Design and Cost /Benefit Analysis of WLAN vs. TLAN in a Manufacturing Environment

By

Dale M. Eppert

Submitted to
the Faculty of the Information Engineering Technology Program
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Engineering Technology

University of Cincinnati

College of Applied Science
June 2001

Design and Cost/Benefit Analysis of a WLAN vs. TLAN in a Manufacturing Environment

By

Dale M. Eppert

Submitted to
the Faculty of the Information Engineering Technology Program
in Partial Fulfillment of the Requirements
for
the Degree of Bachelor of Science
in Information Engineering Technology

Dale M. Eppert	Date
Mark Stockman, Faculty Advisor	Date
James F. Sullivan, Department Head	Date

Acknowledgements

I would like to thank the faculty of the College of Applied Science, without whose support and guidance this project would not have been possible. I would like to thank Marilyn Bourquien and her Information Services staff at Cincinnati Incorporated for providing facilities, hardware and timely instruction. I would like to thank Enterasys Networks, particularly Chris Rosen for his vision and David Schardine for his time and patience. I would especially like to thank my family for providing support and keeping me focused on what is really important.

Table of Contents

Table of Contents (cont.)

List of Illustrations

Abstract

Upgrading a manufacturing floor network requires a cost/benefit analysis between extending the network by hard wiring to each client, or installing a wireless local area network. These are the options Cincinnati Incorporated faced when determining the best method for replacing an aging token ring network and forty workstations on the manufacturing floor. This project determines the costs of extending the corporate Ethernet backbone by hardwiring to each workstation throughout the shop floor, to the cost of installing a wireless local area network. A wired or tethered local area network will provide a fast, secure method of transferring data to and from the shop floor workstations. A wireless local area network can provide a flexible network that easily extends the range of the network throughout the shop, and take advantage of new tools being developed for wireless mobile computing. While the costs and issues of installing a tethered local area network are well known, wireless computing is a relatively new technology that has some security issues. This project details some of the security and installation issues involved with wireless local area networks, and provides a basis for determining which local area network will have the greatest return on investment.

1. Introduction

Current procedures for delivering information to the manufacturing floor at Cincinnati Incorporated are time consuming and create confusing paper trails that are hard to follow. For instance, to replace an existing part on a new machine requires new manufacturing drawings, new assembly drawings and an Engineering Change report. The new manufacturing drawings are created in CAD and printed on a plotter in another part of the building. The drawings are collected from the plotter and either picked up by someone or dropped into the inter-office mail system to be sent back to the engineer. The engineer then reviews the drawing for errors, verifies the accuracy of the drawing and sends it back to the reproduction facility where it will stay until enough drawings are collected for microfilming. Once microfilmed, the drawing is then ready to be published for programming, routing and manufacturing. Meanwhile, the engineer requests pertinent assembly drawings from reproduction so they are kept from being sent to the assembly floor for use. The engineer alters these drawings to include the new part and the reproduction process begins again. After these changes an Engineering Change Report (ECO) is written and distributed through the inter-office mail to the appropriate department heads. The department heads distribute that information to the people in their department to act upon the proposed changes. The whole information delivery process primarily occurs via a ‘sneaker net’ and can take weeks to be finalized.

Upgrades to the document storage system and improved network performance have changed this. Manufacturing floor electronic information access has been primarily limited to inventory tracking and control. With new Electronic Job Ticket (EJT) software recently purchased by the Information Services (IS) department, drawings will be released by the engineer into the Project Data Management (PDM) database, then immediately copied from the database and converted into a .pdf format. These drawings will then be immediately viewable over the new EJT web page. With this new software the information that is now readily available to shop floor personnel has been increased. Not only is the current information database available, but so too are current engineering drawings, engineering changes and procedures in .pdf format. This information is now stored on the company intranet and is accessible from the manufacturing floor. Impending drawing changes can be noted on assembly drawings before the change will even take place. Assembly department heads know of assembly changes immediately so they can react accordingly. Engineering procedures are now available to assembly personnel in electronic format to be printed out along with pertinent drawing files.

2. Problem Statement

The infrastructure for providing this information, however, was not in place. There is a fiber optic Ethernet backbone on the manufacturing floor that provides connectivity to the various CNC machines via their DataLink™ control system, and to employee time clocks. There is also a token ring network that connects the AS-400 Materials Requirements Planning (MAC-PAC) software that is displayed on 'green screen' monitors. The token ring terminals are 14 years old, and need to be replaced by terminals that can process greater information at a higher rate. In a meeting with Marilyn Bourquien, Manager of Information Services at Cincinnati Incorporated (2), she suggested that a wireless network could possibly provide greater flexibility and cost benefit than could a tethered Ethernet connection. Even if the initial cost of the Wireless

Local Area Network (WLAN) was greater than that of a Tethered Local Area Network (TLAN), the initial expense could be made up in network flexibility, addition of a growing array of wireless technologies and ease of management. The project is to identify the initial cost of both the WLAN and the TLAN, and to identify the future cost advantages of the wireless technology.

With a slumping economy and tight budgets everywhere, the decision to provide the shop with a new network structure is not taken lightly, and the solution must provide a reliable, secure network infrastructure. In order to demonstrate a sound proposal to obtain funding for the project, a complete cost benefit analysis was performed. To this end, it was necessary to design and budget both a wireless and a tethered shop floor network. The design and budget process includes the layout and design of both competing topologies, the cost analysis of the various topologies, specifications of the proposed networks, a site survey, installation and testing of a WLAN and a report on potential future growth.

3. Problem Solution, Project Description and Intended Use

This networking project had two goals. The first was to complete a cost/benefit analysis of a wired Ethernet versus a wireless Ethernet deployment in a manufacturing environment. To this end, a shop floor layout has been created of both a proposed wired and a proposed wireless network. These layouts were used to illustrate the network structure and to develop a bill of materials for each topology. The second goal was to verify that a WLAN is a feasible option to the TLAN. I did this by installing and testing a wireless local area network on the manufacturing environment. The installation of the WLAN replaces an existing token ring network and extends coverage of the “fast”

Ethernet backbone to the entire manufacturing floor. The WLAN will connect new thin client terminals that will replace AS-400 “green screen” terminals currently located on a token ring network. The new terminals will allow users to access the ‘Materials Requirements and Planning’ database, engineering drawings, procedures and the company intranet.

The wireless network needs to be a robust network capable of providing access to the entire shop floor. The network must also be cost effective and secure. Testing was done with various Windows operating systems and security protocols. To provide full coverage to the manufacturing floor a site survey was used to locate and properly configure the APs. The WLAN eliminates the need to hardwire each terminal and will facilitate future upgrades and changes to the network.

3.1 User Profiles

The primary users of the wireless network are network managers who administer the network, shop floor assemblers and machinists. Network management will be through Information Services (IS) engineers that maintain and administer the network. Information Services is responsible for assigning IP addresses and setting up users rights and roles. Manufacturing floor personnel have varying degrees of computer literacy, but all are familiar with basic functions, such as opening files, browsing the network and navigating the graphical user interface (GUI). The AS-400 system has been in place for over 20 years. The shop floor personnel use it on a daily basis for tracking parts and logging work orders. I provided training for the use of the new terminals and software. The wireless network is invisible to them and no networking expertise is required of them.

3.2 Design Protocols

This networking project involved the use of XP, Windows 2000, Windows 2000 Advanced Server and Windows 98 operating systems. Cisco Systems and Enterasys Networks provided the wireless hardware I used. This hardware included a Cisco Aironet site survey kit and a multi access point wireless network provided by Enterasys. The Enterasys products consisted of three RoamAbout wireless access platforms, six wireless network interface cards (nics) and three Range Extender antenna kits.

4. Project Design and Development

The project was completed in phases. (For a complete Timeline, refer to appendix A.) In the first phase, Senior Design I, the problem was identified and the determination of the solution, a cost benefit/analysis of a wireless versus a tethered LAN, was decided upon. Each network topology then was laid out on the shop floor plans and a preliminary bill of materials was created. In Senior Design II, a site survey for the WLAN was performed and the feasibility of installing a WLAN on the manufacturing floor was determined. The original WLAN layout was then adjusted according to the site survey findings. Senior Design III consisted of installing, tracking the performance of and instituting various security protocols on the wireless network. For a complete project flow chart, refer to figure 1.

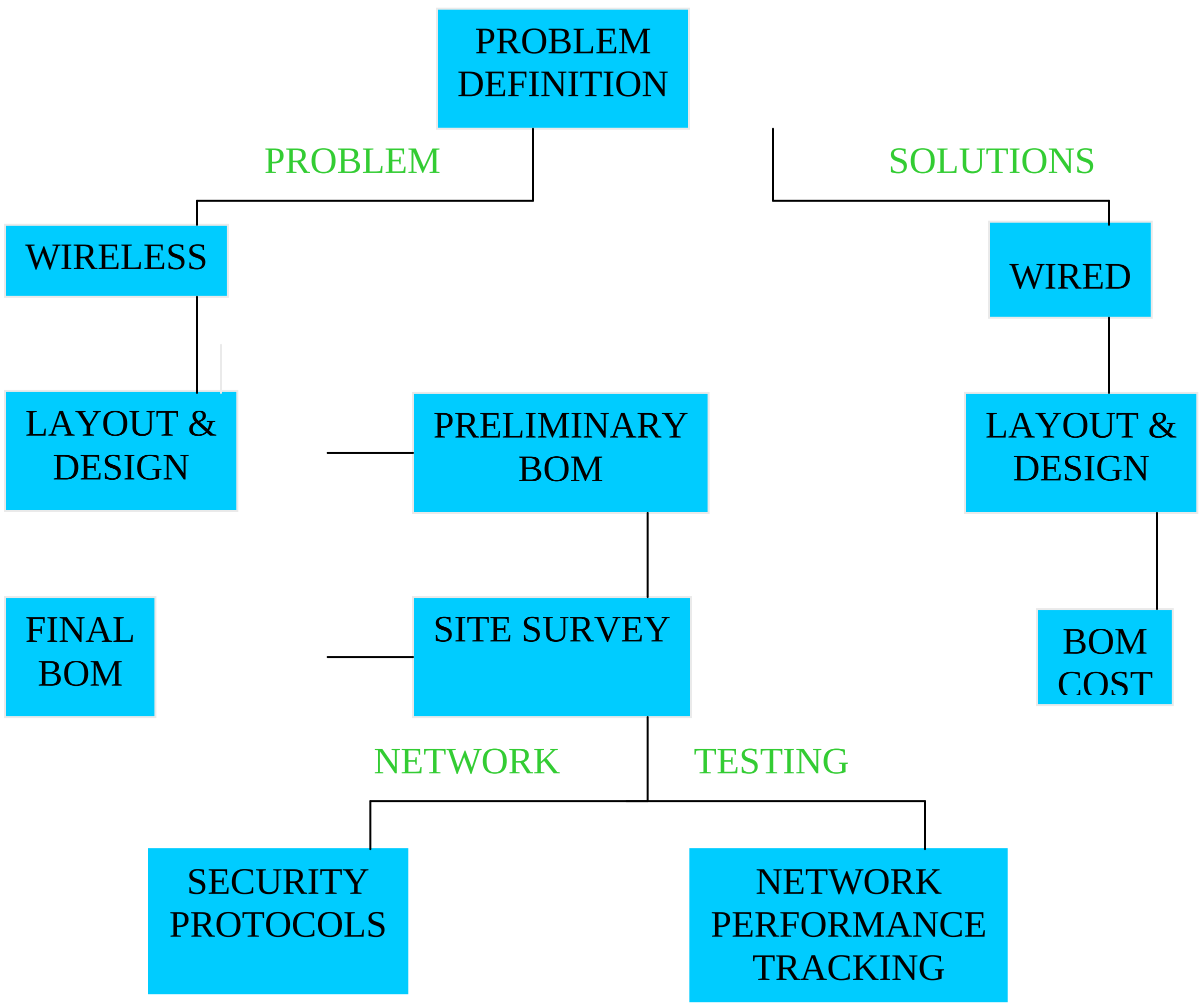

Figure 1: Project organization chart

5. Deliverables

The goal of this project was to determine the feasibility of installing a WLAN in a manufacturing environment, compare the costs associated with installing both a WLAN and a TLAN and to determine the benefits associated with each Ethernet topology. The result allows the IS department at Cincinnati Incorporated to make an educated choice, and have a turnkey solution, for extending the corporate Ethernet to the manufacturing floor. To that end I completed the following tasks:

1. Wired network
    a. Layout of shop floor showing:
        i. Proposed wiring runs – cable lengths
        ii. Upgrades to equipment racks as needed
    b. Bill of materials listing equipment and installation costs
2. Wireless network
    a. Layout of shop floor in 3-D showing building structures and sources of RF interference
    b. 2-D Layout of shop floor showing:
        i. Existing terminals
        ii. Proposed locations of Access Points (APs)
        iii. Coverage area of APs
        iv. Wiring runs to APs
    c. Site survey
        i. 2-D layout listing results of site survey
        ii. Show actual AP coverage
        iii. Show AP statistics such as signal strength and signal to noise ratio
    d. Bill of materials listing costs and specifications of hardware and installation
    e. Network installation
        i. Install multi access point wireless network on the shop floor
        ii. Test and configure network for optimal performance and roaming clients
        iii. Institute security protocol
3. Report on benefits of wireless network and potential areas of growth for Return On Investment

6. Project Identification

In Senior Design I, I set a project plan in place and developed the preliminary layout and Bill of Materials for both the WLAN and the TLAN.

