

Deploying and Taming the Wireless Beast

Justin Landry
Pennington Biomedical Research
6400 Perkins Road
Baton Rouge, LA 70808
225-763-2586
Justin.Landry@pbrc.edu

Robyn C. Richard
Pennington Biomedical Research
6400 Perkins Road
Baton Rouge, LA 70808
225-763-2586
Robyn.Richard@pbrc.edu

ABSTRACT

In today's technical world it is hard for Higher Education Institutions to keep up with new technology. As wireless technologies are setting the trend, universities are struggling with a means of standardizing, organizing, and maintaining this new trend.

At Louisiana State University's Pennington Biomedical Research Center wireless technology has been introduced to the faculty, staff, and students in the past year. The demand for wireless came about by the expansion, which the Pennington Center has been undergoing, in recent years. With more employees being hired and new buildings being built, wireless has become a relatively inexpensive and quick way to meet the computing demands of the faculty and staff of Pennington Biomedical Research Center (PBRC). There are several fundamentals that are involved when implementing a wireless LAN. The fundamentals used for PBRC wireless LAN include research and development, procurement of equipment, surveying the coverage area, testing the coverage, making sure the LAN is secure, and Launching the new wireless service to the users.

This paper will reflect the implementation process that Pennington Biomedical has been undergoing and the strengths and weaknesses that have been discovered along the way. We realize that wireless products and services are constantly changing and improving as we are doing the best to keep up with the latest developments.

Categories and Subject Descriptors

C.5 [COMPUTER SYSTEM IMPLEMENTATION]: C.5.m Miscellaneous

General Terms: Design, Security.

Keywords

Wireless, Security, Support, Technical, Implementation, Network.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SIGUCCS'04, October 10–13, 2004, Baltimore, Maryland, USA.

Copyright 2004 ACM 1-58113-869-5/04/0010...\$5.00.

1. INTRODUCTION

Pennington's Biomedical Research Center's Computing Services entails a Technology Services Group (TSG), who support and maintain all aspect of Pennington's computing. Two employees, one full time and one part time, chose to specialize in wireless technology. As the decision of specialty came about, there was an urgent need for a wireless LAN. The TSG team of two educated themselves, while at the same time, came up with a plan to implement and launch a Wireless LAN throughout Pennington. The following is a thorough explanation of the plan and launching process.

2. RESEARCH AND DEVELOPMENT

2.1 Research Wireless Standards

There are several different flavors, so to speak, of Wireless LANs. Pennington's Computing Services technicians, who were interested in expanding their wireless LAN knowledge, took hold of the wireless implementation project. The first step at TSG was to get familiarized with the more popular standards such as 802.11b and 802.11g that are more commonly used in today's market. After getting familiarized with these two standards, the technicians chose to start out with 802.11b but opted for access points, as you will see later, that were upgradeable to the 802.11g standard. The reasoning behind this was simple, at the time 802.11b access points were cheaper than 802.11g access points. Also, the goal was to make sure that the users would adopt wireless wholeheartedly before funds were invested.

2.2 Evaluation of Hardware

The next step in the implementation process was to evaluate access points, antennas, and wireless cards. Some products of the vendors tested were Linksys, Cisco, Dell, 3Com, and Netgear. Most of the equipment tested was similar in most fundamental aspects. Each access point tested came with its own pair of rubberized antennas. Upgradeable antennas that allowed for stronger signals from the access points were ultimately chosen. Each vendor recommended various types of antenna's ranging from bidirectional to omni directional with different frequency and power levels. (see Figure 1.) Omni directional antenna made by the Cushcraft Corporation at 3dBi with a frequency between 2.4 to 2.5 GHz proved to be a reliable choice. These antennas are being used with Cisco 1200 series access points and Cisco 350 series client adapters. Cisco was a logical choice being that Pennington's network infrastructure already employs Cisco switches and routers. The 1200 series access points are highly manageable and integrate well with the backend RADIUS servers.

