STEM and Robotics

Extreme Networks for Primary and Secondary (K-12) Education

Introduction

Primary and secondary education (or K-12 as it's called in the US and Australia) is all about delivering better educational outcomes, and preparing students for a rapidly-evolving workplace. In the past, education was simply about reading, writing, and arithmetic; and learning facts about history and geography. Today those are still important but a simple good search can easily provide facts-on-demand. A cloud-driven network is also crucial to keep pace with new leading technology and operate as a smart classroom that exceeds staff and student expectations.

Other skills have become a much higher priority for students to learn, including STEM skills (that is, science, technology, engineering, and math); and collaboration skills. In fact, many schools now teach classes on web search. Class project reports are no longer simply written or typed out, but now must include rich multimedia.

Robots, labs, drones, and STEM learning are important for preparing students for the jobs that will be available when they graduate. Augmented, virtual and mixed reality (AR/VR/MR) play a growing role at all levels of education, not just increasing student engagement, but reducing costs as students can travel to and explore remote lands and historic times from within the classroom.

The Internet of Things can improve the efficiency of the physical campus infrastructure, including HVAC and physical security. The range of IoT devices appearing on campus includes: eBooks and tablets; sensors in the hallways, entrances, classroom spaces, and buses; all sorts of fitness bands and wearables; virtual and augmented reality headsets; robots; video cameras and sensors; smart displays; smart lights; and smart locks, to name a few.

Critical Technology Issues

Insufficient Connectivity and Bandwidth for STEM and Robotics Devices and Controllers

Robots, labs, drones and STEM learning technologies require continuous connection to the network. These devices and environments provide an enormous amount of data that can be analyzed and turned into actionable information. This presents the challenge of providing adequate wireless bandwidth to handle the streams of data and to rapidly respond as necessary. For these devices to operate smoothly there can be no bottlenecks from the Wi-Fi access points, back through the wired switches, and all the way through to the broadband internet connection and the data center.

With these new devices coming and going on the network, it can be a challenge to provide easy onboarding, and to imbue them with appropriate access to resources. Some devices should be permitted to join the network only from designated locations, while it is important for other devices to maintain network access from all locations across the campus.

Risk to Student Privacy and IT Resources

In the midst of the diversity of devices on the network, student and faculty privacy and security must be fully maintained. FERPA is just one of the US federal laws that protect the privacy of student education records. While the network must be capable of connecting all devices, it must also be very selective in doing so. Authorized devices should be expeditiously and effortlessly onboarded, while unauthorized devices must be prevented from gaining access to the network. The best way to implement this is with a defined policy as to which devices, users and apps can access the network resources from defined locations at specified times of day. This policy needs to be implemented consistently across the network. Firewalls prevent access from outside sources and web filters prevent visits to malicious sites that can damage the network. To smoothly implement network policy across all resources requires integration with firewalls and web filters. The network must be capable of both controlling and monitoring all devices and network activity.

Unapproved applications and rogue devices pose a constant risk to the network. If a rogue device were to appear on the network, it could permit unauthorized access or interface with the devices. A means to monitor all devices and applications that operate across the network is vital.

Continuous Availability

The connections with the STEM and robotics devices must be highly available or fault tolerant to insure uninterrupted teaching and learning. This may require redundant access points, controllers, and switches.

Visibility into device usage, website access, bandwidth consumption, and patterns of activity is important for optimizing the user experience and verifying that all digital educational content is reliably delivered. This tracking and visibility is also vital for optimizing the infrastructure design and for short-and long-term network planning.

Providing Adequate Technical Service and Support

As schools become adoptive of STEM and robotics labs and other 21st century technologies to provide personalized education, it is vital that any service or technical issue be resolved immediately on a 24x7 basis.

Round-the-clock access to a global technical access center (GTAC) ensures that all support questions can be answered promptly to keep the network functioning at all times. Prior to installation, it is important to survey and assess the RF characteristics of the site to determine optimal placement of access points and switches. Depending on the level of network support resources available on campus, network training and managed services may be required.

The solution described below provides school districts as well as universities and colleges with the network infrastructure necessary to insure reliable implementation of STEM and robotics labs on campus. This includes the means to efficiently onboard and manage both school-owned and student-owned STEM devices on the network, as well as maintain adequate data bandwidth to accommodate the data steams involved. The entire cloud-driven network can be managed from a window. That single window can also set policy for all devices, to determine which resources each device can access across the network. The policy is based on a range of parameters including user, device type, location, time of day, and 40 more attributes that set device access rights.

Extreme Networks is the only company in the industry that takes an architectural approach to bringing products to market from R&D to product release. As a result, all of our network products from wireless to wired are managed by a single Extreme Management Center console for easy administration by resource-constrained IT teams. Our open, standards-based, and comprehensive SDN enables simple integration with third party technology such as web filters and firewalls. Extreme Networks' cloud-driven networking solutions give every educator and student a better experience, every community a better connection, and every IT organization a better partner.

Summary

Today's STEM and robotics lab require a network that can reliably connect a wide variety of devices, many of which are date bandwidth intensive. Such network connections can become a vector for security breach, if not properly managed and monitored. Extreme Wi-Fi provides the dependable, high-density, and high-performance connections required. Extreme Management Center helps shape traffic within the network to insure bandwidth and performance where it is needed for high digital loads. ExtremeControl makes sure only the authorized STEM and IoT devices get access to the network. Extreme Switching provides both the connections and the PoE power to IoT devices in the classroom.

Extreme Networks provides campuses with the solutions to create open, cloud-driven educational networking solutions that are intelligent, adaptive, and secure. Whether it's online testing, virtual and augmented reality, STEM and robotics, or flipped classroom initiatives, more than 17,000 schools and 4,500 campuses worldwide rely on autonomous networks from Extreme to improve their educational outcomes.

Additional Resources

To learn more please visit the Extreme Networks K-12 and Primary/Secondary Education Solution Center.

Extreme networks

http://www.extremenetworks.com/contact