYOD

When Intel first coined the term **BYOD** or *"Bring Your Own Device"* in 2009, the idea of people bringing their own PCs, tablets, or smartphones in to work or school was something of a novelty. Clearly the phenomenon has taken off, and nowhere more than in higher education. There are compelling reasons why BYOD has exploded, beyond the obvious cost savings. Employers and schools are finding that when given the opportunity to choose their device, users are saved from the effort and time needed to get accustomed to new devices and can therefore accomplish tasks with ease and efficiency. BYOD has profound implications for higher education because it creates the conditions for student-centered learning to take place.

While BYOD provides tangible benefits to students and professors, it presents a complicated problem to IT staff. IT is being asked to ensure the security and privacy of students and their devices/data, while supporting access to material from a client that IT doesn't control at all. The largest enterprises in the world struggle with this issue, and IT leaders in education are also feeling the pain. Getting on the network has to be simple or users will not remember how to do it and IT will be overwhelmed with calls for help. Access has to be non-intrusive, or students will simply remove the roadblock. And the policies that are applied to the user while on campus, or accessing university resources should not necessarily affect their connections in other situations.

The security and accessibility answer lies in automatic actions that are taken predominately by the network itself. The method by which controls stay in the background allows the Wi-Fi network to provide the same type of experience as that of the wired network. The network should be able to tie into any type of authentication scheme supported by the college, which allows administrator's devices to be separated from students', staffs', guests', etc. Security and QoS policies can be established based on the users' context, including their identity, device type, location, and application. Individualized access keys take security a step further and are discussed in the next section.

Onboarding BYOD devices can be a daunting task. While the delivery of thousands of devices to the college or university just before the start of a term can be a cause for celebration, putting certificates and policies onto each device is a support nightmare. This is another activity that should be handled by your network itself, if possible. These features together will provide context-aware policy enforcement and safely onboard devices to the network.

Finally, whenever considering BYOD, it is useful to incorporate questions about guest lecturers, aides, or others who will require access to the campus network and to protected data. These users need some access, but you may want to limit it by role or time of day. Another related issue is the guest network, which visitors and others may want to access. Guest networks should be a standard offering on campus, and may also need to be capable of being rolled out and pulled down in the case of an event. Internet and perhaps some intranet access would be appropriate in this use case, but the majority of a campus's resources must be off limits.

Wi-Fi: What You Really Must Know

- Wi-Fi is a broadband connection that runs on two different bands:
  - **2.4 GHz**, with three non-overlapping channels in the U.S.
  - **5 GHz**, with 13 non-overlapping channels without
- DFS certification; 26 with DFS certification (bear in mind that many wireless clients do not use the DFS frequencies)
- Most RF devices—microwaves, for example—run on the 2.4 GHz band; interference can be an issue
- Any Wi-Fi networking gear that you buy should be approved by the Wi-Fi Alliance to ensure interoperability
- Test devices in the area in which they will be deployed; do not buy off the datasheet!

BYOD Considerations

Whether you are actively implementing a BYOD program today, or are simply allowing students and professors to bring devices onto the network, BYOD will affect your Wi-Fi network. Some elements to consider include:

- How do you enable access to guest lecturers or guests today?
- Does your Wi-Fi infrastructure enable role-based access control?
- Can your infrastructure facilitate a differentiated experience when the user is on campus or accessing university resources?
- Does your approach require the installation of agent software? If yes, what happens if the agent is removed?
- Does your approach require additional devices or software? If yes, what?
- Apple devices are widely deployed in colleges and universities, and advertise that services like printers or Apple TV devices are available using a specific protocol called Bonjour. You should be sure that your Wi-Fi vendor supports a Bonjour gateway, and you should ask if the vendor's technology requires any tradeoffs in implementation.

SECURITY

Network security is inextricably linked with BYOD, but it is also an issue of its own. Protecting student data has been a concern in higher education for years. In the era of online testing, security and privacy take on a whole new level of importance. Your wireless network must have all of the security and privacy of the strongest wired elements in your network. Advanced security is considered a feature by some vendors and licensing for it comes at a cost; you must ensure that these features are included in your initial estimate, along with any costs for upgrades and expansion. Please note that you may have to ask probing questions to get complete information about security from Wi-Fi networking vendors, since some technologies have evolved from what was originally consumer-grade devices. In addition, if you are considering a controller-based architecture that features distributed or local forwarding, it is important to ensure that you are aware of which security features, if any, are omitted when traffic bypasses the controller. If a branch or cloud-based controller solution is dependent upon the WAN for security applications, be sure to fully consider what features will fail if the WAN does.

