Higher Education Networking Guide

Building the Foundation for Tomorrow's Digital Campus:
A higher education networking solution guide

Alcatel·Lucent
Enterprise

Technology has become integral to the lives of many post secondary students. Most don't remember a time without the internet. A time before it became so ubiquitous. Today, students expect to be able to connect with any device, anywhere on campus – whether it's to communicate, be entertained, or to access educational resources.

For modern students, the way a college or university integrates information technology (IT) into the fabric of campus life can be just as important as their chosen field of study or the structure of the curriculum.

In response to the wide adoption of technology, the methods used for student learning continue to evolve. Digital learning processes and experiences are now equal in importance to traditional lectures and seminars for many students. Online courses, testing, and assessments are now part of most curricula. Laptops have become a primary tool for students. There has also been an explosion of mobile devices on campus and students are downloading an increasing number of applications that enhance their digital learning experience.

When designing a campus network, it must meet the technology expectations of students, but the university administration, staff, faculty, and IT department should also be considered. For IT, security will be one of the primary concerns, but other concerns include deployment and procurement costs, device on-boarding, network speed and coverage, and training and operational issues. University administrators will want to leverage technology to create an environment that attracts more students, enhances the success rates of existing students, enables access to advanced research, and improves the rankings and reputation of the school. The administration will also have budget concerns but most will understand the importance of building a strong and secure network, with excellent coverage for the entire campus.

This document provides six tangible recommendations for IT departments to use in designing efficient and cost-effective campus networks that enable collaborative, digital learning experiences.

According to EDUCAUSE's 2018 Top 10 IT Issues survey, improving student success is ranked as the #2 priority. Institutions are especially looking to leverage technology to achieve progress on this goal.

Market trends: Institutions undergoing a digital transition

Three trends that will have the biggest impact on college and university campuses around the world over the next few years are mobility, the Internet of Things (IoT) and cyber security.

Mobile devices used by students, staff, and faculty

A recent industry report states that the total number of mobile broadband subscriptions now exceeds 4.5 billion and will grow to 8.3 billion by 2022.[1] On college and university campuses, mobile devices are used by students, staff, and faculty alike and – when combined with laptops, tablets, and IoT devices – are threatening to overwhelm campus networks with increasing bandwidth demands. On average, each American college and university student owns 5.6 devices and uses them for more than 137 hours per week.[2] Further, two-thirds of students report connecting two or more devices to the internet at a time.[3]

To provide internet connectivity for these devices, Wi-Fi has become the dominant technology. The main benefit being its flexibility; allowing users to be located virtually anywhere, using any device. At the same time, expectations continue to grow as consumers grow accustomed to having excellent performance at all times.

The Internet of Things (IoT) is just starting to grow

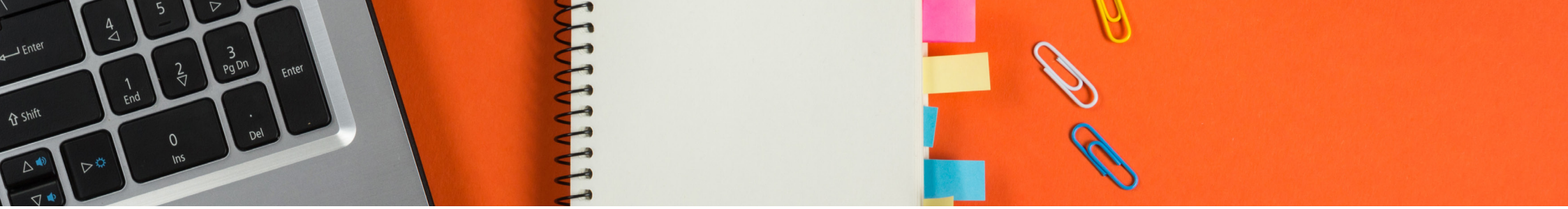
Gartner predicts that there will be 11.2 billion IoT devices in use worldwide by the end of 2018, reaching 20.4 billion by 2020.[4] On campus, IoT devices are already plentiful and their number will only grow, ranging from student-owned wearables, to connected smartboards and projectors in the classroom; from robots in various labs to hi-tech building management solutions that control heating, ventilation, and air conditioning (HVAC) systems, surveillance cameras, and lawn sprinklers.

Cyber security concerns persist

Unfortunately, viruses, malware, data breaches, and ransomware attacks are becoming more common. In addition to increasing in frequency, the cost associated to recover from these attacks and infections is also increasing.