6.1 Project Planning

According to Matthew Gast in *802.11 Wireless Networks: The Definitive Guide* (5), there are two components to network planning. The first is physical planning, and the second is planning changes to the logical network. The first step in the design of the network was to obtain floor plans. Floor plans should not only include the actual building map, but also the existing physical network. Physical planning for a TLAN is fairly straightforward. For a TLAN, the floor plan is used for locating the existing terminals that need to be replaced along with the existing wiring cabinets and any additional terminals that may be needed. Once the terminals are located, wiring routes will be planned and any additional hardware such as switches, routers and patch panels can be added.

Physical planning for a WLAN is more involved. A complete site survey will need to be done. A site survey ensures the system will fulfill the necessary requirements, defines Access Point (AP) layout and identifies potential sources of interference. It will be important to gather specific network requirements before considering the wireless system. Some of the pertinent issues that need to be addressed are:

- What is the number of terminals in the shop that will need to be replaced or added?
- What does the network coverage area need to be?
- What is the maximum number of users?
- What types of data will need to be transferred across the network and what type of throughput is needed?
- How much mobility is needed and what type of future growth is needed?

After the first meeting with Marilyn Bourquien, I planned another meeting to determine these issues. In that meeting it was determined that the network should plan for:

- 40 shop terminals need to be replaced.
- Coverage area will include the entire shop floor. Areas that will not be covered include outside receiving or storage areas, the new Customer Productivity Center, or offices other than those that exist on the shop floor.
- The number of users on the shop floor is currently 250 employees, but the network should plan for twice that with only approximately twenty-five or fifty considered frequent users.
- The types of data to be transferred will be the MAC-PAC user interface, Intranet access and, primarily, drawings and engineering procedures (EPs) in .pdf format.
- Throughput will be low, with the typical file size approximately 125 – 250 Kb.
- Mobility is not currently an issue beyond the ability to relocate terminals and move CNC machining centers, but will be important for future growth, such as hand held inventory control units.

6.2 Preliminary layout

For each topology, I used shop floor plans and created 3-D models of the manufacturing floor using Solid Edge solid modeling software. For the TLAN, I modeled the entire shop floor (Figure 2) and laid out existing equipment racks and the fiber optic Ethernet backbone (Figure 3).

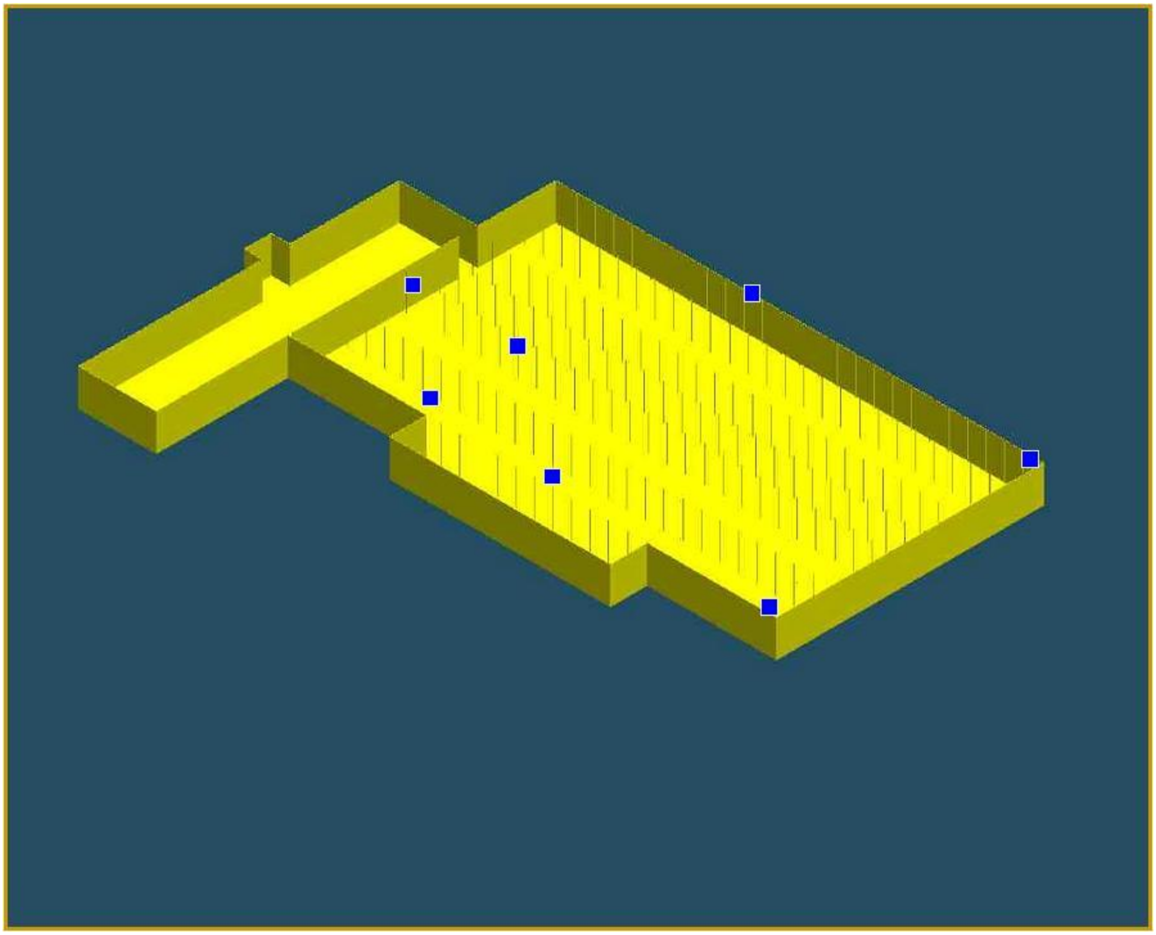

Figure 2: 3-D Layout of manufacturing floor

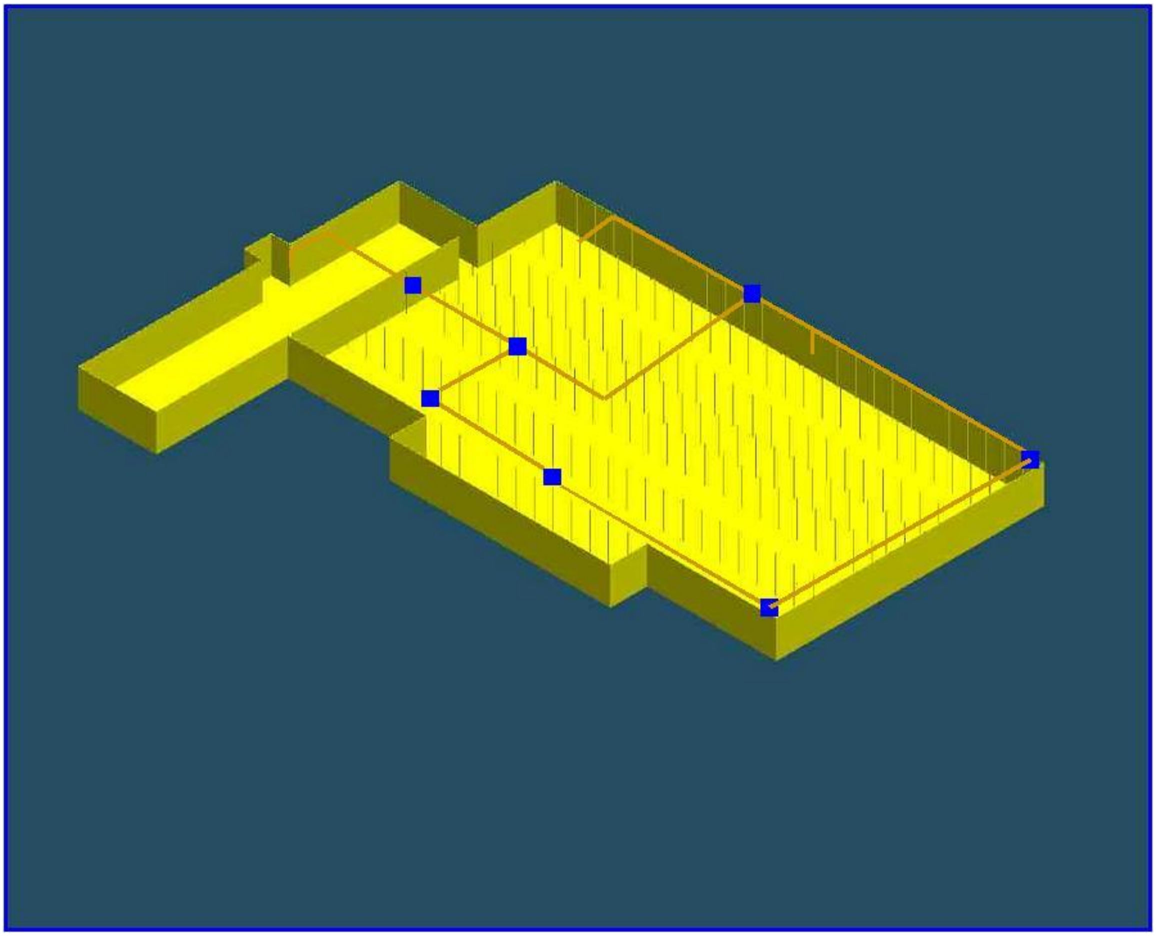

Figure 3: Fiber optic wiring diagram

I then designated the locations of all the existing terminals that needed to be replaced (figure 4).

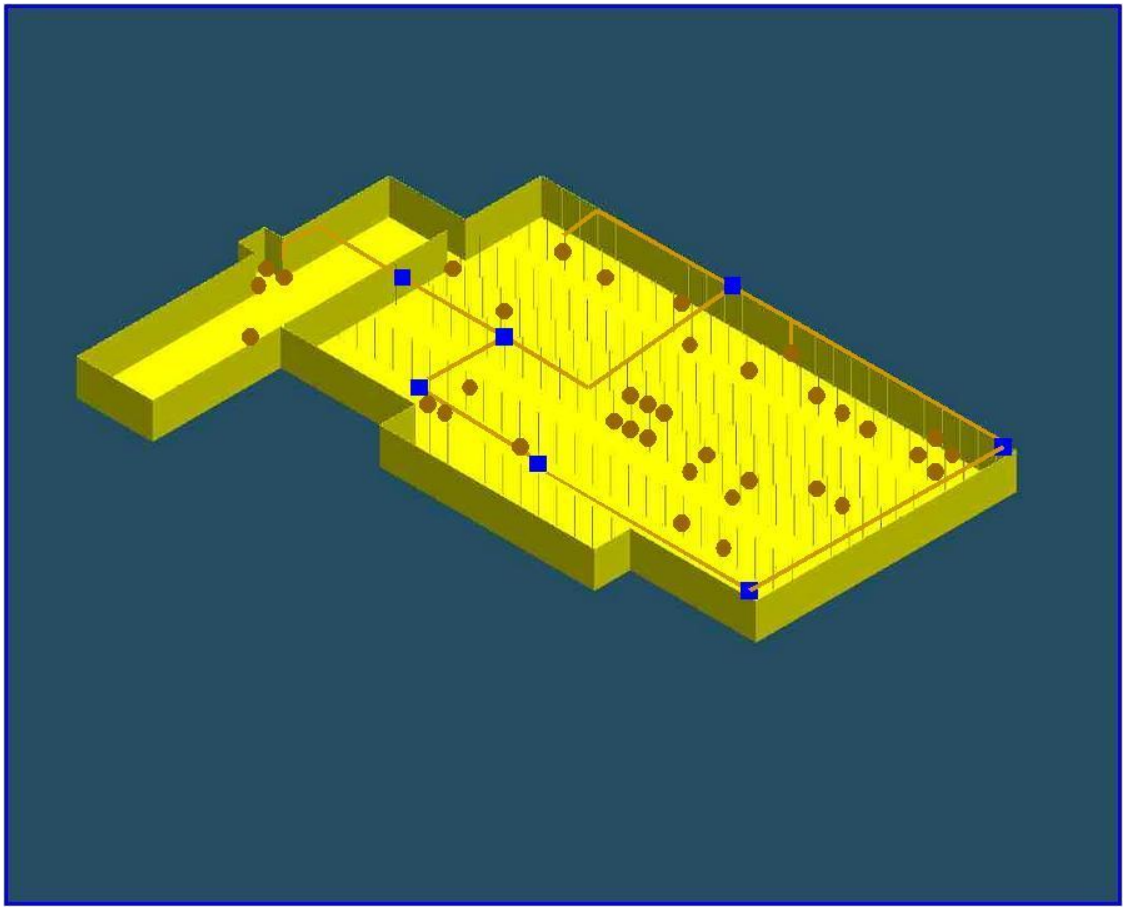

Figure 4: Existing terminal locations

After determining the locations of the existing terminals, I then laid out measured wiring routes to each terminal (figure 5).

