



# Managing WiFi in Higher Education

## Overview

Colleges and universities have been perhaps the earliest and most aggressive adopters of WiFi technology over the past five years. WiFi offers a simple way to provide network connections in hundreds of campus locations that could not be reached cost-effectively with wired Ethernet: classrooms, libraries, administrative offices, and even outdoor areas and athletic facilities.

Today, nearly every college and university has a rapidly growing WiFi network on campus. As student laptop usage expands, it is common for university IT departments to be responsible for wireless LANs with more than 1,000 nodes and several thousand simultaneous users.

*These IT departments function very differently and have vastly different resources and priorities than their peers managing comparable wireless networks in Fortune 500 corporations.* To control costs and meet network performance requirements, the university IT staff needs specialized software solutions designed to address their specific needs. In general, proprietary solutions offered by WiFi hardware vendors fall short of the need.

To develop a wireless management system for universities, AirWave Wireless worked closely with leading organizations like Indiana University, the University of Wisconsin, Vanderbilt University and many others. The AirWave Wireless Management Suite software allows IT to successfully operate and support wireless LANs on campus by addressing:

- **Ease of use for a diverse IT staff:** Colleges and university IT departments employ a diverse staff, ranging from student interns and graduate students to highly skilled network engineers. All these individuals need

## EXECUTIVE SUMMARY

Managing WiFi networks in the complex operating environment of a typical college or university generates challenges that are quite different than other wireless networks. The university network is larger and more diverse, operating environments are more varied, and resources are more constrained. For a university IT department, the only way to support a wireless LAN cost effectively is with a robust management solution.

The AirWave Wireless Management Suite gives IT the level of control it needs:

- **Manageability** -- Configure and control WiFi infrastructure, regardless of manufacturer or architecture.
- **Security** – Detect devices and enforce security policies across all WiFi devices.
- **Visibility** – View real-time information on every user and device, as well as historical trend reports for planning and analysis.
- **Flexibility** – Fit the WiFi management solution to the existing network infrastructure

With the AirWave Wireless Management Suite, universities can effectively control wireless LANs with thousands of users and a diverse network infrastructure.

information from the wireless management solution to perform their jobs.

- **Long hardware lifecycles:** Universities typically need and expect their network infrastructure to last longer than a Fortune 500 corporation with billion-dollar IT budgets.



- **Complex multi-vendor and multi-architecture networks:** University networks often grow over a period of years, in multiple phases across different schools and departments. The result is typically a highly heterogeneous network infrastructure with multiple generations of products from multiple vendors.
- **Diverse security policies driven by the diversity of end-user devices:** College students and faculty often select and purchase their own computers and other WiFi-enabled devices, forcing IT to implement complex, multi-layered security policies reflecting this diversity.
- **“Rogue” access points that interfere with WLAN performance:** Students often install their own WiFi access points on the university network, interfering with the authorized WiFi network and making end user problems hard to diagnose.
- **Trend reporting for efficient planning of growth:** Operating with more constrained budgets and resources than their corporate colleagues, the university IT staff must monitor budgets and network usage more carefully to avoid unnecessary spending as their WLANs grow.

The AirWave Wireless Management Suite™ is specifically designed to meet these needs and provide the university IT staff the ability to control their WiFi networks effectively.

## Ease of Use for a Diverse IT Staff

**Challenge:** University IT departments employ a wide range of people, from highly skilled network engineers to part-time student employees who may staff the Help Desk to handle first-level user problems. Yet, these diverse employees all need information from the wireless management solution to do their jobs: the Help Desk needs real-time user monitoring information to diagnose user issues while network engineers need to be able to monitor and configure the entire network remotely.