Post secondary institutions are especially vulnerable to these issues because of the extensive use of mobile and IoT devices. The education sector was reported as the number one industry victimized by ransomware. In 2017, cyber-espionage was present in 26% of breaches of higher education organizations.[5] In February 2017, more than 60 universities – including Oxford, Cambridge, and New York University – were compromised.[6] In May 2017, the "WannaCry" ransomware plagued thousands of institutions in 99 countries.[7]

1 "Ericsson Mobility Report", June 2017; https://www.ericsson.com/assets/local/mobility-report/documents/2017/ericsson-mobility-report-june-2017.pdf
2 "2017 College Explorer Market Research Study", Refuel Agency; http://www.refuelagency.com/insights/college-explorer/
3 ECAR Study of Undergraduate Students and Information Technology, 2016, Educause Center for Analysis and Research (ECAR); https://library.educause.edu/resources/2016/6/2016-students-and-technology-research-study
4 "Forecast: Internet of Things – Endpoints and Associated Services, Worldwide, 2016", February 7, 2017; http://www.gartner.com/newsroom/id/3598917
5 «Education Industry Insights: State of Privacy and Security Awareness», Jay T. Conrad, April 10, 2018; https://www.mediapro.com/blog/education-industry-insights-privacy-security-awareness/
6 "Lone hacker Rasputin breaches 60 universities, federal agencies," ZD Net, February 16, 2017; http://www.zdnet.com/article/lone-hacker-breaches-60-universities-federal-agencies/
7 "Massive ransomware cyber-attack hits nearly 100 countries around the world," The Guardian, May 12, 2017; https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs



Smartphones are particularly attractive to cybercriminals who can develop malicious apps and observe web browsing on mobile devices. Similarly, IoT devices present challenges for campus IT departments because these devices often do not prioritize security. Many of the recent security breaches associated with universities and colleges have been accomplished by taking advantage of the minimal security measures associated with IoT devices.

According to a January 2017 report by Verizon, an American university recently suffered an attack that caused the school's network connectivity to become very slow or even inaccessible. In this case, the hackers used the more than 5000 IoT devices on campus – including light sensors and vending machines –to make hundreds of Domain Name Service (DNS) lookups every 15 minutes.[8]

The main fear with these attacks and infections is that sensitive information – such as student records, research data, and other intellectual property – are at risk. At the same time, however, the unfettered exchange of information is one of the defining principles of academic institutions. This puts IT departments – tasked with protecting the network and the data that traverses it – at odds with these core principles and can result in more vulnerabilities – and the attacks that exploit them.

Analytics can also be used to improve security. By providing visibility and information about the network, users, devices, and apps being used over a period of time, baselines can be established. This baseline can be used to predict future issues, suggest ideal times for network upgrades, and to send notifications when unusual network traffic patterns are detected.

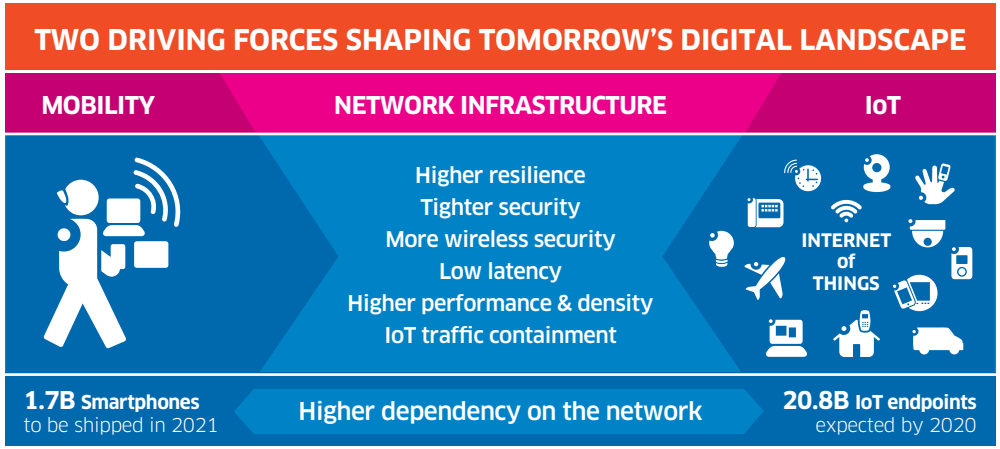


Figure 1: Mobility and IoT are shaping the academic networks of tomorrow

Stringent network requirements are required

The growing number of mobile and IoT devices – alongside the associated security concerns – requires more stringent network requirements, including higher resiliency, tighter security, increased wireless coverage, low latency, and improved performance.

Expect these two driving forces – mobility and IoT– to shape how education is done in the future (as shown in Figure 1). Is your network ready for the digital campus of the future?

8 "University attacked by its own vending machines and other IOT devices," SC Media, February 10, 2017; https://www.scmagazineuk.com/university-attacked-by-its-own-vending-machines-and-other-iot-devices/article/637300/

Expectations for the modern campus network

In the 21st century, the campus network has become an important asset for attracting and retaining the best students and faculty, boosting learning and research, reaching off-campus students, providing lifelong learning, and creating a more collaborative learning environment.

In addition to student expectations, however, a campus network must also meet the technology requirements of the university administration, staff, faculty, and IT department.

Next-generation networks must make connectivity ubiquitous, reliable, and secure

Thanks to programs like "One-to-One Student Computing" – which was first introduced to K-12 schools in the United States in the late 1990s – many children are exposed to technology in the classroom from a very young age. A 2016 review from Michigan State University examined 15 years' worth of research studies, reporting that giving every student a laptop had a statistically significant positive impact on student test scores in English/language arts, writing, math, and science.[9] As a result, most students are "digital natives" by the time they enter college or university.