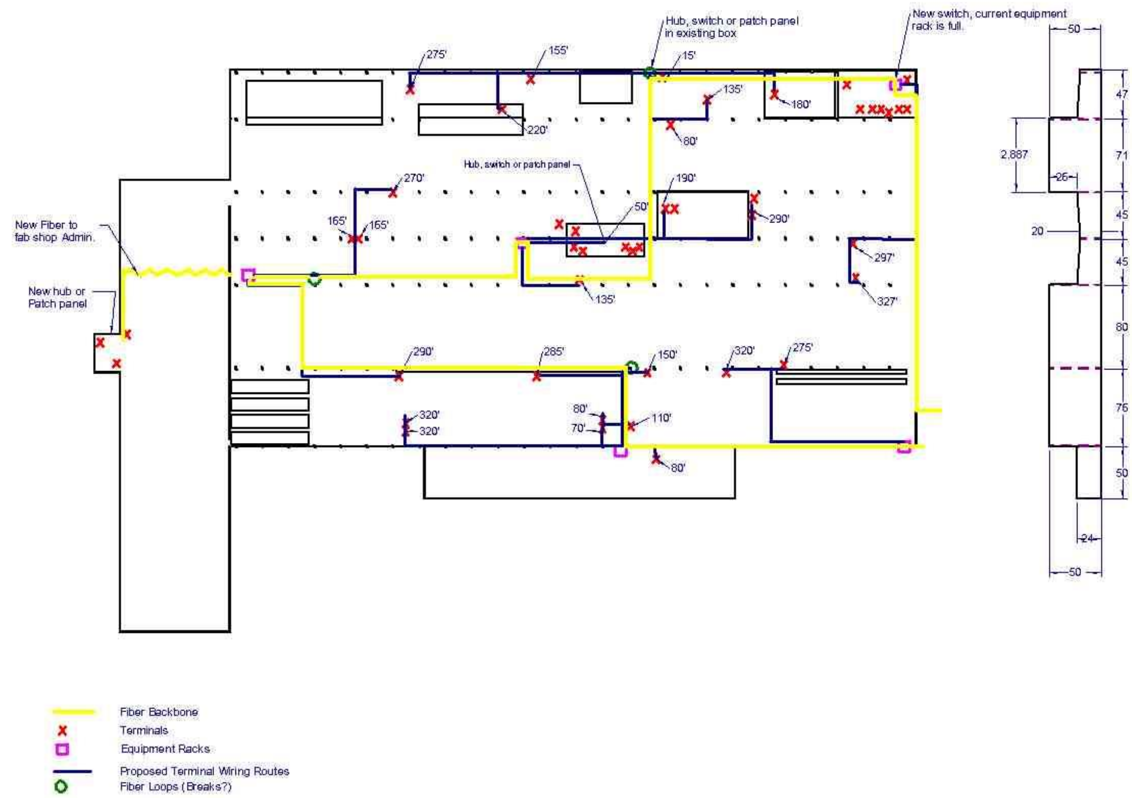

Figure 5: TLAN wiring routes

Some of these wiring routes were longer than the 100 meters that CAT5 cable can reliably deliver information, so I designated the areas where additional hubs, switches and upgrades to existing wiring cabinets were needed. Due to the size and height of the fab shop, the entire 100 meters of CAT5 cable length would be used before spanning the distance of the ceiling rafters. This resulted in the need to add an additional optic fiber run from the equipment rack across the rafters to the location of the existing MAC-PAC terminals.

For the WLAN, I used the same floor plans to map out possible sources of RF interference, the preliminary locations of the APs and their coverage areas. Any large storage racks, large overhead cranes, and high noise generators such as machinery, microwave ovens and cell phones on the 2.4 GHz range were identified and isolated (figure 6).

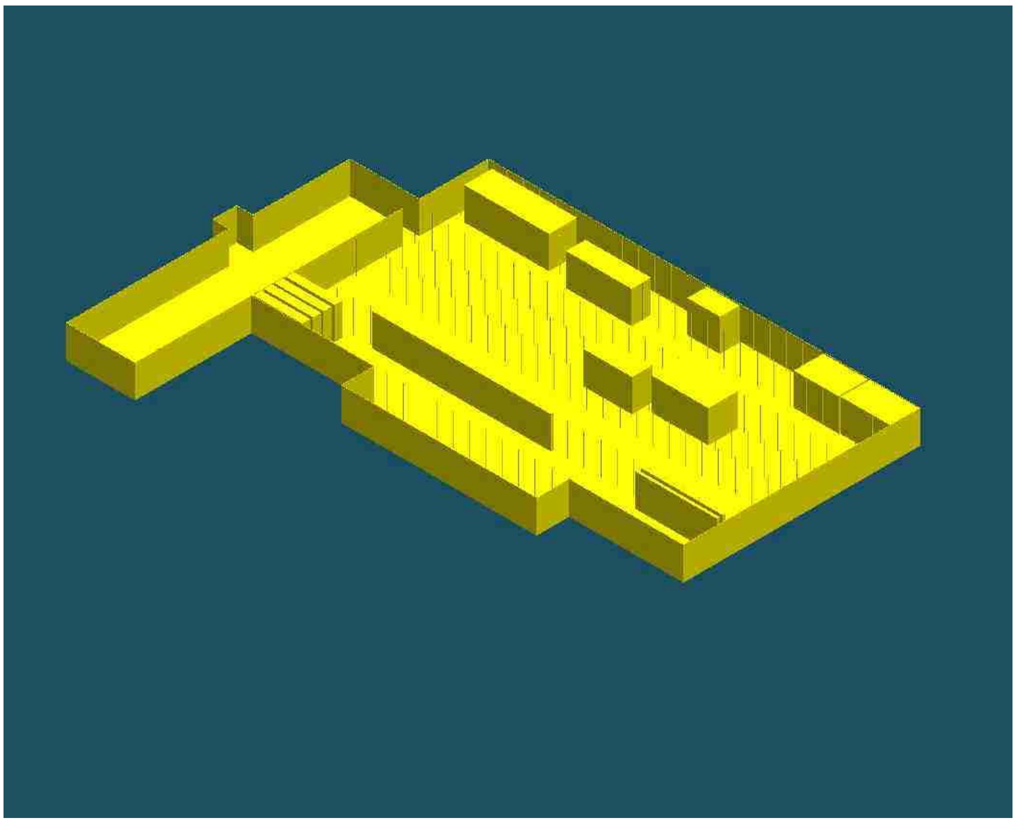

Figure 6: Shop floor model with interference generators

The preliminary locations of the APs and cell design were then mapped out on the floor plans (figure 7).

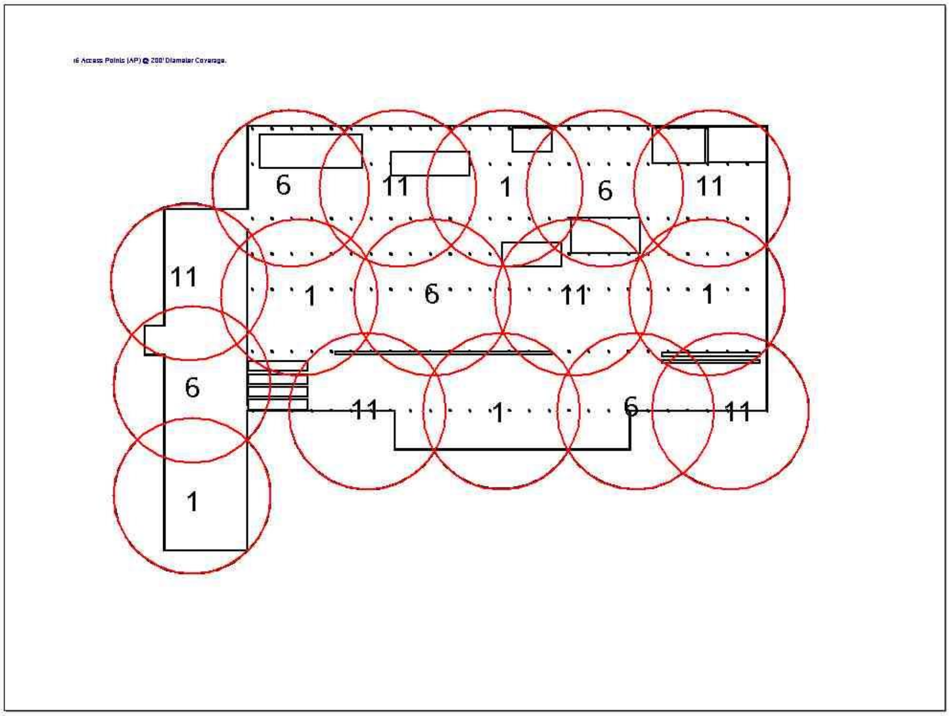

Figure 7: Preliminary access point locations and coverage areas

The cell designs show the coverage area of each AP. Adding the location of the client terminals shows the potential usage and throughput needed for each cell location. The logical configuration of the cells is also illustrated to avoid matching the frequencies of adjoining cells. After the cell layout was completed, a preliminary estimate of the hardware needed was drafted. This estimate covers antennas, switches, cabling runs (Figure 8) and the layout of the equipment racks with the existing and additional hardware as needed.

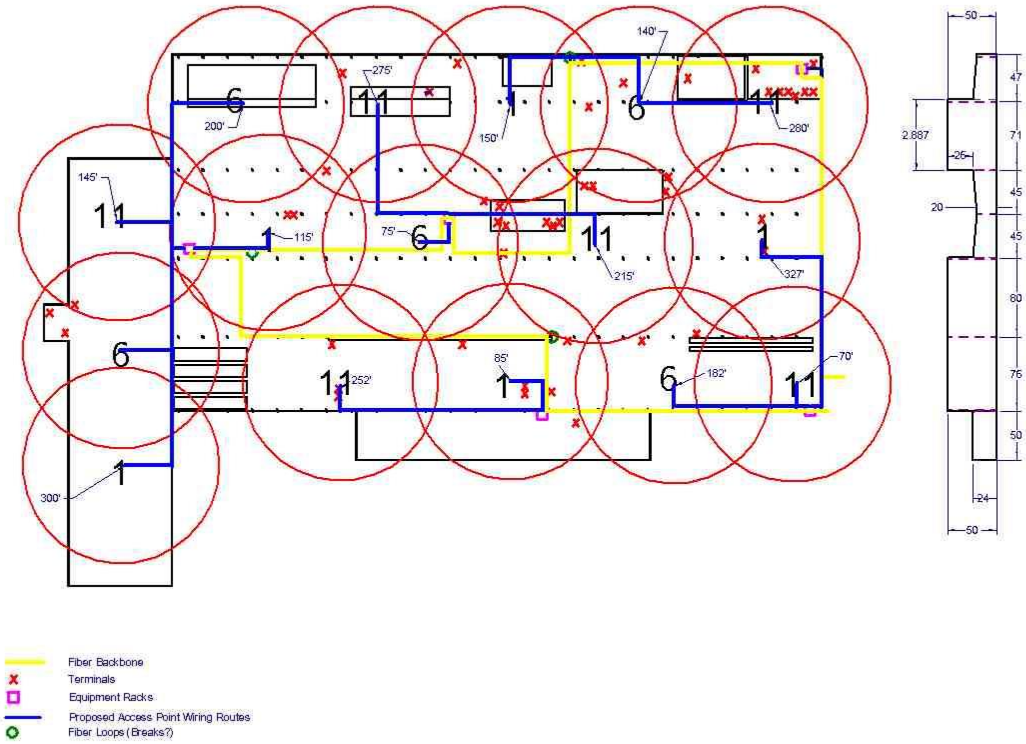

Figure 8: Access point wiring runs

The second component of planning for an enterprise network, the logical changes to the network, deal with the management of IP addresses. The TLAN will need to have sufficient IP addresses allocated to handle all the new terminals. The WLAN will need to be set up on a single subnet, if given enough available space, so as to allow mobility throughout the plant. Managing the network will require software for trouble shooting and diagnostics of the network. At this point security considerations are taken into account and may take the form of MAC addressing, WEP encryption, IEEE 802.1x standards, Virtual Private Network (VPN) technology or RADIUS (Remote Authentication Dial-In User).

6.3 Estimating Costs and Bill of Materials

With marked up floor plans in hand, the next step was to develop a rough estimate of the cost of each type of topology. Because the site survey is such an important part of the WLAN deployment, the cost associated with the site survey was also taken into account. Many vendors will provide site surveys for a fee that can then be credited to the installation of the WLAN. Costs associated with a site survey include man-hours and equipment needed to do the site survey. As a rule of thumb, a site survey may take from thirty to sixty minutes per AP. The equipment needed to do a site survey can be found in a site survey kit. The kit I used contained one Access Point, RP-TNC connectors (for external antennas), four PC card adapters with several different types of ceiling and wall mounted antennas and mounting hardware for the APs. One or two laptop computers are typically used, but not provided with most kits. For an in depth analysis of RF interference, it may be necessary to use a spectrum analyzer. A spectrum analyzer determines RF interference that may degrade the performance of the WLAN, and costs from $3,000.00 to $20,000.00.

