Laying the groundwork for tomorrow's digital schools

Primary and Secondary Education Networking Guide

Alcatel·Lucent Enterprise

A network foundation for digital learning

Advanced technology in elementary and secondary schools creates new ways for students to learn, and changes how teachers plan and deliver lessons. It also provides the digital tools for school administrators to simplify operations, better comply with regulations, and deliver a safer environment for students and teachers.

Is your school network ready for the digital education innovations of the future?

This guide provides information and strategies for how school administrators and IT teams can design efficient and cost-effective IT networks that enable dynamic digital learning experiences. This secure, high-performance platform supports administrative innovation for today and into the future.

Changing realities for students and learning

Today, most students in primary and secondary schools have never experienced life without the internet or smartphones, and this reality is reflected in the classroom. Digital learning processes and experiences are enhancing traditional textbooks and upending conventional classroom teaching methods. Online lessons, testing and assessments are now part of most curricula. Laptops, tablets and smartphones have become primary instruction tools for students, who are downloading an increasing number of online apps to enhance their digital learning experience.

The underlying IT network that supports these innovative educational advances must be a cost-effective investment today, while also extending value into the future as a platform for new technologies entering the educational space. These include:

- The Internet of Things (IoT)
- Augmented and virtual reality
- Learning experiences in coding
- Makerspaces
- Robotics and other STEM initiatives (science, technology, engineering and mathematics)

In today's educational facilities, the network must address the needs of school administration, staff and IT departments. For these audiences, data privacy plus network and device security are of primary importance. Other considerations include:

- Deployment and procurement costs
- Ease of device onboarding
- Network speed and coverage
- Training and operational simplicity

To support these diverse users requires pervasive wireless connectivity and a robust, secure wired Local Area Network. Wi-Fi is the dominant wireless networking standard as it allows users to be located virtually anywhere and to employ any device. However, as use of mobile devices increases, existing networks can easily be overwhelmed with increasing bandwidth demands.

Preparing your school network for tomorrow's digital advances in learning, teaching and administration requires a thoughtful approach and a comprehensive strategy to ensure investments are future proof and ensure optimal interoperability.

This document provides eight tangible recommendations for IT departments in primary and secondary schools to use in designing efficient and cost effective school networks. Building a school network infrastructure that addresses these requirements will enable more collaborative digital learning experiences, support more creative teaching methodologies, and empower administrators with the latest monitoring, analytics and management tools..

Market trends

Primary and secondary schools are undergoing a digital transformation. Technology is the driving force for enabling more personalized and dynamic learning experiences for primary and secondary students. These advances are impacting the classroom in a variety of ways.

- **Digital and immersive textbooks**. Today, digital textbooks have displaced paper textbooks in many primary and secondary classrooms. They have advantages over physical books, including instant availability, ease of updating, and the ability to store many e-books on a single device. However, digital textbooks are in turn being displaced by immersive textbooks that employ interactive technologies, advanced user-experience design, and gamification to enhance instruction, make learning more engaging, and address differing learning styles.
- **Game-based learning**. Game-based learning blends video game technology and online learning tools to make teaching and training more engaging. These technologies are designed to take advantage of virtual and augmented reality to increase student engagement and content retention.
- **Blended learning and the flipped classroom**. The blended learning model combines classroom and online learning to give students more control over the time, pace and place of their instruction. Blended learning is ceding importance to the flipped classroom model in which students watch video lectures on their own and then attend class for discussions and collaborative activities.
- **1:1 student to device ratios**. Many educational institutions have made the commitment to a 1:1 ratio between students and devices. This is now shifting to a one-to-many paradigm where different tasks require different devices, and students need access to laptops, tablets and smartphones depending on the project.
- **Digital testing**. Online testing and assessment technology helps teachers and administrators more accurately and meaningfully measure student achievement. Digital testing can provide detailed insights into the success of learning methods and offer detailed metrics and analysis for developing remediation solutions. These platforms provide visibility into how individual students are interacting with online content, enabling ongoing monitoring of individual learning.
- **Predictive assessment capabilities**. At the cutting edge of assessment technologies is the development of predictive assessment capabilities that can track student proficiency without actual testing. By monitoring how individual students are interacting with educational content and relating that data to past testing scores, advanced analytics platforms can make predictions about the progression of students without having to submit them to constant testing. The same platform can also provide teachers with targeted recommendations and relevant lessons to address the needs of individual students.
- **Bring Your Own Device**. With the Bring Your Own Device (BYOD) movement students and teachers bring their private devices to the network. This may be a boon in districts that can't afford to equip classrooms with a variety of devices, but implementing BYOD securely and effectively can present challenges. Many conventional IT networks weren't designed to support a diversity of devices and protocols, and the school's underlying infrastructure must be sound enough to support multiple disparate devices and networks while guaranteeing interoperability and security.

The role of technology

The role of technology in primary and secondary education has moved beyond the substitution of physical textbooks by e-books. To take advantage of the opportunities offered by these advancing technologies will similarly require moving beyond the constrained IT networks found in most schools today.

IT networks that keep pace with today's students

The advances mentioned above are moving so fast and are proving effective because today's students are more technologically sophisticated than ever before. These students expect to experience the same innovations in their classrooms as they do in social media and entertainment.

Students today also understand that familiarity with advanced technologies is important beyond the use for teaching. Gaining proficiency with a variety of device types and having experience with applications such as augmented or virtual reality help students prepare for success in tech-intensive university education.

According to a 2017 survey of 43,559 undergraduate students in 124 institutions in 10 countries conducted by EDUCAUSE Center for Analysis and Research, 96 percent own a smartphone, 93 percent own a laptop, and 85 percent use their laptop for academic purposes in most or all courses. Students surveyed also approved of teaching methodologies that embrace technology. Forty-six percent of respondents said they get more involved in courses that use technology, and 78 percent agreed that the use of technology contributes to the successful completion of courses. Eighty-two percent preferred classroom methodologies that feature a blended learning environment.[1]

1 EDUCAUSE, Technology Research in the Academic Community, Student and Faculty Technology Use Study, 2017
2 Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016

IoT supports institutions educational, safety and operational needs

Connected teaching technologies and the IoT are already prevalent in the classroom and in use for campus security and administrative purposes.

