opengear

WHITE PAPER

Getting Smart About Network Resilience In Education

From distributed campuses to new digital initiatives and security requirements, network engineering teams are constantly facing evolving challenges. Cloud computing, 5G and integrated networks are contributing to classrooms transforming into digitally sophisticated environments. These along with the integration of IoT and distance learning into curriculums has created an even greater need for always-on connectivity. This white paper discusses the proper solutions for educational institutions to deploy to ensure network resilience needs are met.

GETTING SMART ABOUT RESILIENCE

Over the past few decades, technological advancements at the edge have sparked a transformation throughout the education landscape. From distributed campuses to distance learning and smart classrooms, complex education networks are constantly expanding with new digital initiatives.

For colleges, universities and K-12 (Kindergarten through 12th grade) institutions, networking and IT teams are facing new challenges. These facilities are essentially small enterprises located in a local space or could consist of buildings located across the country. Charged with maintaining large, local wireless and fixed WAN networks that include multiple locations and span broad geographies, engineers are reliant on having always-on access. From identifying security threats, to supporting disparate collections of network devices and maintaining privacy information, these challenges impose responsibility on school IT operations staff to keep networks constantly running.

LEARNING REMOTELY

The global pandemic has increased the integration of distance learning into the digital curriculum. Not to be confused with online learning, the main differentiators between that concept and distance learning includes location, interaction and intention.

Online learning, which still requires constant connectivity, allows students to learn together in the classroom with an instructor and also complete digital assignments. It usually involves in-person interaction between a student and teacher on a regular basis – this technique is blended with other strategies in the classroom. It's a supplemental way of switching things up to provide a variety of learning opportunities for students.

Distance learning has becoming increasingly popular with the current regulations and mandates revolved around work, travel and life in general with almost every region closing the doors to its schools. This approach has teachers check in digitally and students' complete assignments at home. There is no in-person interaction and digital forms of communication are relied on such as learning management systems (LMS) for the school, video calls and discussion boards.

One challenge with online and distance learning is that if the network is down, students aren't able to access learning materials, complete assignments or check in with teachers. So a thoughtful approach to network resilience is a necessity for schools implementing these learning techniques.

INTEGRATING IOT INTO CLASSROOMS

Schools and universities across the world are building smart Internet of Things (IoT) into their educational networks. IDC predicts that in 2025 there will be more than 40 billion connected devices. The advancement of these devices, along with cloud computing, integrated networks and 5G will allow the internet to transform physical classrooms into digitally sophisticated environments. The idea behind using IoT in the classroom is no longer just about internet accessibility, it's about extending connectivity beyond traditional smart devices to engage students, create immersive learning experiences and solve common challenges. These include:

Just since 2012, internet speeds at colleges have nearly tripled as interconnected devices, services for streaming and gaming platforms have flooded onto education scene, battling for room on the network.

The RESReport conducted a study on major bandwidth usages on college campuses, findings include:

- 52% for gaming
- 61% for music streaming
- 78% for rich web content
- 88% Netflix and streaming services

Data Collection: IoT allows education institutions to manage four key areas, which are energy management, monitoring students' healthcare, classroom access control and improving learning.

Personalized Learning: IoT allows each student to be evaluated and monitored on an individual basis, allowing instructors to modify coursework as needed.

Human To Machine Interaction: This allows students to learn at their own pace using interconnected devices such as smart pens, tablets and digital textbooks. It also saves time and resources while maintaining a higher standard of teaching.

