Network Planning for BYOD and 1:1 Learning Initiatives
Introduction

Today, K-12 schools provide access to digital resources that allow students to graduate with essential tech skills. Many districts have already embraced 1:1 computing initiatives; others are exploring a budget-friendly BYOD course; and others are working on various combinations of the above. We know that interactive learning and mobile devices can bring the curriculum to life, but schools need an infrastructure in place to deliver the goods. Schools need a new network architecture that meets the requirements of today’s campus—across campus, public venues and remote sites. But most of all, the infrastructure has to be scalable, affordable, and secure.

T&L Editors
How Students Learn

Today’s students are technology junkies who stay connected around the clock. Many of them have tech-savvy teachers and are already well versed in the latest technology skills, but far too many attend schools with outdated equipment and instruction that’s far from the cutting edge. For post-high school success, all students will need to know how to continue to acquire the latest tech skills.

We’ve all heard about how digital learning (any type of learning facilitated by technology) is essential in transforming our schools. The Digital Learning Imperative, published in June 2012 by The Alliance for Excellent Education, showed how digital learning and technology provide access to the most recent information, tools, and resources, allowing students to:

- participate in higher-level courses or earn college credits in high school;
- access dynamic digital content (e.g., science simulations) that allows for more in-depth research and understanding;
- interact with subject-matter experts;
- create their own products;
- work on innovative solutions to real-world issues; and
- personalize learning.

Networking infrastructure, specifically Wi-Fi coverage, is essential to implementing a digital learning initiative. Handheld devices and multimedia applications drive the need for a holistic approach to Wi-Fi coverage. The sheer number of devices and their multimedia traffic represents a whole new scale for consumption of wireless resources, capacity, and security concerns.

Whether districts choose 1:1 laptop programs, iPad deployments, BYOD, or a combination of all three, one thing is absolutely definitive: They must construct a supporting network that is solid, scalable, and secure.
Networking Infrastructure Components

A strong network infrastructure starts with a plan. Try to determine how extensively teachers and students will use digital curricula, as this will allow you to pinpoint the amount of tablets, laptops, smartphones and other mobile devices your district will need. That number will impact the size and scope of the wireless and wired networks to provide reliable, enterprise-quality connectivity.

Next, identify Wi-Fi coverage needs. Robust connectivity is necessary in districts in which students and teachers use tablets and laptops during class. Schools with 1:1 and BYOD initiatives may put an access point (AP) in every classroom to ensure sufficient Wi-Fi capacity. Other areas that you may want coverage include main hallways, libraries, auditoriums, lunchrooms, parking lots, and stadiums.

Once you’ve gotten a handle on coverage needs, it’s time to focus on affordability, scalability, and security.

Affordability
Because financial resources are tighter than ever, schools need solutions that address their current and future needs. School networks must be able to move forward with advances in technology, devices, and applications while providing compatibility for legacy devices.

Security
Obviously, security is paramount, especially when students bring school-owned devices home. Threats come from inside and out. School Wi-Fi coverage must protect internal assets, block malware, support guest access, and isolate sensitive traffic from the rest of the networks. It should allow you to differentiate access by user and device, and ensure that any student-owned device can pass a minimum posture assessment.

A common solution is to use a firewall that monitors all data entering or leaving the network, blocks data that does not satisfy specified security policies, and prevents unauthorized users from accessing the network. Firewalls can also serve to limit packets and control bandwidth for different classes of users, such as students and guests. In addition to a firewall, schools must also consider wireless-intrusion-protection systems that safeguard the network from unauthorized or rogue APs and...
clients, and other devices that can potentially harm network operations.

To comply with CIPA, schools must use Internet filters and other measures to protect the children from harmful online content. This gets even more challenging when laptops and other mobile devices go home, since the district is still responsible for protecting students when they view Internet content from school-issued devices at home. While this is typically not a function of the Wi-Fi, finding a Wi-Fi solution that simplifies the integration of a content solution such as OpenDNS is a must.

**Scalability**
Planning for mobile devices is a moving target. Today, your district might be providing wireless access to 100 PCs, but in six months that number could double. And once you let students BYOD, the amount of devices can quadruple. Ultimately, you’ll want your wireless network to be able to support thousands of concurrent devices with minimal IT involvement.

For K-12 districts with numerous buildings, the key is to be able to extend wireless connectivity within a given building and across several campuses without sacrificing feature richness, affordability and ease of use. Many districts start with standalone, consumer-grade APs, only to find that this option does not offer enough scalability, reliability, manageability, and security. Depending on the scale and a number of other network engineering reasons, schools may choose a distributed or centralized Wi-Fi architecture. These options are detailed in the next section.
Wi-Fi Architecture Considerations

While there is no one-size-fits-all Wi-Fi solution, the truth is that enterprise-grade APs that use a distributed Wi-Fi architecture can offer the simplest, most efficient, cost-effective Wi-Fi solution. A distributed Wi-Fi architecture means the wireless configuration and decision-making is done on the APs without a central appliance or controller. With a distributed solution, Wi-Fi and security functions are distributed to the individual APs that make up the Wi-Fi coverage. Adding Wi-Fi coverage is as simple as adding a new access point. New access points pull their configuration from one of the already installed access points.