Smart audio-visual equipment such as interactive displays, smart boards and digital projectors have been fixtures in classrooms for some time. Apple TV is also popular in classrooms for online streaming content via Wi-Fi. This technology makes it easy to mirror screens from student iPads; watch streaming news, videos and other content; and take part in group video calls via services such as Skype and FaceTime.

Science classrooms and labs are increasingly connected. A growing emphasis on STEM education plus interest in encouraging Maker culture requires the support of new device types, including robotics, Raspberry Pi and other development platforms.

IoT has a growing presence in education, particularly in campus security applications. These include surveillance cameras, smart door locks and connected buses. In addition, integrated school safety technologies provide students with smart ID cards to strengthen facility access management systems. IoT also offers easier management and cost containment of infrastructures such as HVAC, lighting and landscape management.

A more connected school infrastructure requires a more powerful IT network

Supporting these innovations in teaching, learning and administration requires high performance connectivity, across the entire educational facility. In the classroom teaching apps that are cloud based and tailored to mobile devices underscores the need for pervasive Wi-Fi. The use of IoT (including surveillance, sensors and wearable tech) requires that schools provide a network that can securely support this new generation of technology. Gartner, Inc. forecasts that 11.2 billion IoT devices will be in use worldwide by the end of 2018, and will reach 20.4 billion by 2020.[2]

As students bring more specialized and diverse devices to the classroom as part of the BYOD movement, the proliferation of device types requires a platform that is device agnostic. As demands on the network continue to expand, will they overwhelm existing school networks?

ISTITUTO ZACCARIA DEI PADRI BARNABITI
LOCATION: **MILAN, ITALY**

In existence since the beginning of the 17th century, Padri Barnabiti's Zaccaria Institute includes a primary, secondary and a high school focusing on the Humanities, Science and Languages.

Challenge

The institute needed more secure, high-performance wireless coverage to guarantee adequate connectivity for a new generation of devices, including tablets, IP cameras, smartboards and IP fixed telephones. All wireless services also had to be available and secure for personal mobile devices (BYOD).

Solution

Alcatel-Lucent OmniAccess® wireless access points delivered a high-performance wireless mobility solution with flexible deployment options for a wide range of indoor and outdoor environments. The solution offered application awareness, ensuring that devices are connected to the best access points as users move around the grounds, always with wireless intrusion protection.

Benefits

Technical: The OmniAccess solution automatically recognizes users, devices and applications thanks to connectivity permissions. It also reduces management complexity while ensuring the maximum level of protection.

Financial: The solution provides easy integration of systems integrated in a second step, such as Wi-Fi badges or DLNA (Digital Living Network Alliance) standard protocols for video distribution and multimedia content.

User experience: Digital innovation becomes the heart of the educational process by allowing a dynamic and collaborative sharing of knowledge.

> **"Up until now, we have been continually searching for solutions and services which are useful for both teachers and students. We are very satisfied with the process improvements for technological innovation. Thanks to these improvements, the use of our wireless devices is fully operational and secure."**
>
> P. AMBROGIO VALZASINA, DEAN OF PADRI BARNABITI'S ZACCARIA INSTITUTE - MILAN

Facing the security challenges of a connected school

Connected schools that offer more innovative, digital content can provide more engaging learning experiences and improve the outcomes of primary and secondary schools. However, reliance on connectivity also brings network security challenges to these schools.

Growing use of mobile devices and IoT systems increases the exposure and possibilities to cyber-attacks. These risks include higher threat of ransomware attacks and other cybercrime, as well as the exposure of sensitive data and private information such as student and school employee records.

In fact, education is the second most impacted sector—behind healthcare—with lost or stolen records globally.[3]

The Journal, an education technology publication, reports that the rate of cybercrime against schools in 2017 is on pace to increase more than 100 percent over 2016.[4]

One of the reasons that hackers increasingly targeting schools is that the networks contain valuable data, and their systems are relatively easy to crack. According to a Miami Herald article, many school districts have set up wireless systems to make connectivity easy, unlike corporations with trade secrets and data to protect. "With free Wi-Fi in school buildings and a generation of students glued to their smartphones, there are thousands of opportunities for a hacker to gain access to a school network. Students downloading free apps on their phones or hopping from one school computer to the next can spread a computer virus faster than the flu during flu season."[5]

This is particularly a risk in schools that have BYOD policies. According to the Australian Bureau of Statistics, 79 percent of children aged 5-14 years in Australia use the Internet, and over 86 percent of these access it from school. In fact, Australia is one of the world's highest users of technology in classrooms, with 81 percent of Australian students using desktops, laptops or tablets at least once a week at school (which is significantly higher that the global average of 54 percent).

Australian schools have instituted a BYOD approach to devices, allowing students to bring their own personal mobile electronic devices to school for the purpose of learning. As the influx of uncontrolled devices and digital tools increases, primary and secondary school IT departments are faced with building an infrastructure that can support a variety of devices from multiple manufacturers while ensuring that the school network and all connected devices are secure from cyberattack.

Cyberattacks against schools can take on a number of different forms.