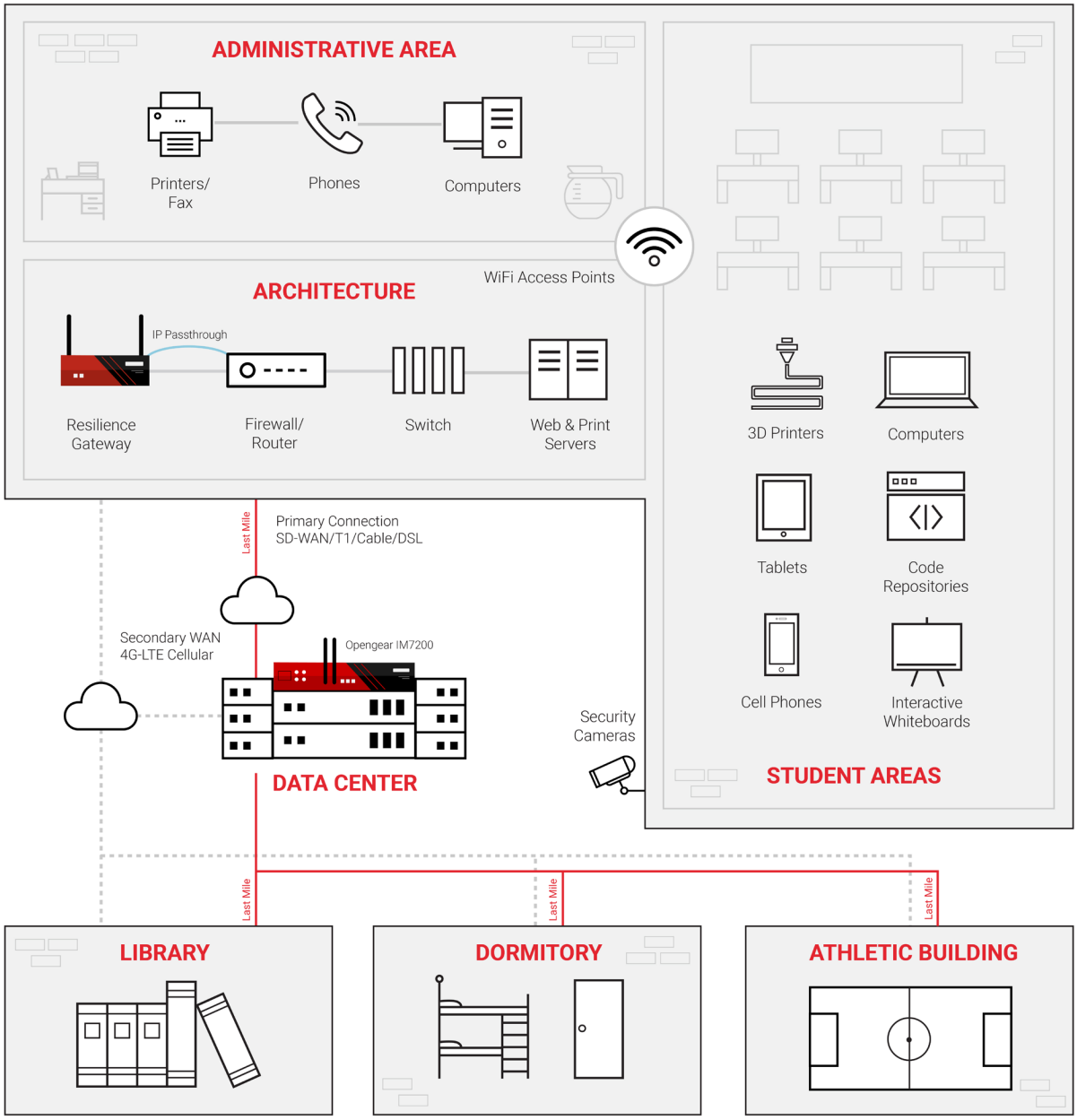
Security: Due to the large amount of data collected within the walls, education institutions are targeted by hackers. GPS tracking, facial recognition and remote RFID checks can detect any potential intruders and help maintain HIPPA compliance.

IN-BAND AND OUT-OF-BAND

There are two ways to manage a network, through in-band management and Out-of-Band management. In-band is managing the network through the network itself. So, if an outage occurs, there is no way to reach the affected devices and remediate the issue.

Out-of-Band management provides an alternate way to connect remote devices without directly accessing the IP production address in the data plane and is also independent from an enterprises' primary ISP. Providing the ability to manage, monitor and access devices without interfering with normal operations, it is separate from the production network.

EDUCATION INFRASTRUCTURE



Students and faculty continue to demand faster, more innovative applications and devices. Although these IoT devices allow educational institutions to bypass limitations imposed by traditional cloud based networks, they do place a greater strain on the network which increases the likelihood of an outage, creating a need to analyze current IT infrastructure at each facility.

As campuses grow, IoT systems of the future will be edge-heavy not only in number of devices, but also in the level of sophistication with the provisioning, monitoring, management and remediation needs that come with it.

Many educational institutions aren't considering device and system management as something that is highly distributed, with the need to setup a management plane that is separate and works independently from the data plane or production infrastructure.

