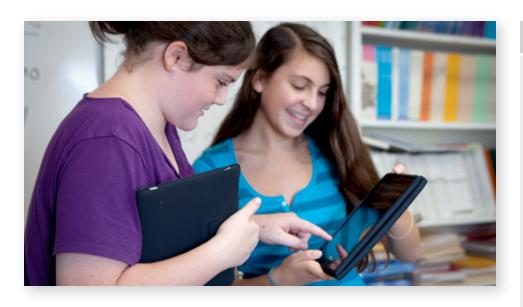# Classrooms at Risk
Solving the Challenge of Student-Owned Devices

Overview

Today's K-12 classrooms are loaded with technology, both classroom-based technology aids, such as intelligent whiteboards, and portable electronic devices, such as laptops, netbooks, tablets and smartphones. Teachers are using the school's network to supplement their curriculum with Internet and cloud-based education applications and content. The need to engage digital learners requires the use of a multitude of education tools, which in turn drive the need for 1:1 computing, where each student has his/her own WiFi-enabled networking device. As schools continue to struggle with budget cuts, 1:1 computing often takes the form of students bringing their own devices to school.

Similar in nature to the Bring Your Own Device (BYOD) scenario in the enterprise, where workers use their own laptops or tablets as their primary networking devices, students are often bringing their own networking devices to school. In many cases, it's out of necessity. Schools typically can't afford to provide a laptop or other networking device for every student. Yet, there is an increasing need for students to have such devices to enable them to better engage in their education. Consequently, many school districts encourage their students to bring their own networking devices to school and have established policies and guidelines to define appropriate use for these devices. The influx of personal networking devices into the classroom, which exemplifies the "consumerization of IT", has increased the need for wireless network connectivity and is fueling 802.11n network rollouts and upgrades in schools. The end result is a student body equipped with a variety of networking devices and ample access to a wireless network. A 1:1 computing model and high speed network access are important components of a 21st century learning environment; however, the IT department must have sufficient visibility and control to ensure students' privacy and safety as well as enforce appropriate network behavior.

Benefits

Business Alignment

- Mobile access to education tools with advanced QoS capabilities to support multimedia applications

- Role-based network access and service provisioning provide differentiated services for customer-specified user roles (e.g., teachers, students and guests)

Operational Efficiency

- Provide out-of-the-box network policies based on K-12 operations best practices

- Automated access provisioning for any device type entering the school's network to support 1:1 technology initiatives

Security and Compliance

- Provide demonstrable controls for compliance audits (e.g., Children's Internet Protection Act (CIPA))

- Granular access control enforces Acceptable Use Policies with robust security for private/BYO devices to ensure student privacy

- Complete visibility and control of the school's airspace ensures that only the school's WLAN is able to provide network connectivity

Support and Service

- Industry leading customer satisfaction and first call resolution rates

- Lifetime warranty on access points and controllers to minimize total cost of ownership

Exploiting Technology to Enable Unauthorized Network Access

Technology-savvy students utilize their school's wireless network to satisfy their social desire to be "always-connected", which is proving to be a challenge for teachers, administrators and IT directors. By the time students reach middle school, they already have an established on-line presence and an electronic social network. The desire to communicate and interact with their world far outweighs students' ability to discern prudent on-line behavior. The explosion of personal networking devices combined with pervasive network access can lead to problematic student behavior, such as accessing inappropriate material on the Internet, engaging in cyber-bullying, cheating or other activities that might disrupt the classroom.

Driven by laws such as the Children's Internet Protection Act (CIPA), many school districts have adopted an extremely heavy-handed approach and ban the use of all personal networking devices. Such stringent policies are in direct conflict with the need to engage 21st century learners and school districts rarely have the resources to provide every student with a networking device. The solution is to strike a balance by encouraging students to bring their own devices and providing them with network access tempered by appropriate safeguards to ensure proper netiquette by enforcing local policies as well as state and federal laws.

Unfortunately, students have discovered applications such as MyWi, soft-AP and WiFi tethering, that enable them to bypass the managed network and gain unfettered access to the Internet. These applications enable a dual-mode (cellular and WiFi) device to operate as a rudimentary wireless access point and provide other WiFi devices with an unsecure Internet connection via the cellular network. Even though the students connecting to a MyWi-enabled device are not on the school's network, they are on school property and the school administration is still responsible for their behavior.

Controlling the Airspace

In an environment where students are allowed to utilize their own networking devices, the ability to maintain control over the WLAN and its associated airspace is directly dependent upon network visibility and granular network control. An Enterasys WLAN solution compiles and maintains a list of authorized users for the school's network by detecting, authenticating, classifying and authorizing every device connecting to the network in a fully automated and dynamic fashion, thus lowering overall operational costs while maintaining the necessary levels of security.

The Enterasys WLAN solution provides complete visibility over the school's network as well as its airspace. Utilizing a combination of tunable parameters relating to signal strength and location, a MyWi-enabled device operating on school property is automatically detected and identified as an unauthorized access point (an access point that is operating in the school's airspace but is not part of the school's network). Once an unauthorized access point of any kind is detected, the Enterasys WLAN solution pinpoints its physical location, generates appropriate notifications to the IT staff and automatically blocks WLAN connections to the unauthorized device. Therefore, the Enterasys WLAN solution effectively thwarts the ability for any unauthorized access point, including MyWi-enabled devices, from operating on school property and prevents students from gaining unauthorized access to the Internet.

This ability to detect and preclude the use of MyWi-enabled devices while simultaneously supporting the "consumerization of IT" is yet another example of how an Enterasys WLAN solution can be leveraged to address evolving requirements in the IT infrastructure. An Enterasys network (either wireless, wired, or both) provides a high degree of automation, visibility and granular control to ensure student safety while reducing operational costs for IT departments.

Why Enterasys for K-12

Enterasys networking solutions provide unique capabilities that are leveraged by K-12 IT staff around the world to control and prioritize access to education applications, ensure continuing availability of networked resources, provide wireless and wired services to administrative staff, teachers, students, and guests, and ensure enforcement of appropriate access control to student and institutional data.

Enterasys is committed to helping our K-12 customers deploy and optimize networking solutions that are uniquely tuned to their environment and specific needs. To that end, Enterasys provides network policy templates based on best practices as well as policies unique to K-12. These policies leverage the existing network design and provide immediate value with no risk, and serve as building blocks toward more advanced capabilities. As a strong complement to our technology offerings, Enterasys customer support offers unparalleled expertise and customer care to ensure our K-12 customers get the help they need to keep their operations up and running and enabling the highest quality education. To find out more about Enterasys and our award-winning networking solutions, please visit www.enterasys.com

Contact Us

For more information, call Enterasys Networks toll free at 1-877-801-7082, or +1-978-684-1000 and visit us on the Web at enterasys.com

Thought Leadership
Patented Innovation

enterasys®
Secure Networks™

Delivering on our promises. On-time. On-budget.