- During the WannaCry cyberattack in May 2017, ransomware infected computers in 10 schools in southern Taiwan.
- In Jamaica, a database containing information about more than 14,000 local students from 16 island high schools was held hostage by hackers who demanded a ransom to release the data.
- In 2015, three high school seniors from Commack High School in Long Island, New York, were charged with hacking into their school's computer system.[6]
- In October 2016, an Irish primary school's computer system was encrypted by hackers, rendering the school's files, which included children's names, dates of birth, and Personal Public Service numbers, inaccessible.
- In 2017 hackers infiltrated a Montana public-school network. The hackers sent texts and emails threatening military style mass killings unless it was paid $150,000 in Bitcoin. The school was disrupted for nearly a week affecting more than 15,700 students.[7]

Beyond the safety risks, lost school time and ransom payments, school districts also find that after-the-fact remediation of school IT networks is a costly way of fixing security problems. Data breaches can cost schools up to $300 per compromised record.[8]

3 Digital Education: Data Breaches Cost Education Companies $300 Per Record, Study Finds, 2015
4 The Journal, K-12 Cyber Incidents Have Been Increasing in 2017, 2017
5 Miami Herald: "Hack attacks highlight vulnerability of Florida schools to cyber crooks" 2017
6 ABC News: "NY High School Students Accused of Hacking Computer System to Change Grades" 2015
7 Flathead Beacon: Authorities: Overseas Hackers Seeking to Extort Community with Cyber Threats 2017
8 Digital Education: Data Breaches Cost Education Companies $300 Per Record, Study Finds 2015

Challenges IT teams face when delivering a connected learning environment

The future of education will be impacted by two fast-evolving technology trends: Mobility and IoT. Each has its own IT requirements and will create higher demand and dependency on the network infrastructure.

Mobility requires connectivity anywhere, and goes beyond offering Wi-Fi in the classroom. It requires a seamless experience and. connectivity needs to be provided everywhere in the school, including science labs, gymnasiums and libraries.

IoT requires easy, fast and dependable connections to link devices, sensors, gateways and the cloud, to make sure they operate efficiently and effectively together. IoT-ready networks need to offer ruggedized services, because in school settings these technologies may also operate in harsh environments such as playgrounds and school buses. In addition to enhanced security, the growing number of mobile devices and IoT, networks demand more stringent network requirements, including:

- **More wireless coverage**: Wi-Fi networks need to extend across the entire school property, but they also need to deliver higher performing Wi-Fi to serve higher densities of wireless users in classrooms because of 1:1 and BYOD mobile learning initiatives.
- **Higher performance, lower latency computing**: School districts must plan for resiliency in the network. If the infrastructure is not reliable teachers will revert to traditional teaching practices. While few schools require a super-computer, an emphasis on STEM coursework, coding classes, maker spaces and the need to support virtual and augmented reality can stretch the computing capacity of ad hoc, limited capacity computing network. Schools need an underlying IT network with the power to easily scale fast performance when required.
- **Tighter security**: The increased use of mobile and IoT devices means more exposure to hackers. To minimize the possibilities of security breaches, it is necessary to implement a comprehensive strategy that includes security at the user, device, application, perimeter and operating system levels.
- **Simple and safe IoT traffic containment**: However valuable, IoT networks can pose risks to assets across the entire school network. Even small IoT systems can put tremendous pressure on a school's underlying network infrastructure, as each IoT sensor and device represents an entry point for potential security threats. Schools need a segregated, isolated environment with the right conditions for IoT devices and applications to run efficiently and securely.

Schools don't need the added cost, operational, and management complexity that can accompany a network upgrade. To benefit fully from connected education technologies, schools need a unified network experience with reliable support for a growing mobility and IoT network.

PAULDING COUNTY SCHOOL DISTRICT
LOCATION: **PAULDING COUNTY, GEORGIA**

The Paulding County School District is the 13th largest school district in the State of Georgia.

The K-12 District has 19 elementary schools, 9 middle schools and 5 high schools. Current enrollment is 28,500, and there are 3400 employees.

There are between 8000-10,000 wireless connections on the District's network at any given time.

Challenge

The school district faced bandwidth shortages in the classroom, and wireless capabilities were limited and unable to meet demand. Also, networking technology varied from school to school. The district wanted a standardized network solution to deliver consistent wired and wireless connectivity across all schools.

Solution

Dedicated switches in each classroom offer reliable bandwidth to support e-learning while access points in the hallway deliver quality wireless services for BYOD devices. A central management suite provides unified management of wired and wireless networks.

Benefits

Financial: Implementing managed switches in classrooms reduced maintenance, local travel needs and costs. Upgrading the wireless network qualified the district for federal and state matching funds.

User experience: Students can securely connect their devices to the network, promoting anytime anywhere digital learning.

Educators have greater bandwidth to support teaching and e-learning tools and devices.

> **"We're progressively putting the solution in place at each of our schools and we've been getting a lot of great feedback. The infrastructure is simple to implement and its benefits are immediate."**

JULIE ACKERMAN, EXECUTIVE DIRECTOR TECHNOLOGY, PAULDING COUNTY SCHOOL DISTRICT

Now is the time to improve your school network infrastructure

Because technology is integral for education, the performance, security and reliability of the underlying technical network is critical for enabling collaborative, digital learning experiences and effective administrative operations.

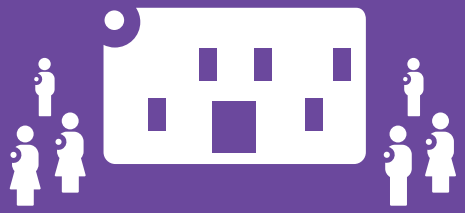
The growing number of, and reliance on, mobile and IoT devices, and the associated security concerns, demand more stringent network requirements to ensure the school's IT platform is ready to support future digital classrooms and school operations.

Read on to learn about our recommendations for designing an efficient, secure and cost-effective primary or secondary school network that can meet the technology expectations of students and teachers, and enable more collaborative digital learning experiences.

School districts in the US reveal their digital priorities and practices

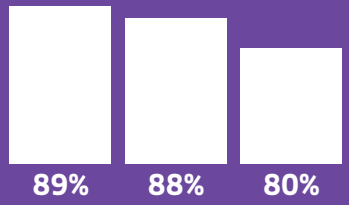
The Center for Digital Education and the National School Boards Association in the U.S. have conducted the Digital School Districts survey, since 2004, to identify emerging trends around primary and secondary leadership, governance, accountability, engagement, data management and security. According to the survey, the top five digital priorities for school districts in 2018 are:

1. **Personalized learning**
2. **Digital content and curriculum**
3. **Professional development**
4. **Mobility (one-to-one and/or BYOD)**
5. **Upgrade Classroom Technologies**



School districts identified in 2017 the top three drivers for improving digital infrastructure:

1. Preparing children for the 21st century economy
2. Improving student performance
3. Supporting innovative teaching practices



Mobility in 2018:

- **89%** of districts use mobile devices for assessments
- **88%** of districts have a mobile device policy in place.
- **80%** of districts train teachers or have policies regarding how to protect student privacy when using mobile apps

Eight Recommendations for an efficient, secure, cost-effective school network

1. Understand the limits of the existing network

The first step in building a next-generation primary or secondary school network is to analyze and evaluate the capabilities of the existing network infrastructure. The core network itself may be outdated and unreliable. It may be too complex and structured with too many layers to efficiently support multimedia applications.

