

Wireless Implementation at Bethune-Cookman College

Prepared by John Hofmann
Director of Technical Services
Coordinator of Wireless Applications
The Center for Information Technology
Bethune-Cookman College

As of December 18, 2002

The first step in our process was deciding that we wanted to overlay our wired network with wireless. We feel that it would be unwise to depend totally on wireless. However, there are some places on campus where only wireless exists because of the difficult logistics at certain locations for installing wired connections.

Our next step was finding a vendor. We have been fortunate because we found a vendor who is virtually unlimited in scope of work. For trustworthy recommendations and installation we only have one phone number to call. Of course, we have also been in communication with others on wireless recommendations. Our experience has been that our vendor's preferences usually are the same as many of those with whom we collaborate.

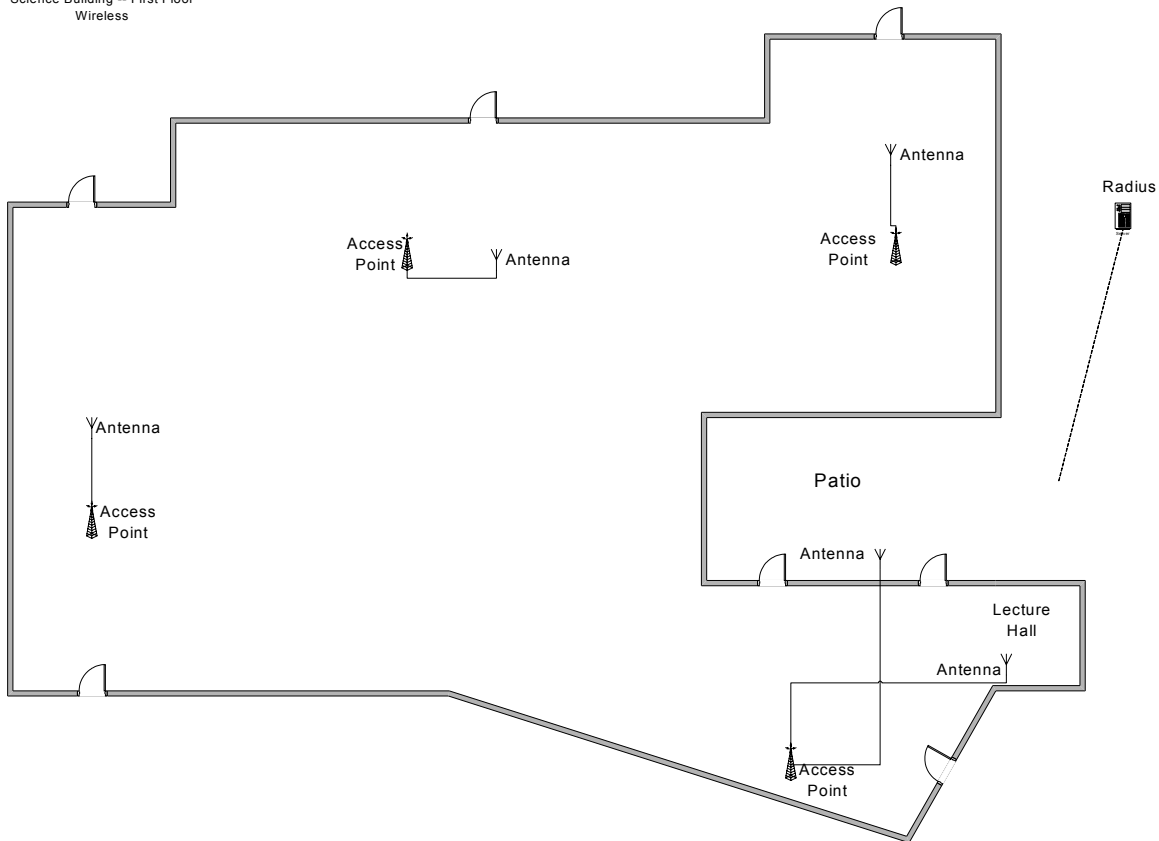
The next consideration was how much wireless coverage to have installed. This decision was driven by cost. While we eventually want to blanket the entire campus, we didn't have the funds available to do that in one big project. So, we determined how much money we had and ordered as much as we could afford.

