

From “Zero” to 802.11n in Six Months

Presented by Jason LaMar, Ohio Wesleyan University

**Ohio Higher Education Computing Council Conference
Wright State University | March 26, 2009**

× Ohio Wesleyan University

- + Private, traditional 4-year liberal arts college in Delaware (20 miles north of Columbus) founded in 1842**
- + Roughly 200-acre campus with 50+ buildings**
- + About 1,950 FTE students (undergraduate only) and 650 faculty and staff**
- + Merged Libraries & Information Services (LIS) division since summer of 2004**

× Previous Limited Wireless Solution

- + Starting in 2004, about 15 Cisco Aironet 12XX “fat” APs across four buildings (no residences)
- + Bluesocket Wireless Gateway for AAA via username/password captive Web portal
- + 128-bit WEP security with shared key
- + Manual “touch” setup of every individual laptop for students, faculty, & staff » either USB flash drive load or keyed data entry
- + No regular guest wireless access (too difficult)

× **New Campus-Wide Wireless Solution**

- + Fall 2007 mandate » Ubiquitous, high-speed, secure wireless network ASAP
- + Winter 2007/2008 RFP » Outside consultant to assist with vendor demos & selection
- + Early spring 2008 finalists » Cisco and Aruba (noting that OWU is a Cisco wired shop)
- + Late spring 2008 selection » Aruba wins (based on 802.11n offering with small AP footprint using standard PoE)

× **New Campus-Wide Wireless Solution**

- + Two Aruba 6000 chassis (one in each of two different data centers for redundancy) with one M3 controller module each
- + Roughly 450 AP-124 (ext.) and AP-125 (int.) access points » 50/50 dispersion between controllers with full solo failover capabilities
- + Depending on cost breakdown, either Cisco PoE switches or PowerDsine midspan PoE injector bricks or hubs

× **How OWU Implemented “n” Wireless**

- + May 2008 » Contracted campus-wide site surveys; began determination of security and authentication scheme
- + June/July 2008 » AP cabling and mounting in all residence facilities; installed fiberglass enclosures to protect APs from student abuse
- + July/August 2008 » AP cabling and mounting in all academic/administrative facilities
- + Late August 2008 » Launch ... but no “n”?

× **Dilemma #1: Using 802.1X NAC**

- + 802.1X is a network access control (NAC) method that authenticates users against RADIUS, which in turn talks to AD or LDAP
- + Scenario A » EAP-TTLS + PAP + RADIUS (Extensible Auth. Protocol Tunneled Transport Layer Security + Password Auth. Protocol)
- + Industry standard, high-level security, BUT ...
- + Unsupported natively on Windows (XP or Vista) » requires third-party app, SecureW2

× **Dilemma #1: Using 802.1X NAC**

- + Scenario B » PEAP + MS-CHAPv2 + RADIUS (Protected Exten. Auth. Protocol + Microsoft Challenge Handshake Auth. Protocol)
- + Supported natively on all clients (Windows)
- + Required almost all users to reset their LDAP passwords once
- + More work for IT, less work for end users
- + Scenario B adopted

× **Dilemma #1: Using 802.1X NAC**

- + Even though something like EAP-TTLS + PAP is best, it requires a small standalone app on Microsoft Windows (SecureW2) to work
- + Using something like PEAP + MS-CHAPv2 may cause other admin complications, but it is natively supported on all wireless supplicants (even Windows)
- + Decision depends on “IT pain” focus

× **Dilemma #2: Securing 802.11a/b/g/n**

- + Two basic encryption methods:
TKIP/WPA (old) and AES/WPA2 (new)
- + Tech. progression was WEP » WPA » WPA2
- + 802.11a/b/g typically was TKIP/WPA
- + 802.11n is designed for AES/WPA2
- + To achieve high-throughput mode (300Mbps),
802.11n can only use AES (not TKIP)
- + Some legacy wireless devices can't use AES

- ✘ **Dilemma #2: Securing 802.11a/b/g/n**
 - + Scenario A » Use one wireless network SSID (service set identifier) that forces AES for all, making older, incompatible clients unusable
 - + Scenario B » Use multiple SSIDs (one for 802.11a/b/g with TKIP, and one for 802.11n with AES), maybe causing user confusion
 - + Scenario C » Use one SSID with TKIP only, and forget about 802.11n for now
 - + Scenario C adopted in August 2008

× **Dilemma #2: Securing 802.11a/b/g/n**

- + Scenario D » Aruba offered “weak encryption” mode for 802.11n over TKIP in late 2008
- + January 2009 » High-throughput “n” capabilities deployed in addition to a/b/g while still using single SSID with WPA only
- + Obviously, WPA2 would be better (and will be inevitable), but Aruba’s weak-encryption flavor of 802.11n offers best of both worlds for now

✘ **Epilogue (Other Things We Learned)**

- + October 2008 » Second SSID implemented for unencrypted guest access (think coffeehouse connection) with captive Web login portal for Homecoming alumni
- + Cloudpath XpressConnect would have been lifesaver, if we had known about it sooner (automated cross-platform “network access wizard”) » <http://www.cloudpath.net/>

Thank You

<http://jason.owu.edu/ohecc09.pdf>

Presented by Jason LaMar

Director of Information Services, Ohio Wesleyan Univ.

jrlamar@owu.edu | 740-368-3131