Maintaining the network may be too expensive because many of the elements have reached the end of their life cycle. Additionally the aging infrastructure may not support the new wave of multimedia applications, because it was never designed to provide the capacity needed to meet the instant on, multi-device load generated by today's students. As well, the wireless portion of the network may be outdated.

The network may provide spotty coverage in some areas of the school and facility, while it is not available at all in others. The access points (APs) may not support the latest mobile devices with the new generation of wireless technologies and protocols, such as 802.11ac Wave 2.

Lastly, the network may not be structured to enable efficient, ongoing management. Most school networks are managed in silos, with different platforms for local area network (LAN) configuration/management, wireless LAN (WLAN) configuration/management, and service level management. This makes it difficult to enforce consistent, reliable behavior for the entire network that will meet student and teacher expectations. Consider a cloud-based network management for further simplification of the IT operational tasks.

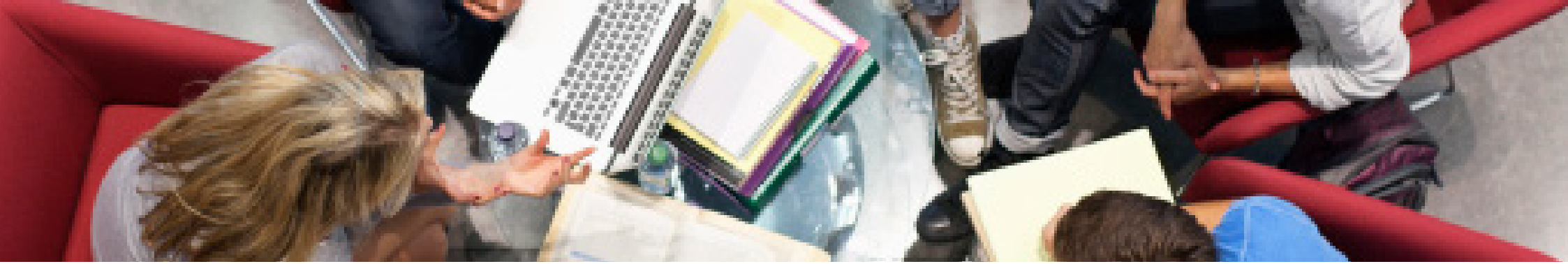
2. Deliver a high performance access network

Supporting digital learning requires a WLAN infrastructure that can handle a large influx of mobile devices and the bandwidth-hungry applications running on them. There are several things you can do to prepare for this:

- **Plan for density**: Students carry multiple mobile devices which are either school provided or their own (BYOD). Adding teacher devices, classroom tools like projectors and printers, and all sorts of new IoT devices, means planning for density is planning for success.
- **Assess WLAN bandwidth requirements**: Determine what is required to support instructors teaching style, including mobile devices. For example, if teachers expect to use video-based teaching aids that stream video to multiple devices, a WLAN network capable of supporting multiple, high quality video streams will be required. An HD-quality video stream uses 4 Mb/s of bandwidth per user and interactive learning games require multi-megabits of bandwidth per user.
- **Handle bandwidth needs with 802.11ac Wave 2 technology**: Gigabit Wi-Fi devices are already available to students. Adopting 802.11ac Wave 2 Wi-Fi technology, enables faster data rates and multiple concurrent downstream communications to multiple wireless devices, resulting in better support for increased users, devices and applications.
- **Eliminate roaming issues**: As students roam between access points, their devices can get stuck on an AP instead of associating with a closer one that has a stronger signal. The ideal network infrastructure should eliminate this so that older generation devices or disproportional distribution of users don't drag down the network.
- **Adjust LAN access to support new generation access points**: 802.11ac Wave 2 APs typically generate an aggregated throughput above 1 Gb/s. To avoid bottlenecks and cabling rework, upgrade to access switches that support 2.5 G/5G ports (with PoE) and 10G uplinks.

802.11ac Wave 2 was only recently made available and it features many benefits over previous technologies, including:

- High capacity rates of up to 3.47 Gb/s per radio, compared to 54 Mb/s on 802.11 g, 450 Mb/s on 802.11 n and usual 1.3 Gb/s on 802.11 ac Wave 1.
- Multi-user, multiple-input multiple-output (MU-MIMO), which allows for concurrent downstream communications for multiple connected devices (which is ideal for areas with high density of devices). MU-MIMO also allows client devices to connect and disconnect to the network faster, so more clients can use the network.
- Four transmitting and receiving antennas (compared to three with Wave 1), resulting in the data rate being sustained for greater distances.
- Support for a greater number of available channels, with potential for greater bandwidth and flexibility, while supporting more users, devices, and applications.



3. Ensure the core/data center is not a bottleneck, while reducing cost per student

The core is the most critical part of the school infrastructure because it must support more than 80 percent of all LAN and Wi-Fi user traffic for applications and communications. To get the full benefit of a next-generation access infrastructure, evaluate the network traffic to determine where the bottlenecks could occur, what is needed to ensure the network can identify and prioritize education-critical applications, and the type of network elements required to reduce latency for all traffic.

