aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

Higher Education Networks for the Smart Digital Campus

Deliver exceptional experiences for students, staff, and IT

Higher education institutions are under constant pressure to support demands from administrators, faculty, staff, and students. Digital curricula, classroom collaboration, and context-aware services are moving to the cloud. Campuses are essentially small cities, and new Internet of Things (IoT) devices are flooding into labs, buildings, and facilities, forcing IT to find ways to secure IoT network communications. Students are using more devices in class, for remote learning, and in residence halls, and IT is being asked to support personalized learning for everyone. Finally, calls for improved campus safety are driving requests for gunshot detectors, location-enabled panic button, wireless video surveillance cameras, and vaping sensors.

Aruba's Edge Services Platform provides always-on, secure connectivity with an architecture that is extensible across a broad range of IT, IoT, and operational technology (OT) applications. Built on a Zero Trust Security framework, the platform unifies wired, wireless, and WAN operations and security wherever users learn, work or roam. To improve operational efficiency, the Edge Services Platform uses AI-driven insights and automation to predict issues and optimize the network before users are impacted. The results empower faculty, staff, and students to create, innovate, and collaborate in ways never before possible, with unparalleled privacy and security.

> Higher education is a popular target for phishing scams. Cyberattacks on these institutions have resulted in the exposure of over 1.3 million identities. Over the last year, nearly 56% of colleges and universities have seen an increase in phishing attacks.

CONNECTIVITY MUST BE UNIFIED, ALWAYS ON AND AUTOMATED

Campuses run non-stop, and so must the networks that support them. Students need network access at all hours. Classes and research projects run day and night, and public safety systems must be ever vigilant. For all these applications, network performance must be consistently reliable.

> Automation can help alleviate the high percentage of unplanned network downtime that is caused by human error (Gartner, 2019).

High-Performance Wireless Networks

Aruba's Wi-Fi 6 (802.11.ax) infrastructure is designed to support campuses of any size with always-on secure connectivity. Seamless roaming allows network access on the move, while high density capabilities supports both lecture auditoriums and sports facilities packed with fans. Learning management and unified communications systems can be prioritized to deliver latency-sensitive data, voice, and video without delay, loss, or jitter.

Hitless updates and hitless failover ensure that the wireless network can stay current with the latest security updates, tolerate faults, and be available whenever needed. No assessment or online test interruptions, no lost research and experimental data, no dropped calls.

The infrastructure leverages industry-leading tools to auto-adapt to changing environments and applications: ClientMatch to optimize roaming performance; AppRF to optimize the performance of critical applications; Adaptive Radio Management to enhance radio performance; and AirSlice to manage bandwidth allocation.

Customer Quote: "Our multi-year strategy to leverage technologies like mobile, Artificial Intelligence, IoT, cloud, analytics, and Blockchain depends on infrastructure like our Aruba Wi-Fi to serve as a foundation."

– Radha Krishnan, Associate VP of Information Services, Seneca College, Canada

Smart Switches from Edge to Core

Aruba's Edge Services Platform includes wired and wireless networks that work together to deliver a consistent and secure network experience. Aruba designs its own semiconductors so its switches can provide blazing fast and highly granular visibility into the performance of the switching fabric. SmartRate power-over-Ethernet (PoE) allows Wi-Fi 6 access points to operate at >1Gbps over existing cabling, eliminating the need to rip and replace cable plants to obtain multi-gigabit wireless performance.

The Aruba AOS-CX operating system features a time-series database that provides deep visibility into data traversing the switching fabric. Intuitive software-defined management tools, built-in analytics, and programmable scripting offer unparalleled insights into network and device activity, fault isolation, and system performance. Upgrades and updates can be easily enabled, reversed, and changed without impacting the network or the people who rely on it.

Customer Quote: "We chose Aruba because it is the leader in its field…we worked closely with team to deliver a wired and wireless network infrastructure to support 'anytime, anywhere' learning."

– Stephen Castellas, Senior Manager, Global Networks, RMIT, Melbourne

Redundant Aruba AOS-CX switches operating in Active-Active mode will deliver non-stop operation in the event of a fault. Virtual Switching Extension (VSX) ensures that traffic loads are validated before returning balanced traffic loads to the Active-Active pair. Once the first core switch completes the transfer, the process repeats for the remaining core infrastructure.

The Network Analytics Engine (NAE), included with AOS-CX, provides a built-in framework for monitoring and troubleshooting networks. NAE detects problems in real-time and analyzes trends using the time-series database so IT can predict future performance and security issues.

AOS-CX, coupled with high-performance switches, delivers the throughput, performance, and actionable insights IT administrators need to handle the massive amounts of data now being generated at the network edge in every college and university.

PROTECT THE NETWORK FROM END-TO-END

While higher education institutions have been investing in cybersecurity, unsettling breach statistics and costly ransomware attacks show more needs to be done to protect people and information. Traditional security solutions create a secure perimeter and detect attacks and malware based on their patterns or signatures. This model is unsuitable for colleges and universities where there is no perimeter: students, staff, and faculty move on and off campus, and need network access everywhere.

Aruba's Zero Trust Security framework dynamically segments network traffic. With policy management, analytics, and automation, the risks of security breaches are minimized while detection and response are enhanced.