According to a 2016 study from the Educause Center for Analysis and Research (ECAR), 78 percent of students agree that the use of technology contributes to the successful completion of courses.[10]

Worldwide, nearly 50 percent of the population has an internet connection at home.[11] When asked about the importance of Wi-Fi, 60 percent report that they can't go more than one day without Wi-Fi.[12] As a result, students:

- Expect Wi-Fi to be on campus
- Use Wi-Fi for everything, from their laptops, tablets, and smartphones, to their gaming systems, televisions, and streaming video services
- Want to be able to connect everywhere on campus, from their classrooms and dorm rooms, to the cafeteria, common areas, and even in sports stadiums and

- Harbor concerns about security – owing to the publicity around the number of recent attacks, viruses and infections – that need to be balanced with accessibility and ease of use

9 "One-to-One Laptop Initiatives Boost Student Scores, Researchers Find," Education Week, May 11, 2016; http://blogs.edweek.org/edweek/DigitalEducation/2016/05/one-to-one_laptop_test_scores.html.

10 ECAR Study of Undergraduate Students and Information Technology, 2016, Educause Center for Analysis and Research (ECAR); https://library.educause.edu/resources/2016/6/2016-students-and-technology-research-study

11 "Internet World Stats," March 31, 2017; http://www.internetworldstats.com/stats.htm

12 "50 Incredible Wi-Fi Tech Statistics That Businesses Must Know," Feb 12, 2014, SalesForce; https://www.slideshare.net/ValaAfshar/50-wi-fitechstatsforbusiness/49-More_than_27_billion_peopleused

GORDON
COLLEGE

> **“We are getting great range for our wireless both indoors and outdoors. Having solid wireless throughout campus enables us to create a next generation learning environment that is attractive to students and beneficial to the college’s standing.”**
>
> Chris Hansen,Director of Network and Information Systems, Gordon College

Gordon College • Wenham, Massachusetts, USA

Challenge

- Create an advanced network with ubiquitous wireless coverage that would enhance learning for existing students, secure state accreditation for curriculum delivery, serve as an asset for recruiting new students, and support next-generation teaching tools.

Solution

- Renew the WLAN and the supporting LAN infrastructure offering higher throughput and automated secure registration of users and devices.

Benefits

- **Financial:** Pervasive wireless is an asset for recruiting students and securing a vital revenue stream for the college. Virtual chassis helps the college avoid upfront capital costs in favor of a pay-as-you-grow model.
- **User experience:** Students have access to ubiquitous, reliable wireless on campus, including in outdoor areas like the quad. Guest access to the wireless network is fast and secure, with credentials sent via SMS.

University administration, staff, and faculty also rely on connectivity

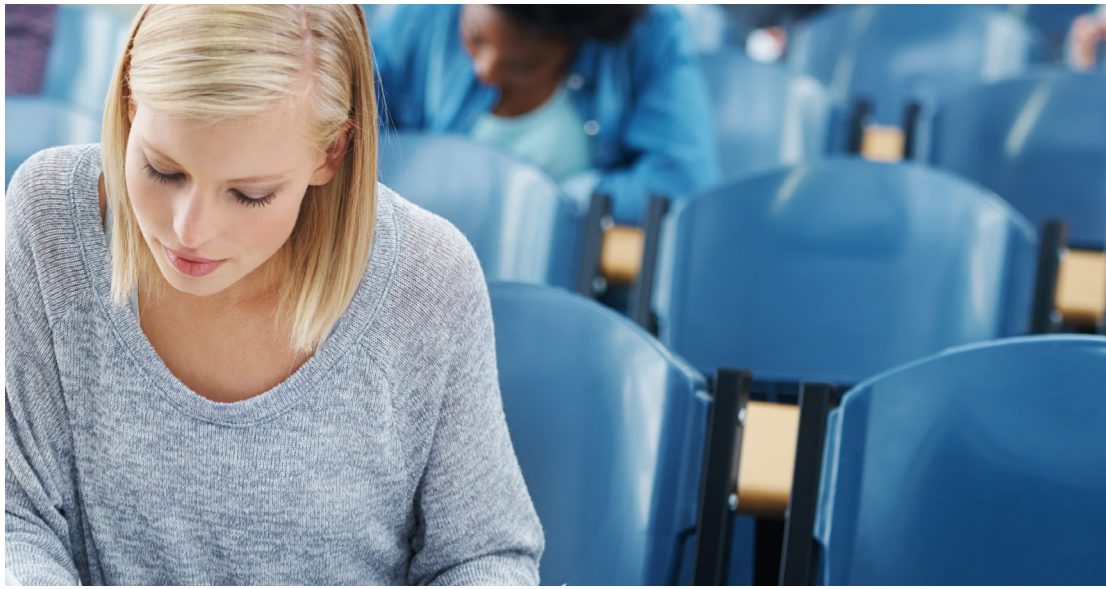
University administrators – including chancellors and vice chancellors – want to leverage technology to create an environment that attracts more students, enhances the success rates of existing students, enables more advanced research, and improves the rankings and reputation of the school. Naturally, the administration will also have budget concerns but most will understand the importance of building a strong and secure network, with excellent coverage for the entire campus.

Many professors in engineering and science faculties have labs full of sensors and actuators. Typically, they prefer dedicated networks with specific requirements. And, in many cases, they don't want to ask the IT department for approval for every device that is added to their network.

IT department challenges increased

One of the most important groups to be consulted before investing in a network infrastructure is the IT department. Aside from their technical expertise, they are also likely to have specific requirements that need to be considered.