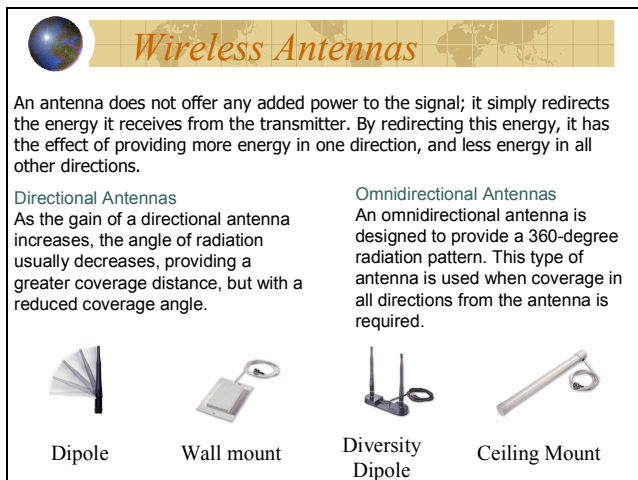


Figure 1. Wireless Antenna Hardware

2.3 Cost Assessment

When the idea of wireless first grabbed the attention of the Technology Services Group, there was no given plan of action for implementing wireless. As the PBRC campus and employee base began to grow, TSG learned that money could be saved by using wireless for network access in areas where traditional hard wiring would be too costly or impossible to install. As with every purchase, from mice to desktops, a budget had to be enforced, so the idea of saving money while deploying a reliable product was very appealing to the TSG staff and the PBRC users. Computing Services was able to save approximately 50% of the cost of deploying a wired network by setting up wireless in areas that proved to be too costly or unimaginable for a wired network. The TSG staff completed around 95% of the work needed to install a wireless network, while 10% of the work needed for an installation of a wired network was done by an outside wiring contractor. The money saved in labor alone, justified the use of wireless in some areas around the PBRC campus.

2.4 Educating the Staff

A major hurdle in the research and development phase was educating the TSG staff about wireless and the implementation process over the next few months. The staff was educated using different training methods.

2.4.1 Training Classes

Training classes were a logical first step. The TSG staff was divided into groups of four or five and held two to three hour training classes covering all of the information that the wireless team had learned over the past several months. After the formal class lectures, each group had the opportunity to ask questions about the findings and view some of the equipment sought for PBRC's wireless LAN.

2.4.2 Continued Education

For continuing education, the wireless team developed a website that is updated when new information and new discoveries on the latest wireless trends, hardware, and documentation. The combination of the initial classes and the opportunity for the PBRC employees to continue their learning of Wireless and the project progress online, have combined for a very smooth

introduction to wireless for the staff at the Technology Services Group.

3. PURCHASING

After the research and development stage, the wireless team turned their attention towards the purchasing of the equipment needed for the stage that would follow, the surveying and testing stage. In order to avoid wasting funds, the team wanted to make sure that equipment was purchased as needed. This was done by ordering the right amount of equipment needed to conduct the surveying and testing through the same vendors which TSG uses with normal procurements of computer equipment. The purchasing phase started by estimating how many access points would be needed in the areas required for wireless. This was done by using blueprints for each building and aligning the most logical locations for access point setups. Also taken into account was the specification on signal strengths from the makers of the products purchased and the known wireless standards. With these factors in mind, equipment to cover the first building was purchased.

4. SURVEYING AND TESTING

4.1 Setup Access Points

A crucial step was the actual surveying and testing phase of wireless deployment. In the purchasing stage above, blueprints of the buildings were used to setup wireless access. At this time, the team made an educated guess for the position of each access point in each of the buildings, giving a solid starting point for the surveying and testing phase. Once all of the access point locations were chosen, the access point and antenna were setup in its respective location and the team proceeded with the plan.

4.2 Check Wireless Coverage

After the access points and antenna's were setup in each building, the wireless team used a simple process of developing coverage maps for those areas. First, a laptop was setup with one of the wireless cards. Next, the wireless client utility was installed on the laptop which allowed for monitoring and reporting of fluctuations in the wireless signal. From there, the laptop was installed on a roll cart with the necessary tools needed to complete the wireless survey. Using this cart, the signal strength and quality readings every three feet in every direction in each building were tested. The observations were recorded on scaled down versions of blueprints for each building. After the surveying for each building was finished, color coded coverage maps were designed showing the signal strength and quality within the buildings that were tested.

4.3 Evaluate Equipment Needs

After these initial surveys, the wireless team convened for a meeting, discussing the effectiveness of the equipment purchased. The team was very pleased with the performance of the access points, antennas and client adapters. It was felt that there was no reason to order different equipment and the decision to deploy what was originally purchased was made. The need for purchasing more powerful antennas was determined to be a future possibility. It was agreed that some of the access points needed to be repositioned to create the desired coverage area. So from here, the access points that were thought to be underperforming were repositioned and the same steps described above were performed until the desired coverage area was reached and agreed upon.

4.4 Document The Coverage

When all of the wireless networks were installed in each of the projected areas, each coverage map was compiled into online PDF files that could easily be accessed by the TSG staff. This would serve as a useful tool later when wireless was officially launched to all of the users campus wide.

5. SECURITY

5.1 Test Security Protocols

Security is a major component when considering a wireless LAN. There are certain protocols available for securing a wireless LAN; which all contain pros and cons. The different types of security protocols that were considered when implementing wireless on Pennington's campus were Cisco's LightWeight Extensible Authentication Protocol (LEAP), Extensible Authentication Protocol – Transport Layer Security (EAP-TLS), and Extensible Authentication Protocol – Tunneled Transport Layer Security (EAP-TTLS). EAP-TLS is a certificate-based security method that requires both server and client side certificates for authentication. EAP-TTLS is also a certificate-based security method, but it only involves the server side for authentication. Cisco's LEAP entails user password authentication and supports mutual authentication. Both EAP-TLS and EAP-TTLS were turned down as an option because of the certificate-based factor that both entail. Certificate-based authentication requires a certificate sign-up service and added support and maintenance on the client and server sides. The security method chosen was Cisco's LEAP. There are various reasons for choosing LEAP. Being that all switches and routers throughout Pennington are Cisco, it was an easy transition to implement Cisco Access Points and wireless cards accompanied by the LEAP protocol.

