

Wireless Committee meeting
650 Kommas, Board Room
January 17, 2007

Attending: Bryan Morris, Tim Urban, David Thurm, Rob Wineriter, Dave Packham, Nelson Beebe, Steve Adams, Hang Wong, Greg (HSC), Brad, Pieter Bowman, Mindy Tueller, Jon Ross, Dave Maughan, Bo Mendenhall, Andrew Goble (late: Earl Lewis and Dave Huth). By phone: Joe Breen, Isaac, Derrick Albright

I. uconnect SSIDs – Andrew Goble

Hotspot can be set up now – anywhere except HSC IP space – to any building with a demark switch. Secure ssid can safely be shut off now. Don't hesitate. Insecure – more are still running it. Some waiting for the semester to get farther underway before they have time to move to hotspot. Bryan wants to know if he needs to support it. HSC-ITS has turned it on in a few spots. John Stratton may keep it on. Per Rob W – a few groups have said they'd like to keep it on. Don't plan to support it campus-wide; just for exceptions (like groups who need to get to campus resources for longer period of time). Difference between uconnect and insecure is encryption (insecure is encrypted only for login). The client install does seem to cause problems for some guests.

NetOps sees more people using insecure than uconnect; HSEB is not broadcasting insecure and people are unsure about hotspot so they are using the uconnect network in HSEB. Uconnect installer has had a few problems according to Isaac; people are unhappy about the bandwidth limitations on hotspot so they go to uconnect – good - this is how it's supposed to work.

Committee recommendation on insecure: we'd prefer departments to turn it off and use uconnect, but bring their requests to continue to use it to this group. Bottom line: the insecure.utah.edu network is supported but not encouraged. Jon Ross: should we contact the areas that are using insecure and educate them if they aren't aware of the deal? Rob W has spoken with most of them and most want to go to hotspot. The NOC does have info on who is using insecure; all new deployments are uconnect or hotspot only. CHPC will be getting rid of insecure altogether shortly; hotspot is running and meeting their needs. We'll deal with questions as they arise. *should put the uconnect SLA on the Wireless Committee website.

II. Campus Wireless / Task Force Funding – Mindy Tueller

It's the annual SCAC process time again. In order to send out those forms, the wireless funding options needed to be clarified. There are three ways to do departmental wireless: request central funds through OIT at anytime and have OIT install and maintain them (the best and most encouraged option); request money through SCAC during the annual window (right now) to maintain them yourself; or buy them yourself. The first two options would be a part of the overall campus wireless initiative. Requests for SCAC money to do departmental wireless also come out of the central fund which comes from several central sources; these must meet specific guidelines including the Campus Wireless Standards. The overview for this can be found at

http://www.it.utah.edu/leadership/committees/wireless/Campus_Wireless_Initiative_2006.pdf. This document has links to the OIT Request form, the Campus Wireless Standards document, and the SCAC website. All requests to OIT go first to Dave Huth, then to the SCAC committee for an outside review, then to Bryan Morris for prioritization and actual installation.

There is still confusion about wireless money and the SCAC process. Nelson Beebe said the College of Science met yesterday and is unhappy and unclear about the amount of funding and its origin. Need to clear this up for all academic departments involved in the SCAC process. Derrick Albright has some concerns about how his money was handled last year.

Other concerns: Brad: if a department has OIT maintain its APs but needs an SSID for the dept and doesn't want to call the CHD for every minor tweak – what about sharing responsibility? Bryan – knows that local visibility is very important for department LAN managers. OIT wants to do something like Looking Glass or Nagios – give the LAN managers a view of the AP by pulling information from the central switching architecture. OIT will put the SSID anywhere in the building if the department hands them a VLAN; about the local LAN manager resetting the equipment – would need to work on that. That's as painful as it should ever get. Brad wants to do local radius authentication for his users before they would hit the campus mesh. Joe can show Brad how CHPC is doing it; Rob says the UMNH is doing it too. Bryan will work with Brad to get his radius authentication working as he needs it.

III. Draft or Pre-802.11n equipment, etc. – Andrew Goble

Want to hash out a coherent policy on where the campus stands on this kind of equipment. If you go with the OIT maintained equipment you are “future proofed” – per Bryan. Andrew: we need a ratified standard to come out in order to roll out an “n”-compatible infrastructure. Need to have a backwards-compatible infrastructure for a while, though. We will still need to support b. Pre-n gear can run in a compatibility mode with an a, b or g client. N is a dual band technology (in Andrew's understanding). Do we need to have some research assignments on n? Rogue n APs in non-compatibility mode present a serious challenge – they'll stomp all over the other equipment and it's hard to detect them. Andrew is worried about what happens when users start using n equipment – Rob W says it's already happening. N standard is supposed to surpass 100 MB – need to keep that in mind for wired ports. May need to have gig ports.

Committee recommendation: n is not supported until there is a standard. If you buy n equipment and it interferes with the campus initiative, you'll have to turn it off.

IV. Finally: common time to meet monthly? 4th Wednesday of each month will be when we try to meet.

Next – Earl Lewis and Dave Huth are overseeing a meeting on hotspot. They will be using a project management process used regularly by OIT to formalize it and get it on track.