For most IT departments, network security may be one of the primary concerns when considering any network investment, but other concerns include deployment and procurement costs, device on-boarding, network speed and coverage, and training and operational issues. Networks that can simplify operations are appealing to IT departments because it frees highly-trained personnel to handle more complex tasks or more strategic initiatives.



When it comes to IoT specifically, the IT department is challenged by the number of different IoT projects taking place across the campus; from professors and staff (as mentioned above) to the Security Department, who might want to deploy digital signage, door locks, and security cameras across campus. All of these requirements come with technological and operational challenges.

University of Portsmouth

> **“Our new technology enables us to extend wireless coverage to students across the campus, regardless of their location. Technology has evolved significantly over the past few years, and we now feel that we’re much better prepared for the next generation of communication as new students enter the University.”**
>
> James Holland, Network and Security Services Manager, University of Portsmouth.

University of Portsmouth • Portsmouth, UK

Challenge

- The university needed to invest in IT, telephony and networking infrastructure, in order to become more competitive on a global scale and consequently attract the best students, academic staff and research investment.

Solution

- A campus wide refresh of the WLAN using the latest technology to provide quality connectivity even in high-density areas.

Benefits

- Widespread wireless Internet coverage for students, academics and support staff enables improved access to resources, regardless of location and device.
- Increased coverage in areas of higher density, such as the University Library and lecture theatres.
- The solution also enables new maintenance jobs to be requested on the move, enabling health and safety issues to be addressed as they arise.

Recommendations

This section provides some recommendations for designing an efficient and cost-effective campus network that can meet the technology expectations of students and enable more collaborative, digital learning experiences.

Understand the limits of the existing network

The first step in building a next-generation campus network is to objectively analyze and evaluate the capabilities of the existing network infrastructure. Although most campuses have an infrastructure that supports basic access and mobility requirements, most are not structured to meet the expectations of students, staff, and faculty. 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 this network may be too expensive because many of the elements have reached the end of their life cycle, so parts and support are no longer available. Most importantly, this 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.

The wireless portion of the network may also be outdated. It may provide spotty coverage in some areas of the campus, 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. Typically, most campus networks are managed in silos, with different platforms for local area network (LAN) configuration/management, wireless – LAN (WLAN) configuration/management, and service level management. To effectively manage the network, the IT team must tackle each system separately. This makes it difficult to enforce a consistent, reliable level of behavior for the entire network that will meet student and faculty expectations wherever they are on campus.

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

- High capacity rates of up to 3.47 Gb/s per radio, compared to 54 Mb/s on 802.11g, 450 Mb/s on 802.11n and usual 1.3 Gb/s on 802.11ac 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 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.

UNIVERSIDAD DEL PACÍFICO

> **“To access the learning management platform and virtual desktops with full academic software from anywhere and on any device, and to be able to convert a conventional classroom into a laboratory are invaluable technological facilities for students and teachers in the process of teaching and learning at the Universidad del Pacifico.”**
>
> Ugo Ojeda del Arco, Director of Information Management and Technology Innovation

Centro Universidad del Pacifico (UP) • Lima, Peru

Challenge

- Universidad del Pacifico had platform management and maintenance issues being caused by the obsolete former infrastructure of the university. The university needed to replace their existing network and wireless infrastructure with a converged infrastructure solution, using the latest technology to benefit both their students and staff members and also enable BYOD adoption.

Solution

- The university network is now fully powered over Ethernet and all backbone connections have been upgraded with 20 Gbps link aggregation. Their core switches are now 40 Gbps links to the DMZ, running through a firewall. The university is also now covered by a 802.11n dual-channel wireless network, and will use the new 802.11ac standard in all new halls.

Benefits

- **Financial:** Thanks to the Alcatel-Lucent Enterprise solutions, the university saved $120,000 in the first year. Two virtual labs were created leveraging VDI (virtual desktop infrastructure) and BYOD, removing the need of substantial additional investment.
- **User experience:** Alcatel-Lucent Enterprise solutions enabled all students and staff members to enjoy high performance connectivity and easily adopt BYOD.

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 are each bringing up to five mobile devices on campus. Add teacher devices, classroom tools like projectors and printers, and all sort of new IoT devices – means planning for density is planning for success.
- **Assess WLAN bandwidth requirements:** Collaborate with professors to determine what is required to support their teaching style, and inclusion of mobile devices. For example, if your professors expect to use video-based teaching aids that stream video to multiple devices, you'll need a WLAN network capable of supporting multiple, high quality video streams. An HD-quality video stream uses 4 Mb/s of bandwidth per user and interactive learning games require multi megabits of bandwidth per user.
- **Prepare your network to handle massive bandwidth needs with 802.11ac Wave 2 technology:** Gigabit Wi-Fi devices are already available to students. Consider adopting the new 802.11ac Wave 2 Wi-Fi technology, which provides 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:** Finally, look for a solution that solves "sticky client" issues. As students roam between access points (APs), their devices can get stuck on an AP instead of associating with a closer one that has a stronger signal. The ideal campus network infrastructure should eliminate this so that old generation devices or disproportional distribution of users does not drag down the entire network.
- **Adjust your LAN access to properly support the new generation Access Points:** 802.11ac Wave 2 AP's typically generate an aggregated throughput above 1 Gb/s. In order to avoid bottlenecks and cabling rework, consider upgrading to access switches that support 2.5 G/5G ports (with PoE) and 10G uplinks.