Managing an IoT system in this environment involves the use of alternate connectivity and dedicated management devices that provide resilient access to the IoT devices at the edge of the infrastructure for management purposes. These intelligent devices will require continuous provisioning, configuration, monitoring and remediation to provide resilience.

CREATING THE IDEAL NETWORK

Networks are the lifeline of a campus. This infrastructure connects students to resources and devices needed for learning that are spread throughout geographically dispersed areas. Due to this unique set up, when designing a campus network, there are five essential architectural components to support evolving educational requirements.

Cisco's Pathfinder report states that these are:

Wired/Wireless convergence: Primary modes of network access are wireless and mobility. To ensure consistency with both, wired and wireless traffic must be treated the same, with the enforcement of specific policies in regards to operations, administration, security and more.

IP convergence of non-IP networks: Non-IP infrastructures including security and utility networks benefit from a single IP-based fabric. Converging disparate campus infrastructures allows individual networks for each service be funneled into one.

High availability: Switches in campus infrastructures need scalability to support increasing requirements and deployment options. Needing to be resilient and highly available, chassis and per slot bandwidth in the hundreds of gigabits are necessary to meet IT demands.

Connectivity models: Campus networking must evolve to meet growing types of connectivity requirements from new end points such as mobile devices, smart phones, laptops and more. What's needed is a flexible network architecture that is able to support any connectivity requirements without having to introduce new technologies to address individual end point types.

Automation: The constantly growing number of connected devices requires automation to ensure reliable operations. REST APIs can instill automation in the application processes, enabling communications and interoperability.

Education facilities are sprawling, with equipment located in the array of buildings that may be a few yards or miles away. Lacking the dedicated technical staff at these edge locations, if a disruption occurs, it may take longer to remediate, bringing all learning to a complete standstill.

Network outages on a campus can result in:

- **Disruption of educational processes:** Challenges with accessing necessary resources can interrupt progress with learning.
- **Loss of staff productivity:** When staff aren't able to access financial, operational systems and learning management applications, normal day to day tasks are impacted.
- **High recovery costs:** Performance drop offs, wireless outages and poor connectivity can cause damage to an educational institutions reputation.

ADDING RESILIENCE TO THE EDUCATION NETWORK

Smart Out-of-Band provides an alternative path to devices located at remote sites, when the network is down. Providing access to edge infrastructure from anywhere, it is separate from the production network so issues are able to be in identified and remediated remotely.

It enables educational institutions to improve day to day operations by providing always on access and allowing engineers to remediate issues with proactive monitoring. Preemptively recognizing and remediating issues, truck rolls are reduced and learning is able to continue without interruption. *Smart* Out-of-Band is scalable, providing the ability to manage infrastructure at distributed sites. Troubleshooting and remediation at the network's edge allows schools to detect faults before they become failures which minimizes downtime and operating costs.

***Smart* Out-of-Band allows educational institutions to:**

- Detect and remediate issues automatically
- Operate independently from the in-band network
- Send automated alerts of network issues via email or SMS
- Find network and environmental inconsistencies

The resilient backup connectivity allows schools to reduce the time-consuming nature of dispatching engineers to data center sites to make configuration changes and troubleshoot issues to ensure operation continuity.

GETTING SMART AT THE EDGE

Extending Your Reach: *Smart* Out-of-Band and Failover to Cellular™

Smart OOB™ allows administrators to manage infrastructure at the edge, detecting faults before they become failures. Automation combined with advanced troubleshooting and remediation at the network's edge allows schools to reduce operating costs and minimize downtime using distributed, remote console servers.

Failover to Cellular™ provides continued internet connectivity for remote LANs and equipment over high-speed 4G LTE when the primary link becomes unavailable. Robust IP Passthrough technology allows for easy integration into existing installs or can be rapidly deployed for instant-on connectivity for remote networks and branches. In the event of a disruption, engineers are able to manage, access and monitor all devices.

CONCLUSION

Continual digital innovations are poised to reshape learning approaches. As IoT connected systems continue to scale, campuses expand and teaching strategies become more digital, educational institutions can't rely on centralized data centers to process and collect large amounts of data that are constantly being collected.

All of these factors are challenging educational institutions to diversify their networking initiatives to ensure constant connectivity. *Smart* Out-of-Band ensures that these schools have always-on network access to deliver the network