2017
EDU Buyer’s Guide
The definitive guide for evaluating education K-12 networks
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What To Expect From This Guide</td>
<td>3</td>
</tr>
<tr>
<td>Wi-Fi and WLANs Today</td>
<td>4</td>
</tr>
<tr>
<td>Basic Terminology</td>
<td>4</td>
</tr>
<tr>
<td>Which Access Point is for Me?</td>
<td>5</td>
</tr>
<tr>
<td>Getting a Wi-Fi Deployment That Works</td>
<td>6</td>
</tr>
<tr>
<td>Steps You Can Take to Avoid Interference Issues</td>
<td>7</td>
</tr>
<tr>
<td>Vendor-Specific Architectural Considerations</td>
<td>8</td>
</tr>
<tr>
<td>Considering Both Architectures</td>
<td>9</td>
</tr>
<tr>
<td>Handling BYOD</td>
<td>9</td>
</tr>
<tr>
<td>BYOD Considerations</td>
<td>11</td>
</tr>
<tr>
<td>Security</td>
<td>11</td>
</tr>
<tr>
<td>Security Concerns</td>
<td>12</td>
</tr>
<tr>
<td>Application Visibility and Control</td>
<td>12</td>
</tr>
<tr>
<td>What Can You See?</td>
<td>13</td>
</tr>
<tr>
<td>How Do You Provide Control?</td>
<td>13</td>
</tr>
<tr>
<td>Other Uses for AVC—Did You Know…?</td>
<td>13</td>
</tr>
<tr>
<td>Considerations</td>
<td>14</td>
</tr>
<tr>
<td>Cost</td>
<td>14</td>
</tr>
<tr>
<td>Deployment, Installation, and Management</td>
<td>14</td>
</tr>
<tr>
<td>Ongoing Management and Troubleshooting</td>
<td>15</td>
</tr>
<tr>
<td>How to Buy Wi-Fi</td>
<td>16</td>
</tr>
<tr>
<td>E-rate Modernization Overview</td>
<td>16</td>
</tr>
<tr>
<td>E-rate Process Overview</td>
<td>16</td>
</tr>
<tr>
<td>Changes to E-rate Covered Products and Services</td>
<td>17</td>
</tr>
<tr>
<td>SUMMARY</td>
<td>18</td>
</tr>
</tbody>
</table>

Copyright ©2017, Aerohive Networks, Inc.
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, many 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 classroom to the courtyard. Teacher 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 educational 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. We’ve also highlighted some common perspectives we’ve seen from teachers and administrators, which can add a dimension beyond connectivity.

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 and WLANs Today

Basic Terminology

The IEEE (Institute of Electrical and Electronics Engineers), authors of the 802.11 specifications, 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.

With the advent of the IEEE 802.11n standard, which started in 2007, 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 approval of the 802.11n standard, Wi-Fi networking went mainstream.

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

The 802.11n standard introduced some important technological elements; most important has been the concept of an antenna technology called MIMO, which stands for 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.

802.11ac is Here

In January 2014, the IEEE approved the 802.11ac standard. With this new standard, several advances were realized, including more dense modulation (this just means packing more data onto the same radio wave), more channel bonding (think of this as taking two 2-lane highways and turning them into a single 4-lane highway), and the possibility for more antennas. The first 802.11ac products available today do not include all the specifications from the approved standard. We refer to this as Wave 1 802.11ac, because there were so many big changes with this specification that the chip manufacturers needed time to design it into their products. Most Wi-Fi vendors will introduce the next wave as the chips become available.

The 802.11ac standard is relatively new, so it must be better, stronger, faster, more...right? Well, sometimes. On one hand, 802.11ac can be a great choice for education, and some vendors have led with the offering by making it very cost competitive. There are, however, a few things to be aware of before you rush out and buy a bunch of these 802.11ac access points. First, 802.11ac can generate close to gigabit speeds. This sounds fantastic on the surface—and it is—but it brings up a very important point. Your Wi-Fi network has to connect to your wired network. If your super-fast access points are terminating into a legacy switch, your traffic will run into the networking equivalent of a brick wall.

In addition, 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 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?

The simple answer to this question is that each Wi-Fi specification has benefits. In fact, your best answer may not be 802.11n or 802.11ac, but whether you can use 802.11n and 802.11ac. Like all IEEE standards, 802.11n and 802.11ac are interoperable, and the best AP deployment may well be a mixture of both. 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. At the same time, because the only thing that you can be sure about in networking is that it is all going to change, today’s future-proofing is tomorrow’s legacy gear.
A very good foundational question to ask any vendor, however, is whether their architecture allows you to mix 802.11n and 802.11ac 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 802.11n AP to an 802.11ac 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. And like radio, 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 2.4GHz 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 2.4GHz 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, 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 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 untenable, 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.

Wi-Fi: What You Really Must Know

• Wi-Fi is a broadband connection that runs on two different bands:
  – 2.4GHz, with three non-overlapping channels in the U.S.
  – 5GHz, 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 2.4GHz 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!
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 are distributed 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.** As APs become capable of much greater speed, 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.

### 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 reconfiguration, 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...

- **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?**

### 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 was something of a novelty. Clearly the phenomenon has taken off, and nowhere more than in education. There are compelling reasons why BYOD has exploded, beyond the obvious cost savings; according to the 2014 NMC Horizon Report for K-12, “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.” The report goes on to say that BYOD “... has profound implications for primary and secondary education because it creates the conditions for student-
centered learning to take place." The report concludes that 56 percent of American school districts are implementing BYOD programs, and that schools in the UK are beginning to follow suit. In fact, BYOD practices provide such compelling benefits that many schools augment school-owned devices with a request to parents to consider purchasing devices for their children.