Ensure your core/data center is not a bottleneck while reducing cost per student

An efficient, high performance access network is only as good as the core network it connects to. The core is the most critical part of your campus 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, you'll want to ensure your core network is ready to handle all the traffic coming from the access layer. Evaluate the traffic to determine where the bottlenecks could occur, what you'll need to ensure the network can identify and prioritize education-critical applications, and the type of network elements you need to reduce latency for all traffic.

When planning your 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 your wired infrastructure by reducing the number of layers in your network design - in many cases it is possible to eliminate the distribution layer, reducing your capital expenditures (CAPEX) and operating expenditures (OPEX)
- Choosing newly-designed, less power-hungry switches with lower power requirements; and
- Vendors that support pay-as-you-grow strategies that reduce budget pressures, but don't compromise product features

Improve the 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 purpose, 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. Furthermore, if links ever 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 independently of the size and complexity of the network. This considerably reduces the operational time to do moves/adds/changes and improves the network scalability.

Enable pervasive mobility, supporting access to students, staff, and guests

Ensuring that all devices coming into the campus environment get their fair share of network resources – on both wired and wireless networks – can best 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, faculty, staff, and guests will connect to the campus network with a variety of personal devices, creating an access and traffic management challenge. 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 simply accept the connection or sign in using their school credentials, if you want to map traffic back to an individual user.

Unified Access provides the same network services for wired and wireless

Alcatel-Lucent Enterprise offers a Unified Access solution that 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 done 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 and
- Security is maintained throughout the network

This 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. As users move around campus, each group is treated consistently by the network wherever they go. Depending upon their permissions, each group of users are granted different access rights. For example, professors could be given different permission than students, based on a different VLAN, with reserved bandwidth and different traffic priorities assigned to them.

UNIVERSITY OF TECHNOLOGY SYDNEY

> **“Communication and collaboration are core to every part of our business and the use of our Wi-Fi network has been increasing at a rapid pace. At UTS we make heavy use of technology to enrich teaching and learning. We engage with students through social media, video and electronic communications. If we didn’t have a fast, well designed network underpinning all this, it just wouldn’t work.”**
>
> Peter Gale, Information Technology Division Manager, UTS.

University of Technology, Sydney (UTS) • Sydney, Australia

Challenge

- UTS required a robust, high-performance network infrastructure to support their billion-dollar campus expansion plan. Wireless access was essential for highly connected students and faculty with multiple devices across campuses and housing developments. Building a secure WLAN network in a high-density urban environment with large volumes of non- university device interference was also taken into account.

Solution

- New generation Wi-Fi providing broad coverage and fast speed, high performance core to support the increased overall traffic and an end-to-end management system providing simpler IT operations and better control.

Benefits

- **Financial:** The new Alcatel-Lucent Enterprise network management, access points, and switching solutions have significantly reduced the upfront costs as well as the costs associated with maintenance and upkeep with a fully integrated system.
- **User experience:** The advanced Alcatel-Lucent Enterprise network provides students, staff and faculty with the technology they need to succeed today.

- Simplification of device on-boarding, allowing users to self-enroll and once authenticated, future connections will be automatic, without requiring the user to re-authenticate
- 802.1X authentication with Advanced Encryption Standard (AES) security features, allowing users to self-enroll, automatically generating and installing device certificates through a web portal with no IT assistance
- Elimination of difficult and time-consuming tasks for providing Wi-Fi access to campus visitors by enabling self-registration or sponsors to validate guests through a university-branded portal they can use without calling your help desk
- Enforcement of a differentiated network access based on contextual information, granting network access privileges based on user roles (for example, students, faculty, or staff), device types (laptops, tablets, or smart-phones), and location (classrooms, common areas, or dorm rooms), which also enables secure management and enforcement of differentiated policies.

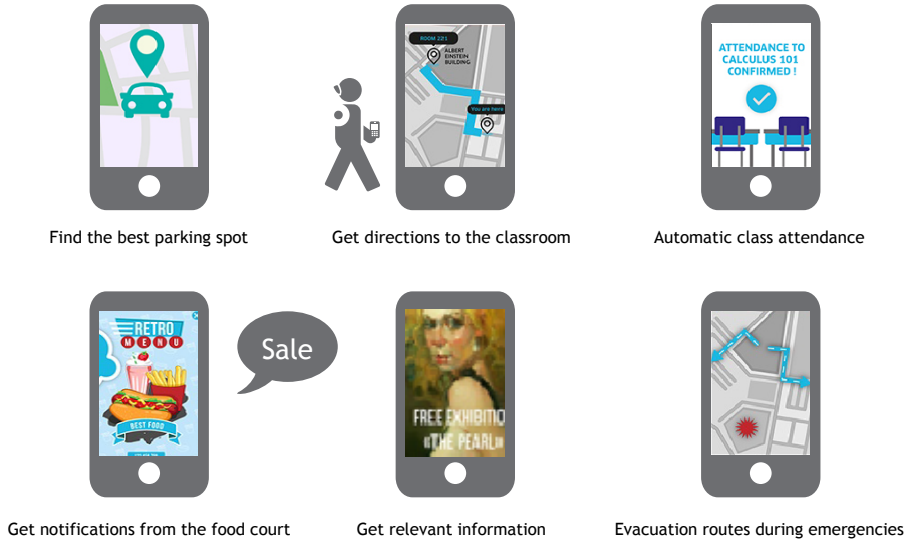
Consider Location Based Services for an outstanding student experience

Location services can offer better campus safety, provide students with an improved experience, reduce operating costs and even bring some additional revenue to the university.