Know what is on the network

With IoT devices springing up seemingly everywhere, it can be challenging to know what is or should be on the IT network. AI-powered ClearPass Device Insight simplifies device identification and onboarding using machine learning to identify and profile IoT device types so they can be automatically dynamically segmented, remediated, or quarantined.

Zero Trust Security access

Once devices are identified, ClearPass Policy Manager profiles, authenticates, authorizes, and tightly manages network access using granular, policy-based access controls. Users and devices have restricted access to only those network, IT, and application resources for which they have been approved. ClearPass also ensures that users and devices are compliant with regulations governing student privacy and personally identifiable information.

Separate student, staff, and IoT traffic

Dynamic segmentation establishes secure tunnels between IT, IoT, and plant operational technology (OT) devices and their associated applications. This perimeter-less zero trust micro-segmentation is applied to wired, wireless and WAN networks, so no matter where users and devices work or roam micro-segmentation will remain in effect. Policies are carried across the network end-to-end, regardless of the location of the user or device or the switch port carrying the traffic, i.e., student learning traffic is isolated from student records, public safety cameras, and administrative traffic.

ACT QUICKLY WITH INTUITIVE AI-POWERED MANAGEMENT TOOLS

Aruba's Edge Services Platform includes assurance and orchestration features to maximize up-time, optimize user experiences, and reduce the time to troubleshoot issues to root cause. Automated network assurance delivers AIOps insights from a single pane of glass, while edge-to-cloud experience monitoring generates automated AI-based alerts that proactively pinpoint critical application and network issues.

Optimized remote site connectivity, visibility, and management

Aruba's SD-Branch solution leverages SD-WAN capabilities to deliver secure connectivity to remote satellite campuses and research facilities. Offering service level agreement (SLA) monitoring over Internet, MPLS, and cellular WAN links, the solution encompasses WAN, WLAN, wired networks, and security management.

Deployment is a snap, and can even be done by non-technical personnel without an IT truck roll. An Aruba mobile app is used to scan barcodes on Aruba devices and configurations are downloaded automatically to Aruba Central cloud-managed gateways. There is no faster or more intuitive way to connect and bring-up remote sites than Aruba's SD-Branch solution.

AIOps Assurances for optimized performance

Aruba delivers customized recommendations through AI-based machine learning to improve network and application performance based on anonymized comparison with peer environments. If a change could increase performance by 10%, it is recommended to the Network Admin who can then authorize the settings change. Aruba User Experience Insight provides IT a real-time view of the end-user experience and clear action steps to resolve any issues before a service ticket is opened. These powerful tools bring much-needed help to enable already overwhelmed IT staff to take necessary action and stay ahead of issues

UNIQUE SOLUTIONS FOR IMPROVED EXPERIENCES AND STUDENT SAFETY

Colleges and universities are places of learning and community. The safety of faculty, students, and staff used to be taken for granted, but no longer. Today's natural disasters, civil unrest, and active shooters impact campus safety and are a major concern for first responders. Network infrastructure can help by quantifying the nature of the threat, identifying safe and unsafe areas, and automatically guiding people to safety. While networks can't prevent incidents from occurring, they can lessen the impact of incidents by keeping faculty, students, staff, visitors, and first responders safer.

Access Points as IoT Platforms

We are accustomed to thinking about Wi-Fi access points in the context of secure wireless network access, and for many years that was their primary function. Not so today. Aruba Wi-Fi 6 access points include radios for wayfinding, geofencing, location tracking, sensor monitoring, door locking, and actuator control. These capabilities transform Aruba access points into secure, multi-purpose communication systems that are both network access on-ramps and full-fledged IoT platforms.

> **Customer Quote:** "The Meridian based app enables users to navigate easily and safely around the campus. This benefits both students in their first semesters and visitors. Most importantly, we have created a solution that highlights easy access routes."
>
> *– Carsten Hellmich, Technical Project Manager, Hochschule Hannover*

Aruba's location-based services bridge the gap between digital and physical worlds. Using signals generated and received by Aruba access points, our location-ready infrastructure enables turn-by-turn wayfinding navigation of campuses and buildings, proximity-based messaging for guests and students, asset tracking, and location analytics.

Third-party safety devices supported by access points include, among others, mobile panic buttons, gunshot detectors, occupant detection, electronic door locks, and vaping detectors:

- Mobile panic buttons both call for help and identify the location of the individual in distress
- Gunshot detectors identify the type of weapon and muzzle flash rate, so first responders can arrive prepared
- In the event of an incident, the occupant detection system will push a message asking occupants if they're safe and then generate an interactive 3D site model telling first responders where to go first
- Electronic doors locks can be used to secure buildings and dorm rooms, and remotely provide access to response personnel and
- Vaping sensors can be used to enforce no-smoking regulations in bathrooms and dorms.

All manner of low-voltage building systems - including comfort, intrusion detection, energy management, access control, personnel and asset tracking, man-down, call button, leak detection, security, and gunshot monitoring - can now reliably and securely communicate over shared infrastructure. The resulting savings in equipment, installation, and maintenance costs over deploying dedicated control networks is significant.

A PARTNER ON YOUR SMART DIGITAL CAMPUS JOURNEY

The most dynamic and transformative experiences happen at the edge. Aruba's mission is to harness and secure data at the edge, and, in partnership with our customers, to enable the most meaningful education digitalization initiatives. Start the journey by contacting your local Aruba salesperson or reseller today.

SO_HigherEducationNetworks_SK_051920 a00099194enw