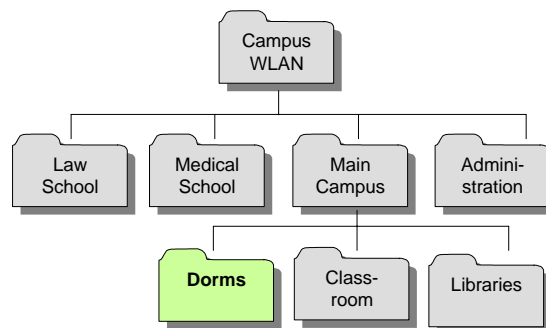
This diversity imposes a significant challenge for any management solution. First, it must be sufficiently easy to use and understand for part-time Help Desk employees while provided all the higher-level functions required by the engineers. Second, the system must provide multiple levels of administrative access, to prevent student or other workers from gaining access to areas that would allow them to change security policies, passwords, etc.

Proprietary, vendor-provided configuration tools may be designed only with the network engineer in mind, providing 'one-size-fits-all' administrative access and requiring days of training to master the complexity of the tool.

**Solution:** The AirWave Management Platform (AMP) is designed for the entire IT staff. With AMP's easy-to-use web-based interface, the Help Desk can quickly locate the remote user quickly (preferably by username), determine where he is, view real-time performance and usage data, and access historical information for diagnostic purposes.

Using AirWave's VisualRF module, the Help Desk can see where each user is located and can assess the RF environment for likely sources of interference. With this data, they can diagnose problems quickly, determining whether the issue is client-based or network-related. When a network problem is detected, they can quickly and efficiently escalate the issue to the networking group. Network Engineers can use AMP to manage device configurations and policies across Wi-Fi networks with thousands of wireless APs.

As important as what AMP allows university IT staff members to do is what it prevents them from doing if they don't have the appropriate permissions. AMP uses a password-protected role- and responsibility-based management model that allows administrators to define exactly what any user can see or do.



AMP users may be granted (a) read-only (“monitoring”) access that allows them to view WLAN performance and user data but not to change the configuration of any devices or (b) read-write (“management”) access that permits them to make configuration changes. Users may also be restricted to viewing information or managing devices on certain segments of the wireless network. A part-time student worker may be granted monitoring access to data from the wireless LAN in



the dorms but be prevented from seeing data from the rest of the network. Similarly, a network engineer in the medical center may be given read-write privileges for the medical school network, but monitoring-only privileges on the rest of the network.

## Long Hardware Lifecycles

**Challenge:** Hardware vendors used to serving the corporate market may assume that WiFi hardware will be replaced every two years. As a result, older products may be 'end-of-lifed' as new products and architectures are introduced -- and vendor-provided management solutions may not continue to support the older platforms. In higher education, however, tight capital budgets may require that WiFi hardware remain in place for four or five years, or more.

**Solution:** The AirWave Management Platform™ software provides ongoing support for legacy hardware, enabling the university IT department to extend the useful life of its existing infrastructure investment. The AMP software, for example, supports the complete Cisco Aironet product line (dating back even to early Aironet hardware that predates Cisco's acquisition of Aironet) as well as newer Cisco Airespace products.

## Complex Multi-vendor and Multi-architecture Wireless Networks

**Challenge:** Wireless networks in higher education are quite often complex and heterogeneous, with hardware from multiple vendors and product generations. In part, this is due to the longer hardware lifecycles in the education market: vendor product lines evolve significantly over time, creating diversity when older products are retained. Many universities today have a combination of intelligent 'stand-alone' wireless access points as well as newer "thin APs" and wireless switches.

However, many other factors also contribute to this trend toward diversity in the higher education market including:

- **Decentralized or 'federal' IT structures:** Especially in large universities, different schools (i.e., business school, medical center, law school) may have their own somewhat autonomous IT departments that make their own purchasing decisions. These departments may choose different products or architectures to meet their own specific needs.

- **Multi-phase deployments:** Network rollouts in higher education tend to occur in multiple phases, with significant installations often done during the summer when activity is lighter. Thus, organizations may add several hundred APs in a short period of time (Phase I) in one area of campus, followed by another major installation (Phase II) one or two years later. In the time between these phases, vendor product lines evolve and new competitors appear, making it common for different products to be used in each phase.
- **Competitive bid requirements:** Especially in public universities, the IT department may be required to solicit competitive bids from multiple vendors whenever they embark on a major WLAN deployment. In a competitive and rapidly changing market, this often means that several different vendors' product are used on the network.