One of the most used technologies for such services is based on Bluetooth Low Energy (BLE) technology, which provides a good compromise between cost, precision and flexibility. Typically this type of technology includes a beacon infrastructure and an SDK that provides functions as geolocation, way-finding, geofencing and analytics. Through the combination of these functions with a mobile app software it is possible to offer a variety of services that can provide the edge to differentiate your institution from the others.

Examples of possible location services include:

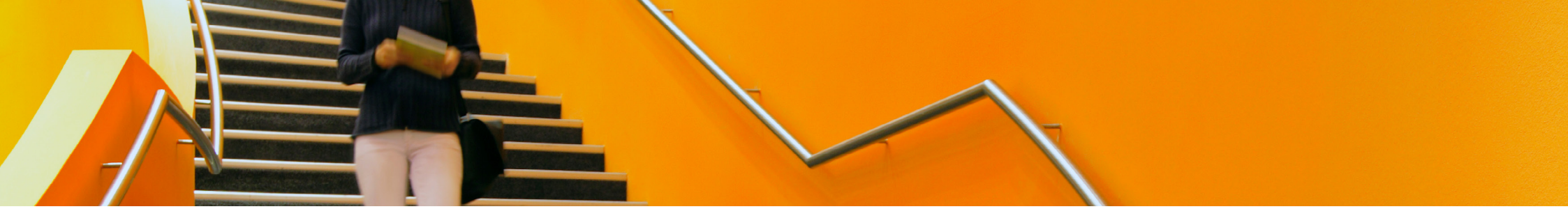
- Find the closest available parking spot to your class
- Get directions to the classroom and average walking time to reach it
- Automatic class attendance
- Directions to a shelf in the llibrary where a book is located
- Finding the best place to meet a friend (sharing location via social media)
- Provide notifications on promotions and lunch specials when approaching the food court
- Provide info on artifacts like paintings, monuments, etc
- Emergency notifications with recommended evacuation routes



Find the best parking spot | Get directions to the classroom | Automatic class attendance

Get notifications from the food court | Get relevant information | Evacuation routes during emergencies

Figure 2: Location based services



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.

IoT Enablement

IoT Enablement provides the appropriate network resources required for IoT systems to operate efficiently. Different devices – such as HVAC sensors, science lab devices, 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 this virtual containers, QoS and security rules are applied to ensure the IoT system counts with the necessary network resources to run efficiently and securely.

To simplify device on-boarding, IT can create a fixed number of profiles (for example, one for student devices, one for faculty devices, one for HVAC systems, and one for the security department). All of 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

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 using various virtualization techniques. In addition, profiles can be assigned to different user groups. As users move around the campus, 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.

Intelligent Fabric (iFab)

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 a 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.

With iFab highly-trained IT personnel are freed up to handle more complex tasks or strategic initiatives!

Offer in-depth security

Network security is a major concern for every university and college, especially with the growing popularity of the IoT. The modern approach to security is to provide not only firewalls, but protection at every level (as shown in Figure 2), 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, 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)

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

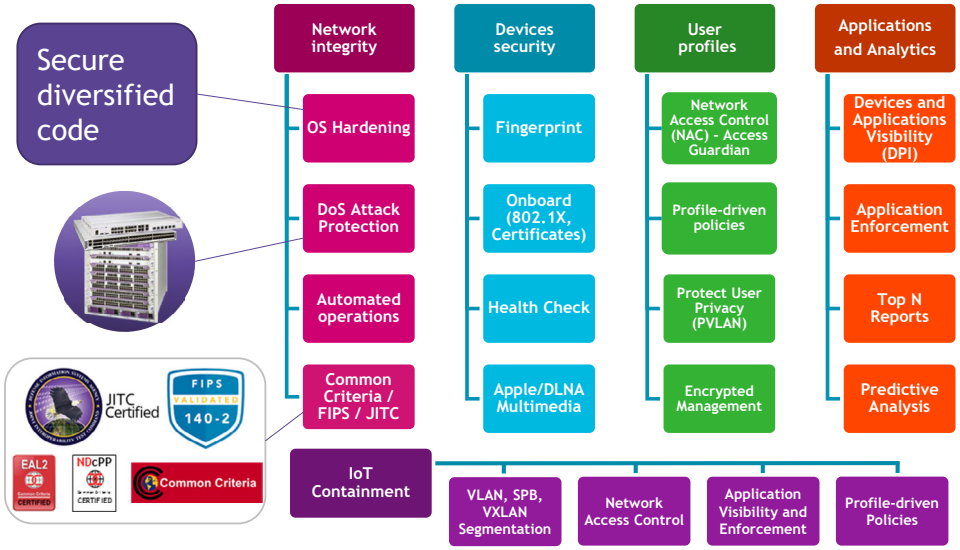


Figure 2: The modern approach to security is to provide protection at every level

- Media Access Control security (MACsec) is an IEEE standard (802.1AE) that provides security in wired ethernet LANs. MACsec can be used to encrypt traffic that might travel to an off-campus data center that is used for back-up and/or disaster recovery, for example.
- Integrated Distributed Denial of Service (DDoS) protection: Unfortunately, DDoS attacks are a growing threat for enterprises and need to be addressed. A DDoS attack is an attempt to make a network resource unavailable to its intended users. It 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 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 mostly used. 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 mostly use and which users are consuming the most bandwidth.