One of the most important considerations when deploying a secure Wi-Fi network is what is required to get access to the network. Many home networks use a Pre Shared Key (PSK), in which access to the network is provided when you put in a specific password. The problem is that most people using PSK have the same password for all users, which poses many issues. One issue is that the network cannot tell users apart if they all come in with the same credentials. The most troubling issue, however, is that if PSKs are the only security method used, it is quite likely that an access key will remain in place long after it should have been removed; it can happen any time a user logs on but fails to log out. This can leave an open door for anyone to join your network and wreak havoc. Look for vendors that enable users to get their own unique keys, and provide network automation that removes the burden of administering keys from IT.

Authentication and access control are likewise required for Wi-Fi networks in the school. Authentication will allow the network to know who is a professor, an administrator, a student, or guest, and provide them

appropriate access based on that information. While this is important for any users, it is often forgotten in the case of guests, where dynamic, configurable pre-shared keys—unique to each guest—can be configured to expire and should protect each connection. It should be possible to easily provision more granular access controls as well, including putting users onto separate VLANs if desired, to limit access by device type, time period, or by user role.

Security Concerns

Security should be an integral part of your Wi-Fi network, not an add-on feature. Here are some questions to ask your vendor to help ensure that you get what you need:

- What security features are built in to your solution? Are additional appliances or licenses required?
- If you offer a controller-based and a distributed control model, and I move from one to the other, are there costs involved?
- If you provide a firewall, is it a full, stateful, "5-tuple" firewall?
- Do you integrate with industry-standard authentication methods?
- How do you enable a guest network in your solution? How do you provide access to it? Do you have offerings beyond PSK?
- What type of physical security do your devices, including the AP, feature to ensure data on them cannot be compromised—even if stolen?

APPLICATION VISIBILITY AND CONTROL

Application Visibility and Control, or AVC, is a part of multiple elements that should be considered when you are looking at a WLAN. This feature delivers complete Layer 7 awareness, where applications, user authentication, and privacy are handled, among other critical services. AVC enables the ability to see what applications are being used on your network—including peer- to-peer applications—and to take actions to ensure that your bandwidth is being used in the way that you intended.

The ability to visualize the applications that are running on your network is an extremely powerful tool, and one that has been enthusiastically embraced. This type of visibility, previously only available inside the network via devices such as Intrusion Prevention Systems, can be amazingly helpful in adopting a BYOD model. This is particularly true when considering the fact that many students are more knowledgeable and experienced computer and networking users than most staff. The problem is circular, and, like the Ouroboros, seemingly endless: online testing, or simply the desire to offer more advanced curricula demand the adoption of mobile devices; BYOD is enabled to ensure that the greatest poss ible number of students have access to the best gear available; unacceptable use eats campus bandwidth, costs money, and is ultimately discovered; students go back to using pen and paper, which degrades the value of moving to a computer-enabled curricula to begin with and could even open the door to possible court challenges.

What Can You See?

There are several considerations for enabling AVC, and any WLAN architecture that offers it should give you a few different ways to proceed. One area to review is the method being used to visualize the application. If the architecture is looking only at the DNS or at the URL of the traffic, for instance, it cannot really tell you if the end user is utilizing an application for a legitimate purpose related to schoolwork or just seeking entertainment. Another issue here is how the solution handles new or custom applications, such as YikYak.

If a solution uses only available application signatures to recognize traffic, it may not see an app that you care about. Because there is no way to stay totally current with developing applications, the system should give you the ability to create your own custom signatures. Still another question is whether the solution can see atypical uses, such as peer-to-peer traffic.

How Do You Provide Control?

The legacy method of providing application control was to simply whitelist or blacklist traffic. Today's users will not stand for such absolute policies. If they cannot get to a desired site, or use a particular application, their assumption is that the network is down. And you, the professors, parents, administrators, Facebook, Yelp, and everyone else they can reach will hear about it. Rather than prohibit certain sites or apps wholesale, you may choose to simply throttle the amount of bandwidth that can be consumed by them. Another way to get to the same end is to use QoS rules to prioritize preferred traffic, such as that which is related to campus activities. You may want to prioritize testing above all other traffic, for example, to ensure that it cannot be "edged out" of the bandwidth required.

