NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

ENTERPRISE IMPLEMENTATIONS OF WIRELESS NETWORK TECHNOLOGIES AT THE NAVAL POSTGRADUATE SCHOOL AND OTHER MILITARY EDUCATIONAL INSTITUTIONS

by

Joseph L. Roth

September 2002

Thesis Advisor:	Don Brutzman
Co-Advisor:	Alex Bordetsky

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2002	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: Enterprise Implementations of Wireless Network Technologies at the Naval Postgraduate School and Other Military Educational Institutions	**5. FUNDING NUMBERS**
6. AUTHOR Joseph L. Roth	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT

The purpose of all information systems is to assist people in transitioning data into information, and then information into knowledge. In order to reach IT modernity, three things need to occur: a convergence of single open platform data exchange (e.g., Extensible Markup Language (XML)), the development of new doctrine to manage this information (e.g., Net Centric Warfare), and the creation of a robust mobile secure network (e.g., 802.11). The heart of this research will focus on the last element.

Future wars will be fought using wireless mobile networks. Wireless research is being realized at the Naval Postgraduate School (NPS) Wireless Warrior Group. The Wireless Warrior Group is designing and implementing the new unclassified wireless network at the NPS using the IEEE 802.11 standard. The Wireless Group was founded by the author of this thesis and is currently made of 150 members consisting of staff, faculty, and students from a variety of different curriculums.

The purpose of Wireless Warrior is to develop the doctrine of wireless networking by making it a part of every student, staff, and faculty daily communication and production. Only through constant scrutiny and use can real solutions emerge. The entire campus becomes a computer lab. Wireless Warrior provides a fertile ground for students to write new applications, to communicate and collaborate in ways unthinkable just a few years ago. Wireless computing does to computers what the cell phone did to the wired telephone. It is an educational and operational force multiplier. Wireless mobility is the future of warfare, and usable, supportable, secure mobile communication is what wins wars. This thesis documents the NPS journey into the wireless domain.

14. SUBJECT TERMS IEEE 802.11; Wireless; Local Area Networks, Educational Network Design	**15. NUMBER OF PAGES** 212
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

ENTERPRISE IMPLEMENTATIONS OF WIRELESS NETWORK TECHNOLOGIES AT THE NAVAL POSTGRADUATE SCHOOL AND OTHER MILITARY EDUCATIONAL INSTITUTIONS

Joseph L. Roth
Lieutenant Commander, United States Navy
B.S., George Washington University, 1992
M.A., University of Maryland, 1997
M.A., Naval War College, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

and

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2002

Author: Joseph L. Roth

Approved by: Don Brutzman
Thesis Advisor

Alex Bordetsky
Co-Advisor

Chris Eagle, Chair
Department of Computer Science

Dan Boger, Chair
Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of all information systems is to assist people in transitioning data into information, and then information into knowledge. In order to reach IT modernity, three things need to occur: a convergence of single open platform data exchange (e.g., Extensible Markup Language (XML)), the development of new doctrine to manage this information (e.g., Net Centric Warfare), and the creation of a robust mobile secure network (e.g., 802.11). The heart of this research will focus on the last element.

Future wars will be fought using wireless mobile networks. Wireless research is being realized at the Naval Postgraduate School (NPS) Wireless Warrior Group. The Wireless Warrior Group is designing and implementing the new unclassified wireless network at the NPS using the IEEE 802.11 standard. The Wireless Group was founded by the author of this thesis and is currently made of 150 members consisting of staff, faculty, and students from a variety of different curriculums.

The purpose of Wireless Warrior is to develop the doctrine of wireless networking by making it a part of every student, staff, and faculty daily communication and production. Only through constant scrutiny and use can real solutions emerge. The entire campus becomes a computer lab. Wireless Warrior provides a fertile ground for students to write new applications, to communicate and collaborate in ways unthinkable just a few years ago. Wireless computing does to computers what the cell phone did to the wired telephone. It is an educational and operational force multiplier. Wireless mobility is the future of warfare, and usable, supportable, secure mobile communication is what wins wars. This thesis documents the NPS journey into the wireless domain.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my advisors, the wireless group, the NPS Staff, NPS Leadership and my fellow students for the opportunity to learn.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. WIRELESS TECHNOLOGIES

The purpose of any network is to provide safe and timely transport of the data and maintain non-repudiation for all data transforms. For wireless technologies to have value they must provide a significant gain over any inheritable, exploitable vulnerability brought in. Information technology is undergoing a revolutionary shift from platform-centric computing to net-centric computing. The Navy is following suit by attempting to re-orient doctrine from platform-centric (ships, aircraft, and submarines) into a net-centric warfare focus. The only way to do this is to be continuously connected to the network to especially include highly mobile users. The focus of this thesis is to show the proper strategy on how to incorporate 802.11 wireless technologies into the Navy's notion of Net Centric Warfare, FORCEnet [1].

> FORCEnet is the architecture and building blocks of sensors, networks, decision aids, weapons, warriors, and supporting systems integrated into a highly adaptive, human-centric, comprehensive system that operates from seabed to space, from sea to land. By exploiting existing and emerging technologies, FORCEnet enables dispersed human decision-makers to leverage military capabilities to achieve dominance across the entire mission landscape with joint, allied, and coalition partners.

The goal of FORCEnet and net-centric warfare is much more than a technology enhancement. It is a mindset in which one is continuously connected to the network at high speeds. The best place to develop this doctrine is by practicing it everyday through low cost wireless technologies at the Naval Postgraduate School, the Navy's premier educational research institution. This chapter explores the relationships between wired and wireless technologies, general perception of wireless capabilities with in industry, and sets the framework for the following chapters.

Before one can understand wireless networking one must first understand wired networking. The fundamental models of networks are the OSI, DOD, and TCP/IP models. In May, 1974, the Institute of Electrical and Electronic Engineers (IEEE) published a paper titled "A Protocol for Packet Network Interconnection." The paper's authors -- Vinton Cerf and Robert Kahn -- described a protocol called "TCP" that incorporated both connection-oriented and datagram services [2]. This became the foundation for the TCP/IP and DOD models. The Open System Interconnection (OSI) Model was established in 1983 through the International Organization of Standards (ISO). The diagram below in Figure 1.1 shows how they all relate to each other

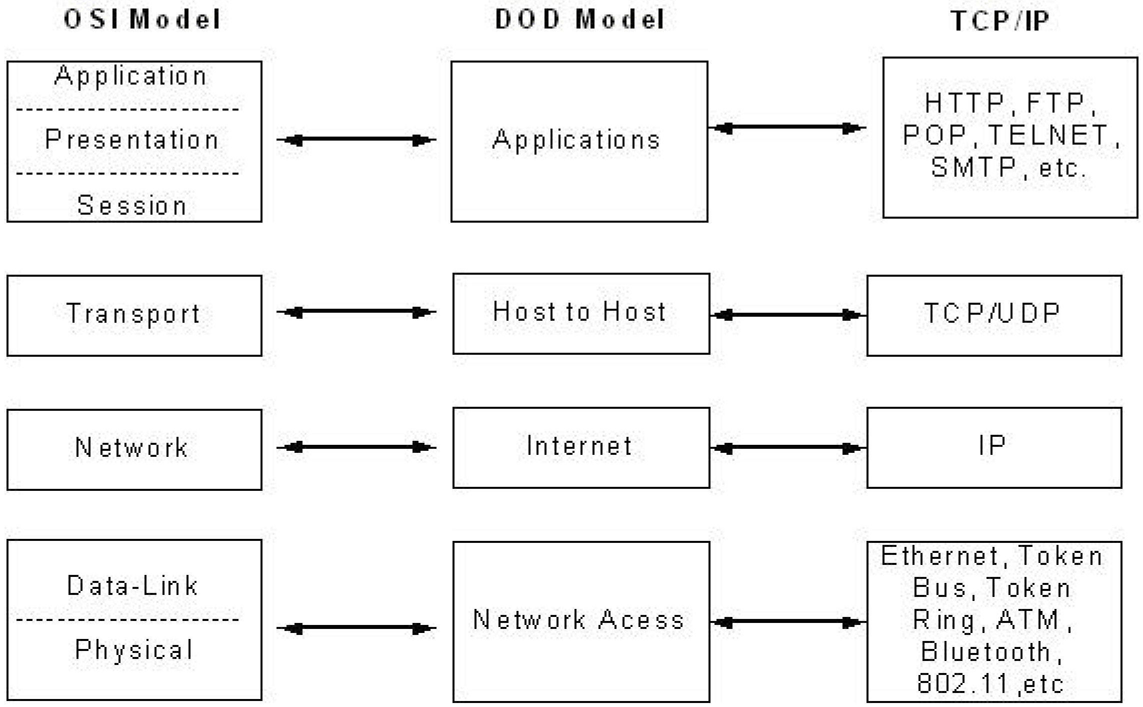


Figure 1.1. OSI/DOD/TCP/IP Model Relation Diagram.