For most enterprise deployments the choice of IEEE standards will, as of this writing, be 802.11b or 802.11a. (1) 802.11b will deliver up to 11 Mbps data rate in the 2.4 GHz band (half-duplex, so actual throughput is up to 5.5 Mbps)[i], whereas 802.11a will deliver up to 54 Mbps in the 5 GHz band. The tradeoff between 802.11b and 802.11a is that 802.11a will avoid interference in the busy 2.4 GHz bandwidth and deliver higher throughput, but the cell coverage is typically smaller thereby effectively doubling the number of APs. Work is currently being conducted on 802.11g wireless standards that will boost throughput in the 2.4 GHz bandwidth to 54 Mbps. The cost analysis quotes prices and vendors for each WLAN standard.

In addition to the Ethernet backbone that already exists, hardware includes new terminals for accessing information. This requirement will be common to each topology and consists of fully functional PCs and network computers. Network computers are thin clients that borrow all the operating system, application programs and data from a central network server. (4) Network computers cost from $500.00 to $1000.00 and can significantly decrease the cost of a network deployment such as this. For the WLAN network, hardware costs include AP hardware and any upgrades to existing switches and patch panels that were required. AP hardware may include not only the antennas, but also any power drops that are necessary to run them. Instead of running new power drops to each AP, a better investment was to purchase line-powered enabled devices. To include line-powered enabled devices to the network, existing switches, patch panels and cabling may need to be replaced with line-powered compliant hardware or used in conjunction with power injectors that can be installed in-line. Power injectors are in-line devices that allow enough amperage to run through the CAT5 cable to power the AP. Power injectors can be placed after the hardware in equipment racks to prevent having to purchase line powered enabled hubs and switches.

On the administrative side of the network, additional software and hardware will be needed for managing the network. This may include a RADIUS server and WLAN specific security software. Since there already exists an Ethernet backbone throughout the shop, a TLAN will not need any new administrative tools to operate it.

The costs associated with a TLAN include the costs of installing additional wiring and possible upgrades to existing Ethernet hardware. The costs associated with running new CAT5 wiring to each terminal includes the manpower for pulling the new wire, any shop modifications that may be needed to pull the wire, and Ethernet connectors. Depending on anticipated growth, additional equipment racks may be needed to service less accessible terminals. In this case it will be necessary to run additional optic fiber to those equipment racks. The Bill of Materials (BOM) for each topology can be found in appendix D, E and F.

7. The Working Prototype

In Senior Design II, I acquired enough wireless hardware to perform a site survey and verify that a wireless network is a feasible alternative to a TLAN on the manufacturing floor.

The site survey

The site survey verifies the preliminary layout and confirms coverage area and sources of interference. The site survey consists of placing APs in various locations and checking their coverage area. Site survey statistics such as data rates within the coverage areas, signal strength and signal to noise ratio, packet error rate and latency caused by multi-path were recorded and documented. Tools used for the site survey include portable laptop computers loaded with Cisco Aironet PCMCIA network cards, Cisco Aironet 350 Access Point, Netgear 8 port dual channel hubs and various patch cords and power strips.

Installation and configuration of APs and clients

The deployment of the wireless network included the installation of the APs as determined in the design and the installation of the client adapter cards. All APs and clients are configured for optimal performance and security settings. Configuration of the APs and clients means setting AP MAC addresses, IP addresses and SSID's and configuring the APs for client roaming. Security settings include MAC address filtering, WEP encryption and EAP technology.

Vendor comparisons

To ensure a fair comparison and competitive pricing, multiple vendors were invited to demonstrate their products. I used Cisco products for the first site survey and network testing. Enterasys came in to demonstrate site survey capabilities and are currently in use for the longer term network testing. A bill of materials for the final network design includes multiple vendors and product specifications.

7.1 Hardware Acquisition

After the initial problem definition and solution was proposed in Senior Design I, I learned from the IS department at Cincinnati Incorporated that due to poor sales, the budget for continuing with testing and installation of the wireless network at Cincinnati Incorporated has been withdrawn. This development left me without any resources for acquiring hardware for the project. Therefore, the initial step in creating a working prototype was to acquire hardware on my own. The Information Services (IS) department at Cincinnati Inc. was able to supply me with four laptop computers, these were old laptops returned by sales and services, and two Netgear 8 port hubs for extending the network farther from the existing equipment racks. IS also provided me with their network hardware contact, Perry Buffington, President, Protocol Communications.

The search for WLAN hardware began with searching the Internet for WLAN equipment manufacturers. I contacted Cisco, Intermec and Symbol Technologies for help in acquiring the necessary hardware. Cisco looked to be the most promising. Their website featured corporate grant programs such as a community Grant Program and Network Hardware Grant program that provided start-up network equipment for different organizations. I contracted several people at Cisco and their third party Grant provides about how to submit my grant information. Cisco's program is set up to provide low-income communities and non-profit organizations with Grant proceeds. I was told I did not qualify, as they do not supply to Universities, for-profit and institutions or individuals.

My next attempt for funding was to investigate Professor Said's suggestion that I install the network at OCAS. I had tried to use this tact while requesting grants from the aforementioned companies, that the hardware would be used at UC-OCAS, to no avail. I hoped that some type of real monies could be obtained from the University for purchasing WLAN equipment. This angle also proved fruitless for lack of money and/or interest.

Perry Buffington, the IS contact, finally located a site survey kit that I could borrow for a period of (10) days. Mr. Buffington was an invaluable resource, not only for obtaining the site survey kit, but he also made himself available to answer any questions I had and provided real world background into network installations. The site survey kit he provided contained:

- Cisco 350 Access Point width (2) dual diversity antennas
- (1) Inline power injector

- (2) 2.2 dBi yagi omni directional antennas
- (1) 5.5 dBi wall mount patch antenna
- (4) PCMCIA 350 network client adaptor cards
- (1) 9-pin serial port adaptor, (2) 8' patch cords and software for loading the client adapter and AP firmware.

With this equipment in hand, my working prototype was successfully tested and demonstrated.

7.2 The Site Survey

The heart of the WLAN deployment project is the site survey. The purpose of the site survey is to refine the preliminary design, to redesign the network to any sources of RF interference, and report on these findings. The site survey report:

- Assessed and charted actual coverage of the APs
- Determined actual bit rates (throughput) throughout the coverage area
- Recorded the Packet Error Rate (PER), or the number of frames received in error. (5, p. 287)

There are tools available that can measure the amount of multi-path dispersion, that is, how much the signals bounce off obstructions that were not used in this site survey. The site survey was used to determine optimal AP locations and sources of RF interference in the 2.4 GHz and 5 GHz bandwidth that may need to be eliminated. Dedicated hardware devices such as a spectrum analyzer, or software running on a laptop can provide signal quality measurements. Some hardware vendors will supply a site survey kit with all the tools necessary. The site survey also evaluated the types of antennas that can be used. For different parts of the shop additional range extender antennas were needed to ensure adequate coverage. Once the optimal location of the APs was determined, the proper configuration of the AP was set. The configuration of the AP included the AP name, its operating channel, coverage area, IP configuration and antenna type and configuration.(1)

7.3 Configure the Access Point

The initial set-up of the working prototype began with initializing the AP with the client adapter software and drivers. Equipment needed for configuring the AP consists of:

- A computer connected to the same network as the AP
- A CAT 5e patch cable for connecting to the inline power injector, then another from the injector to the network
- Loading the IPSU (IP setup utility) software onto the network computer
- Connecting a 9-Pin straight thru serial connection cable from the network computer to the AP
- Using a terminal emulator such as HyperTerminal to connect the COM1 or COM2 port and the computer to the RS-232 serial port on the access point.
- Port settings 9600 Baud, 8 data bits, no parity, 1 stop but, Xon/Xoff
- Using IPSU setup screen to input the AP MAC address
- Clicking GET IP add to resolve AP IP address assigned by network DHCP server
- SSID factory default is “Tsunami”

Once the AP was configured, I removed the serial port connection. The AP now has system parameters accessed through a web browser using TCP/IP. To open Access Point Management Pages, the user opens an Internet browser and types in the AP’s IP address. At this point, the Summary status home screen, or the express setup screen appears (Figure8).

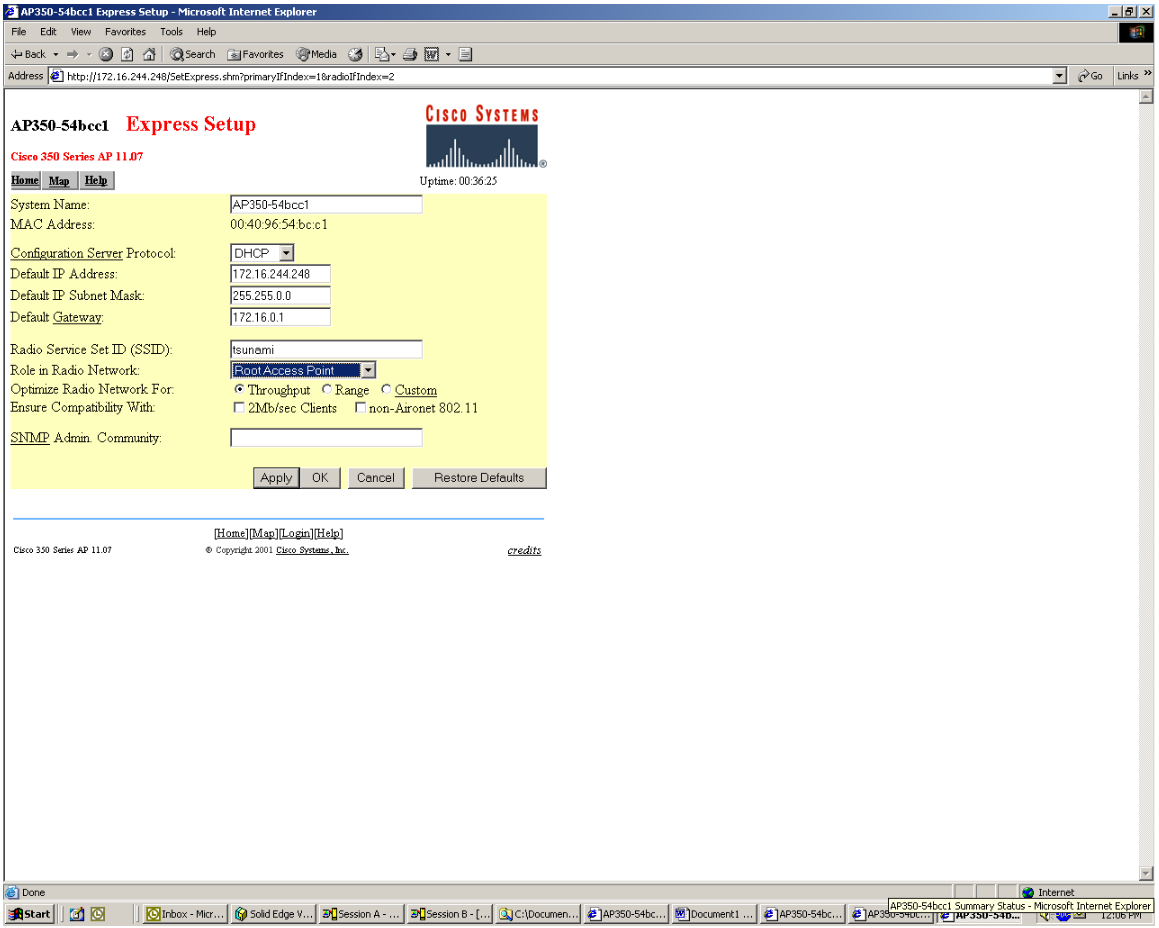

Figure 9: Aironet AP express set-up page

7.4 Configure the Client Adapter

Installation of the Client adapters consisted of downloading the latest firmware and drivers for the specific operating system, installing the PCMCIA card and loading the drivers. Once installed, the client adapter could be configured with the Cisco Aironet Client Utilities (ACU) software. The ACU contains properties screens to configure the parameters for each property.

7.5 Installation and Tools

The installation of the working prototype consisted of locating the Access Point in various locations in the shop as specified by the initial layout of the Access Point

Coverage Chart, then using the laptop computers to map Actual AP coverage.

Equipment needed for installation of the AP included

- Power strip and 100’ extension cord – for extending power to remote locations for the on-line power injector
- 200’ CAT 5e patch cable for extending network coverage from the various equipment racks to cat walks located above the shop floor
- Netgear hub for increasing distances that the network could be extended for remote AP locations too far from existing equipment racks.

The access point was located in three main areas of the shop to get a baseline for coverage areas in these distinct locations. Each location presented different coverage problems. The first location had high ceilings with large floor to ceiling steel storage racks. The 2nd location was an area of high ceilings with low-level storage racks and high concentrations of RF interference from heavy machinery. The 3rd location represented an area of low ceilings crowded with offices and storage racks. Each location had high amounts of overhead crane traffic.

7.6 Testing

After configuring the client adapters and AP, the AP was installed in each one of the previously described locations. I then took a laptop client to each location where a terminal currently exists on the shop floor. Using the site survey tools included with the ACU, I documented the Signal quality, Signal strength, noise level, data rate and signal to noise ratio at each location. Most testing was done during off-production hours to get a baseline for the noise level.[ii] These measures define the quality of the connection between the client and the AP.

