Education

The Whys and Hows of Deploying Large-Scale Campus-wide Wi-Fi Networks

Brad Noblet | BN Consulting

ARUBA®

n e t w o r k s

Introduction

Ubiquitous Wi-Fi across an enterprise or campus is a very positive and exciting experience for your students, faculty, staff and visitors to your institution. Having instant access to email, the internet, and other IT services irrespective of location can dramatically change the way your constituents live, work, study, learn, and play. If wireless coverage is also converged with voice and video, the experience is even further enhanced. And today, everyone who comes to your institution has experienced wireless access to the internet somewhere—at home or work, or in coffee houses, libraries, airports, or hotels. As a result, it is no wonder that when people come to your campus they not only want but most often expect wireless access to all the information and services your institution provides.

In fact, data from the 2006 Campus Computing Project revealed that 60.5% of colleges and universities increased their campus IT budges for wireless. "The expansion of wireless networks on campus mirrors the explosive growth of wireless in the consumer and corporate sectors over the past three years," confirms Kenneth C. Green, founding director of the Project. "Consequently, it should be no surprise that students and faculty come to campus expecting their college or university to provide the same wireless connectivity that they experience elsewhere," Green added.

The Challenges: Why Many Institutions Lag in Wi-Fi Deployment

Deploying a large-scale, campus-wide Wi-Fi system presents many challenges that delay ubiquitous adoption in higher education. These challenges are coverage, capacity, density, and security.

Coverage Challenges

University and college campuses typically encompass a wide geography; possibly a few square miles sporting tens if not hundreds of buildings to be covered plus acres of outdoor areas where coverage would be desirable. Given the limited Wi-Fi Access Point (AP) coverage radius of 100' to 200', many numbers of APs are required to extend coverage ubiquitously, which, depending on the vendor you chose, can be costly. Also, each AP must be connected to the network backbone to provide complete coverage. In some cases, it can be physically difficult to extend that backbone into an area or location where coverage is desired.

Capacity Limitations

Coverage alone is not the key to a successful campus-wide deployment. Sufficient capacity and roaming support are required for IT applications as well as converged communications. Since most institutions have experienced the limitations of the legacy Wi-Fi they deployed a few years ago as wireless hotspots in libraries and student centers for example, it is not hard for them to imagine the significant difficulty of scaling the capacity of legacy wireless. Single radio APs supporting only 802.1b/g are often not upgradeable, limiting the number of available channels for coverage. This factor certainly limits the available capacity while increasing the possibility of interference between APs—a result that even further reduces the available capacity. Each legacy AP operates independently of others in its coverage area making it unaware of neighboring APs, their frequency of operation or their power level—for an even greater probability that the APs will interfere with one another. Roaming support between legacy APs is

spotty at best, and seamless hand-offs to other subnets is non-existent. These factors add to the complexity and expense of additional equipment to try and resolve these issues.

Installing legacy APs (or 'fat' APs, called this because each AP needs to be programmed and managed in a distributed fashion) creates another set of challenges. Without a central point of intelligence, it's very difficult to ensure that coverage does not significantly overlap neighboring APs. On the other hand, one cannot readily ensure that areas have been fully covered. As a result, many highly skilled man-hours and sophisticated testing equipment are required to install each AP and ensure proper operation across its coverage radius. The sheer number of APs required for ubiquitous coverage can be hundreds to thousands, making installation and maintenance prohibitively expense. In addition, your campus environments are not static. People and objects constantly move around, creating obstacles and reflection points for Wi-Fi radio signals. True mobility changes planned coverage patterns which can create poor quality of service (QoS). Wi-Fi also operates on publicly shared radio frequencies. This means there are many opportunities for interference from non-Wi-Fi sources as well as from others who may place their own Wi-Fi APs in close physical proximity to your equipment. This is especially problematic for universities and colleges located in densely populated areas and major cities. Legacy APs have no capacity to identify these sources of interference so institutions trying to scale to a campus-wide wireless deployment are faced with costly on-site skilled man hours to track down, identify and eliminate interference problems.

Density Requirements

Campus environments are often required to support highly dense populations in a given location. A lecture hall or auditorium for example, can hold populations of 100, 500, or more individuals with devices that need network connectivity simultaneously. This is becoming more common as instructors increase their use of multimedia in classrooms and rely on the network for internet access, testing and evaluation, and other applications that require streaming of data, voice or video. The requirement to provide high-density wireless is certainly orthogonal to the capability of legacy APs to service such environments. In addition, address space management and routing can be complex without the participation of some sort of regional intelligence.