Centralized Wi-Fi architecture, in comparison, relies on a centralized mobility controller for a number of Wi-Fi coverage functions, including configuration, management, roaming and security, to name a few. The centralized approach is typically better suited for schools and districts that have more complex Wi-Fi requirements. As an example, the more the number of APs, the easier it is to design a network with a centralized controller, as APs don’t need to be configured with VLANs. Another common-use case is to have a singular policy for wired and wireless. In some cases there is need to add VPN for remote access. In both these cases, mobility controllers can act as the single interface to support hundreds of APs, wired switches, VPN and even remote devices.

Perhaps the best of all worlds is to find a solution that offers a combination of distributed and centralized Wi-Fi architectures. Regardless, when you’re doing your scouting, look for a feature-rich Wi-Fi provider that:

- Provides comprehensive security that includes guest access, a firewall and intrusion protection against rogue APs.
- Offers high performance to accommodate a range of device and traffic types, including data, voice, and video;
- Scales easily, both within a given site and across sites; and
- Allows users to roam without logging in each time they move from one AP to another.
Aruba’s K-12 Wi-Fi Solution

Aruba Networks offers the best mix of distributed and centralized Wi-Fi architectures designed for the affordability, security and scalability schools need. Aruba’s solution includes:

**Aruba Instant**, which employs a distributed architecture, can be installed at a single school site or at multiple locations. It’s a feature-rich, enterprise-grade Wi-Fi that combines affordability and configuration simplicity. A district can start with Aruba Instant and protect its investment as needs grow. If the number of sites expands or the district needs to integrate wired, wireless and VPN connectivity into one cohesive solution, it can re-image Aruba Instant APs as 802.11n campus APs and migrate to a centralized Mobility Controller architecture.

Unlike other Wi-Fi management products, Aruba Instant eliminates the need to configure and troubleshoot individual APs or dispatch IT personnel onsite. From a remote location, IT leaders can centrally configure, monitor, and troubleshoot Aruba Instant Wi-Fis, upload new software images, track devices, generate reports, and perform other vital management tasks.

The Apple Connection: Enabling access to Apple Bonjour services like AirPlay and AirPrint is more crucial than ever in K-12. Bonjour-enabled Apple TVs, for example, allow teachers to easily project to HD televisions in the classroom from their mobile devices. Aruba AirGroup, an integrated capability of Aruba wireless LANs, is an essential companion to Bonjour in schools. First and foremost, Aruba AirGroup extends Bonjour services across multiple IP subnets. Additionally, AirGroup has the ability to distinguish between shared devices and personal devices so only teachers have access to the classroom AppleTV. AirGroup can also add location relevance to show only shared devices in close proximity to the user.

One of the main benefits of Aruba AirGroup is the improvement of Wi-Fi performance. AirGroup essentially filters network traffic generated by Bonjour to greatly minimize the unnecessary chatter.

With **Aruba ClearPass**, IT directors can discover all devices on the network—including personally-owned devices, printers, phones, and guest devices—and get contextual information about them. ClearPass automatically classifies and stores this information within profiles that are used to enforce network access policies. ClearPass lets you enforce these access policies across any existing network infrastructure, regardless of vendor. In a nutshell, ClearPass simplifies troubleshooting for BYOD.

**ClearPass Guest**, a key component of Aruba ClearPass, is a scalable, easy-to-use visitor-management solution that delivers secure wireless network access to guests, employees, and their mobile devices. ClearPass Guest streamlines workflow processes, allowing receptionists, employees and other non-IT staff to create temporary accounts for Wi-Fi access. Once registered, ClearPass Guest delivers account login credentials.
to users via SMS text message or email. Accounts can be set to expire automatically after a specific number of hours or days.

**Are You an Apple District?**
Aruba Networks has added a number of innovations in its Wi-Fi solution to make it the best choice when Apple devices are on the network. These include:

- Aruba has the only Wi-Fi that automatically detects and prioritizes Apple FaceTime calls over lower priority traffic, making sure FaceTime calls are clear and uninterrupted.

- Aruba AirGroup makes it possible to use Apple Bonjour services at school or at work. With AirGroup, only the necessary set of services are made visible to mobile devices, based on the user identity and location.

- Aruba ClearPass allows users to self-register new iOS and MacOS devices, so you can take IT out of the equation when your staff or students BYOD. ClearPass can even revoke access for devices that are lost or stolen.

- With Aruba’s Adaptive Radio Management (ARM), Apple devices can be used in large, dense environments like stadiums and auditoriums. ARM maximizes the efficiency of the wireless network for Apple devices and guarantees reliable delivery of high-priority and latency sensitive traffic.

- Aruba AirWave network management software gives you visibility of mobile device types and operating systems as they connect to an Aruba Wi-Fi. Apple device inventory reports can be customized based on location, time period, and Wi-Fi SSID.

---

**Resources**

- Best Practices for Wi-Fi in K-12 Schools
- Aruba Wi-Fi for Apple
- Bring Your Own Device
- Aruba Primary Education Solutions
- Aruba AirGroup: Get Your Wi-Fi Ready for AirPrint and AirPlay
- The Digital Learning Imperative: How Technology and Teaching Meet Today’s Education Challenges

Sponsored By