



Aruba's User-centric Network for Higher Education

What's your vision? To make technology a central element of the campus experience? To move disparate communication services to a single flexible network? To create a truly ubiquitous mobile network that securely serves every student, administrator and faculty member, everywhere, on any device, exactly as they need?

Aruba has pioneered a new approach to help you achieve your vision. Aruba's User-centric Networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system for higher education institutions. The result is a centrally managed solution designed to offer the speed of a wired network and the adaptability of a wireless network with uncompromised security and a low total cost of ownership.

Unique Aruba Capabilities

Aruba delivers industry-leading innovations in campus mobility, providing a solution that can be implemented as a seamless overlay atop the existing network.

ADAPTIVE 802.11N

Aruba's high-performance 802.11n products make the all-wireless campus a reality. Aruba offers an adaptive solution that easily integrates with existing architectures and scales to meet the grueling network demands of higher education. Featuring 3x3 Multiple-In Multiple-Out (MIMO) operation, a field-upgradeable design, and full functionality with standard 802.3af Power-over Ethernet (POE), Aruba's 802.11n access points can be used for wireless access, intrusion detection monitoring, traffic analysis, secure enterprise mesh, or remote access point applications. The mode of operation is determined by network-downloadable software, a feature that allows the access points to be repurposed and updated without the time and expense of physically accessing the device.

FUTURE-PROOF DESIGN

The Aruba architecture lays the foundation for future network-based applications. It is built on reprogrammable silicon, providing blazing performance and allowing for simple, non-disruptive upgrades. Many schools start with basic wireless functionality and add new features as they go: wireless intrusion protection, voice over Wi-Fi for maintenance and public safety, wireless mesh back-up of fiber links, or location tracking for equipment leased to students on campus. With Aruba, these additions are accomplished with a simple software upgrade, not a massive network rework. Standards updates, such as encryption or authentication types, can also easily be incorporated without disruption to the network.

IDENTITY-BASED SECURITY

As students, faculty and administration moves around campus, it is essential to maintain, but limit, access to their defined network resources. Traditional access control methods, determined by point of network entry, break down

The Aruba Advantage:

- **Adaptive 802.11n:** Deploy 802.11n as needed and let the network adjust automatically
- **Future-proof:** Software upgradeable design to support future applications
- **Identity-based Security:** Security follows users as they move across campus or across the world
- **Application-aware:** Optimized for converged data, voice and video support over wireless
- **Central Management:** Easy to configure, monitor and troubleshoot with centralized control

with mobility and WLANs. Access control must now consider user identity, role, device type, location, time, and other relevant user and device characteristics. Mobility should integrate seamlessly with the existing AAA infrastructure, such as RADIUS, LDAP, or Active Directory. The Aruba Networks architecture is uniquely capable to provide these capabilities. Unlike other solutions that tie policies to specific SSID/ VLANs to secure and segment a network, Aruba implements a stateful firewall to tie specific security policies to distinct roles and users. This policy is tied to the user, making it consistent wherever the user roams.

APPLICATION CONTINUITY

Educational institutions can extend the value of their Wi-Fi investment by using it to support other disparate systems on campus such as mobile voice, broadcast video, surveillance systems, and building controls. Using a single unified and secure system can provide significant savings. Because the Aruba system is application-aware, it is optimized for convergence, providing security and special handling of traffic based on the application type, device and user. Aruba's capabilities enable universities to

take advantage of IP convergence and consolidate disparate, hard-to-manage systems onto a single infrastructure.