The DOD and TCP/IP models have four layers while the OSI model has seven. The TCP/IP is what is used in industry. The OSI model is more descriptive having more layers, is used in academic settings, and is often called the reference model. Each layer is oblivious to the exact technologies used as long as the proper interface standards are maintained. This process is called layer encapsulation. This means that the application which is part of the process layer does not care what kind of network it is using. It may be wired or wireless. Conversely the Network Access Layer does not care which application is running. The advantage of this model is that as technologies improve different layers can be easily updated due the modularized structure. IEEE 802.11 wireless technology can be substituted for IEEE 802.3 Ethernet wired technology.

To understand the structure of the communication medium is the key to maximize its capability and to focus on defending its weakest areas. This concept of modularization is often counterintuitive to the end user. Users tend to think in terms of entire systems and often incorrectly focus efforts on trying to solve the wrong problems. An example of this might be a system showing a symptom of slow response time. The problem may lie in a poorly written application. It may lie in the fact that the internet was temporarily congested, or it might be that the system was configured improperly. In either case the user does not think in terms of system layers and may focus blame in the wrong area. When a layer is replaced with a new technology and there are problems, often the wrong lessons are learned.

There is a common joke that there are two additional layers in the DOD model that sit on top of the application layer. These layers are the Political and the Budgetary layers. What this means is that system design is based on three areas technological, political, and budgetary. This also means that technological decisions are not always made based on the best technological solutions. Perception is everything. Here is a list of common misconceptions in favor and against the use of 802.11 wireless technologies.

- Wireless will solve all wired problems
- Data rates will be maintained irregardless of location and scale
- Wireless Free Net movements will cause installation costs to approach zero
- One should shun all things wireless because of the wireless security vulnerabilities
- Wireless has no real value beyond its initial toy snake oil attraction.

The effect of these misconceptions in the military is that on the one hand operators will have false expectations of a Star Trek capability without properly understanding the costs associated with building, developing and maintaining the infrastructure. Line communities tend to want more and more capabilities without looking into possible negative externalities of security and support. The military staff and support communities tend to focus more in the opposite direction where, often due to budget constraints and poor manning levels, they tend to see no personal advantage in adopting a new technology. They often feel they will be blamed for any security breaches introduced by the technology as well as forced to work long hours to support a capability they do not see value in. The proper path lies between these polarized views.

The truth is that 802.11 wireless is an augmentation technology, not a replacement technology. It can add connectivity to areas where wired technologies cannot be used due to cost or geographic infrastructure infeasibility. Wireless 802.11 data technology has the potential to be a force multiplier due to its potential capability coupled with commercial availability and low cost. The value validation for the military can easily be found in the commercial and academic sectors.

For the last 15 years, the commercial sector has invested and received significant ROI (Return On Investment) using wireless technologies for the vertical markets of inventory management and retail price marking. With the improvement and acceptance of IEEE 802.11 open standards, costs have dropped drastically making this technology look extremely attractive at a low cost. One may ask if you have a well wired LAN, why would one want a wireless LAN? Even if it is so cheap, what is the added value of wireless? Bob Metcalfe, the founder of 3Com corporation and the inventor of Ethernet, the ubiquitous networking protocol, stated that the value of the network is equal to the square of the number of nodes [3]. The more nodes a network has the more value it is worth. What wireless brings is not only a significant increase in the number of nodes but mobility.

A more comprehensive equation would show that the value of the network is equal to the square of static nodes plus the cube of the mobile nodes.

$$\mathbf{V = N_s^2 + N_m^k} \qquad \mathbf{(1.1)}$$

where

V= Value of the Network

N_s = the number of static nodes

N_m = the number of mobile nodes

$k > 2$.

A perfect example of this is the telephone (first assume k =3). When the first telephone connection with its infrastructure was built, it had a limited value because it provided a single fixed point-to-point communication. But after the 100th telephone connection with its related infrastructure was built, it had more than 100 times the value than the first. It did not provide just 100 point-to-point connections, it provided 10,000. Now if we add mobility into this equation one would only need roughly 21 mobile phones to have the same value of 100 non-mobile phones for the same rough value of 10,000 connection, i.e., $21^3 \approx 100^2 \approx 10{,}000$. It is recommended that further thesis research be performed in defining network value and providing a rigorous proof/definition for k.

The NOP research group report documents increased employee productivity, cost savings and other benefits achieved by end users and IT network administrators from more than 300 U.S.-based organizations. Among the most significant results revealed by end users was that using wireless LANs allowed them to stay connected to the corporate network one and three-quarter hours more per day, amounting to a time savings of 70 minutes for the average user and increasing their productivity by as much as 22%. Respondents also reported that wireless networking had a measurably positive impact on return on investment, more than 3.5 times the amount IT staff had anticipated [4].

According to Sage Research a venture capitalist research firm found that companies that embraced 802.11 wireless technologies received an overwhelming positive response. The main conclusion characteristics are:

- Self-reliance of being able to get the info you want, when you want it
- Instant gratification of being able to solve a problem on the spot
- Sense of empowerment by eliminating common process bottlenecks ("I'll get back to you on that")
- Satisfaction of impressing customers with speedy, accurate response to their requests

Sage Research interviewed numerous companies that had over 1000 employees and had used 802.11 wireless technologies for over a month [5].

These same advantages documented in both NOP and Sage are equally germane in the business and support aspects of military life as well as bringing great possibilities into how we implement our command and control systems.

The specific wireless weaknesses are that data can be jammed, intercepted, forged, or altered. One can minimize the effect of jamming by using spread spectrum technologies, causing the transmission to be transmitted over a wide and varied range of frequencies. This might then force the enemy to use a lot of power to cover a wide range of spectrum which is not cost effective in terms of power resources, and the technique would easily give away his position making him an easy target for a reprisal attack. As for interception, data can be encrypted at the link layer to prevent data transmission analysis as well as at the application layer to prevent content analysis. Link layer traffic analysis is equivalent to monitoring the Pentagon for late-night large Pizza Hut deliveries. Prior to the first US strike in the Gulf War when the press saw large amounts of pizza deliveries to the Pentagon they knew that something big was brewing. The press was in fact monitoring the amount of pizza traffic. The way to counter this vulnerability is to either mask the pizza deliveries by making the pizzas in the Pentagon kitchens or by ordering a lot of pizza every night. The same is true in the world of wireless as well. By using encryption at the link level coupled with constant transmission whether there is data on them or not ensures that there is little to no correlation between the amount of data transmitted and the amount of information transmitted.

There will never be a totally secure information system. Wireless networking is not exempt from this truism. Nevertheless most security concerns can be mitigated through risk assessment and properly identifying appropriate external value-added protections as mentioned earlier. Security is important but it is not the only factor. Often military strategy encompasses situations where security is of low importance. Specifically in areas of strategic deterrence and presence, it is desirable for the enemy to know our capabilities in order to dissuade them from acting or to pressure them into a desired outcome. Other concerns are that there are situations where the importance of the timeliness or reliability of communication outweighs the importance of its secrecy. Historically during the American Civil War both the North and the South used the same telegraph lines for communication. Both sides could have destroyed the lines, and both sides could intercept each other's messages. Both sides valued the capability of communication far greater than secrecy and left the lines intact. During the Kosovo conflict the KLA used cell phones as their primary means of communication which could easily be intercepted. Often the military gives a lot of lip service to security but operational need always reigns supreme.