At various locations, I cleared the statistics page then downloaded a large file from the network. During the download, I noted the data transfer rate and time it took to download the file. After each download, I checked the ACU statistics page and noted the received and transmit statistics there. Noting the packet error rate gives an indication of the level of multi-path interference[iii] at each site (Figure 9).

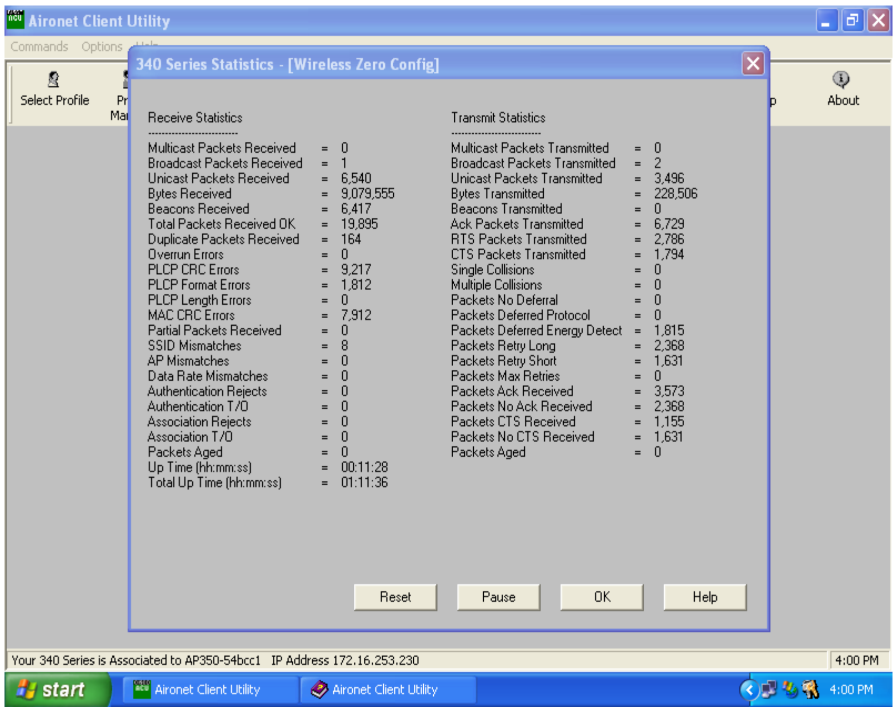

Figure 10: Screen shot of client utilities statistics page

Crane operation is a constant at Cincinnati Incorporated. The need to locate the AP as high as possible for increased coverage means that these cranes will move back and forth between the AP and the client antennas. To test the affect of the cranes on network performance, I performed a link test and watched performance as someone moved the cranes back and forth between the client and AP.

Various security protocols can impact network performance. Due to the nature of various authentication protocols, the amount of traffic the network experiences can increase as the AP and the clients "speak" to one another to verify they are who they say they are. An example of this is Shared Key Authentication. Before even transmitting data, the client and AP greet each other:

- Client requests packet
- AP sends a challenge text packet
- Client sends encrypted challenge text packet
- The AP then sends an Authentication Response packet

To test the affect of the additional traffic associated with increased security levels, I instituted 128 bit shared key authentication on the AP and client, then compared network performance to non-secure network performance.

To emulate a normal "busy" network, I located all four clients at various locations within the AP coverage. I implemented 128 bit shared key authentication on each client, then started a link test on each of three clients. The link test sends packets of a specified size to the AP to test connection performance. While three of the clients were performing the link test, I moved the fourth client to previous test locations and compared network performance against previous test results.

7.7 Conclusions from the Working Prototype

The installation and testing of the WLAN provided some interesting results. The initial layout of the APs and their coverage areas were based on published results of RF interferences and rules of thumb for adequate coverage. The actual coverage of the APs has been significantly greater. One reason for this is that multi-path effects of signals reflecting off of material racks can actually accelerate the signals, thereby effectively increasing the signal range. With one AP located in one of the more open areas of the shop, adequate coverage extended to the entire shop floor except some of the offices located farthest from the AP. With increased traffic on the network, coverage area of the AP did decrease, but still far exceeded expectations. The preliminary results of this testing suggests that the number of APs needed for complete shop floor coverage will decrease from (24) to (10). The added coverage also means there will be no additional fiber breaks or additional switches/hubs needed.

Early discussion with Enterasys to provide additional WLAN equipment seemed to be going nowhere. Enterasys did provide a limited site survey and product demonstrations at Cincinnati Inc. After negotiating with Chris Rosen from Enterasys Networks, Enterasys provided enough hardware to add the finishing touches to the end product. Namely, the network installation and testing that included:

- A multi Access Point network installation
- Test and configure the network for optimal performance and roaming clients
- Institute and test security protocol.

8. Proof of Design

In Senior Design III the proof of design was needed to complete the project and consisted of installing and testing an actual wireless network. The network installation included determining which users would be used for network testing, determining the needed coverage area, testing for client roaming and securing the network. After performing the site survey and demonstrating the feasibility of installing a wireless local area network on the shop floor at Cincinnati Incorporated, I then installed and tested the larger wireless network.

The site survey at Cincinnati Incorporated was performed using Cisco Aironet wireless hardware. The Cisco hardware was also used to test the feasibility of installing a wireless network and to demonstrate a limited wireless network. To more fully test a wireless implementation, Enterasys Networks provided me with enough hardware to evaluate the usefulness and functionality of a wireless network over a period of three months.

8.1 Network Installation and Testing

The installation of the network began with configuring the laptops for use on the shop floor, determining the personnel that would be testing the wireless network, then locating and installing the Access Points (AP). Testing the network consisted of performing another site survey to determine the best location of the APs for the test network, monitoring network traffic and uptime over a longer period of time and logging user comments of the wireless network. Due to the short time that the evaluation hardware is to be installed at Cincinnati Incorporated, securing the network was a matter of limiting access to the company network from the shop floor and physically securing the hardware. To test the security requirements of an actual enterprise wireless deployment, I installed Windows 2000 Advanced Server on a laptop and used it to implement various security protocols. The security protocols implemented were:

- IEEE 802.1x
- SSL/TLS Security Authentication
- Public Key Infrastructure
- Rapid Re-Keying

The following report focuses on deployment and monitoring of the Enterasys wireless network, implementation and testing of various WI-FI security protocols, discussion of emerging wireless tools for the manufacturing sector and a final cost/benefit analysis of the wireless LAN vs. a TLAN in a manufacturing environment.

8.1.1 Determining the Coverage Area and Users

For testing the installation of the wireless network, I chose to deploy wireless laptops to shop personnel that fit specific requirements:

1) They have a use for a mobile computing platform
2) They have a need to access MAC-PAC or the OCE CAD drawing software
3) They could physically secure the laptops
4) They were located within the proposed wireless coverage area

The personnel I chose consisted of the maintenance supervisor, Quality Control manager, stockroom manager and the laser assembly manager. Keith, the maintenance supervisor, already uses a laptop in his day-to-day functions. The applications he needed access to included email and web surfing. This made Keith more of a power user and an excellent source of network performance and coverage area monitoring. Keith also had an office to lock up and recharge his laptop each evening. Keith's office was located in an area that is on the fringe of the AP coverage and was useful in showing that a wireless network could provide entire shop floor coverage, including offices. John, in quality control, often uses MAC-PAC functions for logging work done, inspection results and cycle count adjustments for any parts he may have to scrap. John is centrally located within the wireless coverage area and does not need a roaming platform, but he can lock up the laptop each night along with the rest of his inspection tools. Fred, Stockroom facilitator, has no need of CAD files, however, his day is spent tracking and stocking parts in several stockroom locations. Fred represents a roaming user with a need to access MAC-PAC in places that will present coverage problems for a wireless network. Tom, Laser Assembly supervisor, will need the laptop for accessing and displaying engineering drawings on the shop floor. Tom is now able to show his assemblers current drawings in a format that can be enlarged for viewing small details. All these users were chosen for specific attributes concerning their use of the laptops, and their ability to secure them. They were also willing to carefully monitor network coverage and performance.

8.2 Securing the Network

The reason for an improved network is to supply the shop floor with more reliable access to the Materials and Planning Requirements AS-400 database (MAC-PAC) and access to electronic CAD files.

8.2.1 Wired Equivalency Protocol

By their very nature, wireless networks must broadcast their existence to the world with data frames, called beacons. These beacons contain information about the MAC address of the transmitting AP and the network name also called the SSID or the service set identifier. The challenge is to keep the data that is being broadcast from being passively collected, keep rogue access points and clients from disrupting communication channels and keep hackers from actively accessing the company network.

WEP or the wired equivalent Privacy standard is the standard method for securing wireless networks. WEP uses an encryption key, based on an RC4 algorithm, to protect the data being sent across the network. The way it works, the AP transmits a challenge beacon to a client. The client encrypts the challenge with an encryption key that is shared by both the AP and the client. The client then resends the beacon in encrypted form, if the AP decrypts the key successfully, then communication can take place between the client and AP. This is known as "shared key authentication." An AP that uses a specific WEP key cannot communicate with a client that does not have this key, and the client cannot gain access to the AP or the network behind it. The original WEP standard uses 40-bit encryption, but most vendors now offer 128-bit encryption to offer more secure data transmission.

8.2.2 Why WEP Won't Work

Security experts have already determined that the WEP standard is easily compromised. Various network analyzer tools such as *Netstumbler* and *Airsnort* are available to "sniff" out wireless network information. MAC addresses and SSID's that are broadcast by a WEP based network can be detected to directly access the network or "spoof," or imitate, the client or AP. WEP authentication is only a one way transaction. That is, the AP only verifies that the client has the correct key, the client does not verify the AP is a valid AP. Wireless networks are vulnerable to active and passive attacks. Some of these types of attacks are:

- Client Impersonation – A MAC address is stolen or "spoofed" and used to authenticate intruders
- Access Point Impersonation – A rogue access point diverts legitimate users
- Undetected Modification of Data – Once the encryption key is compromised, data being sent can be stolen or modified.
- Denial of Service – Association/disassociation messages are unencrypted and can be forged to disassociate legitimate clients

Another drawback to WEP encryption is that the encryption key is static, and for network administrators to change the keys they must physically or electronically 'touch' each AP and client.

8.2.3 802.1x Security Protocol

Recognizing that the WEP protocol has limitations, the IEEE has adopted 802.1x as the standard for authentication on wireless networks. 802.1x couples WEP encryption with mutual authentication between a client and an authentication server. Man-in-the-middle attacks occur when authentication messages between the client and AP are intercepted to gain access to network resources or to derive information about the network and users.(3) With 802.1x mutual authentication, only legitimate clients can access with legitimate APs. A client requesting access to the network first challenges the AP for credentials, which can only be given if that particular AP has the authority to communicate with a trusted certificate authority or RADIUS server that owns those credentials (figure 10)

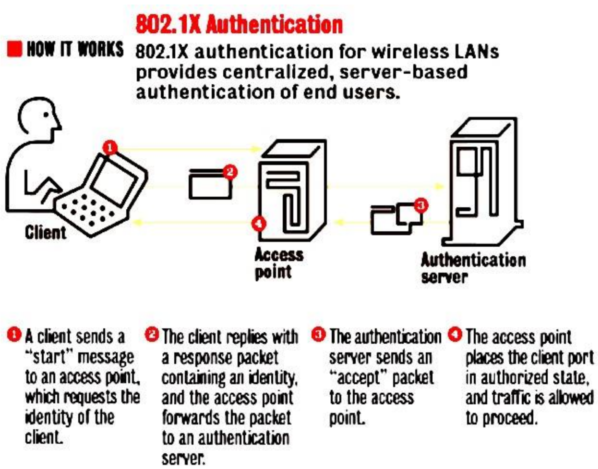

Figure 11: How 802.1x authentication works.

802.1x authentication coupled with WEP encryption allows for mutual authentication of the client and AP. Through WEP, a client computer will request communication with an AP only if they share the same WEP encryption key and SSID. The AP will only communicate with those clients whose MAC addresses are specifically listed in the AP's MAC address filter. Once the client authentication has occurred will the client ask the AP for its credentials. The AP will request those credentials, in the form of certificates, from a RADIUS server on the network. If the Access Point is listed in the RADIUS server's list of valid addresses, credentials will be given to the AP to pass on to the client. Once these credentials are passed onto the client, the client can communicate directly with the network. If a hacker were to identify the SSID and spoof a client or AP MAC address, communication would still not be possible with the network because the that client or AP would not posses the credentials, in the, form of certificates, to access the authentication server. 802.1x specifies a generic EAP or Extensible Authentication Protocol to be used. EAP can take several forms:

- MD5 – Challenge –based password, one-way authentication
- TLS – Certificate-based two-way, mutual authentication
- TTLS – Server authentication via certificates, client via another method

8.3 Implementing Network Security

Since I was installing the wireless network as part of an established corporate network, I was responsible for securing the wireless network, without actually accessing the corporate network itself. In other words, the IS department was not going to allow me access to their servers to implement 802.1x-type authentication. Securing the wireless network, took three forms: The first was physical, making sure laptops would be locked up each night and that APs were located in positions that were difficult to access. The second aspect of security was to limit access from the shop floor to only those resources that were specifically needed. To do this, I implemented security policies on each laptop that would prevent users from accessing denied resources. Policies were implemented through Group Policy. The goal was to allow users access to two buttons: One for MAC-PAC, and one for the OCE Electronic Job Ticket (EJT) where CAD files could be viewed. The third aspect was to secure the wireless network from being hacked into.