**WLAN Fact:** 70% of customers in higher education plan to evaluate new WLAN vendors within 18-24 months.

(Source: AirWave Customer Survey)

Managing a diverse network infrastructure with multiple proprietary solutions is an unappealing and costly prospect. All members of the IT staff involved in supporting the WLAN would need to be trained to use multiple solutions. End user support calls would take longer to resolve as the Help Desk assimilated information from multiple systems. Performance and usage reports would have to be created by hand, with data pulled from multiple different systems.

**Solution:** The AirWave Wireless Management Suite is a vendor- and architecture-agnostic software solution that allows the IT staff to discover, monitor, configure and control multiple vendors' WiFi networking infrastructure from one integrated web console. Whether the university uses a combination of Cisco Aironet and Airespace devices or a mixture of Proxim and ProCurve, the AirWave software manages it all. The AirWave software can even monitor certain outdoor and point-to-point wireless solutions from companies like Proxim, Vivato and Bel Air.



## Diverse Security Policies

**Challenge:** Unlike most large corporations, the university IT department often has little control over the types of end-user devices that connect to its wireless network. Students and faculty frequently purchase and configure their own computers and other devices (running Windows, Mac OS, Linux, etc.). Many universities maintain an open guest policy that permits campus guests to use basic network resources or to connect to the Internet from campus.

This diversity poses makes it difficult for IT to maintain uniform security policies, and makes it especially challenging to implement WPA, WPA2 or other solutions that require some control over (or access to) the client device. Some of these devices may not yet have support for WPA or other advanced WLAN security. As a result, many universities implement mixed security policies, with different solutions used for different classes of devices or segments of the network. Some schools use WLAN gateways (and HTML redirect) for unsecured guest access to the internet, with VPN or WPA required for access to campus network resources.

**Solution:** The AirWave Wireless Management Suite supports the vast majority WLAN security policies in place at colleges and universities. Many schools address their need to maintain multiple simultaneous security policies by implementing multiple VLANs on their wireless network, with different policies and access levels assigned to each. The AirWave software allows IT to configure these VLANs centrally and push the policy out to hundreds or thousands of access points from all vendors, greatly reducing the management burden.

The AirWave software also integrates directly with the authentication servers most commonly used in higher education, including FreeRADIUS and Bluesocket. Unlike proprietary solutions, this allows AirWave to monitor and track users on the network by username (with data obtained via RADIUS accounting records).

## Rogue Access Points

**Challenge:** In the corporate world, employees who connect unauthorized 'rogue' access points to the enterprise networks are subject to a range of disciplinary actions, including termination of employment. Many corporations spend hundreds of thousands of dollars on wireless intrusion

## Representative Customers in Higher Ed

- Arkansas Tech University
- Augusta Technical College
- Ball State University
- Berklee College of Music
- Brookdale Community College
- California State University Northridge
- Centenary College
- Central Connecticut State University
- Florida State University
- Grand Valley State University
- Humboldt State University
- Illinois State University
- Indiana University
- Københavns Universitet
- Ludwig-Maximilian-Universität München
- Madison Area Technical College
- Northern Illinois University
- Oakland University
- Pepperdine University
- Southern New England School of Law
- Southwestern Adventist University
- Texas State Technical College
- The Macaulay Institute
- Thomas M Cooley Law School
- Tulane University
- Union University
- Universidad de Valladolid
- Universität Karlsruhe
- University of Dayton
- University of Denver
- University of Hawaii
- University of Minnesota Duluth
- University of North Carolina at Chapel Hill
- University of North Texas
- University of San Francisco
- University of Wisconsin-Madison
- UPNV - Universidad Publica de Navarra
- Utah State University
- Warwick University



detection systems designed specifically to detect and locate rogue devices.