When planning the new network consider:

- Deploying 10 G/25 G/40 G/50 G/100 G switches that eliminate bottlenecks and support virtual network design
- Right-sizing with small, high capacity switches that can form a virtual chassis and provide multiple terabits per second of switching capacity
- Streamlining the wired infrastructure by reducing the number of layers in the network design—in many cases it is possible to eliminate the distribution layer, reducing capital expenditures (CAPEX) and operating expenditures (OPEX)
- Choosing newly-designed, less power-hungry switches with lower power requirements
- Vendors that support pay-as-you-grow strategies that reduce budget pressures, but don't compromise product features.

4. Improve network capacity and reliability

Shortest Path Bridging (SPB) enables each node to deliver network traffic using the shortest, most optimal path available, resulting in less latency. When multiple links are available for redundancy purposes, previous technologies (such as Spanning Tree), had to choose a primary link. All other links are de-activated, remaining on standby in case the main link fails. This approach is an inefficient use of network resources.

With SPB, all links are kept active at all times, resulting in better capacity and performance. If links fail, the recovery is faster with SPB than with Spanning Tree, meaning no real-time traffic like video or voice is ever impacted.

Network virtualization is easy with SPB—configuration is only needed at the edge of the infrastructure fabric, while all intermediate notes remain unchanged independent of the size and complexity of the network. This considerably reduces the operational time to do moves/adds/changes and improves the network scalability.

Intelligent Fabric

Intelligent Fabric (iFab) simplifies the design and operation of networks, offering self configuration and self-attachment. iFab also provides high performance, resiliency and flexibility. Self configuration reduces the amount of time required to establish connections between nodes. When new equipment is added and cables are connected, new devices are automatically detected. The network is auto configured and operational in just a few minutes. Making moves, adds and changes much easier. This avoids the need to have IT personnel with specific expertise for new equipment installations. In networks with iFab, performance and resiliency are both improved as it leverages SPB (Shortest Path Bridging) technology.

5. Enable pervasive mobility

Ensuring that all devices coming into the school environment get their share of network resources, on both wired and wireless networks, can be achieved with a network solution that offers Unified Access control over network services, and the same quality of experience (QoE) over wired and wireless networks. Students, teachers, staff and administrators will connect to the school network with a variety of devices. This can create access and traffic management challenges. An advanced Unified Access solution allows for:

- Creation of a simple captive portal that displays a web page. This is similar to a Wi-Fi hot spot where students can accept the connection or sign-in using their school credentials, if you want to map traffic back to an individual user.
- Simplified device on-boarding, allowing users to self-enroll. Once authenticated, future connections will be automatic, without requiring the user to re-authenticate.
- 802.1X authentication with Advanced Encryption Standard (AES) security features allow users to self-enroll, automatically generating and installing device certificates through a web portal with no IT assistance.
- Enforcement of a differentiated network access based on contextual information, granting network access privileges based on user roles (for example, students, teachers, or staff), device types (laptops, tablets, or smartphones), and location (classrooms, common areas, or playgrounds), which also enables secure management and enforcement of differentiated policies.

Unified Access provides the same network services for wired and wireless

The Alcatel-Lucent Enterprise Unified Access solution delivers a high quality, user experience on any wired or wireless network. The solution provides a common set of network services, a policy framework, authentication scheme, and a single authentication database that are applied to all users accessing the network with either wired or wireless devices. These network services automate many of the processes that are currently handled manually, and enable IT teams to ensure that:

- The LAN and the WLAN behave and are managed as one network
- Quality delivery of all applications is enforced consistently at all times
- Security is maintained throughout the network

The Unified Access solution is delivered with one management system that provides end-to-end visibility, avoids duplication of tasks, and offers better troubleshooting tools for all network management requirements.

Unified Access enables the management of mobility in a secure and consistent way, with each group of users assigned specific profiles and permissions. Depending upon their permissions, each group of users is granted different access rights. For example, teachers could be given different permission than students, based on a different VLAN, with reserved bandwidth and different traffic priorities assigned to them.

6. Ensure the network is IoT friendly

With so many IoT devices expected to connect to the network, the challenge with any network deployment is to make it as easy as possible to connect these devices, while keeping the network secure.

IoT Enablement does this by providing automated device onboarding and by associating devices to a virtual network using either VLANs or SPB services. These virtual networks include policies defining QoS and security rules that apply to the contained IoT system.

7. Allow for simplified operations

One way to simplify day-to-day operations is to build and operate a single, robust network, with virtual networks for unique requirements, rather than separate, dedicated networks. A single physical infrastructure can support many different devices and users with various virtualization techniques. In addition, profiles can be assigned to different user groups. As users move around the school, their profile defines the type of access they receive.

Another key point is to use a single management system for the entire network. As with Unified Access, the policies applied to users, devices and applications for wired network solutions can be based on the same contextual data as the wireless network. This simplifies the network deployment and management efforts, providing full control of the traffic coming from the access layer.

Your strategy to simplify operations should also include automation. Examples include automated configurations (see Intelligent Fabric), automatic device onboarding and guest self-registrations.

By simplifying operations, highly-trained IT personnel are free to handle more complex tasks or more strategic initiatives, including the support of next-generation digital learning applications in the classroom, or providing full mobility for students.

IoT Enablement

IoT Enablement provides the appropriate network resources required for IoT systems to operate efficiently. Different devices– such as HVAC sensors, science lab equipment and security devices are all assigned profiles, similar to what is done for users in Unified Access. These devices are then placed in a "virtual container," using network virtualization techniques that allow for all devices to use the same physical infrastructure, while remaining separate from the rest of the network. In these virtual containers, QoS and security rules are applied to ensure the IoT system works with the necessary network resources to run efficiently and securely.