8.3.1 Physical Security

Physically securing network resources meant protecting hardware from theft and damage. The Access Points are inherently difficult to access by their very nature. To achieve the best coverage area, the APs were located above the shop floor along the rafters. These locations made theft difficult, but clearance for the AP when the overhead cranes passed by needed to be addressed to prevent damage to the APs and range extender antennas. Securing the laptops and the wireless nics within them was my top priority. Stealing a nic would make accessing the corporate network much easier. To secure the laptops I only distributed them to users that could physically lock the laptops in desks or closets after using them.

8.3.2 Securing User Access to Network Resources

The keys to providing a secure network is to make sure users have access to allowed resources, and are denied access to disallowed resources. To accomplish this on the Windows 98 platforms, I used the *Poledit.exe* policy editor tool. To use this tool, I created a user, SFUSER, on the local computer. I then logged in as SFUSER, ran the *poledit* utility and set the user restrictions as necessary for the local user. For example, to restrict the users from being able to browse the network I removed access to Windows Explorer, removed all menus from the Start menu and reconfigured the ‘F5’ key (typically set to Find) to run only the MAC-PAC program. I set the wallpaper to the official Cincinnati Incorporated wallpaper and put two icons on the Start Menu task bar.

One icon ran the MAC-PAC utility the other was a direct link to the EJT site on the company Intranet.

For Windows 2000 and XP platform clients, I used Group Policy and the *GPEDIT.MSC* utility to limit users access. The use of *GPEDIT.MSC* is similar the *poledit* utility. To use, click Start, Run then type in *gpedit.msc.* The Group Policy console will appear. There are two main branches, User Configuration and Computer Configuration. Changes made to the User Configuration only affect the current user, changes to the Computer Configuration apply to the computer and affect all users on that computer. To control access to Start Menu and Desktop items I went to User\ configuration\ Administrative\Templates\Start Menu and Taskbar or User\configuration\Administrative\ Templates\ Desktop and set the items I wanted (Figure 11).

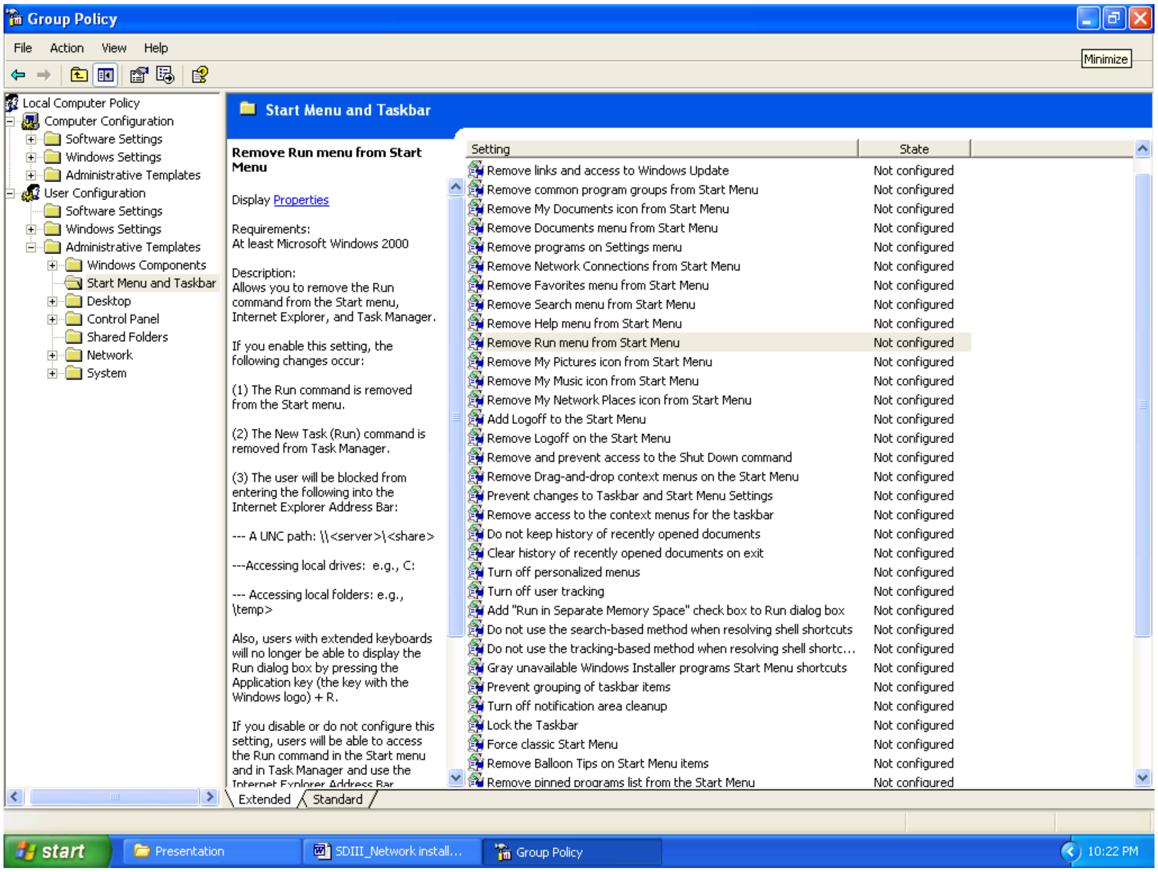

Figure 12: Group policy steps and screen shots

Implementing group policy on each machine secured the network from internal attacks and abuse.

8.3.3 Securing the Air Waves

To secure the WLAN from detection through the use of common wireless network sniffing tools, I used the AP and Client Manager utilities that come with the Enterasys RoamAbout wireless products. The first step was to prevent the SSID or network name from being broadcast. Start the AP Manager utilities used to configure the Access Points, select the list of Access Points to be configured then select the *Wireless Parameters* tab. From this location various wireless parameters can be set, to prevent the

Wireless Network Name or SSID from being broadcast I set **Secure Access** to *enabled* (Figure 12).

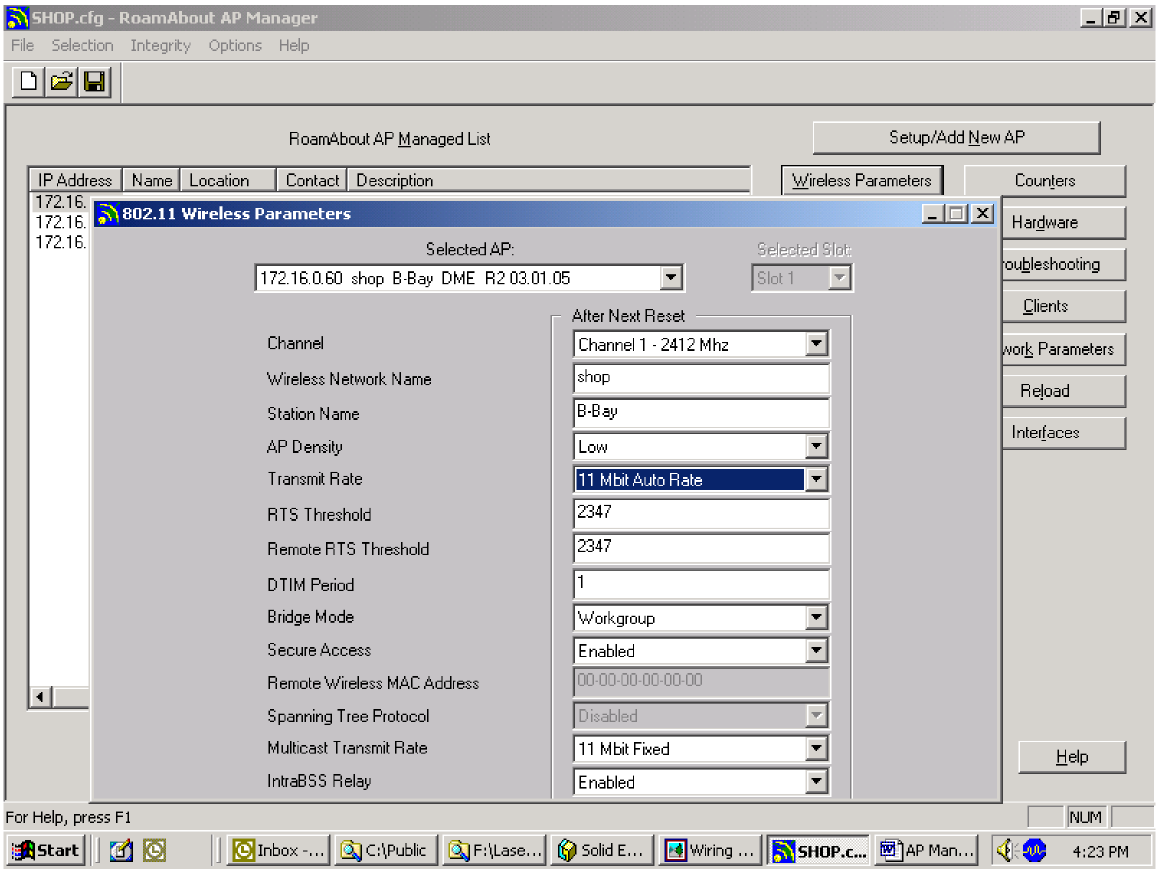

Figure 13: AP Manager wireless parameters

To prevent just anyone from walking into the factory and being able to access the wireless network with any wireless nic, I only allowed clients with specific MAC addresses to associate with each AP. The *Filtering* tab in the AP Manager lists allowed or disallowed MAC addresses (Figure 13).

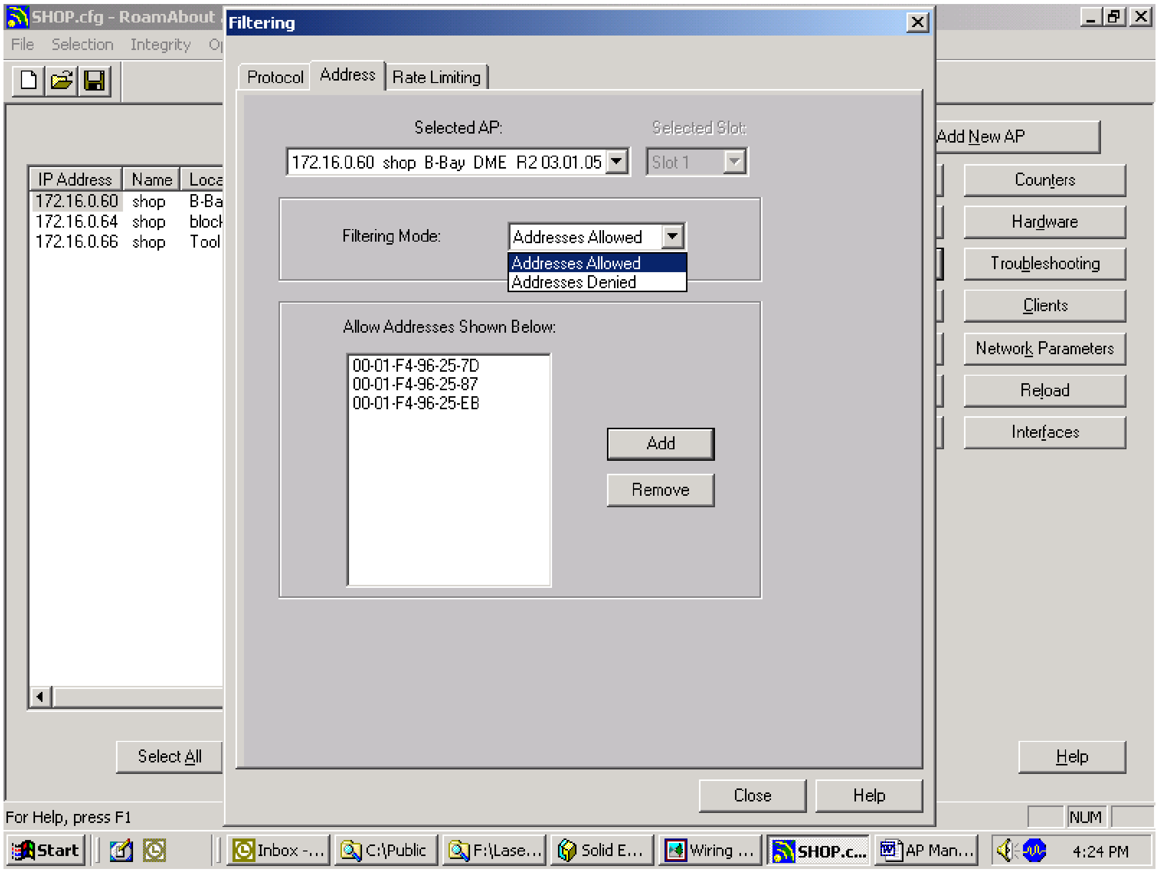

Figure 14: MAC address filtering

To prevent passive monitoring of network traffic, and to verify authentication of the clients I implemented 128-bit key encryption. The AP and Client can each list four (4) encryption keys that can be used to encrypt and transmit or decrypt and receive data. As long as the list on the AP matches the list on the client exactly, the two will be able to associate. Any deviation in any one of these keys will end communication (Figure 14).