Other important factors are usability and supportability. One could have the most secure system design in the world and if users cannot figure out how to effectively use it, essentially one has created a self-inflected denial of service attack. Secondly if you create a network system so complex it cannot be supported, the information system cannot be used and is of no value.

B. OBJECTIVES AND THESIS ORGANIZATION

The objective of this thesis is to:

- Explore the wireless technologies available to the military educator.
- Understand basic antenna theory and the 802.11 architecture.
- Explore the security vulnerabilities and solutions associated with an enterprise wireless campus.
- Develop a wireless policy and implementation plan for the NPS campus.
- Investigate the variety of wireless applications available today.
- Prove that the Wireless Warrior project adds value to the Net Centric Warfare initiative.

Chapters I through IV go over the wireless fundamentals explaining the value of wireless technology to the Naval Postgraduate School and to the military. Specific technologies are explained in terms of the areas they cover and the data rates they can deliver, specifically: wide area, metropolitan area, local area, and personal area networks. The thesis will focus on the 802.11 technology due to its ease of implementation in terms of technical simplicity and low cost. The 802.11 architecture is explored in great detail. Chapter V covers the security vulnerabilities and reviews the variety of tools available for exploitation and defense of a wireless network. Chapters VI and VII define a strategy to implement wireless at NPS based upon a model of supportability, usability, and security.

Chapters VIII and IX describe the different type of wireless applications available and make recommendations for further research.

II. RADIO FREQUENCY (RF) AND ANTENNA THEORY

A. INTRODUCTION

To understand how to properly administrate, support, and design a successful Wireless Local Area Network one must be familiar with the common terms associated with Radio Frequency (RF) theory and antenna placement. Antenna placement is crucial to ensure that proper coverage is maintained. Proper coverage is the ability to meet the geographic and data rata requirements of the customer. It also means that the geographic signal footprint must be protected from being exploited by adversaries. Antenna placement is key to creating the proper design to meet those needs. This chapter goes over the basic RF terms and formulas including Signal to Noise Ratio (SNR), gain, and free space loss. It also covers the attenuation effects of reflection, refraction, diffraction, scattering and absorption. The chapter also includes the different types of antennas used in wireless networks.

B. RADIO FREQUENCY FUNDAMENTALS

An antenna is defined as a device used to send and receive electromagnetic signals. The amplification of a signal is called gain.

Equation 2.1 describes gain:

$$\mathbf{G} = \mathbf{4}\ \mathrm{P}\mathbf{A}\, h \,/\, l^{2} \qquad \mathbf{(2.1)}$$

where

A = Areas (meters^2)
P **= 3.14… (constant)**
h **= Antenna Efficiency (.5 - .9)**
l **= Wavelength (meters).**

The primary units of measure are decibels (dB) and watts (W). dB is a relative logarithmic measurement that compares two power levels and has no specific units. When it refers to signal power the term dBm (dB for microwatts instead of watts) is used, when it refers to antenna gain the term dBi is used. dB uses a logarithmic scale in order to express greater ranges. As a general rule of thumb every increase of 3 dB doubles the quantity measured, and every increase of 10 dB increases the units of measurement by 10 fold. An increase in power caused by an antenna is called gain.

The formula for conversion from milliwatts to dBm is provided in Equation 2.2.

$$\mathbf{P_{dBm} = 10\ Log\ [P_{mW}/1_{\ mW}]} \qquad \mathbf{(2.2)}$$

where

P_{dBm} = the relative power level in dBm
P_{mw} = the absolute power level in mW,
$1_{\ mw}$ = the reference power level in mW.

A positive value of dBm represents a gain and a negative value represents a loss. The amounts of power wireless devices transmit and at which frequency range is restricted and enforced by the government. The regulatory body and their respective regulations differs from country to country. The Federal Communications Commission (FCC) is the enforcement body in the United States and reports to Congress. According to FCC Intentional Radiators, devices that transmit in the 2.4 GHz ISM bands are restricted to 1 Watt with the exception of Point-to-Point and Point-to-Multi-Point modes which have a restriction of 4 Watts [6]. These power values are the Equivalent Isotropic Radiated Power (EIRP). The EIRP is measured at the antenna of the device and takes into account the power the access point has due to amplifiers, attenuators, cable signal loss, and antenna gain. Three factors, transmitter power, line loss, and antenna gain, are combined into the EIRP. The strength of a signal is described as the Signal to Noise Ratio (SNR).

Equation 2.3 describes SNR:

$$\mathbf{S/N = \left(P_t G_t /kB\right)\left(\mathit{l}\ /4P\,R\right)^2\left(G_r /T\right)} \qquad \mathbf{(2.3)}$$

where

P_t = Power of the transmitter (microwatts)
G_t = Gain of the transmitter (dB)
K = 1.381 x 10^{-23} joules/K (constant

B = Bandwidth (Hz)
l **= Wavelength (meters)**
P **= 3.14… (constant)**
R = Range
$\mathbf{G_r}$ = Gain of the receiver (dB)
T = Temperature (K).

Signal loss also called attenuation can be caused by reflection, refraction, diffraction, scattering and absorption. Reflection occurs when a signal bounces off an object. When a transmission is around a lot of objects there may be several paths from the transmitter and the receiver. This phenomenon is called multi-path. Several paths can interfere with one another and degrade the signal. Refraction is when a signal is bent and or weakened because it goes through another medium. Wireless LANs often go through walls which weakens the strength of the signal and can cause multi-path signal degradation. Diffraction is similar to refraction except instead of being bent through an object, the signal is bent around an object. In the end the bending causes the signal to be weakened and can cause multi-path interference problems as well. Scattering is a special form of reflection except that the medium containing the signal is uneven causing there to be several reflected signal returns. Scattering causes the greatest attenuation compared to the others because of the numerous possibilities of multi-path.

The intensity of a signal is inversely proportional to the square of the distance of the transmitter. As the beam gets transmitted it spreads out so the power is diluted over a large area. This phenomenon is called free space loss. Equation 2.4 describes free space loss:

$$\mathbf{L}_{\mathbf{fs}} = \left(l\ \mathbf{/\,4}\,\mathrm{P}\,\mathbf{R}\right)^{2} \qquad \textbf{(2.4)}$$

where

l **= Wavelength (meters)**
P **= 3.14… (constant)**
R = Range (meters).

C. ANTENNA FUNDAMENTALS AND FOOTPRINT SECURITY

There are primarily two types of antennas currently used in wireless LANs: omni-directional and directional antennas. Omni-directional antennas transmit in all directions while directional antennas transmit in a limited area. Using the appropriate type of antenna ensures the coverage footprint is where it is supposed to be. This improves security and efficiency. Figure 2.1 is an example of a omni-directional antenna. The most common types of directional antennas are parabolic, sector, yagi, and patch. The most common directional antenna is the parabolic antenna where it is used primarily for long range communication. It is primarily used for terrestrial to terrestrial and terrestrial to space exchange. Satellite dish television communication is the most popular consumer application. Figures 2.2 and 2.3 show some common antennas.

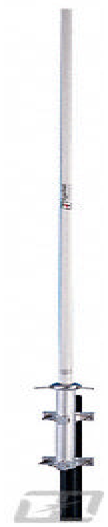


Figure 2.1. 10 dBi Gain Omni-Directional Antenna.

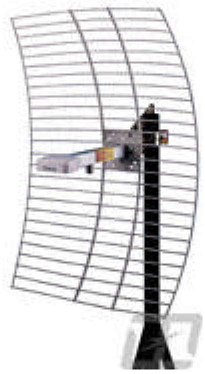


Figure 2.2. 19 dBi Gain Parabolic Reflector Grid Antenna.

