



Key considerations for a campus network edge refresh

White Paper

Key considerations for a campus network edge refresh

Table of contents

Overview	3
Refreshing the edge: What to consider	3
Performance	3
Wi-Fi 5 or Wi-Fi 6?	3
Access, uplinks, and power	3
IoT connectivity, network segmentation, and quality of service	4
Manageability	4
Unified across the LAN, WLAN, and IoT	4
Cloud-based or on-site: Full capability when moving from one to the other	4
Policy management and security	4
Analytics	5
Total Cost of Ownership (TCO)	5
Hard costs	5
Soft costs	5
ALE Digital Age Networking unlocks the value of your edge refresh	5
Performance	6
Management	6
Lower TCO	6
Take your campus to the next level with Digital Age Networking	7

Overview

Your Local Area Network (LAN), wired and Wi-Fi, needs to keep pace with your school or university's academic and business digital transformation – addressing remote work and learning, and the growing Internet of Things (IoT). You may be concerned about reliability, security, and capacity as your switches near their end of life. Your students and faculty may be demanding better performance. You may be worried about keeping your network secure as greater and more frequent cyberattacks target the education industry.

Your end-users rely on a high-performing, reliable, secure network, especially at the edge where the demand is greatest for more connections, wired and wireless. If the edge of the LAN is your most pressing need and you have decided to embark on a network edge refresh, this document can provide some suggestions and insights about what to consider when selecting a vendor.

Refreshing the edge: What to consider

While there are many factors to think about when refreshing your network edge, below are three essential considerations that will ensure your network can deliver IoT benefits and outstanding end-user experience today and well into the future.

- **Performance:** Capacity, security, and resilience whether wired or wireless
- **Manageability:** Fast provisioning, troubleshooting, and analytics regardless of how the management platform is connected (on-site or cloud)
- **Total Cost of Ownership (TCO):** Hard and soft costs, both up-front and throughout the life of the equipment

Performance

Wi-Fi 5 or Wi-Fi 6?

An important decision point is wireless capacity, both indoor and outdoor. Most devices, those used by humans as well as those that talk to machines, are connected to the campus on a wireless local area network (WLAN).

Many Wi-Fi networks in place today cannot handle evolving pedagogy practices, STEM courses and the rapid expansion of intelligent appliances, robotics, automation, and the exponential growth of sensors, cameras, actuators, and door locks, among a nearly endless list. Older Wi-Fi networks are also less secure as they rely on encryption standards that have proven security gaps.

Both Wi-Fi 5, and the recently approved Wi-Fi 6 standard, can enable you to increase WLAN capacity and performance. The choice between Wi-Fi 5 or Wi-Fi 6 is often one of cost, and if your budget permits, Wi-Fi 6 has significantly more capacity, capabilities, and security enhancements.

Access, uplinks, and power

Using Wi-Fi 5 or Wi-Fi 6 access points increases the bandwidth generated by the Wi-Fi network. This means you must also upgrade your edge LAN switches so that they don't become a traffic bottleneck. You will also need to consider the links to your access points, as well as the links to your network core. While modern edge switches can now serve multigigabit speeds to access points over your existing data cable infrastructure, these switches will also require very high-speed uplinks to your core and distribution network.

Your edge switches must also provide sufficient power for your high-capacity Wi-Fi access points (at least 30 watts per port), as well as power for cameras and other directly connected devices. Wi-Fi 5 and Wi-Fi 6 access points can operate with less power but will not deliver the full performance and value for which you paid.

IoT connectivity, network segmentation, and quality of service

With the explosion of devices at the network edge, automation for getting those devices connected securely becomes a business imperative. Your network edge must be IoT aware and provide easy connection to devices automatically. This capability requires access to a comprehensive IoT inventory that enables automatic device detection and connection.

The network must also be able to automatically segment devices into categories. For example, security cameras should be on a separate segment from the HVAC system as they have higher priority and security needs. Only authorized employees should have access to video cameras, much like segregation of duties in SIS systems.

With different segments for different devices, Quality of Service (QoS) is critical. For instance, flexible QoS rules can provide more bandwidth for cameras and less for temperature sensors. QoS can prioritize time sensitive traffic such as real-time alerts. This lets you optimize performance for each user or device connecting to your network edge based on their role, authorization, or priority.

Manageability

Unified across the LAN, WLAN, and IoT

Many network management systems are a collection of tools designed for specific switches and other network elements. They often don't work together, which can increase the time and cost of managing the network. It also makes maintaining consistent security policies across wired and Wi-Fi access cumbersome.

Your network management system should be a single platform that can see, manage, secure, and analyze the entire network, including the LAN, WLAN, and even IoT devices. Since today's network elements and devices are increasingly integrated and interoperable, the ability to manage the entire network reduces costly delays in deployment, analysis, and trouble resolution.

Cloud-based or on-site: Full capability when moving from one to the other

Many management systems offer the option of on-site operation or cloud-based services. For many campuses, cloud-based management systems offer benefits such as automatic upgrades with no interruptions, no maintenance, and high-availability assurance.

Educational institutions that value local control usually prefer an on-site management system. Others require on-site systems for legal and privacy reasons.

If you decide on a cloud-based system, it is essential to verify that all the capabilities of an on-site platform are available from the cloud. Some cloud-based systems offer limited services when compared to on-site capabilities. Pay particular attention to the hardware supported. Some vendors require a totally different product line if you are deploying a cloud-based versus an on-site management platform. For K-12, a cloud-based system enables third-party management of the network, which is eligible for funding by E-Rate. For colleges and universities, it enables flexibility.

Policy management and security

To support a consistent and seamless experience, the network management platform should provide unified policy management across the entire network, to support both wired and wireless users and devices. Security should be centered on a zero trust basis, which assumes no device or user has access to the network until authenticated.