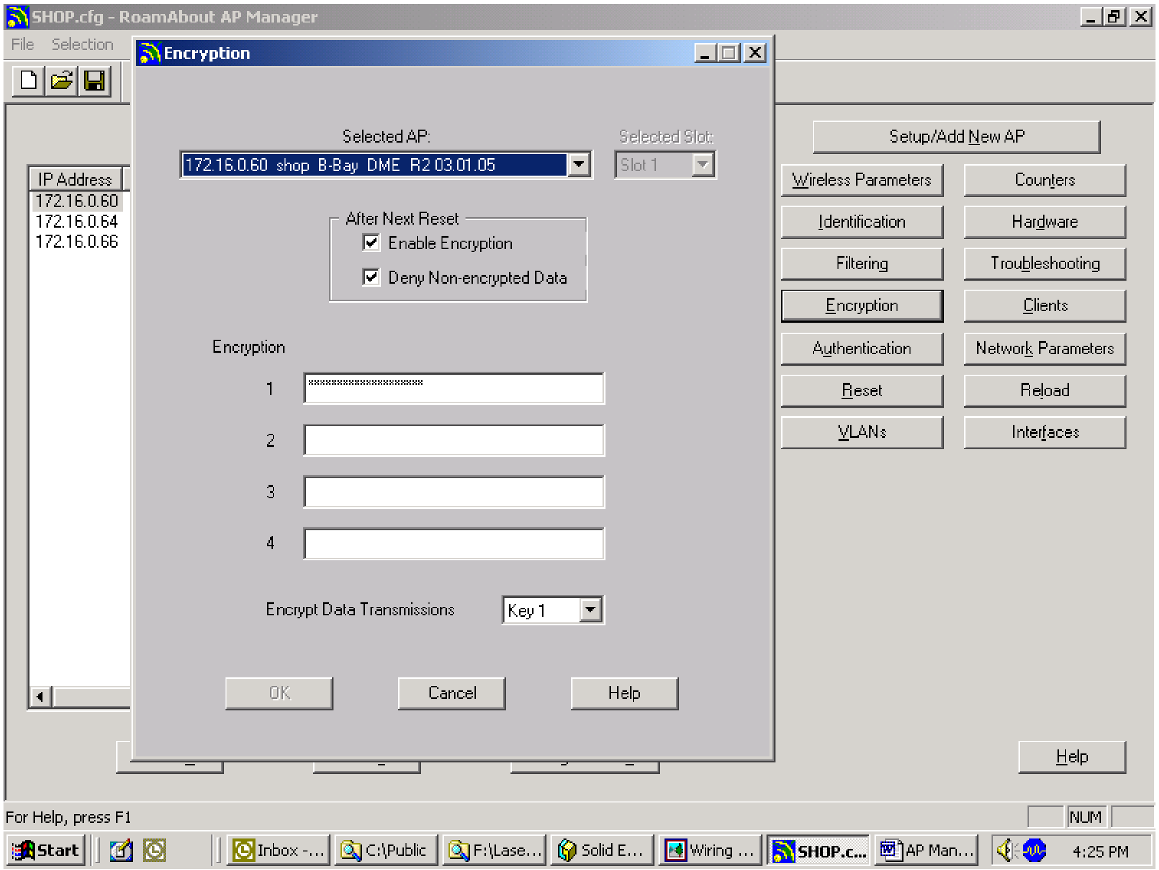

Figure 15: Enterasys AP Manager encryption key settings

Once the AP was configured I had to configure each client computer. The RoamAbout client utility required that the Network Name be entered into the client adapter and then on the Security page the same 128 bit encryption keys were entered as on the AP. Any one of the four keys can be used for encrypting data, as long as they match exactly what the AP has listed (Figure 15)

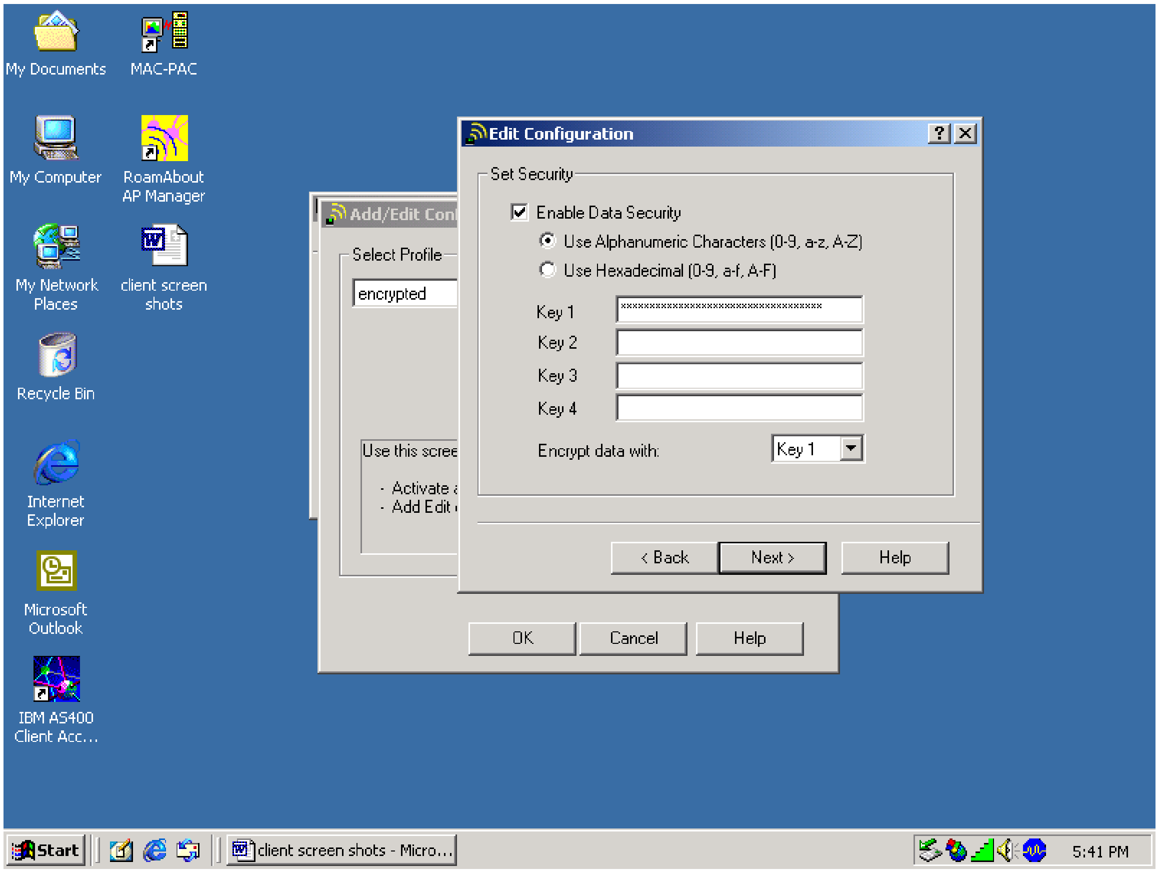

Figure 16: Enterasys client utility encryption screen

9. Testing the Network

Once the network was installed I tested various aspects of the wireless network. Testing took the form of performing another site survey to verify and record AP coverage, testing the network security I had implemented, tracking usage of the network and recording user feedback.

9.1 Wireless network coverage

After installing the APs on the manufacturing floor, I used the Enterasys site survey tools to record the actual coverage area of the wireless network. The site survey was conducted in the same fashion as the earlier site survey. I walked around the shop with a floor layout and marked the areas where the wireless connection was poor or unreliable. I also listed the areas of the shop where roaming from one AP to another took place (Figure 16).

9.2 Network security Testing

To test the security settings, I first used another client computer to verify that the encryption keys were working. By changing the user parameters from encrypted to unencrypted, I would associate and disassociate from the wireless network accordingly. When I removed the client MAC address from the MAC address filter of the one of the APs, I was unable to log back onto the network until I moved into the range of an AP that had the client MAC address listed within its filter list.

The next step was to employ "NetStumbler" wireless network analysis tool to try to determine network information. When I installed NetStumbler on a client computer without any security parameters set, all the network information was readily viewable, including MAC addresses of all active clients and APs, the SSID, the channels the access points were broadcasting on and the type of hardware being used. On the locked down network, NetStumbler was able to detect the AP hardware type, channels that the APs were broadcasting on and the type of encryption being used. However, with *Secure Access* enabled the SSID of the network was not available. The AP MAC addresses were no longer detectable and no other clients were listed. It is interesting to note that when I implemented 802.1x security protocols on a test network, the Network Stumbler application was not able to register the type of encryption being used. This may be because the 802.1x protocol employs multiple security strategies to thwart would be hackers.

The next test was to verify that no other wireless laptops brought into the shop could access the network. Professor Stockman provided his laptop for this test. Upon arrival within the coverage area, the visiting laptop did not detect the wireless network signal until encryption was removed from the AP. Even then, the SSID of the network was not being broadcast to the visitor's computer. Not until I listed the MAC address of the visiting computer into the filter lists of the APs was the SSID broadcast to the visiting computer and access to the network granted.

10. Cost/Benefit Analysis of WLAN vs. TLAN

The total cost of a network deployment includes life-of-network costs associated with upgrades or expansions to the network. The following sections compare and contrast the benefits of each topology and expand on the future of Wireless Local Area Networks.

10.1 Pros and Cons of the TLAN

The benefits of the wired Ethernet are its proven reliability and virtually unlimited throughput. For Cincinnati Incorporated extending the corporate Ethernet is only a matter of tapping into the fiber optic Ethernet backbone that already exists in the shop and extending its reach via CAT5 cable, or where necessary, fiber optic cable. Extending the tethered LAN requires no additional management tools and provides the bandwidth necessary to handle even the most demanding applications.

The drawbacks to a TLAN are its inflexibility, the expense associated with running Ethernet cable and the additional hardware needed for extending the Ethernet to remote shop locations. Every time a new client terminal or PC enabled machine tool is installed or moved, the cable must move with it thereby incurring the wiring cost again. Running Ethernet cable down to and across the shop floor exposes the cable to damage and increased bandwidth loss due to higher RF interference. Access to network resources is as easy as plugging into an available RJ45 wall jack.

10.2 Pros and Cons of the WLAN

Extending the existing Ethernet backbone by installing a wireless LAN opens up new opportunities to employ the ever-increasing tools available for mobile computing. The benefits of a WLAN are:

- Fast and Easy to install
- Mobility
- Scalable
- Flexibility

For Cincinnati Incorporated, installing the APs means mounting the APs in rafters that are secure from unintentional damage, require shorter wiring runs and are easily accessible. Installing a wireless LAN opens the network to the use of PDAs, hand held inventory tracking and control devices and wireless sensors for remote monitoring. A WLAN is scalable meaning additional clients can be easily added to the network or additional bandwidth can be provided by adding additional access points. No longer will network resources be locked in a room or on the other side of the building, with wireless computing personal computers and printers can be placed anywhere within the coverage area. The drawbacks to installing a WLAN are:

- Limited bandwidth
- Inherent security risks
- Difficulty of management
- High initial installation costs.

Additional management tools are needed to secure and manage the wireless network. Without centralized management software, each AP or client may need to be physically accessed by a network administrator when new firmware upgrades are needed or problems arise. An additional authentication server is needed to implement 802.1x security protocols. The initial cost of the wireless hardware may exceed the cost of the initial installation of its tethered counterpart.

10.3 Obstacle to installing a WLAN in a manufacturing environment

Known obstacles to installing WLANs in manufacturing environments include:

- Material and supply racks cause multi-path interference
- High levels of electromagnetic and RF interference
- Limited bandwidth

Metal, tinted windows, cardboard and even people can all have some affect on signal power. High concentrations of metal racks can cause signals to be slowed or accelerated and cause 'dead spots' in coverage areas. Microwave ovens, 2.4 GHz portable phones and poorly maintained electrical equipment can all add to RF interference and signal degradation. Wireless is a shared medium, not switched. Bandwidth diminishes as the number of users increase. High bandwidth intensive applications can significantly degrade the effectiveness of WLANs.

10.4 Mitigating WLAN installation obstacles at Cincinnati Incorporated

The layout of the manufacturing floor at Cincinnati Incorporated allows for the placement of the APs, in most bays, to be placed over forty feet into the rafters of the ceiling. The higher an AP is placed, the greater its coverage area. The bays are expansive and the signals bouncing off of metal structures were found to actually accelerate the signals, effectively increasing the coverage areas. By strategically placing APs in areas that are in line with equipment rack aisles, I was able to provide coverage to stock rooms and equipment rack areas. By monitoring the RF noise levels of the manufacturing floor over a period of eight months, I determined that the actual RF noise levels within the shop are rather low. The difference in RF noise levels between peak and off-peak production hours was minimal. By placing the AP in locations that balance the client usage amongst several access points, bandwidth can easily be shared by many users. The rule of thumb for clients per AP is twenty. In only one area of the shop did I exceed ten users per AP. The types of applications that will be used over the wireless network are small; transferring cnc programs and viewing PDF files are typical.