Other Uses for AVC *(Or, Did You Know?)*

In addition to keeping your network running smoothly as it prioritizes important traffic, AVC features can offer information that can be used to help IT and administrators understand what is actually happening on the network. A good solution will give you the ability to see exactly how your bandwidth is being used, by whom, at what time, and using which device. This information is invaluable for capacity planning. You no longer have to guess why your network is running slowly. You can confidently tell professors the degree to which new materials are being accessed by students. By comparing AVC findings between sites, you can correlate what's working and what's not, and then make changes to policies or infrastructure accordingly.

Considerations

There are a number of different ways networking companies present "AVC," and although most vendors that offer it will be happy to show you colorful charts and graphs, it is well worth your time to know the details about how data is collected, what gear is required to enable AVC, and the degree of expertise required to yield meaningful results. Some questions to ask include:

- What methods do you use to determine applications? Do you use full deep packet inspection (DPI) or something else? If another method, what is it?
- Say I had students eating up my bandwidth distributing saved Bit Torrent data to others. Would your system detect such activity? If yes, how?
- Can I create custom signatures?
- Where does your signature database come from, and how often is it updated?
- Is AVC an integrated feature in your equipment, or does it require additional hardware, software, or licenses? If yes, what is required?

COST: DEPLOYMENT, INSTALLATION, AND MANAGEMENT

The majority of this cost section is dedicated to the consideration of initial deployment and installation of a Wi-Fi solution, as well as to the cost of its day-to-day management. This is because at the end of the day, what you spend on access points for your WLAN may not turn out to be where the bulk of your budget goes. When considering Wi-Fi networking, the deployment, installation, and ongoing maintenance costs must be weighed heavily. Costs should include both initial setup and deployment of the system, as well as the day-to-day issues of management in both the campus and in any dorms. Now more than ever, higher education institutions need to understand the true cost of new initiatives and be able to plan for initial expenses and ongoing costs. It has long been accepted wisdom in the networking world that branch offices— which could be likened to school buildings or campuses—require only a small percentage of your budget to purchase, but the lion's share to deploy, install, and manage.

This issue is in part due to the fact that Wi-Fi networking is still radio. Access points used to require a fair amount of RF understanding to deploy correctly. In many cases this is still true, although there may be different reasons for it. In order to find a Wi-Fi solution that you can afford to own, you must understand:

- What is needed to configure devices, and where is this activity done?
- What is required to install the Wi-Fi network?
- Can installation be done by a non-technical employee? If the vendor answers yes to this question, ask exactly how it might be done.
- How and where are day-to-day management activities handled?

These issues can also depend upon the overall WLAN architecture. As discussed above, different WLAN approaches have different implications on how data forwarding and control traffic are handled. The impact of how the architecture is implemented can quickly increase the cost of deployment and maintenance. Some vendors offer as many as three different architectures: large controller, virtual controller, or access points only. The problem is that the cost of implementation and maintenance varies based on the size and geographic location of each site. Which do I use where? Controller? Virtual Controller? How large a controller to buy? If each site has a different architecture, what will licenses cost at each site? When the IT administrators troubleshoot a problem at a site, the same questions must be asked at every site, because each architecture will require a different methodology for problem isolation and resolution.

ONGOING MANAGEMENT AND TROUBLESHOOTING

Particularly in higher education, it is vital for the WLAN to be easy to troubleshoot. In many cases, the consumer mobile devices being used in the lecture halls, whether university-owned or BYOD, are optimized for battery life, not for radio transmission; unfortunately, the end user will not be aware of that. All users will see is that the wireless network isn't working! It is important to be able to visualize the problem without RF expertise and to quickly track down the primary issue. The optimal WLAN will be one in which it is easy to see the cause of a problem without having to trawl through heaps of incomprehensible, RF-centric logs. AP and user performance should be easy to find quickly and should enable the speedy pinpointing of the issue, which may not be related to the wireless network at all. It is important for the WLAN to provide a means to view a problem all the way down to client-level statistics for faster, more accurate problem isolation even at remote locations.

In addition to monitoring your own network, select vendors have also introduced comparative analytics to allow customers to anonymously and dynamically to compare infrastructure and client metrics to similar-sized deployments and/or industries to help you proactively determine if and where to focus corrective or optimization efforts. Comparative Analytics capabilities allow IT professionals to accurately compare key infrastructure and client metrics both dynamically and over time.