Analytics

Insight into the health of the network, and understanding trends and trouble spots, are vital to resilient operations and minimizing interruptions. The management system should provide network analytics with performance insights and predictive analytics that spot trends. Access to an IoT inventory, for early warning about problems is critical to the user experience and the timely delivery of IoT data for analysis and action.

Total Cost of Ownership (TCO)

When considering the cost of refreshing your network edge, it is crucial to look beyond the price points of switches and access points. Consider the typical five- to seven-year lifespan of the network equipment and take a closer look at both the hard costs such as hardware, maintenance, licensing and support, and the soft costs such as network downtimes and operational efficiency.

Hard costs

Consider the cost of equipment and include licenses for capabilities such as IoT, applications analysis, and registering users who bring their own devices (BYOD). Often, vendors charge by the feature or simply charge more for basic capabilities, based on their brand.

Factor in maintenance over the life of the product and what a maintenance agreement will cover. Some contracts provide only partial support, and others charge extra for response times and levels of tech support.

Soft costs

While hard costs provide a straightforward dollars and cents view of upgrading your network edge, soft costs can often have a more significant impact during the life of the product. Consider the valuable time that is lost if you must manually create an IoT inventory and then research each new device to register and add it to the inventory. Adding an IoT device should be simple, by providing access to an existing database and registering devices automatically.

Security breaches can be costly, as can network failures. It is essential to consider the value of resilience and the security of network switches and access points when comparing equipment prices and maintenance costs.

Troubleshooting time should also be considered. Many education institutions' IT staff are stretched thin – having to use multiple tools for the wired and Wi-Fi edge could add significant time to resolve network issues.

Also, think about interoperability with other elements of your network. Verify whether you can refresh and upgrade in phases to match your needs and budget. A refreshed edge with Wi-Fi 5 or Wi-Fi 6 should absolutely interoperate with the core network until you are ready to upgrade.

Consider the cost of IT staff spending time on network operations and additions instead of providing strategic services to the campus. What is the most valuable use of their time?

ALE Digital Age Networking unlocks the value of your edge refresh

Alcatel-Lucent Enterprise offers a comprehensive portfolio that delivers the network foundation, performance, management, and low TCO to support digital transformation and make the most of IoT and analytics. From the edge, to the core, to the cloud, ALE can help you evolve your network at your pace.

Performance

[Alcatel-Lucent OmniAccess® Stellar Access Points](#) provide scalability and low latency, all without the bottleneck and cost of a controller. The OmniAccess Stellar line offers a range of Wi-Fi 5 and Wi-Fi 6 access points from entry-level, to those for harsh outdoor environments. These access points can handle high-density traffic and large numbers of devices on both 2.4 GHz and 5 GHz Wi-Fi bands.

The [Alcatel-Lucent OmniSwitch®](#) family of edge switches offers both Layer 2 and Layer 3 functionality, including hardened switches for outdoor and harsh environments. These switches provide gigabit and multigigabit access and 10 to 25-gigabit uplinks to accommodate modern access points and easily handle heavy end-user and IoT traffic.

The OmniSwitch family enables you to avoid expensive electrical cabling costs as it provides power over ethernet (PoE) and high power over ethernet (HPoE) to easily handle the demands of modern access points, cameras, and other devices which need switch-connected power. The switches also provide easy device connectivity, automated device segmentation and fine-grained QoS to handle every need.

Management

The [Alcatel-Lucent OmniVista® 2500 Network Management System](#) (NMS) is an on-site system that provides network-wide visibility and advanced analytics for a full view of wired and wireless devices, IoT devices and applications, and predictive analytics for planning.

OmniVista enables easy connection and “fingerprinting” of IoT devices and provides a cloud-based inventory with a library of over 30 million known devices. The system automates the rollout of devices and network elements with policy-driven provisioning for compliance and security.

Single policy management of the entire network is enabled with Unified Policy Authentication Management (UPAM) services. This capability allows wireless and wired devices and end-users to be governed with a single set of policies.

The OmniVista NMS is also available as a cloud-based service, [Alcatel-Lucent OmniVista® Cirrus Network Management as a Service](#). Whether in the cloud or on-site the platforms can manage the same hardware (switches and access points), with the same feature set, providing comprehensive and flexible network management.

Lower TCO

Alcatel-Lucent Enterprise lowers TCO by adhering to industry standards and offering interoperability with your existing wired and Wi-Fi network. You can refresh your edge in phases without the worry or cost of changes to your core network. For example, ALE's edge solutions have been deployed by many customers who have kept their existing non-ALE core networks.

The OmniVista NMS feature set includes all the capabilities many vendors charge extra for such as support for guests, BYOD, Wi-Fi, IoT, management and analytics – all in one software package. OmniVista also lowers cost through its automated provisioning and the elimination of repetitive tasks and expensive on-site support visits.

ALE's distributed Wi-Fi control eliminates controller costs such as maintenance, licensing, and capital expenditures. This allows you to pay as you grow, adding more access points as you need them.

A simple licensing program offers full transparency for both upfront and on-going costs. A single operating system across all ALE products reduces the learning curve and all hardware comes with a Limited Lifetime Warranty (LLW).

Take your campus to the next level with Digital Age Networking

Whether you decide to refresh your network edge in phases or all at once, full consideration of performance, management and TCO will help you make the decision that best serves your campus today and tomorrow.

Many industries are already seeing a payoff from IoT technologies, enhanced access, and user satisfaction. The journey toward an IoT analytics-driven infrastructure transformation and new operating models holds tremendous promise for campuses large and small. That journey begins at your network edge where everything connects.