10.5 Potential Return on Investment of the WLAN

The total cost of a network deployment includes life-of-network costs associated with upgrades or expansions. One of the benefits of a WLAN is the ease with which future growth or changes to the network can be implemented. Potential growth of and changes to the network may justify the higher initial cost of installing a wireless network rather than a tethered network. Changes to the network may include:

- Upgrades to machine tools with PC controls and TCP/IP connectivity
- Hand held inventory control devices
- Parts tracking through the shop using existing bar code technology already in place
- Remote testing and diagnostics for manufacturing equipment and production machine on the assembly floor.
- Addition of new machine tools or relocation of factory assets.

In a white paper released by Cisco Systems titled, “Wireless LAN Benefits study” (Conducted by NOP World-Technology on behalf of Cisco Systems, Fall 2001) pointed to two major benefits of WLANs. The first was cost savings associated with installation and flexibility. These included costs associated with:

- Cabling costs
- Flexibility for adds, moves
- Labor costs for adds, moves
- Reduction in time to set-up and install
- Reduced support and maintenance time

The next benefit of the WLAN was increased productivity due to:

- Mobility within buildings
- Convenience (no need to plug in)
- Time savings
- Improved accuracy, reducing errors by replacing paper with digital

The conclusion of the report, based on input from corporations where WLANs were installed or being tested, was that, on average the financial benefit of installing a WLAN was $450.00 per user, per year.

Another benefit of a wireless network is the growing number of tools available for wireless connectivity. These tools include PLCs for remote monitoring of machines, processes and adverse environments. PDAs and handheld barcode readers will replace the count and log stock tracking procedures that are currently in place.

11. Conclusions

The network installation went well. The feedback I received was positive. The shop floor managers using the network were excited about being part of cutting edge technology. They were eager to get new tools to help increase their productivity. Keith, the maintenance supervisor I used as a test subject is all for the wireless network. He is responsible for wiring new terminals and maintaining the Ethernet infrastructure. Pulling cable for new client installations is difficult. The time and manpower needed to run Ethernet cables saps resources away from his main task of maintaining the company infrastructure and machinery. Information Services realized gains in productivity also. To add the wireless clients to the network Duane, the network administrator, configured the client laptops at his desk in between other tasks. He then handed the laptops to me to install the wireless nics and give the laptop to the users. There was no need to carry entire desktop workstations to the users, attach them to the network and configure them there. A suggestion was made that he could configure several laptops and have them in his office. Whenever a new client computer was needed on the shop floor, he could just hand the user a laptop, wireless nic and a power cord.

To satisfy the deliverables of this project I used a shop floor layout to create 3-D models of the shop. These models I used to illustrate possible sources of RF interference, position the APs for optimal performance and coverage, and layout measured wiring diagrams for both the TLAN and WLAN. I performed a wireless site survey and set up a working prototype to demonstrate the feasibility of installing a wireless network on the manufacturing floor. I then installed a multi-user, multi-access point wireless network and monitored that network over an extended period of time. I monitored the network for performance and any unforeseen problems that may occur with a wireless network. I implemented WEP based security on the network and group policy based security on the client computers. I set-up a small server-based network to implement 802.1x security protocols and tested the effectiveness of 802.1x security against various network analyzer tools such as NetStumbler. I provided a Bill of Materials for each topology and multiple wireless vendors. I compared the pros and cons of a WLAN vs. a TLAN so that IS could make an informed decision about the best way to extend Ethernet connectivity to the shop floor. Finally, I reported on future uses of the wireless network and the potential return on investment.

There were five considerations required of a networking project. These were:

1. To combine some aspects of networking I, II, III
2. Learn some kind of new technology
3. Problem should be real world
4. Could solve a problem existing in a current network
5. Show depth as well as breadth of networking techniques

I fulfilled these considerations by:

a) Setting up Windows 2000 Server with DNS, DHCP, Active Directory and Certificate Authority for the 802.1x test platform. I also used group policy for instituting local user settings on the client computers.
b) I fully explored the concept of Wireless LANs.
c) This project was actually implemented at Cincinnati Incorporated and used to determine the best way of extending the enterprise network to the manufacturing floor.

d) I provided a cost efficient alternative to a Tethered LAN.

e) I showed a breadth of networking techniques by administering APs and clients across the network. I implemented various physical and network security policies. I installed the wireless network hardware. This included the access points, hubs, power injectors and I made up and installed all my own cable runs.

Recommendations

There are several recommendations I would like to make to anyone considering a network project. The first is to fully explore sources of funding for the network project prior to delving into it and be flexible in the initial proposal. Network projects can be hardware intensive and therefore expensive. When funding for this project was pulled I spent months trying to find new sources of funding.

The next recommendation I would make is to be proactive and flexible in scheduling. Networking projects typically involve a lot of other people: such as network administrators and the network users. My schedule depended very much upon the schedules of a diverse group of other people. I spent a lot of early morning, late nights and weekends on the manufacturing floor installing, testing and managing the network. Along these same lines, I recommend scheduling and preparing for the learning curve. New technologies can take time to research and learn. There were a lot of stops and starts associated with learning each vendor's hardware and software and implementing new security techniques. I also strongly recommend using corporate sponsors. They can be an invaluable source of guidance and resources.

Appendix A.

Project Budget

Budget

Budget Man hours	Site Survey	Cost Analysis	Installation
Foot work	40		80
Desk Work	44	48	12

Equipment Cost	Qty.	Unit Cost	Total
Laptop Computer	4	$ 1,400.00	$ 5,600.00
Enterasys R2 RoamAbout Access point	3	$ 1,200.00	$ 3,600.00
Add Mezzanine card	3	$ 250.00	$ 750.00
R2 11 Mb PCMCIA client adapter	3	$ 250.00	$ 750.00
R2 54 Mb PCMCIA client adapter	3	$ 375.00	$ 1,125.00
Cisco Site survey Kit		$ 1,500.00	$ 1,500.00
Desktop Computer and monitor		$ 1,500.00	$ 1,500.00
200' patch cord w/RJ-45 connectors		$ 36.00	$ 36.00
8' patch cords w/RJ-45 connectors	2	$ 5.00	$ 10.00
Netgear 8-port hub	2	$ 180.00	$ 360.00
Other Costs:			
1 seat Solid Edge CAD software		$ 7,000.00	$ 7,000.00
Budget totals:			$ 22,231.00
Total man hours		224 hours	

Hardware components are to be supplied by Cincinnati Inc, Protocol Communications and Enterasys Networks.

Appendix B.

Project Timeline

Time Line

Project	
Shop Floor Layout	Sept. 22, 2002 - Dec. 8, 2002
Preliminary layout of WLAN	Nov. 10, 2002 - Dec. 15 2002
Preliminary Layout of TLAN	Nov. 10, 2002 - Dec. 15 2002
Preliminary Cost of each topology	Dec. 8, 2002 - Jan. 19, 2003
Site survey - Build Prototype	Feb. 10, 2003 - Feb. 24, 2003
Re-calculation of WLAN cost based on site survey results	Feb. 24, 2003 - Feb. 27, 2003
Set-up 2000 server for demonstrating network	Mar. 28, 2003 – April 10
Receive wireless equipment from Enterasys	April 15, 2003
Installation of terminals, network verification	April 15, 2003 - June 8, 2003
Demonstrate wireless project at Tech Expo	May 15-16, 2003
School	
Problem Description	Sept. 22, 2003
First Meeting	Oct. 7, 2002
First draft of Proposal	Oct. 27, 2002 - Nov. 11, 2002
2nd Meeting	Nov. 14, 2002
Timeline	Oct. 29, 2002 - Feb. 20, 2003
Budget	Oct. 13, 2003 - Feb. 20, 2003
Final draft of Proposal	Nov. 24, 2002 - Dec. 8, 2002
PowerPoint Presentation	Dec. 15, 2002
Q2	
Draft of Project Description, Use and User Profile	Jan. 30, 2003
Progress Report 1	Feb. 6, 2003
Draft of Design Freeze	Feb. 19, 2003
Deliverables	Feb. 19, 2003
Progress Report 2	Mar. 6, 2003
Design Freeze	Mar. 13, 2003
Design Freeze Presentation	Mar.20, 2003
Final Presentation	05-Jun-03

Appendix C.

Bill of Materials: Enterasys Networks

Enterasys Networks

Product	Qty	Description	Unit Price	Extended Price
RBTR2-AZ	11	RoamAbout AP w/mezzanine slot	$ 1,249.00	$ 13,739.00
CSIES_AB 350	11	Cable Kit	$ 175.00	$ 1,925.00
CSIES_AB C50	11	Range Extender Antenna	$ 85.00	$ 935.00
CSIBD-AA-128	11	802.11b NIC W/128 BIT encryption	$ 80.00	$ 880.00
CSIBD-PC-128	40	802.11b PC adapter W/128 BIT encryp.	$ 280.00	$ 11,200.00
Installation	11	Includes labor and hardware	$ 400.00	$ 4,400.00
Total Installation cost				$ 33,079.00
With additional .11a cards				
RBTR2-AZ	11	RoamAbout AP w/mezzanine slot	$ 1,249.00	$ 13,739.00
CSIES_AB 350	11	Cable Kit	$ 175.00	$ 1,925.00
CSIES_AB C50	11	Range Extender Antenna	$ 85.00	$ 935.00
CSIBD-AA-128	11	802.11b NIC W/128 BIT encryption	$ 80.00	$ 880.00
RBTBF-AX	11	802.11a NIC W/128 BIT encryption	$ 190.00	$ 2,090.00
CSIBD-PC-128	20	802.11b PC adapter W/128 BIT encrypt.	$ 280.00	$ 5,600.00
CSIBD-PC-128	20	802.11a PC adapter W/128 BIT encrypt.	$ 480.00	$ 9,600.00
Installation	11	Includes labor and hardware	$ 400.00	$ 4,400.00
Total Installation cost				$ 39,169.00

Appendix D.

Bill of Materials: Cisco Systems

Cisco Systems

Product	Qty	Description	Unit Price	Extended Price
AP352	8	802.11 b wireless Access Point	$ 580.00	$ 4,640.00
AIR-352	40	802.11b NIC W/128 BIT encryption	$ 80.00	$ 3,200.00
AIR-PSINJSYS1200	11	In-line power injector	$ 42.00	$ 462.00
AIR-ANT 4941	16	2.2dbi dipole antennas (included)	$ 0.00	$ 0.00
Installation	8	Includes labor and hardware	$ 400.00	$ 3,200.00
Total Installation costs				$ 11,502.00

Cisco 802.11a

Product	Qty	Description	Unit Price	Extended Price
AIR-1200	10	Dual slot Access Point	$ 890.00	$ 8,900.00
AIR-PCM1200	40	802.11a NIC W/128 BIT encryption	$ 130.00	$ 5,200.00
AIR-PSINJSYS1200	10	In-line power injector	$ 42.00	$ 420.00
AIR-ANT 4941	20	2.2dbi dipole antennas	$ 70.00	$ 1,400.00
Installation	10	Includes labor and hardware	$ 400.00	$ 4,000.00
Total Installation costs				$ 19,920.00

Appendix E.

Bill of Materials: Tethered LAN Installation

Tethered LAN

Product	Description	Qty	Unit Price			
Cable and Installation	Includes cable, manpower and terminus block	23	$	1,000.00	$	23,000.00
3COM Office Connect	8-port Hub	6	$	60.00	$	360.00
3 COM Superstack 3	Switch	1	$	600.00	$	600.00
Total installation Cost					$	23,960.00

Appendix F.

Test Protocols

Test Protocols – working prototype

- Install access point and map coverage and throughput in the coverage area
- Create baseline performance numbers and RF noise during production and non-production hours.
- Map signal to noise ratio, Packet Error Rate (PER), latency due to multi-path affects, and lost packets.
- Document affects of crane operation and other sources of RF interference to network performance.
- Determine how the implementation of various security protocols impacts network performance.
- Emulate live network traffic and document affects on network performance.

Test Protocols – Multi- Access Point Network

- Check for roaming hand-off delay as clients move from one AP to the next.
- Measure efficiency of clients to seek out least busy AP on different channels
- Test network security
- Monitor and log network performance over a period of time

NOTES

[i] A half-duplex data transmission means that data can be transmitted in both directions on a signal carrier, but not at the same time

[ii] Noise level – the amount of RF signals the AP receives when no clients are transmitting a level of RF interference

[iii] Multi-Path interference – the affect of RF signals bouncing off of objects. Signals take more than one path from transmit antenna to another than combine in the receiving antenna to cause signal distortion

References

1. Alexander, Bruce and Snow, Stephen. "Preparing for Wireless LANS Secrets to Successful Wireless Deployment." *Packet Magazine*. April, 2002. 36-40

2. Bourquien, Marilyn. Manager, Information Services Department, Cincinnati Inc. Personal Interview. Oct. 24, 2002.

3. Cisco Systems. "Cisco Aironet Wireless LAN Security Overview." http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm. 03/13/2003.

4. Curran, John. "The Network Computer a.k.a Thin Client." http://www.networkbuyersguide.com/search/306002.htm. 1997

5. Gast, Matthew. *802.11 Wireless Networks: The Definitive Guide*. Sebastopol, Ca. O'Reilly. 2002.