APPLICATIONS & INSIGHTS

Wi-Fi is offering a unique opportunity, with a return on investment never before seen, through information, insight, and applications. The leading WLAN solutions are beginning to leverage their access layer solutions and cloud architectures to provide organizations and schools with an increasing amount of value beyond connectivity. This is a new area to explore with your vendors, requiring a conversation outside of speeds and feeds, and likely a number of new stakeholders within your organization. The smart campus, powered by mobile devices, data, insight, analytics, and applications is very real, offering the opportunity for higher education institutions to not only streamline their operations, but also open up new ways of engaging with their students and staff. When discussing WLAN solutions with your vendors, in addition to asking "how fast is it?" and "how easy is it to manage?", you should include questions like "what value does it offer our school?".

Increasingly, WLAN solutions are utilizing their cloud backend to analyze data points collected from the mobile devices connected to your network. These data points, combined with a rich set of API's and applications, allow your college or university to tap into new business insights that can be used for a wide variety of use cases. Now, your Wi-Fi can be used to determine building space utilization through the tracking of devices, and identify possibilities to re-allocate staff. In-house applications can be created that leverage the Wi-Fi and iBeacons to communicate with your students and staff based on their location, creating relevant engagement and alternatives to traditional communication methods. How about reducing the burden on IT teams for guest administration, by integrating the guest access with a kiosk, so that when a guest enters the office, it automatically generates a secure PPSK for the visitor that is only valid during the visitation times, and when the visitor arrives, their device can be automatically configured for them?

Additionally, Machine Learning and Artificial Intelligence capabilities are starting to be announced by major vendors in the access networking industry. Machine Learning features allow the system to provide enhanced data analytics to display new and insightful information that has never been seen before. Machine Learning paired with a powerful Artificial Intelligence platform provides management systems the ability to stop a problem before it even begins, or the ability to notify administrators of different behavior on the network which could indicate a potential security threat. Wi-Fi is starting to offer far more value than basic connectivity; make sure that you see it in your vendor's offerings.

SUMMARY

Today's Wireless LAN offerings can give colleges and universities tremendous power to enhance the overall learning experience. Deployed correctly, Wi-Fi can help students use their own devices to learn in new and different ways. Professors can look to modern curricula and use new tools to involve classes in ways that have never been possible before. Administrators can see what's really happening on the school network, enabling them to visualize problems before they happen and to plan without overprovisioning. Perhaps best of all, IT can finally have a network that can be configured to maintain security and privacy, while automating processes to the greatest degree possible. Your Wi-Fi network can tie your entire campus network together, with unified wired and wireless policies that can be custom tailored at the touch of a button.

To get that Wi-Fi network, however, you need to ask the right questions. Keep in mind that over time, the operating and management expenses of running a distributed network will dwarf the capital expenditures of the original purchase. Look for a system that is enterprise-class to ensure that you can hone access control by groups, make the most of your authentication infrastructure, and properly segment users. You cannot do your job with less than enterprise-grade security, and it should be built into the system. You must be able to easily obtain a snapshot view of the applications traversing your network—at the campus level all the way to the classroom level—and create custom application signatures if required. And you must be able to immediately visualize and easily troubleshoot the network in order to minimize the time you spend keeping the lights on and maximize the time that you can look forward to what the next year will bring.

About Aerohive Networks

Aerohive uses Cloud Management, Machine Learning, and Artificial Intelligence to radically simplify and secure the Access Network. Our Cloud Managed Wireless, Switching, Routing, and Security technologies provide unrivalled flexibility in deployment, management, and licensing. Credited with pioneering Controller-less Wi-Fi and Cloud Management, Aerohive delivers continuous innovation at Cloud-speed that constantly challenges the industry norm, allowing customers to rethink what's possible. Our innovations and global cloud footprint radically simplify Access Network operation for 30,000+ customers and 10+ million daily users. See how at **www.aerohive.com/customers**.

Corporate Headquarters

Aerohive Networks, Inc.

1011 McCarthy Blvd

Milpitas, California 95035 USA

Phone: 408.510.6100

Toll Free: 1.866.918.9918

Fax: 408.510.6199

info@aerohive.com

www.aerohive.com

International Headquarters

Aerohive Networks Europe LTD

The Courtyard

16-18 West Street

Surrey, UK GU9 7DR

+44 (0)1252 736590

Fax: +44 (0) 1252711901