In the university setting, rogue APs cause many headaches for IT. If a student connects her own AP in a dorm (or operates her WiFi-enabled computer in ad hoc mode), other students may inadvertently connect to that open network, generating a range of privacy and security problems, and also making it difficult for IT to diagnose the problem when that student calls to report WLAN problems. Unauthorized APs can also overlap and interfere with the campus wireless LAN, causing performance problems for other users. Some inexpensive home-grade access points may even be configured by default to serve DHCP addresses automatically, wreaking havoc on the performance of the wired as well as the wireless network.

Policies regarding rogues in the university setting are not as clearcut and uniform as in the corporate world. Some schools permit students and faculty to connect APs to the campus LAN while others ban them outright. Yet, even where unauthorized APs are banned, schools have difficulty enforcing the policy—almost no educational institution has the budget for specialized wall-to-wall wireless IDS to enforce the policy.

**Solution:** AirWave's RAPIDS™ module uses both RF and wired network-scanning techniques to discover any unknown wireless access points connected to the campus network. RAPIDS' wireline network scans are a reliable way to check for rogue devices even in campus locations that are not yet covered via WiFi. AirWave greatly reduces the cost of rogue detection by conducting wireless scans using the school's existing APs rather than proprietary, dedicated sensors.

If a school's policy is to ban rogue APs, IT can use RAPIDS to detect the rogue and can shut down the appropriate network port using the information provided in the alert. If rogues are not prohibited outright, AMP enables IT to minimize the impact of the rogue device on the campus network by altering RF channel and transmission power settings. The AirWave software helps IT track and triangulate the location of the rogue devices, putting this information at the fingertips of the Help Desk staff responsible for diagnosing any rogue-related user problems.

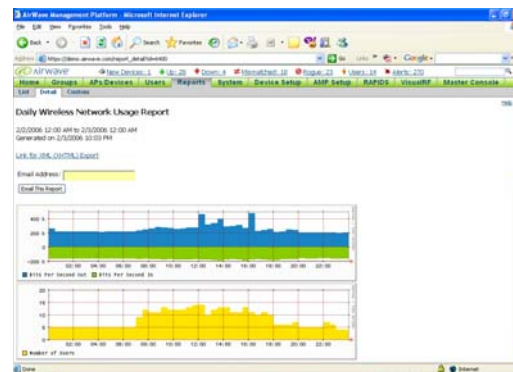
## Trend Reporting for Efficient Planning

**Challenge:** Universities operating within limited capital budgets typically cannot afford to 'overbuild' their wireless LANs to provide excess coverage and capacity in all locations. Instead, IT needs to monitor WLAN usage closely and carefully assess where they may need to increase capacity.

Tracking and predicting network usage patterns requires detailed historical trend reports dating back not just weeks but months or years. IT needs to understand not just average usage patterns but how those patterns vary:

- What are the most utilized nodes on the network?
- How often is capacity an issue in those locations?
- How do usage patterns vary in different locations by time of day? Is there high usage in the libraries during daylight and evening hours but low usage late at night? Is there low usage in the dormitories during daylight hours but high usage late at night?
- How do usage patterns change during exam periods?

**Solution:** The AirWave Management Platform provides both the real-time and historical information that the IT staff needs to answer these questions and plan their network growth accordingly.



AMP retains historical user and performance data for a year or more, enabling the IT staff to run detailed trending reports for specific locations or globally across the entire network. AMP's UI uses a flexible folder design that allows IT to



## Managing WiFi Networks in Higher Education

efficiently gather and study more granular trend and performance data from a specified subset of the APs on the network.

### **Conclusion**

College and university IT departments have unique needs for managing their wireless networks. These needs typically cannot be met with limited, proprietary management tools provided by the hardware vendors themselves. Instead, specialized management solutions like the AirWave Wireless Management Suite are needed to give IT the control and visibility it needs to manage such large and diverse networks cost-effectively.

### **AirWave Wireless, Inc.**

1700 South El Camino Real  
Suite 500  
San Mateo, CA 94041

+1.650.286.6100

+1.650.286.6101 (fax)

[info@airwave.com](mailto:info@airwave.com)

[www.airwave.com](http://www.airwave.com)