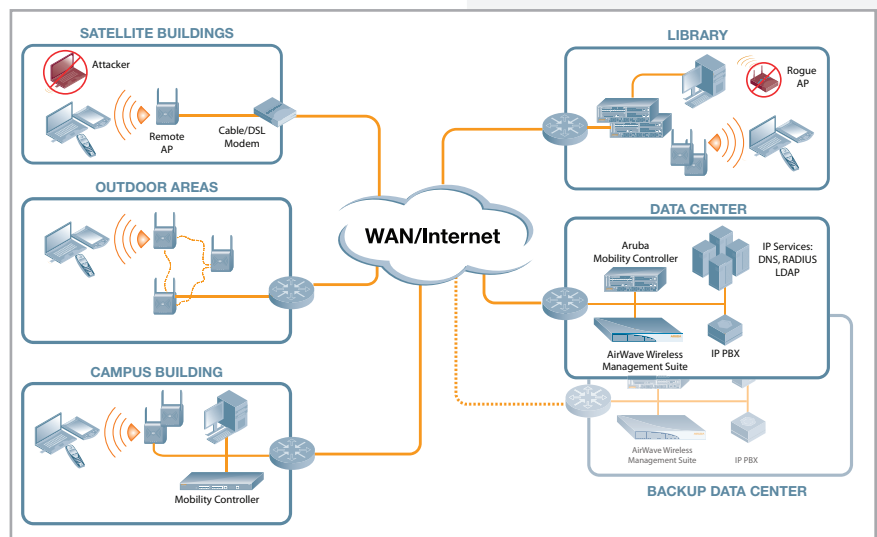
CENTRAL MANAGEMENT AND CONTROL

Aruba's centralized network architecture enables network monitoring, control and troubleshooting to be performed from a single location regardless of whether the network spans a campus or continents. For universities that are part of a system of colleges, a separation of duties may be mandated between IT managers at each college. Aruba offers a "manager of managers" capability that logically separates the information available to each management user hierarchically. Aruba's infrastructure provides remote packet capture so IT managers don't have to walk across campus or worse, drive somewhere, to troubleshoot problems. Additionally, Aruba offers a full real-time view of the RF environment for each building that is part of the campus network. The network manager can perform all maintenance and upgrades centrally from one location, receiving alerts on intrusion or other security events as they happen.

The Aruba Networks Education Solution

The Aruba solution consists of three key components – thin Access Points (APs), central Mobility Controllers and software modules for the Mobility Controllers; and an optional component – AirWave Wireless Management Suite by Aruba. APs provide secure wireless connectivity to devices and connect over existing LAN/WAN systems to tunnel all wireless LAN traffic (over a GRE or IPsec tunnel) to a Mobility Controller installed in the data center or in a local building depending on traffic flow requirements. The Mobility Controller is the central point of configuration, management, application continuity services and security. With software modules for Mobility Controllers, Aruba offers the ability to deploy the right level of functionality today and add capabilities as needed in the future.

Following is an explanation of a wireless network in an education environment with centralized IT services:



Data Center: Depending on the number of remote locations and total number of APs, one or more master Mobility Controllers are installed in the data center. These controllers can also terminate APs used for wireless connectivity in the data center building and remote APs used in small remote offices and home access applications. A master controller can support up to 500 remote controllers and is the single interface for configuration and management. A master controller can also back up a controller in a remote location in the case of an outage. To scale for larger deployments, multiple master controllers can share the load of managing local controllers and APs in remote sites, and the MMS can be used as the single interface of management and configuration.

Campus Buildings: Depending on the number of APs required in each location, a different model of Aruba Mobility Controller (called a local controller) is installed. All Aruba controller models run the same software and have the same functionality, but differ in AP capacity – from up to 6 to 2,048 APs. Each local controller gets its configuration from the master controller. Application continuity and PCI security levels are enforced at a per-user level by the local controller. Local controllers also offer Wireless Intrusion Protection and can offer provide authentication services and/or pass-through requests to the data center. Each local controller automatically calibrates the RF coverage to optimize application performance and cover any coverage holes. Further, to extend wireless coverage in areas that are hard or costly to wire, Aruba APs can backhaul over Wi-Fi using the award-winning Secure Enterprise Mesh technology.

Outdoor Areas: Most Aruba APs can be deployed in covered outdoor areas for use cases such as stadium retail vendors, surveillance cameras, blue light call boxes, or just outdoor student network access. For harsh outdoor conditions, ruggedized APs are also available. In cases where the Ethernet network has not been extended to these outdoor locations, any Aruba AP can create a mesh connection back to an Aruba network-connected AP that has been enabled for mesh. The AP will continue to act as a standard thin AP with a connection back to the controller through at least one other AP that acts as a mesh hop.

Remote Users and Temporary Offices: Remote APs are a cost-effective solution to provide secure and centrally managed wireless connectivity to locations that only need a small number of APs. Remote APs can connect directly via Ethernet to a public/private Internet connection or to the LAN. Remote APs automatically discover the master controller, establish a secure VPN tunnel back to the data center and extend secure wireless connectivity to a single remote user or a group of users. Application traffic can be tunneled back to the data center or bridged locally. For cases where more than one AP is needed at the remote site, additional APs can be connected to power sources and create a mesh connection back to the network-connected remote AP. The result is a wireless office that can be set up on the fly without any Ethernet LAN cabling and without IT resources.



WWW.ARUBANETWORKS.COM

1344 Crossman Avenue, Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550