While BYOD provides tangible benefits to students and teachers, 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 at school or accessing school resources should not necessarily affect their connections in other situations. While parents might support the purchase of a device for school use if they are financially able to do so, they are not likely to be inclined to purchase another device on which their child can play games over summer break.

The answer lies in automatic actions that are taken as much as possible 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 district, which allows teachers’ devices to be separated from students’. 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 school 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 substitute teachers, aides, or others who will require access to the school 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 parents and others may want to access. Guest networks should be a standard offering inside the school, 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 school’s resources must be off limits.

BYOD Considerations

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

- How do you enable access to substitute teachers or guests today?
- Does your Wi-Fi infrastructure enable role-based access control?
- Can your infrastructure facilitate a differentiated experience when the user is inside the school or accessing school 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 schools, 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 K-12 for years, as shown in the Federal Educational Rights and Privacy Act and the Children’s Online Privacy Protection Acts in the U.S.; the Data Protection Directive in Europe, and the Privacy Act in Australia, to name just a few. In the era of online testing, security and privacy take on a whole new level of importance. The fact is that 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 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 teacher, 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. What follows are some questions to ask 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 actually 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 a relatively new capability for WLAN gear, 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: Common Core, 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 possible number of students have access to the best gear available; unacceptable use eats schools 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 teachers, 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 school 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—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 teachers 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 teachers 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 central office and in the schools.

![Pie chart](image)

What percent of your department's workload is spent reacting to technical problems (as opposed to working in a proactive mode)?

- 100% 3.8%
- 75% 14.8%
- 50% 26.6%
- 25% 21.3%
- 12.5% 12.3%
- 8.6% 8.6%

2014 CoSN K-12 IT Leadership Study

Copyright ©2017, Aerohive Networks, Inc.
This problem looms large in IT leaders in the education space; the 2014 Consortium of School Networking IT Leadership Study quantifies this intuitive truth, saying, “60% reported that district technology staff has no time to implement new classroom technologies, impacting students directly. Due to this time crunch, school systems will likely struggle when adopting 1:1 and BYOD environments, virtual/blended learning, online assessments, and the transition from textbooks to the digital content needed for successful mobile learning environments.”

The same study goes on to say that 47 percent of respondents report that budgets are not adequate to meet all the technology needs in a school district. Now more than ever, districts 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?
- Could 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 very 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 & Troubleshooting**

Particularly in education, it is vital for the WLAN to be easy to troubleshoot. In many cases, the consumer mobile devices being used in the classroom, whether school-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.
How to Buy Wi-Fi

E-rate Modernization Overview

Three out of five schools in America lack the Wi-Fi needed to deploy 21st Century education tools. New digital learning options offer educators the chance to engage students and personalize learning, but over half of school buildings have outdated wired infrastructures that cannot support interactive and individualized learning tools. With the decreasing costs of tablets and other mobile devices, increases in Wi-Fi speeds, and cloud-based software, schools and libraries are offered a chance for a technology transformation that would have been impossible even five years ago.

E-rate Process Overview

The E-rate process is fairly straightforward. As soon as a district or library decides on the products to request, the designated administrator will file a Form 470, which opens the bidding process to deliver the requested products. Once the vendor has been selected, the next step is to file a Form 471, which is the actual application for funding. The USAC (Universal Service Administrative Company, the organization designated by the FCC as the administrator of universal telecommunications services) will review the application, and approved services will be funded. It is expected that 90 percent of all applications for the 2017 Funding Year will be completed by September 1, 2017. Upon receipt of a funding commitment decision letter, the applicant will file a Form 486 to notify the E-rate program that it is receiving services. Installation may begin as early as April 1, but actual services may not begin until July 1, 2017. All of the forms are now available online and can be filed electronically to help streamline the process.
Changes to E-rate Covered Products and Services

As part of the E-rate modernization plan, the FCC has voted to increase the annual funding cap to $3.9 billion. E-rate will continue to prioritize Category 1 services, focused on providing high-speed broadband connectivity to schools and libraries, as part of the modernization order. However, legacy services, such as email, web hosting, cellular data plans, and SMS texting plans will no longer be funded by E-rate. In addition, funding for Voice over IP (VoIP) and telephone services has been phased out. Category 1 services have a maximum discount rate of 90 percent. The modernization order also released $1 billion in reserves for 2015 and 2016, which is primarily targeted at providing Wi-Fi in schools and libraries. Using E-rate funds, organizations can purchase Wi-Fi access points, Wi-Fi services, such as management or managed services, as well as new technologies like caching servers. These internal connectivity services are part of Category 2 E-rate funds. Category 2 services are funded at a maximum discount of 85 percent, with a budget of $150 per student for schools and $2.30 per square foot ($5 for urban) in libraries.
SUMMARY

Today’s Wireless LAN offerings can give schools 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. Teachers 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 district 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 district 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. Finally, once you have determined the Wi-Fi network that will help move your institution into the future, E-rate is making it easier to apply for—and qualify for—the dollars you need to make that network a reality now.
About Aerohive

Aerohive (NYSE: HIVE) enables our customers to simply and confidently connect to the information, applications, and insights they need to thrive. Our simple, scalable, and secure platform delivers mobility without limitations. For our customers worldwide, every access point is a starting pint. Aerohive was founded in 2006 and is headquartered in Sunnyvale, CA. for more information, please visit www.aerohive.com, call us at 408.510.6100, follow us on Twitter @Aerohive, subscribe to our blog, join our community, or become a fan on our Facebook page.

---

2 2014 CoSN K-12 IT Leadership Study

---

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