Security Concerns

As if all these factors aren't enough to make wireless deployment problematic, the overarching fear for campus-wide Wi-Fi deployment is security. More and more data propagated over the network carries some sort of sensitive or personal information that must be protected. Groups and services must also be isolated from one another to ensure quality of service as well as properly authorized access to resources. The Wi-Fi airwaves are public making them an easy target for snooping. Legacy APs support weak or no encryption making that information readily accessible to moderately smart "hackers". An even bigger challenge comes with supporting centralized network authentication. Most legacy APs rely on external, proprietary systems to implement some form of centralized wireless network access control. While adding additional complexity and expense, they create major integration challenges with existing, centralized IT authentication systems. That means supporting multiple databases for authentication bring

with it the complexity and inaccuracies of database synchronization not to mention the number of additional man-hours required to operate and service these points of integration.

To scale Wi-Fi across the campus, many APs are required; both for coverage as well as capacity. With hundreds to thousands of APs required and cost points well above $500 per legacy AP (not to mention the massive number of man-hours required for proper installation as discussed above), the cost to deploy ubiquitous wireless can be daunting. Operating and maintaining such an environment is not much better. With no central point of automated intelligence, operating and maintaining legacy APs requires much manual intervention and on-site support that can drive up staffing requirements significantly.

The Solution: Wireless Switching, 'Thin' APs and Centralized Control

Many of the challenges in deploying large-scale, campus-wide wireless as discussed above, stem from the fact that there is no central or more specifically, regional coordination and control of AP frequency and power levels within a give location. Without this regional intelligence, APs will increase their probability of interfering with one another dramatically reducing desired coverage and capacity. At best, coverage within that geography will certainly not be optimized and most likely will be ill-defined. As stated above, this situation will only worsen as people and objects move through an area, changing the coverage patterns and characteristics.

To solve these problems, Aruba Networks pioneered a technology known as wireless switching. By connecting APs within a region to a central intelligence or wireless switch, their coverage patterns can be optimized by comparing them through the switch with one another. Interference and capacity can now be enhanced because the switch can determine and select the best frequency and power level for each APs operation in proximity to other APs within that area. The result is the availability of maximum wireless capacity with just the right amount of overlap to minimize inter-AP interference while enabling effective client roaming between APs.

Solve the Capacity and Coverage Challenge: Simplify Deployment

With most of the intelligence centralized, Aruba APs become very 'thin', functioning primarily as a radio and spreading the cost of intelligence across many APs instead of duplicating it on each AP. This means a much more cost effective AP component and makes the deployment of hundreds to thousands of APs highly affordable. It also provides more opportunity to integrate full radio support for all existing and emerging standards (including 802.11b/g/a/n) into a single unit. To make deployment easier, Aruba APs support standard tunneling protocols to allow their connection to the existing wired infrastructure. This enables switches to be centralized in a protected, serviceable environment such as an IT machine room. In addition, switch capacity is maximized by virtualizing switch ports across all APs instead of just those in close, physical proximity to the switch.

Deploying wireless still means some wiring must be installed with which to connect APs to the network backbone. Emerging technologies such as mesh (which Aruba has announced and will start shipping in July) will eliminate some of this wiring. Because mesh operates by using some of the airwave capacity, a

full mesh topology is not required or recommended. Many APs will use existing wired switch ports for connectivity leaving only areas that are not within reach of a wired port to take advantage of the mesh technology. For those instances and locations, Aruba has enabled a single-hop mesh technology that allows APs in close proximity of one another to share a wired connection. This approach leverages the advantage of mesh without creating a significant impact on airwave capacity. As installation of low volume wire can be anywhere from $500 to $1000 per drop, this can also save a significant amount of money and time for your total wireless deployment.

Aruba also offers a line of wireless bridges to link remote regions of your campus to the main network when deployment of network backbone access to those locations is prohibited by cost or physical access.

Provide Outdoor Coverage

If you are deploying Wi-Fi access outdoors, it is often possible to cover many areas from inside buildings and other structures. Placing an AP in a window allows desired outdoor coverage while eliminating the expense of outdoor mounting and protective enclosures. Placing the AP indoors by a window also makes it much more accessible for service when required. Experience has shown that many buildings enclose or adjoin outdoor areas of interest making this a viable option. Be sure to verify the type of window glass through which your signals will travel. Older buildings may have glass that contains lead which can affect signal propagation.

When covering outdoor spaces, pay attention to AP height. Many think that locating an AP outside on a high point such as a rooftop or tower will provide increased range or more reliable outdoor coverage. But most people (and their laptops) are only four to six feet off the ground. A tower or roof mounted outdoor AP that is too high will radiate its signals in a pattern that will force the majority of the energy to move above the user's head. Always try to match the AP height with its intended users.

Resolve Third Party Interference

The 802.11 standards upon which Wi-Fi is based encompass license-free radio frequency (RF) spectrum. This means that any interference occurring within that spectrum must be tolerated. In other words, you can't control interference from other devices legally sharing your radio spectrum. Using switch intelligence to select appropriate frequencies and power levels, you can ensure that interference from undesired sources is minimized. Directional antennas may also be deployed to reduce interference. This not only increases the strength of the desired signal but also rejects signals to the side and in back of the antenna. When the number of undesired signals received by the AP is reduced there are fewer signals present to interfere with the desired signal. This too has the effect of dramatically increasing the strength of the desired signal making communications highly immune to interference. The switch also has the capability to identify rogue APs and other noise sources which helps with the identification and elimination of those signals.