Predictive analysis monitors and analyzes trends for multiple days and weeks. An artificial intelligence (AI) algorithm build 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 the 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.

A comprehensive portfolio: From campus 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 also includes WAN routers and comprehensive network management platforms.

Figure 3 depicts the Alcatel-Lucent Enterprise portfolio that is available for educational institutions.

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 OmniSwitch® (OS) 6350/6450 families, passing to the multi-gig OmniSwitch 6560 family and all the way to the advanced OmniSwitch 6860E family which includes gig and multi-gig ports, integrated DPI and SPB. There are also two hardened switch families for outdoor and harsh condition areas: OmniSwitch 6865 and OmniSwitch 6455.
- 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 these APs include the Unified Access technology so that when they are combined in one network, they can offer a consistent QoE and a single management system (on premise OV-2500 or cloud-based OV-Cirrus).

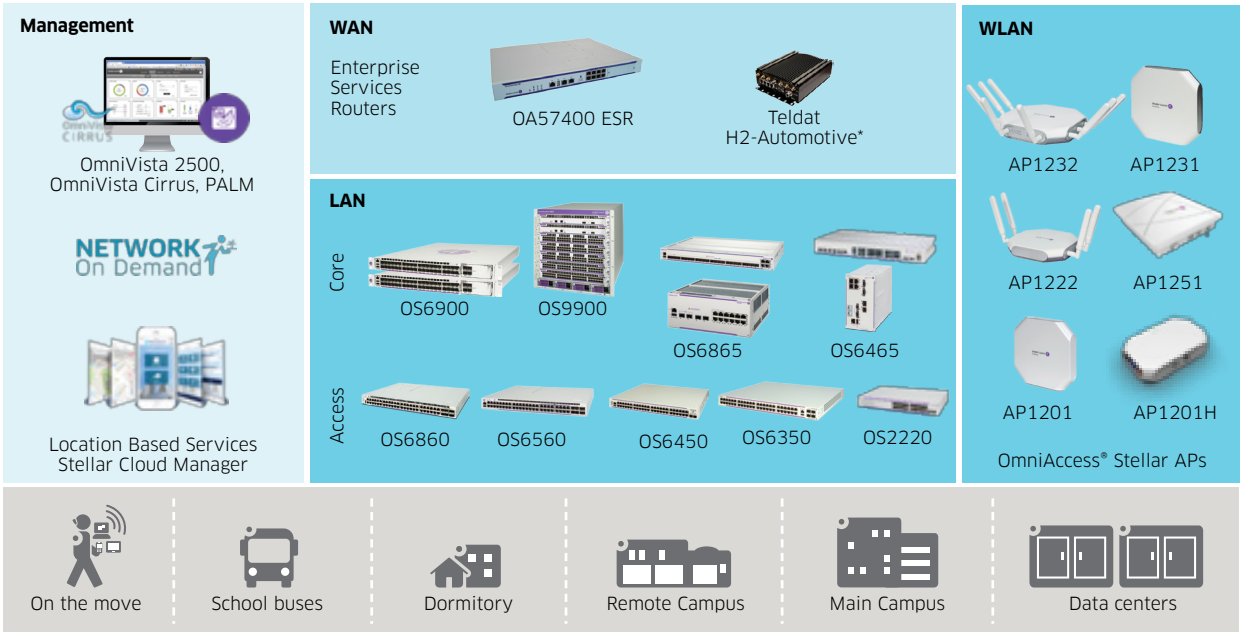
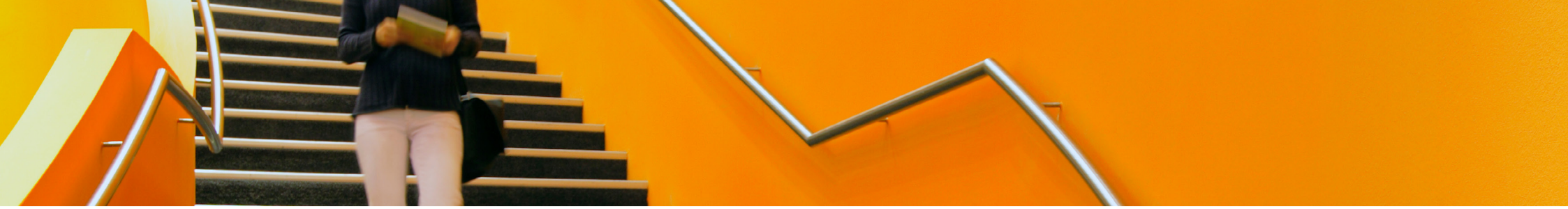


Figure 3 – Alcatel-Lucent Enterprise Network Portfolio



A resilient and high-performance core

The network core includes high-performance wire-rate 10 GigE / 25 Gig / 40 GigE / 50 Gig / 100Gig 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.