5.2 Assure Data Protection

The basic setup for Pennington Center's Wireless LAN includes two RADIUS servers running ODYSSEY[1] software and (25) twenty-five Cisco 1200 Series 802.11b/g Access Points. The campus coverage area is presently 50%. It is the intention of Computing Services to have wireless service throughout the entire campus by December 2005. By the time the entire campus is wireless ready, there will be a total of 60 Access Points. Presently, all Pennington client computers use the Cisco Aironet wireless cards and the Cisco Wireless utility to support the LEAP authentication in order for users to connect to the network. Pennington has two service set identifiers (SSIDs) known as Guest and PBRC wireless. Each SSID is unique and follows a different security method. The Guest SSID uses an open authentication protocol and is openly broadcasted for anyone who wants to connect wirelessly. The Guest SSID is on the Pennington DMZ and is placed behind the firewall which prevents network access. The PBRCwireless SSID is on the Pennington network but requires LEAP password authentication to connect and is not openly broadcasted. Connection to PBRCwireless requires an active directory user name and password.

5.3 Close The Gaps

Recently, security vulnerabilities have been a major issue with wireless. Pennington is subject to the Federal guidelines of the

Health Insurance Portability Act (HIPAA) of 1996 and therefore must maintain tight security on all electronic data. The new security authentication protocol Protected Extensible Authentication Protocol (PEAP) is currently being reviewed for possible implementation for use with the PBRCwireless SSID. PEAP is supported by Microsoft Windows XP, Cisco, FunkSoftware, and various other vendors. PEAP (See Figure 2.) creates an encrypted SSL/TLS tunnel between the client and the authentication server, and the tunnel then protects the subsequent user authentication exchange. The change from LEAP to PEAP would allow more users that have personal laptops with different vendor wireless cards to use this protocol without requiring a Cisco Wireless card and utility.

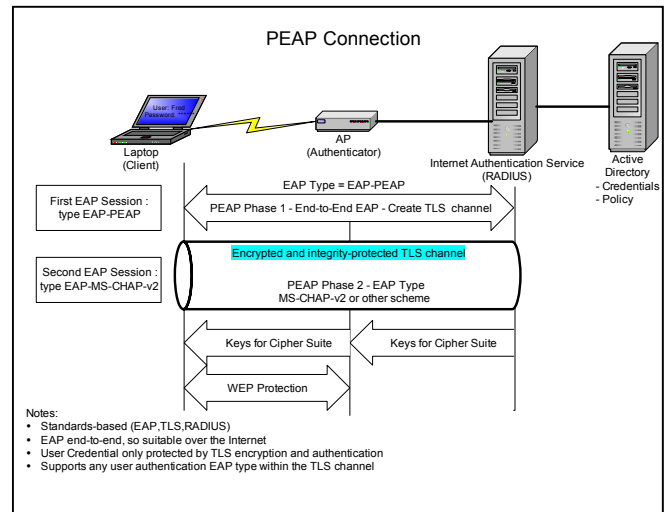


Figure 2. PEAP Connection Schema

PEAP is argued to be the most secure protocol available in Wireless LANs.

6. LAUNCHING

There were a few technicians who were part of the TSG team on implementing and launching the Wireless LAN at Pennington Biomedical Research Center. All technicians had wireless LAN knowledge through documentation, online knowledge bases, and training. Once wireless connections for both SSIDs were tested within the Computing Services Department, the TSG team gave other TSG staff an in-service on the technical aspects of connecting to both SSIDs. Once the Computing Services staffs were comfortable with the Wireless LAN and its support issues, the announcement was made to faculty, staff, and students. As soon as the campus is entirely wireless ready, there will be additional training classes offered on PBRC wireless.

The common denominator for support issues dealing with PBRC wireless have been users who have a wireless setup at home, or elsewhere, and also want to connect to Pennington's wireless network. It is mandatory for users to receive training in regard to the wireless restrictions at Pennington and the changes in configuration that have to be made in order to connect to PBRC wireless. It is realized that supporting the wireless connectivity will be an ongoing effort, as the wireless venture grows enterprise wide.

7. CONCLUSION

The implementation and launching process of Pennington's Wireless LAN is an ongoing process that is continuously being evaluated for improvements in security, efficiency, etc. Feedback from Pennington's faculty, staff, and students has been overwhelmingly pleasant. It is the mission of Computing Services to continue to strive for a totally wireless campus that is tightly secure, reliable, and user friendly. All efforts will be made to keep this mission in mind and to preserve the initial intentions of Pennington's Wireless LAN.

8. REFERENCES

- [1] <http://www.funk.com/radius/>
- [2] Microsoft Corporation. The Advantages of Protected Extensible Authentication Protocol (PEAP): A standard Approach to User Authentication for IEEE 802.11 Wireless Network Access. Positioning Paper, June 2003.