The relatively easy part of the project was installing access points. First-time users of a wireless connection often are in awe of the technology. Yet setting up for wireless networking is very easy. The hard part is making a wireless network reasonably secure.

Our local vendor is Empire Computing. They recommended Orinoco access points and Avaya wireless cards. Each access point can hold two wireless cards.

We decided to have the wireless installation done on the first floor of our Science building. We already had one access point in place to provide access in a patio area of the building. Three more access points were installed with small external antennae on corridor ceilings. The access points are hidden from view above the drop ceilings. Two antennae are connected to the access point we already have. One was moved to give wireless coverage for our science lecture hall while the other continues to provide ample coverage for the patio. See the diagram on the following page.

Science Building -- First Floor
Wireless



The access points have been set up with a specific network ID (SSID). "ANY" will not work if you visit our campus with your wireless card. However, this is trivial, as the latest software automatically detects the SSID of a wireless network.

For Security, we are using a Windows 2000 server set up as a domain controller, running Steel-Belted Radius from Funk software. Basically the machine is a radius server. With the radius software we are able to input MAC addresses from each wireless card that will be used on our network. The card's address must be listed on the radius server to use our wireless network.

The Orinoco AP's also allow denial of access based on MAC address. With only a few AP's this would be both less expensive and reasonably workable. However, with many AP's, the process would be laborious for each MAC address added. In the radius software the administrator tells it what access points are on the network. The access point software has a tab for enabling the use of a radius server and indicating its IP address. The access points and radius server have a "shared secret" (password) in common. This password is also the one given to MAC's stored on the radius server in active directory.

To add a MAC address to the radius server, Active Directory is used. A new user is created where the MAC address is the username. The format is XXXXXX-XXXXXX, where X represents each character of the MAC address. Only one hyphen is used. After creating the user, I edit the properties and add a description, such as the name of the wireless card's owner. I also add the user to a group I set up. The name of the group can vary. I used 'wireless' as the name.

In the radius software 'wireless' is the user enabled for authentication. This works quite well. Once radius is set up properly, it does not have to be modified at all – except to add additional access points.

Radius -- even for Windows -- is not extremely user-friendly. I have found the documentation almost useless for my application. Even installing the software takes great care. It's not just a matter of running setup and accepting the defaults.

I also recommend using private IP addresses whether the connection is wireless or wired. That's something we are doing on our network that provides an additional layer of security from hackers outside our intranet. Of course, I believe machines with persistent connections ought to have a personal firewall.

Using encryption with wireless has been considered, but for now we are not implementing it. One important consideration in the design was striking a balance between security and ease-of-use. Simply informing our users of the encryption key(s) compromises security and (in my view) necessitates changing the key fairly often. We may implement non-mandatory encryption at some point for users who are concerned about data security but insist on being unfettered by wires.

For highly confidential data transfer, it might be safer to use a wired connection. Even though our radius server will prevent people from strolling onto our network, wireless communication is radio signals. With sophisticated equipment, placed close enough to our network, at exactly the right time, data could be intercepted.

We have tested the installation. The entire first floor has excellent wireless access. A user can walk down the corridors with a portable computer, downloading a file. As the user walks away from one access point, he approaches another and connectivity is not broken.

Costs

The largest single expense of this project was the Radius software at \$4579.20. The three access points we added were \$2028. Labor, including installation and configuration was \$1350. The remaining costs were for various parts such as wireless NICS (for the access points), antenna cable, adapters, Ethernet splitter, antennae and UPS's.

REFERENCES

1. <http://www.commsdesign.com/story/OEG20020716S0003>
2. <http://www.theregister.co.uk/content/55/26434.html>