Virtualization techniques are used to eliminate inefficiencies introduced by protocols like Spanning Tree. Instead of disabling all redundant links and using them only if the main link or switch fails, virtualization enables the network to keep multiple links active and to fully utilize all available resources. Virtual Chassis (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 chassis, require less space and power, and be deployed at a lower cost. The VC also provides fast re-convergence if equipment fails, without impacting real-time application user experience, such as voice or video.

The core products incorporate the award winning Intelligent Fabric (iFab) technology offering 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 ALE's 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 distances of the building or campus makes the traditional three-layer architecture more cost effective. The OmniSwitch 6860E and the OmniSwitch 6900 switches described above make an excellent option for this type of architecture layer.

Reliable and flexible WAN connectivity

The Alcatel-Lucent Enterprise campus solution uses the Alcatel-Lucent OmniAccess® Enterprise Services Routers (ESRs) for branch office WAN connectivity. The ESR offers in a single compact from 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 University or Athletic department buses.

Protecting your investment with open standards

The Alcatel-Lucent Enterprise portfolio supports open standards and interfaces – including software defined networking (SDN) support with Openflow, Python scripting, and RESTful APIs – to ensure interoperability, support future alternative network architectures, and investment protection. Note that many of the proposed enhancements that SDN architectures try to offer – like connecting applications with network services dynamically, increasing automation and improving QoS – are already provided by ALE integrated technologies, with a much simpler and less expensive methodology.

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 form a centralized single pane of glass. It is offered in two versions: a 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.

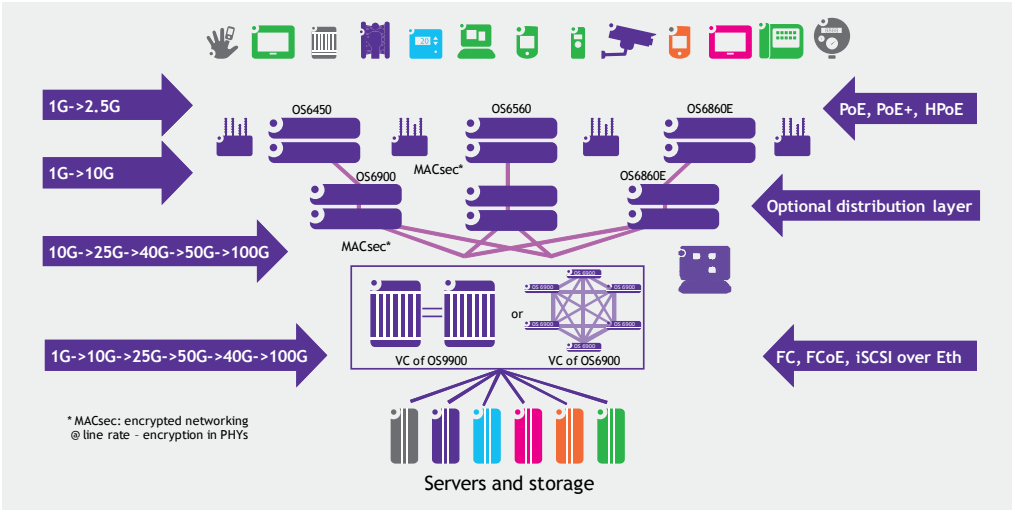


Figure 4 – The Alcatel-Lucent Enterprise portfolio offers the performance, resilience, and all interfaces needed to connect your institution

The Alcatel-Lucent Enterprise portfolio offers the performance, resilience, and all interfaces needed to connect your institution from the user devices and IoT endpoints all the way to the data center. Providing a variety of speeds and interfaces to best fit your specific needs. The diagram above summarizes the multiple options available.

Conclusion: Technology is becoming increasingly central to education worldwide

For many students, the way a college or university integrates IT into the fabric of campus life can be just as important as their chosen field of study or the structure of the curriculum. Most students don't remember a time before the internet and they expect to be able to connect with any device, anywhere on campus; whether it's to communicate, be entertained, or to access educational resources.

In addition to student expectations, a campus network must also meet the technology requirements of the university administration, staff, faculty, and IT department.

When designing an efficient and cost-effective campus 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 faculty
- Deliver a high performance network: Provide a WLAN infrastructure that can handle a large influx of mobile devices and the bandwidth-hungry applications running on them
- Enable pervasive mobility: Ensure that all devices coming into the campus environment get their fair 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 campus network has become an important asset for attracting and retaining the best students and faculty, boosting learning and research, reaching off-campus students, providing lifelong learning, and creating a more collaborative learning environment. The growing number of mobile and IoT devices – alongside the associated security concerns – requires more stringent network requirements to ensure that it is ready to support the digital campus of the future.

Higher Education Networking Guide
Building the Foundation for Tomorrow's Digital Campus
December 2019

Connected Education

Where education connects with technology that works. For your school, college or university. With a 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.

Alcatel·Lucent
Enterprise