The Yagi antenna named after Dr. Hidetsugu Yagi who co-invented it with Professor Shintaro Uda in 1924 at Japan's Tohuku University [7].

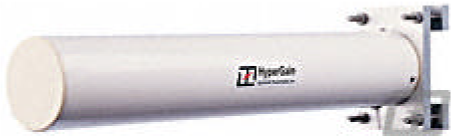


Figure 2.3. 14 dBi Gain Yagi Antenna.

The Yagi antenna recently became popular with wireless hobbyists due to their simplicity; for example, users are able to make them out of Pringles cans and coffee cans. Figures 2.4 and 2.5 show some home-made antennas.

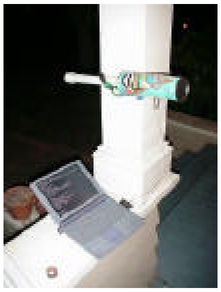


Figure 2.4. A Homemade Yagi Antenna Made from a Pringles Can Antenna on the Cheap (er, Chip) [8].

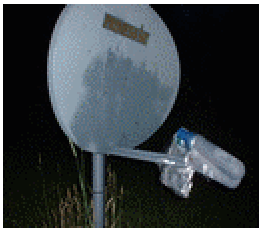


Figure 2.5. A Converted Satellite Antenna for Use with an 802.11 LAN [9].

The low cost of antenna and wireless equipment has induced great security concerns. While in the past it may have been acceptable to use a single access point connected to very large omni directional gain antenna, this may not be appropriate or efficient. By using directional antennas, varying the power and turning it off when not in use will ensure reliability with overexposing a footprint which an adversary might exploit. In terms of efficiency when designing an 802.11b wireless network there are only three non- overlapping channels. If the power is turned down then the flexibility of channel reuse for greater areas of coverage is possible. Otherwise the number of users per access point will significantly increase. In summary, antenna selection is critical for proper coverage**.** There has been a lot of work in the military concerning TEMPEST testing. TEMPEST stands for Telecommunications Electronics Material Protected from Emanating Spurious Transmissions and was the name of a U.S. government project to study susceptibility of some computer and telecommunications devices to emit electromagnetic radiation (EMR) in a manner that can be used to reconstruct intelligible data. This is an area where further research should be performed to minimize signal loss and interception for wireless 802.11 devices**.**

D. SUMMARY

When designing a wireless network it is important to have a basic understanding of RF fundamentals to include S/N ratio, gain, and free space loss. Secondly, it is equally important to understand the different types of antennas available and their effect on the intended and unintended wireless coverage areas.

III. WIRELESS WANS, MANS, LANS AND PANS

A. INTRODUCTION

The focus of this chapter is to describe the different types of wireless networks available. Their limitations and capability are described based on their range, data rate and mobility. These technologies are then compared for NPS campus suitability.

B. WIRELESS NETWORK TYPES

Wireless networks are compartmentalized based on the geographic scale of their coverage. In general, the coverage areas and data rates share an inverse relationship with each other. That is the greater the coverage area, the slower the data rate and the greater the data rate the smaller the coverage area. The largest area wireless networks are called wireless Wide-Area Networks (WANs). Networks that cover city areas are called wireless Metropolitan-Area Networks (MANs). Networks that cover campus size or smaller networks are called wireless Local-Area Networks (LANs). The smallest wireless networks are the wireless Personal-Area Networks (PANs). They exist primarily in ad hoc form and are used as cable replacement for peripherals like printers or projectors. It is vital for anyone designing a wireless network to know which technology to use and the implications of that decision in terms of coverage, data rate, cost, and security.

C. WIRELESS WANS

WANs are controlled by the Telcos and use cellular technologies as their means of delivery. There are a variety of technologies used in the transmission of data in the wireless WAN arena. They are loosely described based on the generation (abbreviated G) of their development: 1G, 2G, 2.5G, and 3G. The First Generation (1G) cellular devices developed in the 70s and 80s are analog systems restricted to voice only transmission. The three major 1G standards are the Advanced Mobile Phone System (AMPS), the Total Access Communication System (TACS) and the Nordic Mobile Phone System (NMT). NMT and TACS have been replaced in Europe with newer technologies and are no longer in use. AMPS is still the most widely deployed system in the United States. It uses Frequency Division Multiple Access (FDMA) as its data-link method.

The Cellular Digital Packet Data (CDPD) service allows TCP/IP to run on an analog AMPS networks at 9.6 – 19.2 Kbps data rates. CDPD was developed in the early 90s.

The Second Generation (2G) cellular systems were developed in the late 80s and early 90s and are digital networks. 2G consists of two competing technologies for link access: Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA). North Americans have chosen to follow both routes of CDMA and TDMA in the IS-136 and IS-95A technologies. Most of the world has chosen TDMA technologies. CDMA has only one 2G implementation developed by Qualcomm, the IS-95A. TDMA has three 2G implementations: Digital AMPS (D-AMPS), Global System for Mobile Communication (GSM), and Personal Digital Cellular (PDC). They are all incompatible with each other. D-AMPS is also known as the IS-136 from the Electronics Industries Association/Telecommunication Industries Association (EIA/TIA). It is the digital follow on technology from AMPS.

GSM is the prevailing system throughout the world. It has coverage throughout Europe, Asia, and Africa. It has over 120 million users worldwide in over 120 countries. Nevertheless, it has gained little acceptance in the Unites States. Its success in Europe is due to the European Telecommunication Standards Institute (ETSI) mandating the standard for all of Europe. This is why European wireless WAN efforts have eclipsed North American. They no longer face a Telecom Tower of Babel standards war. The Japanese have their version of 2G called PDC. Most 2G technologies had a maximum data rate transmission limitation of 9.6-14.4 Kbps.

The 2.5 Generation represents the telecommunication standards fielded in the 1999-2000 time period. It consists of three technologies: IS-95B, iMode, and Global Packet Radio Service/Enhanced Data Rates for Global Evolution (GPRS/EDGE). IS-95B is the follow-on CDMA technology increasing data rate transmissions to 64 Kbps. iMode is a service in Japan that allowed email and web surfing functionality to cell phones. GPRS/EDE is often referred to as almost 3G or 2.75G. GPRS allows the GSM network to use packet data at 171 Kbps. The EDGE enhancement to GPRS increases the data rate to 384 Kbps. EDGE/GPRS is based on the TDMA family history.

Third generation (3G) represent the 2001- time frame. 3G's focus and goal is multi-media everywhere by 2007, specifically 2002 in Japan and Korea, 2003 in Europe, 2004 in the United States and 2007 in the third world [10]. 3G proponents want to provide audio, video, internet at high speeds and do this with small devices that are always on and require little battery demand. 3G supports three mobile network environments: high speed, medium speed and slow speed. High speeds in excess of 75 mph are limited to data rates of 144 kbps, medium speeds between 75 mph and 5 mph are limited to 384 kbps, and slow speeds less than 5 mph are limited to 2 Mbps. There are two competing implementation the CDMA 2000 and the W-CDMA. The CMDA 2000 is backed by Qualcomm and Lucent and have already implemented part of the infrastructure in Brazil, Korea, and the United States (Verizon, Sprint, and U.S. Cellular). CDMA 2000 will be implemented in four stages. W-CDMA is geared to be a replacement of the TDMA/GSM infrastructure with CDMA technology. It has been built in Japan and on the Isle of Man in the United Kingdom. W-CDMA enjoys support from NTT-DOCOMO, Ericsson, and Nokia.