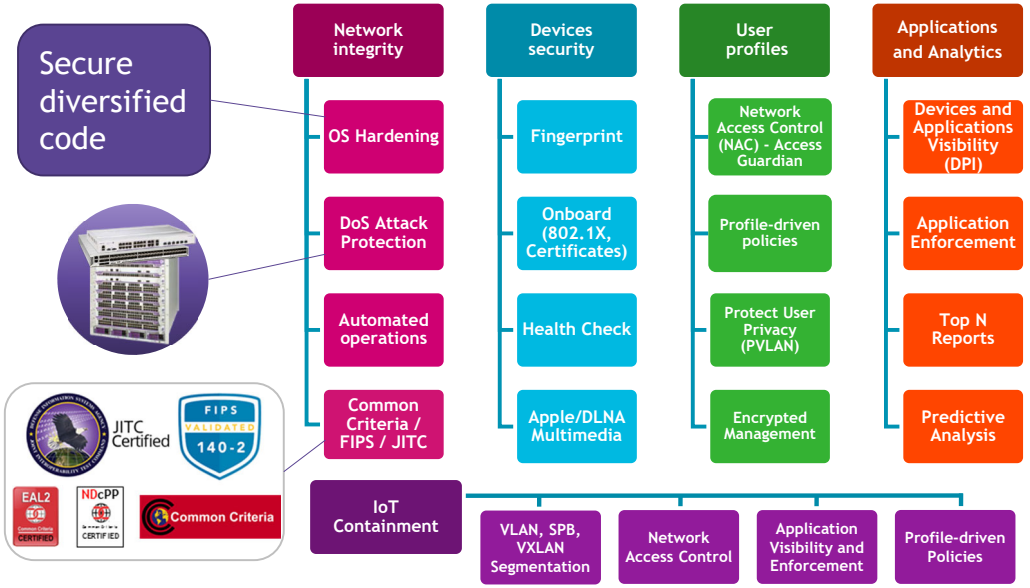
To simplify device onboarding, IT can create a fixed number of profiles (for example, one for student devices, one for teacher devices, one for HVAC systems and one for security systems). All this information is sent to all switches and Wi-Fi APs in the network and, when devices connect, they are assigned to the appropriate virtual environment and communication is limited to the devices within that environment and the application in the data center that controls these devices. This is beneficial as it minimizes any potential damage resulting from a malicious attack, by limiting the number of devices accessible within the same profile. If a breach occurs, the rest of the network is not exposed, as other devices are contained in other parts of the network.

8. Offer in-depth security

Network security is a major concern for every primary and secondary school, especially with the growing popularity of mobility and the IoT. The modern approach to security is to provide not only firewalls, but protection at every level (as shown in Figure 1), including:

- At the user level, verifying that users are always authenticated and authorized with the correct access rights (using profiles).
- At the user device level, checking that devices are authenticated , classified, and eventually put into quarantine if their behavior becomes suspicious.
- At the application level, setting rules associated with specific applications (including blocking and limiting bandwidth or who can use them)
- At the IoT device level, using containerization (as described above) to fine-tune security rules and limit the spread of security breaches.
- At the network level, taking measures to remove vulnerabilities in the physical equipment, including network devices, switches, routers and access points (APs)

Figure 1. The modern approach to security is to provide protection at every level



Other security technologies that should also be included in any network solution include:

- Media Access Control security (MACsec), an IEEE standard (802.1AE) that provides security in wired Ethernet LANs. MACsec, for example, can be used to encrypt traffic that might travel to a remote data center that is used for back-up or disaster recovery.
- Integrated Distributed Denial of Service (DDoS) protection. A DDoS attack temporarily or indefinitely interrupts or suspends services of a host connected to the internet. There are multiple known techniques used by DDoS attacks (for example, SYN attack, ARP flood attack, ICMP Ping attack) and smart network devices should automatically detect and block devices attempting to create such disruptions.

Smart Analytics

Smart Analytics allows for improved IT business decisions and network planning. This can be achieved by providing visibility and detailed information about the network, users, devices and applications being used on the network.

Deep packet inspection (DPI) capabilities provide details not just on what people are accessing online, but what applications are being used most. Data can then be aggregated, presented and acted upon. For example, certain apps can be restricted and bandwidth can be reserved or limited. Insights can be garnered on what tools are being commonly used and which users are consuming the most bandwidth.

Predictive analysis monitors and analyzes trends for multiple days and weeks. An artificial intelligence (AI) algorithm built into the analytics tool creates baselines based on “normal” network traffic behavior, then can predict what will happen in the future. For example, warnings can be provided when it’s time to upgrade a switch that is about to run out of available bandwidth.

Finally, analytics can also be used to improve security. Based on the same established baselines, the AI algorithm can send notifications when unusual network traffic patterns are detected.

ANKABUT
LOCATION: **UNITED ARAB EMIRATES**

Ankabut is the United Arab Emirates's advanced network for research and education.

It's a network connecting all universities and education institutions in the UAE to enhance education and research in the country.

Challenge

Ankabut is the UAE's advanced network for research and education, connecting all universities and educational institutions in the country. Ankabut required a resilient and reliable solution for a CDMA Packet Data Network and an Ethernet Backhaul network to connect 70,000 users on 56 campuses of 20 different universities. This solution will serve as the foundation for a second roll-out expanding to 1 million users, including all UAE primary and secondary schools and other higher education institutions.

Solution

The Alcatel-Lucent OmniSwitch 6860 Stackable LAN Switches are compact, high-density Gigabit Ethernet (GigE), Multigigabit and 10 GigE platforms designed for the most demanding converged networks.

Benefits

After deploying the ALE solution, Ankabut had a flexible and future-proof foundation for educational solutions and powerful collaboration and information sharing between geographically disparate virtual teams and institutions.

The Ankabut network was easy to deploy, providing connections and collaboration among 20 universities and 56 campuses, increasing system redundancy, resiliency and high availability, while simplifying operations and management of the network.

> **"Alcatel-Lucent is for us the 'brain of technology,' I think state-of-the-art technologies come from Alcatel-Lucent. The whole requirements built for the data center came from Alcatel-Lucent's expertise."**
>
> DR. AHMED DABBAGE, DIRECTOR OF TECHNOLOGY & SERVICES DEVELOPMENT, ANKABUT

A comprehensive portfolio: From school to data center

ALE features a broad product portfolio that extends from the access (LAN and WLAN) to the core network and data centers.

It includes WAN routers and comprehensive network management platforms. Figure 2 depicts the Alcatel-Lucent Enterprise portfolio that is available for educational institutions.