Solve the Density Dilemma

As mentioned above, wireless switching enables effective deployment of required AP capacity for supporting large populations in a single location. Through central control of frequency and power, large

numbers of APs can be placed in a given geography increasing its capacity to the desired level. It should be noted that in especially high-density areas, wireless address space management will be heavily stressed. Due to the transient, mobile nature of wireless users, wireless network addresses can be quickly consumed. You can avoid problems by ensuring that you have extra address capacity in each wireless subnet coupled with short lease times for those addresses—around 15 minutes.

Unify Security

As mentioned above, wireless switching enables effective deployment of required AP capacity for supporting Deploying an Aruba wireless switching architecture can simplify integration with existing authentication systems providing one unified model for network authentication and authorization. Through support of the 802.1x protocol coupled with a captive portal interface, Aruba switches work in concert with existing, centralized authentication systems to deliver a common methodology for authentication and authorization. Gone are the days of having to maintain and synchronize multiple databases. In addition, Aruba provides a mechanism for mapping SSIDs and their associated traffic to individual VLANs further separating groups and services from unauthorized access or unwanted interaction. The ability to authenticate by individual user also has the effect of strengthening resistance to denial-of-service attacks for any given service. Of course, following the standard, Aruba has enabled the latest protections for data through its support of all Wi-Fi encryption standards including WPA2. Aruba takes securing communications one-step further by also providing VPN termination within the switch.

Summary

Aruba wireless switching has certainly simplified large-scale Wi-Fi deployment making it possible for higher education institutions to economically deploy and manage secure, dependable, campus-wide wireless access.

Large geographies are easily covered, maintaining interference free access while delivering the desired capacity—even for converged services. Security policy has been unified with existing central services enabling a common user experience while insuring effective information security and integrity.

Experience has shown that wireless switching is the only Wi-Fi technology capable of scaling to the enterprise campus.

About S. Bradley Noblet

Brad Noblet is a veteran Information Technology executive of thirty years. His breadth of experience extends from managing the development, delivery and support of IT products to forming and leading major IT companies. Over the last six years he has successfully leveraged his industry management experience toward delivering high quality, visionary IT environments for Higher Education. During that time, Brad served as Dartmouth College's Director of Technical Services then becoming its CIO. At Dartmouth he was responsible for creating the College's and the industry's first enterprise class converged (voice, video and data) network in addition to advancing and managing its central IT operations. His vision for IT, reflected in the infrastructure, applications and services he deployed while at Dartmouth brought much recognition to the College from industry, Higher Education and the national press touting Dartmouth as a leader in IT.

A 1982 graduate of Indiana University at Bloomington in Computer Science, Brad was that school's Manager of Data Communications, with responsibility for the institution's statewide data network. He then left for private industry, working in product development and management for a number of hardware manufacturers including Codex Corp., Ungermann-Bass, Tandem Computers and the Wellfleet Communications division of Bay Networks.

At Ungermann-Bass, Brad served as Director of Engineering then General Manager of several business units. He is credited with the creation and development of Ungermann Bass' flagship product, Access/One, the world's first smart hub. He joined the Wellfleet Division of Bay Networks in 1995 as General Manager of that business unit delivering over $600 million in annual revenue. He is credited with creating forty new products during his tenure at Wellfleet that resulted in growing its revenue by $200M in less than two years.

Since leaving Bay Networks in 1998 and before joining Dartmouth in 2001, Brad was involved in a number of start-up ventures focused on the converged voice, data and wireless sectors. He is regularly quoted in industry journals and the national press, being touted as an expert in networking and provides consultation for several Fortune 500 companies and Higher Education institutions.

About Aruba Networks, Inc.

Aruba securely delivers the enterprise network to users, wherever they work or roam, with user-centric networks that significantly expand the reach of traditional port-centric networks. User-centric networks integrate adaptive WLANs, identity-based security, and application continuity services into a cohesive, high-performance system that can be easily deployed as an overlay on top of existing network infrastructure. Adaptive WLANs deliver high-performance, follow-me connectivity so users are always within reach of cmission-critical information. Identity-based security associates access policies with users, not ports, to enable follow-me security that is enforced regardless of access method or location. Application continuity services enable follow-me applications that can be seamlessly accessed across WLAN and cellular networks. The cost, convenience, and security benefits of user-centric networks are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, visit Aruba at http://www.arubanetworks.com.

ARUBA
n e t w o r k s

1322 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. +1.408.227.4500 | Fax. +1.408.227.4550 | info@arubanetworks.com
http://www.arubanetworks.com