Wireless Network Narrative

Background

Wireless networking is garnering a lot of press because everyone from Starbucks to McDonalds is implementing wireless networks. Grassroots directories of "free" wireless networks are springing up on the Internet as well as "sniffer" software to detect operating networks. Hotels are positioned to field wireless in great numbers of the next five years – primarily for business travelers.

In our world of education, wireless is also being implemented broadly. In our area, we surveyed four community colleges – Foothill, Diablo Valley, Ohlone, and Los Medanos. All four currently have wireless deployed. Wireless has been implemented for both administrative and instructional uses.

The survey indicates wireless is in its infancy at these institutions. Each institution is planning on expanding wireless access into all areas of campus operations. Two of the schools have Internet cafés where students can connect to use the Internet. Other uses are for presidential conference rooms, connecting portable buildings, and computer labs. The survey is included at the end of this document.

All four schools reported not having a formal policy governing the implementation of wireless networks. Thus, ours will be one of the first of California community colleges.

So, exactly what is wireless networking? It is simply a replacement for the single cable that connects every campus computer to the network. Instead of wiring, a small radio transmitter and receiver replace the wiring allowing communication over limited distances – typically 300 feet or less.

Wireless technology is implemented as two physical items: the client wireless adapter card connected to the user's computer, and a wireless access point connected to the physical network.

For IT, the freedom of untethered operation has been offset by fears of loss of control of operating networks. Wireless networks are typically viewed with suspicion because of the "out-of-site" connection to network this technology provides. The concern is that any random person could connect to the network and use it without permission. The team discussed these concerns at great length and came to some logical conclusions.

First, we do not house any nuclear-class secrets on any of our systems – especially the Instructional ones. We should temper our need for control by the knowledge of the data we are trying to secure. Further, we already have systems

in place to guard sensitive data on the machines wired network. This is needed because we already allow random persons to connect to our instructional networks using wired connections. The team saw little difference in security risk with wireless technology, especially on the Instructional network.

As with all technology, demand is driven by wireless network price points – which are now less than $100. The technology is easy to setup and use. The purpose of our initiative is to implement policies and get in front of this technology before ad hoc implementations drive a patchwork policy.

Our strategy is to implement wireless technologies to provide ubiquitous access to enterprise data, application, and services.

Wireless Standards

As one might expect with relatively new technologies, there are several standards for wireless networks. Fortunately, most are interoperable – that is, generations are backward compatible. The team has tested two of these wireless standards, 802.11a and 802.11b.

The most widely implemented standard, 802.11b, is also the least expensive – around $30 for a wireless access card. The system operates at a frequency of 2.4 GHz, in the same unlicensed spectrum used by microwave ovens to cook pot roast. The range is about 300 feet at a speed of 11 Mbps.

The other standard we tested, 802.11a, is more expensive – $70 or more – and supported by few manufacturers. It operates at a higher frequency spectrum – 5 GHz. The design's strong feature is a speed of 54 Mbps, or five times that of 802.11b. The downside to this implementation is the higher frequency, which has limited range. In our testing, the reception was strictly line-of-site. Any object (door, wall, or co-worker) can block the signal making connection impossible.

Since testing components from these two standards, a third, 802.11g has been proposed and was adopted by the IEEE in early June. Interestingly, manufacturers are already shipping components to this standard. It combines the spectrum and long range of 802.11b with the speed of 802.11a. Further, it is backwards compatible with 802.11b. Today, this is clearly the standard of choice.

CLPCCD Application

The working group recognizes that use of wireless technologies is in its infancy today and that future applications are yet to be known. We do, however, have experience with two deployed systems, one on each campus.

One such service provides general Internet connectivity to patrons of the library, the other implements a mobile computer cart where machines can be transported to different classrooms within a building.

The team developed classes of service after discussing the security and access issues for wireless. The classes recognize the relative sensitivity of data on the network and their usage. The four classes are:

1. OPEN
2. INSTRUCTIONAL
3. ADMIN
4. RESTRICTED

The Open class has the least number of restrictions, but also provides the least access. It is designed to only provide Internet access. Anyone could configure his or her system to operate without intervention by IT. This is the model currently used in the college library. No college-related data is available in this class.

The Instructional class provides access to machines on the college's instructional network where all student computers are connected. Connection to the network requires intervention by IT staff to properly program the wireless client to access the network traffic. This model is currently used in the mobile cart used on the campus. Only college instructional information is available – no student data can be accessed.

The Admin class is designed to carry traffic for our student information system, Banner. It provides the greatest security requiring both setup by IT and data encryption. At present we do not have any Admin class wireless installations.

The final class is Restricted, which is designed for special applications such as HVAC control, which if compromised could cause failure in physical plant. At present we do not have any Restricted class wireless installations.

Recommendations

1. The team recommends submitting the policy for implementation.
2. In addition, we recommend implementing wireless only for instructional networks at present. This is where the greatest need exists and has the least downside risk.
3. While we could choose to control both wireless adapter cards and wireless access points, it is only practical and desirable to control wireless access points. These devices, by definition, do not move, provide access to the hard-wired network, and are therefore are easier to track. We should, however, provide guidance on the selection of wireless adapter cards.

Wireless Survey

		DVC	Foothill	LMC	Ohlone
1	Do you have any formal policies?	N	N	-	N
2	Do you have purchasing guidelines?	Y	N	-	N
3	Have you experienced any bandwidth issues?	N	N	-	N
4	Do you control the brands of equipment?	Y	N	-	N
5	Are the costs more per port than wired?	N/A	N/A	-	N/A
6	Did you add any specific security for wireless?	Y	N	-	N
7	Was there any specific security to protect wired from wireless connections?	Y	N	-	N
8	Has usage feedback been positive?	N/A	N/A	-	N/A
9	Do you use wireless in computer labs?	N	Y	Y	N
10	Do you have an Internet café?	N	Y	Y	N
11	Do you plan on expanding usage into other areas?	Y	Y	Y	Y
12	If expanding, will you need to change your current security configurations?	Y	Y	-	N/A