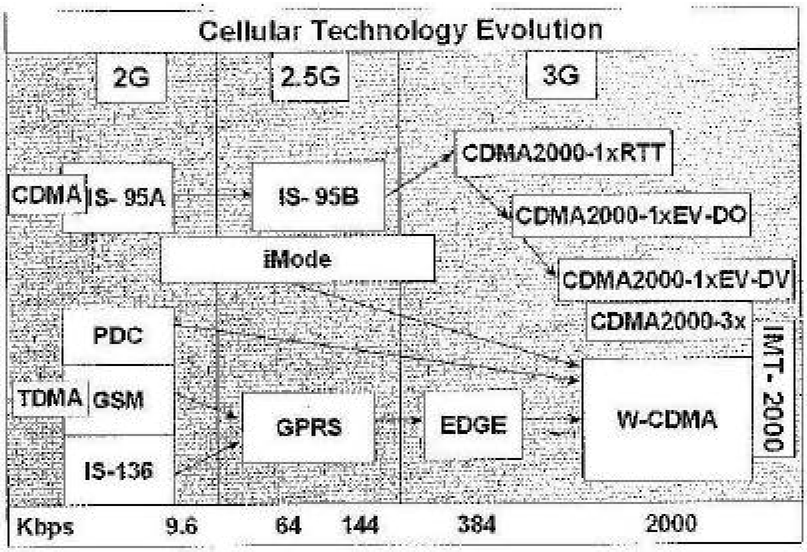


Figure 3.1. Cellular Technologies Showing Standards Evolution Versus Bandwidth [11].

Another set of WAN technologies are the satellite low earth orbit based companies. They provide voice and data rates from 9.6 to 14.4 kbps. They have been financially unsuccessful because of the great cost of launching satellites. Low earth orbit satellites allow for users to have light weight low capacity battery requirement devices, but at a cost for the infrastructure of launching many satellites to provide worldwide coverage. The most popular companies are Iridium (http://www.iridium.com) and Globalstar (http://www.globalstar.com).

D. WIRELESS MANS

The Metropolitan Area Networks (MANs) coverage range can be as wide as 35 miles. It does differ from wireless WAN and wireless LAN technologies because the wireless links are fixed. Lack of end user mobility is the distinct characteristic and restriction of the wireless MAN. The most common wMAN technologies are Multi-channel Multi-port Distribution Services (MMDS) and Local Multi-port Distribution Services (LMDS). They are specified by the IEEE 802.16 fixed broadband wireless access standard. These technologies serve the purpose of the last mile forms of Wireless Local Loop (WLL) or in forms of television signals such as Instructional Television Fixed service (ITFS).

The IEEE has three 802.16 specifications and four Task Groups. The three specifications are 802.16, 802.16a and 802.16b. 802.16 specifications is for devices that transmit in the 10-66 GHz range such as LMDS, 802.16a specification is for devices that transmit in the 2-11GHz range such MMDS and 802.16b specification is for devices that transmit in 2-11 GHz range but do so using unlicensed frequencies such as ISM or UNII. Task Group 1 and 3 develop more physical implementations in the 10-66 GHz and 2-11GHz frequency ranges, respectively.

Task Group 2 and 4 GHz are to allow mutual coexistence with wireless LAN and PAN devices such as 802.11 and Bluetooth in the unlicensed frequency ranges of 2.4 GHz and 5 GHz, respectively.

MMDS in the United States uses five frequency bands from 2.1 GHz to 2.7 GHz. This allows 240 MHz of spectrum. These frequencies are licensed and must be purchased for use from the government. MMDS has a range of approximately 30 miles and can support a single user non-shared data rate of 27 Mbps. Shared subscribers can have data rates up to 3 Mbps. MMDS is frequently used as a wireless cable TV in rural areas where cable installation costs are prohibitive. Installation time is also significantly quicker. Nevertheless MMDS has been less than commercially successful in the U. S. Some argue that its failure is more to do with the political influence of the Telcos than the limitations of the technology.

LMDS is similar to MMDS except that it operates using five frequency bands in the 28-31 GHz range. It has a range of three to five miles and a whopping data rate of 500 Mbps. Its market has been video, voice and data delivery for companies that reside within a city. Because it operates at higher frequencies it is more susceptible to weather interference. Due to the monopolistic/political influence of the Telcos, wireless LMDS companies have been unable to gain market share despite the advantages of the technologies. Companies such as Winstar, Teligent, and XO communication have either filed for Chapter 11 bankruptcy or have seen significant market share decline.

European wireless MANs consist of the Hyperman standard (2-11 GHz) and Hyper Access Standard (40-43.5 GHz). They are similar to the IEEE 802.16 standard. They are regulated by the ETSI Broadband Radio Access Network (BRAN). There is also an American proprietary competing technology with 802.16 and ETSI BRAN called the Broadband Wireless Internet Forum (BWIF). It is promoted by Cisco, Toshiba, and Texas Instruments. BWIF wants their standard, which uses Vector Orthogonal Frequency Multiplexing (VOFDM), to replace the IEEE 802.16.

E. WIRELESS LANS

Frequency range and area of coverage are the distinctive characteristics of wireless LANS. They exist in the US using unlicensed bands at the 2.4 and 5 GHz frequency ranges. These ranges are called the Industrial Scientific and Medical (ISM) and Unlicensed National Information Infrastructure bands (U-NII). They tend to cover areas from a single office up to a university campus. The most prevalent standards are the 802.11, Home RF, and HyperLan. 802.11 is an IEEE standard and the most popular worldwide. 802.11's market is for the business as well as the home. There are three main physical layer implementations of the 802.11 in production. There is the original 802.11 which has maximum data rate of 2 Mbps. There is 802.11b which has a maximum data rate of 11 Mbps and there is 802.11a which has a data rate of 54 Mbps.

802.11b is the most popular and has the greatest range. The 802.11 specification is described in greater detail in the next chapter. Some companies have tried expanding 802.11 into the MAN and WAN markets. Nokia's Rooftop (http://www.wbs.nokia.com), Alvarion's Broadband services (http://www.alavarion.com) and MeshNetworks (http://www.meshnetworks.com) are the most well known.

HomeRF is a home networking standard developed by Proxim in 1998 as direct competitor to the IEEE 802.11. It hoped to capture the home market. It uses frequency hopping encoding to deliver its content. It also supports the Digital Enhanced Cordless Telecommunication (DECT) protocol for voice. It does this by using the Shared Wireless Access Protocol (SWAP). HomeRF version 1.0 operated at the 2.4GHz at data rate of 1.6 Mbps and 4 full voice duplex connections. It lost significant market share to the 802.11b camp which has an 11 Mbps data rate. Finally in August of 2000 the FCC changed it regulation and allowed frequency hopping devices the legality to transmit at 10 Mbps in the ISM 2.4 GHz frequency range. It was too little to late. A new study released by the Allied Business Intelligence (ABI) (Home Networking Equipment - A Practical Assessment of Technologies and Changing Market Dynamics by Navin Sabharwal September 2001) has found that 802.11b wireless local area network (WLAN) technology is decisively winning the battle for in-home wireless networking over HomeRF. The study found that, in 2000, 58 percent of all wireless nodes sold used for the HomeRF technology. However, it accurately projected that 71 percent of all wireless nodes shipped in 2001 would be 802.11b products. 802.11 is the most popular capturing more than 80% of the market. With the proliferation of the IEEE 802.11 standards wireless equipment popularity is growing at a phenomenal rate. The worldwide market for all products based on the 802.11 standard by 2006 will grow to $3.1 billion in annual revenue, from $1.2 billion in 2001, according to research company Dell'Oro Group, in Redwood City, California [12]. Intel stopped making HomeRF devices in favor of 802.11, the Home RF working group conceded the 5Ghz frequency band to the IEEE 802.11a working group and Proxim, the inventor of HomeRF had just purchased Agere, the world's second biggest manufacturer of 802.11 equipment. Although HomeRF has a significant advantage over 802.11 because it has voice capability, it did not succeed because of its lack of influence with the FCC to increase data rates to compete with 802.11. More information can be obtained at the HomeRF web site at http://www.homerf.org.