The high-level overview of the product families is described below and provides a better understanding of where they fit in today's primary and secondary environment.

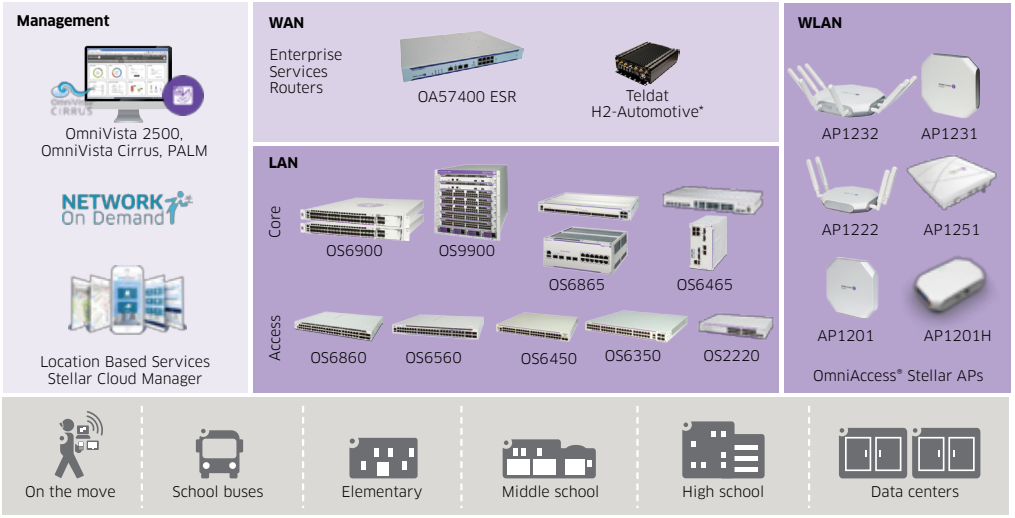
Pervasive network access

Network access includes both wired and wireless equipment:

- Wired access is provided by stackable gigabit LAN switches, starting with the Alcatel-Lucent 6350/6450 families family, passing to the multi-gig OmniSwitch 6560 family and all the way to the advanced OmniSwitch 6860E family which includes integrated DPI and SPB. There are also two hardened switch families for outdoor and harsh condition areas: OmniSwitch 6865 and OmniSwitch 6465.
- Wireless access is provided by a variety of high-performance 802.11ac Wi-Fi access points (APs). Alcatel-Lucent OmniAccess® Stellar family of controller-less APs offers a solution that best adapts to your needs. Models include a variety of indoor and outdoor ruggedized APs with on-premises or cloud-based management.

All of these APs include the Unified Access technology. When they are combined into one network, they offer a consistent QoE and a single management system (on premise OmniVista 2500 or cloud-based OmniVista Cirrus).

Figure 2. Alcatel-Lucent Enterprise Network portfolio



GYMNASE INTERCANTONAL DE LA BROYE
LOCATION: **PAYERNE, SWITZERLAND**

Gymnase intercantonal de la Broye (GYB) is a Swiss secondary school on a 32,000 m2 site at Payerne in Switzerland.

It opened in August 2005 and has 40 class rooms, rooms with special equipment, a library, an auditorium, exhibition space and administrative and teaching spaces.

This has all been designed to accommodate about 1,000 students.

Challenge

The school wanted to provide quality Wi-Fi connectivity across the whole campus, especially in the auditorium, which seats over 300. This required the installation of 60 access points discretely all-around campus. In addition to a perfect signal across the school grounds, GYB also stipulated that the antenna should not be visible. The deployment also needed to be completed during the short winter holidays to have minimum impact on the users during the transition between the old and new solutions. Finally, Wi-Fi security needed to be simple to maintain for an organization whose members had little technical and networking expertise.

Solution

Alcatel-Lucent OmniAccess® 4704 WLAN Controller and Policy Enforcement Firewall Module provided a true user-centric network experience, delivering follow-me connectivity, identity-based access, and application continuity services. Alcatel-Lucent OmniAccess 105 and 135 Wireless Access Points delivered a high performance wireless mobility solution in a wide range of indoor and outdoor environments. Alcatel- Lucent OmniSwitch 6450 Stackable Gigabit LAN switches provide an easy-to-manage edge solution for highly available, secure and eco-friendly campus networks running many devices.

Benefits

The Alcatel-Lucent Enterprise wireless network covered the entire campus with high-performance Wi-Fi to provide students new ways of learning and collaborating by easily using laptops or tablets as everyday working tools. The easy-to-deploy and -manage solution gave GYB's IT department more time away from infrastructure management and interaction with the end users.

“The solution that Alcatel-Lucent Enterprise put forward offered the best value for money when it came to renewing the infrastructure that was at the end of its life. We were impressed as much by the immediate performance as by the increase in efficiency in the management of the whole campus. Since we implemented the solution a few months ago, we have seen that this infrastructure takes up few resources and is highly reliable. We are delighted with our choice.”

THIERRY MAIRE, DIRECTOR, GYMNASE INTERCANTONAL DE LA BROYE, SWITZERLAND

A resilient and high-performance core

The network core includes high-performance wire-rate 10 GigE/25 Gig/40 GigE/ 50 Gig/100 GigE network switches that provide high port density and switching capacity. It includes the market-leading OmniSwitch 6900 Stackable LAN Switch family which comes in a compact 1U form factor and the versatile OmniSwitch 9900 LAN chassis.

The Alcatel-Lucent Enterprise solution employs SPB and Virtual Chassis (VC) technology to create a friction-free LAN. VC technology enables up to six OmniSwitch 6900 Stackable LAN Switches to be combined and behave as a single fully redundant unit. In many cases this can replace expensive chasses, require less space and power, and be deployed at a lower cost, all while providing the level of reliability.

Core products incorporate the award winning Intelligent Fabric (iFab) technology that offer a set of capabilities, including automation techniques that simplify the design, deployment, and operation of the network.