Hiperlan is the European competition to 802.11. It is based on standards developed by the ETSI (http://www.hiperlan2.com). The Hiperlan Global Forum is very influential with the ETSI and consists of Nokia, Ericsson, Dell, and Texas Instruments. Hiperlan transmits in the 5 GHz range and uses Orthogonal Frequency Division Multiplexing (OFDM) as its encoding. Hiperlan version one was a failure and has been replaced with Hiperlan2. Hiperlan2 transmits up to 54 Mbps data rates and has QOS and improved security built into the specification. This is a distinct advantage over 802.11. Chapter IV will go into detail on the make up of the IEEE 802.11 specification.

F. WIRELESS PANS

Wireless Personal Area Networks (PANS) are used primarily for short distances as a cable replacement. They are designed to support low power devices with an ad hoc implementation design in mind. They have been installed on laptops, PDAs, cameras, printers, cell phones, pagers, projectors and other mobile devices. A common application is for users with a handheld portable device to be able to communicate with another in order to exchange phone numbers/contact information. Another example would be for a user to be able to print or use an overhead projector from a PDA. The two most popular standards are the Infrared Data Association (IRDA) and Bluetooth. IRDA was formed to create international standards for the hardware and software used in infrared communication links. The standard was created in 1993 and in the latest IRDA-1.1 standard, the maximum data size that may be transmitted is 2048 bytes and the maximum transmission rate is 4 Mbps in synchronized mode. In asynchronous mode date rates can range from 9.6-115 Kbps. Depending on how much power is applied IRDA can function from 20 centimeters to 2 meters. IRDA has obtained moderate success having been installed in over 300 million devices. Nevertheless it is often difficult to use because it requires both receiver and the sender to be in direct line of sight. IRDA can be characterized as the most successful failure in the history of computer peripherals. The difficulty of use caused by the alignment requirement fostered the growth of a radio replacement.

IRDA is being replaced with Bluetooth. Bluetooth uses radio waves instead of infrared light and does not require alignment like IRDA. It also has voice capability. Specifically it can be integrated for use with mobile cell phone networks. The Bluetooth project was started at Ericsson in 1994. It was named after a tenth century Danish King Harald Blaatland. Blaatland means Bluetooth. He was known as a unifier of people. In 1998 the Bluetooth Special Interest Group (SIG) was formed consisting of Ericsson, Nokia, Intel, IBM, and Toshiba. The Bluetooth SIG has over 1000 members. Bluetooth transmits on the 2.4 GHz range and uses frequency hopping. In asymmetric mode it transmits at 721 Kbps in one direction and 57.6 in the other. In symmetric mode it can maintain a 432.6 kbps data rate. It forms ad hoc networks called piconets and scatternets as shown in Figure 3.2.

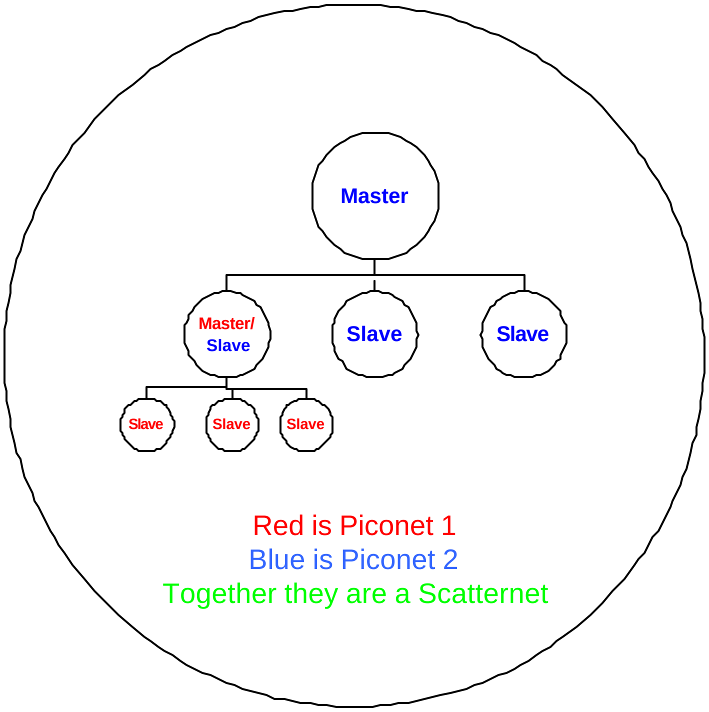


Figure 3.2. Bluetooth Topology.

In 1998 the IEEE 802.11 decided to form the IEEE 802.15 group to focus low power short range wireless networks. The 802.15 has four task groups. Task group 1 incorporates the Bluetooth 1.0 standard. Task group 2 is focusing on reducing problems with other wireless devic es, specifically 802.11b. Both Bluetooth and 802.11b use the 2.4 GHz ISM spectrum. Because Bluetooth is a very low power device and incorporates high speed frequency hopping encoding interference with 802.11 is nonexistent at ranges over 10 feet. When 802.11 and Bluetooth devices are with in a range 10 feet or less of each other the interference is minimal because Bluetooth hops throughout the entire 2.4 GHz ISM spectrum and 802.11 primarily uses only a third, one of the three non overlapping channels. Task Group 3 is attempting to develop high speed PANs at data rates up to 10-55 Mbps at distances less than 30 feet. Task Group 4 is looking to develop devices with battery life that will last for months. Its data rate will be less than 200 kbps. The Bluetooth SIG is independent from the IEEE and is developing Bluetooth as its own standards. It is currently working on Bluetooth version 3.0. It does work closely with the IEEE because of its desire to capture American markets.

G. NPS ANALYSIS

The NPS mobile user expects to have roughly the same functionality as when wired and expects to use small low-cost low-weight commercially available devices to connect to the network. This means data rates in the Ethernet+ range of 10-100 mbps. This eliminates, at least in the short term or until the maturation of 3G technology, wireless WAN technologies as the basis for a campus infrastructure due to limited data rate capability. Secondly, a reliance on WAN technology would create a financial dependence on a commercial service provider. This dependency could be costly to the government and could limit its choice of hardware, and it would be at the whim of the provider for service quality and technological upgrade. Wireless MAN technologies are not light weight or portable in nature and therefore do not suit the needs of the NPS mobile user. LAN and PAN technologies make the best sense for the NPS campus. 802.11 is clearly the dominant wireless LAN technology and is backed up the IEEE and WECA. An 802.11 infrastructure assumes the role of providing wireless network access and Bluetooth devices assume the role of wireless peripheral control. 802.11 is a low cost solution that provides Ethernet speeds and can be scaled to cover the NPS campus as well as the housing areas in La Mesa and Fort Ord. PAN technologies are ad hoc low power devices and therefore require little to no infrastructure to support but are not scalable. In most cases they do have the range for use outside a single office area.

IT administrators might want to start to buy printers and other public use peripherals that support Bluetooth as well as Ethernet. Because 802.11 infrastructure devices become part of the wired campus via wireless means they are able to use any shared network wired device such a network printer. While it is true that 802.11 devices can outperform Bluetooth devices in terms of range and data rate, they do so at the cost of limited battery life. Therefore it is prudent to allow for peripherals to be accessed though both 802.11 and Bluetooth means. This will give the user greater choice and flexibility on how to access peripherals. Bluetooth device-capable peripherals, if properly administered do not necessarily require a user to be part of the network. This will satisfy the temporary user who only wants to quickly print to the closest printer for a few minutes and has no short-term requirement for internet or campus wide network services.

H. SUMMARY

There is a need of for wireless WANs, MANs, LANs, and PANs. This need is causing a convergence of technologies. The trend for network devices for the future is to have several technologies built in to one. Bluetooth is designed for peripheral and ad hoc communication, 802.11 multimode (a,b,g) for wireless LAN communication and some sort of 3G communication for wireless WAN movement. Devices will automatically use the technology that produces the highest data rate. In the near term, the use of 802.11 for wireless access and Bluetooth for peripheral control is the best-suited technology for the NPS campus. The next chapter discusses the 802.11 specification in detail.

IV. IEEE AND THE 802.11 STANDARDS

A. INTRODUCTION

The focus of this chapter is to explain the history of the IEEE 802.11 standard and the purpose of the working groups. An overview of the 802.11 specification is defined to include the Media Access Control (MAC) layer, the various physical layers and architectural topologies. The 802.11 frequency spectrum is defined as well as wireless signal interference issues. The chapter closes with explanation of related organizations to include WECA, WI-FI, and the University of New Hampshire Interoperability Lab.

B. 802.11 HISTORY AND THE WORKING GROUPS

The IEEE 802.11 specification was initially designed in 1997. It allowed for three physical layers: Frequency Hopping (FH), Direct Sequence (DS), and Infrared. FH and DS operate in the 2.4 GHz range with maximum data rate of 2 Mbps. 802.11 Infrared devices were never produced. To improve the standard the specification was broken down into working groups (also called task groups) which were each given a letter designation. Often these task groups improve existing standards or create new functionality. After a working group finishes its research, it offers its standards up to industry for production. Currently the only working groups that have standards in production are the 802.11 (original), 802.11b and 802.11a. In 1999, the 802.11 specification was improved to allow data rates of 11 Mbps. The new specification is called 802.11b and supports only the direct sequence physical layer. This standard was based on the b working group.

The 802.11a specification was also delivered in 1999 which specifies reusing the same MAC layer as 802.11 and 802.11b except that it transmits at the 5 GHz range and like Hiperlan, uses OFDM encoding. 802.11a also has two main advantages over 802.11b. It has a data rate of 54 Mbps and has eight non-overlapping channels (vice 802.11b's three non-overlapping channels). Many vendors have proprietary enhancements that allow a further increased data rate of 108 Mbps. Its greatest disadvantage is its non-backward compatibility with 802.11 and 802.11b wireless equipment which functions at the 2.4 GHz frequency range. Also 802.11a transmission range is half that of 2.4 GHz wireless equipment. This requires enterprises to deploy twice as many access points to maintain continuous 54 Mbps data rate coverage. While the 802.11a and 802.11b specification were both published in 1999, manufacturers had difficulty in producing 802.11a chip sets until November 2001.

The next standard is 802.11g which uses the same MAC/physical layer as 802.11a (OFDM) but is backward compatible with 802.11b by functioning at the 2.4 GHz frequency range. It has the same three non-overlapping channel restrictions as 802.11b. It is expected that 802.11g standard will be approved by the second quarter of 2003. Some vendors such as Linksys Corporation and Dlink are producing proprietary enhancements to their 802.11b units that have data rates of 22 Mbps. Intel, Cisco, and Agere produce access points that allows for dual transmission of 802.11a and 802.11b. These factors have produced speculation that few vendors will produce 802.11g equipment or will not produce single mode 802.11g equipment. The 802.11 trend follows wired Ethernet network cards that are multi-mode 10/100/1000 bps devices. Atheros, a prominent wireless chip manufacturer, announced that it will ship multi-mode 802.11a/b/g chip sets by September 2002.

The remaining task groups are working on improving the 802.11 specification with improved functionality in a myriad of areas.

The 802.11c group is focused on improving bridge functionality. This group has provided the 802.11 MAC specifications to the wired 802.1D group for ease of operation between wired and wireless LANs.

The 802.11d group (not to be confused with the 802.1D) is a combination technical/marketing group with the aim of going after new markets by removing technical barriers and improving regulations.

The 802.11e group is focused on adding Quality of Service (QOS) functionality into the specification. This group would allow for a variety of services such as video and audio on demand, Voice over IP (VOIP) and telephony. These services will significantly increase the consumer demand of the 802.11 product. 802.11e functionality brings wireless media to the masses. The adoption of this specification is not expected until early 2003.

The 802.11f Inter Access-Point Protocol goal is to allow for a deployment of multi-vendor access points. The current 802.11 specification does not define how a user can roam from one access point to another. It is left up to the vendor to implement a proprietary solution. This has caused successful enterprise implementations to go with a sole source access point vendor solution. In organizations that support a multi-vendor access point solution roaming cannot be guaranteed. The 802.11f group is trying to solve this problem. The adoption of this specification is not expected until early 2003.

The 802.11h focus is to improve 802.11a functionality by adding spectrum and power management enhancement as well as defining outdoor use for the European markets.

The 802.11i group's focus is security. Its long term aim is to replace WEP encryption with AES and revamp the authentication procedures. It is working closely with the 802.1X group, the Extensible Authentication Protocol standard. To accomplish this it is expected that users would have to purchase additional hardware. Interim solutions such as TKIP and CISCO PEAP are being suggested as alternatives.

The 802.1X group is based on RFC 2284, Extensible Authentication Protocol or Port Based Network Authentication Protocol [13]. It is more of a security framework than an exact specification. There are numerous variants but each has the general aim to authenticate users and allow them access when they provide the proper information. The greatest advantage of 802.1X is extensibility allowing for continuous improvement and variety of authentication methods. The most popular implementations are EAP/TLS, EAP/MD5, EAP/Kerberos, EAP/SRP, EAP/SIM and EAP/TTLS. These solutions allow for the secure delivery of individual dynamic session keys. A detailed description of 802.1X networks and wireless security implications is described in greater detail in Chapter V.

Several new IEEE groups are being formed in the Fall of 2002 such as the Wireless Next Generation, Radio Resource Measurements, and High Throughput groups.

These groups are so new they do not yet have letters. They are investigating the possible wireless migration and use of Ultra-Wide Band frequencies and desire for high data rates and the implied effect on design. Specific details of these groups have not yet been released by the IEEE.

C. STANDARDS OVERVIEW

The 802.11 protocol is an IEEE specification under the 802.2 family tree. The 802.2 is the upper portion of the link layer and is shared among Ethernet, token bus, token ring, wireless LAN, and Bluetooth. This modularization approach allows for a new medium to be developed and fit right into the 802.2 specification by creating a new link layer/physical layer. This is the advantage of the 802.11 specification. The 802.3 specification also has variety of physical layers such as 10BASE-T, 100BASE-T, 1000BASE-T, and 100BASE-F. 10BASE-T represents 10 Mbps on unshielded twisted pair cable, 100BASE-T represents 100 Mbps on unshielded twisted pair cable, 1000BASE-T represents 1000 Mbps on unshielded twisted pair cable, and 100BASE-F represents 100Mbps on fiber optic cable. All these physical layers use the same 802.3 MAC layer and the same 802.2 Logical Link Layer regardless of the physical layer used. Of course 802.4, 802.5, 802.11, and 802.11 may have different MAC layers to manage their unique physical layers but they all share the same 802.2 Logical Link Layer and higher layers. Figures 4.1 and 4.2 describe how wireless fits in with the other 802 devices.

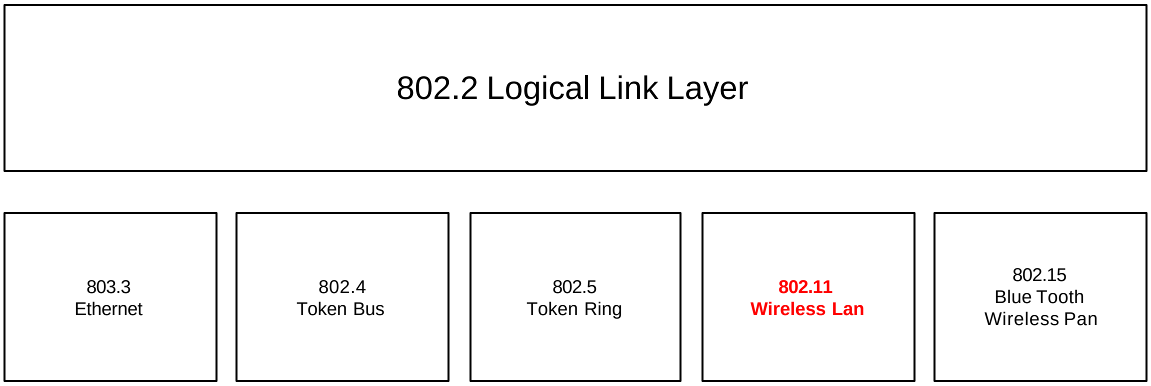


Figure 4.1. IEEE 802 Structure.