An optional aggregation layer

Due to the high performance and high density of the ALE core switches, in many cases there is no need to have an aggregation layer. This lowers the latency and reduces the capital investment. However, in some cases, the architecture and distance of school buildings or facilities make the traditional three-layer architecture more cost effective. The OmniSwitch 6860E and the OmniSwitch 6900 switches described above are excellent options for this type of architecture.

Reliable and flexible WAN connectivity

The ALE education solution uses the Alcatel-Lucent OmniAccess Enterprise Services Routers (ESRs) for branch office WAN connectivity. The ESR offers, in a single compact form factor, an integrated WAN router, LAN switch, and Wi-Fi AP, providing savings in space and cost. It includes multiple options of WAN connectivity with ample redundancy, comprehensive QoS, security, VPN capabilities and even telephony-over-IP (ToIP) survivability. Multiple models are available to support the need from the small, medium and large branch offices, including some ruggedized models that can be used in vehicles like school buses.

End-to-end network management

The management suite includes all tools needed to provision, monitor, analyze and troubleshoot the network. The OmniVista platform can manage the LAN, WLAN, core, WAN and datacenter from a centralized single pane of glass. It is offered in two versions: an on premise version called OmniVista 2500 and a cloud version called OmniVista Cirrus. Both versions offer mostly the same capabilities, so institutions can chose the model that best adapts to their needs. OmniVista Cirrus is hosted in a public and secure cloud with a subscription-based model for 1, 3 or 5-years term.

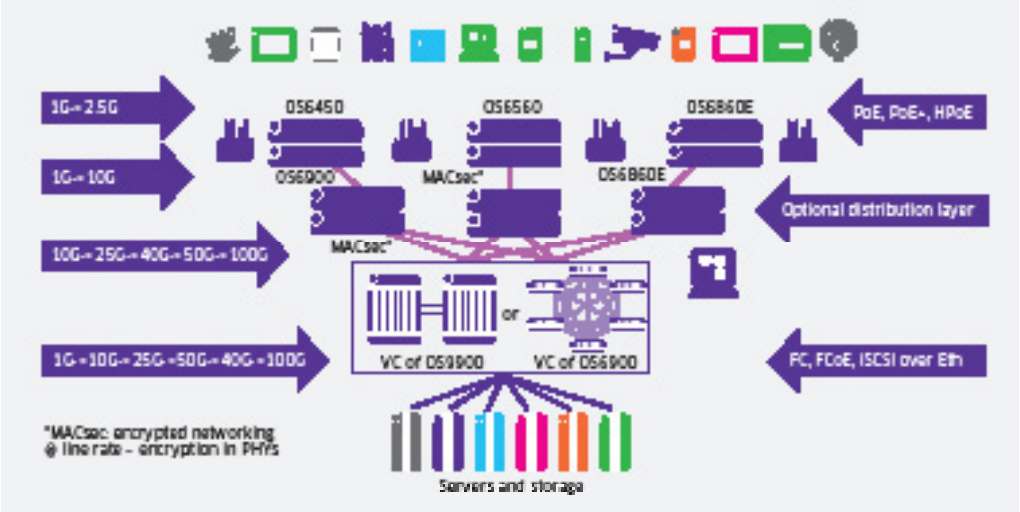
The management suite also includes a unified policy and authentication manager, BYOD and guest access services.

In conjunction with OmniVista, Alcatel-Lucent offers a ProActive Lifecycle Management (PALM) cloud-based application that provides network asset management functionality, including inventory list and visibility into the hardware, OS, warranty and support services.

The Alcatel-Lucent Enterprise portfolio offers the performance, resilience, and all interfaces needed to connect the school, from the user devices and IoT endpoints, all the way to the data center, by providing a variety of speeds and interfaces to address specific needs.

The diagram below summarizes the multiple options available.

Figure 3. The Alcatel-Lucent Enterprise portfolio offers the performance, resilience, and all interfaces needed to connect your institution



Technology is increasingly central to education

For many students, the way a school integrates IT into the primary or secondary school environment can be just as important as their favorite classes, or the structure of the curriculum. Most students today don't remember a time before the internet and they expect to be able to connect with any device, anywhere, in and around the school, whether it's to communicate, be entertained, or to access educational resources.

In addition to student expectations, a school network must also meet the technology requirements of school administration, staff and IT departments.

When designing an efficient and cost-effective school network, it is important to:

- Understand the limits of the existing network: Objectively analyze and evaluate the capabilities of the existing network infrastructure to ensure that it meets the expectations of students, staff, and teachers.
- Deliver a high-performance network: Provide a WLAN infrastructure that can handle a large influx of mobile devices and the bandwidth-hungry applications. Ensure the network core does not become a bottleneck: increase capacity and use technologies such as SPB to maximize infrastructure performance.
- Enable pervasive mobility: Ensure that all devices coming into the school environment get their share of network resources with connectivity everywhere and the same quality of experience (QoE) over wired and wireless networks, with simplified device on-boarding.
- Ensure the network is IoT friendly: Simplify the connection of IoT devices, while keeping the network secure.
- Allow for simplified operations: Build and operate a single, robust network, with a single management system and virtual networks for unique requirements, rather than separate, dedicated networks.
- Offer in-depth security: Provide not only firewalls, but protection at every level, for users, devices, applications and the network itself.

The primary and secondary school network has become an important asset for creating a collaborative learning environment that enables new instructional experiences for students and new opportunities for teachers to plan and deliver more engaging lessons. It also provides the technologies for school administrators to simplify operations, better comply with regulations, and provide a safe environment for students and teachers. The growing number of mobile and IoT devices—alongside the associated security concerns—requires stringent network requirements to ensure that it is ready to support the digital schools of the future.

Brochure
Primary and Secondary Education Networking Guide
December 2019

Connected Education

Where Education connects with technology that works. For your school, college or university. With global reach and local focus, we deliver purpose built networking and communications for the education environment that enable secure, reliable collaboration between your faculty and students.
https://www.al-enterprise.com/en/industries/education

Alcatel·Lucent Enterprise