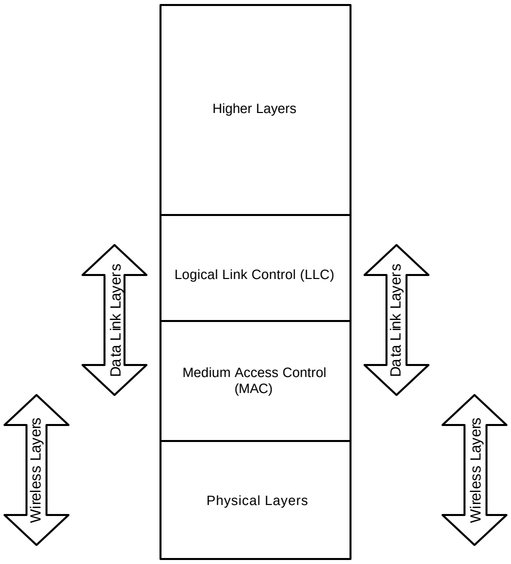


Figure 4.2. Wireless LAN and How it Relates to the OSI Model.

D. THE 802.11 MEDIUM ACCESS CONTROL (MAC) SUB LAYER

The purpose of the 802.11 MAC is to allow access to the wireless medium, allow a wireless network to be joined, and support authentication/encryption. The 802.2 Logical Link layer communicates with the 802.11 MAC through the MAC Service Data Unit (MSDU). They are used to transport higher level data from one MAC to another. The 802.11 data transfer has two types of Media Access Control: Distributed Coordination Function (DCF) and Point Coordination Function (PCF). DCF uses Carrier Sense Multiple Access /Collision Avoidance (CSMA/CA). It is based on the wired Ethernet standard Carrier Sense Multiple Access /Collision Detection (CSMA/CD). The main difference is that in the wireless world collisions cannot be detected because it is difficult for an antenna to transmit and listen at the same time. In other words, wireless devices are a half duplex medium. To improve efficiency and utilization the wireless Ethernet standard was modified to allow for collisions to be avoided by forcing all nodes to positively acknowledge all transmission frames to them. If an acknowledgement is not received it is assumed to be lost and is retransmitted. PCF allows for priority-based access by allowing for a contention–free time period. PCF was designed to allow for basic QOS but has rarely been supported by vendors. The 802.11e working group is improving the QOS functionality to support streaming multimedia applications.

E. 802.11 PHYSICAL LAYERS

The MAC communicates to the physical layer through frames or MAC Protocol Data Units (MPDU). There are four different types of physical layers supported under the 802.11 specification: Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), Infrared, and Orthogonal Frequency Division Multiplexing (OFDM). Infrared (IR) and FHSS are limited to 2 Mbps data rates, DSSS is limited to 11 Mbps data rates and OFDM is limited to 54 Mbps as shown in Figure 4.3

F. 802.11 ARCHITECTURAL TOPOLOGIES

The prime method of communication for all wireless LANs is the service set. It is a common identifier for the LAN in which users access the network. If the topology consists of one or more client computers and an access point, the service set is called a Basic Service Set (BSS).

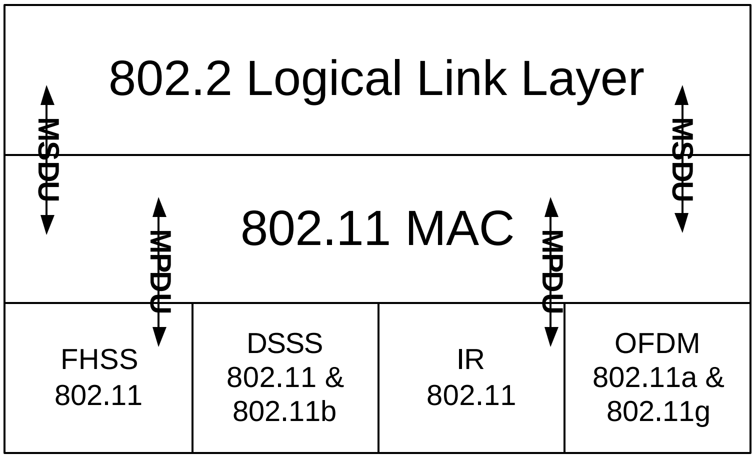


Figure 4.3. 802.11 Physical Layers.

If there are two or more access points then the service set is called an extended service set (ESS). If the topology consists of one or more clients with no access points then the topology uses an Independent Basic Service Set (IBSS). Access points allow wireless LANs to connect to a wired infrastructure. Most vendors implement cards to be either infrastructure mode (ESS/BSS) or ad hoc mode (IBSS). The following diagrams, Figures 4.4 through 4.6 show the different topologies.

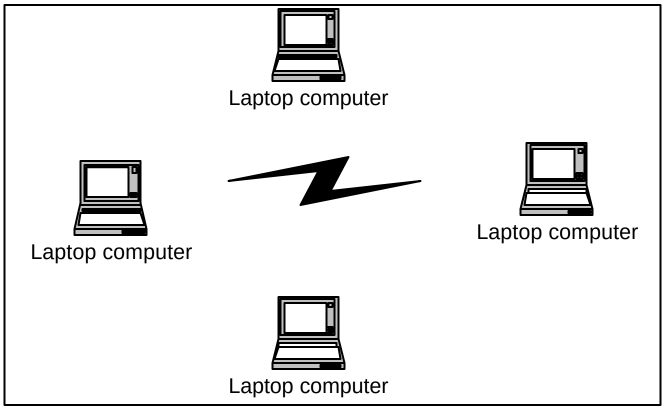


Figure 4.4. Ad Hoc IBSS Topology.

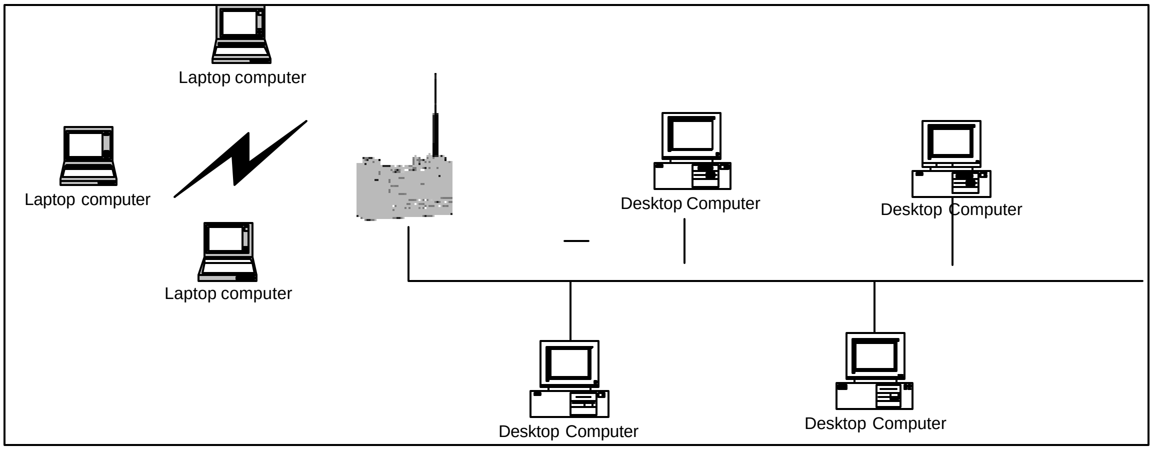


Figure 4.5. Infrastructure BSS Topology.

In order for a client to communicate in either ad hoc or infrastructure mode it must do so through the MAC layer. The purpose of the wireless MAC layer is to provide reliable data up the protocol stack from the physical layers, allowing only authenticated users use of the network, and allow for the encryption of data. It accomplishes these tasks by communicating using different types of MAC service data units (MSDUs) from the 802.2 LLC to the MAC layer. The MAC layer than communicates to the physical layers via a MAC Protocol Data Unit (MPDU).

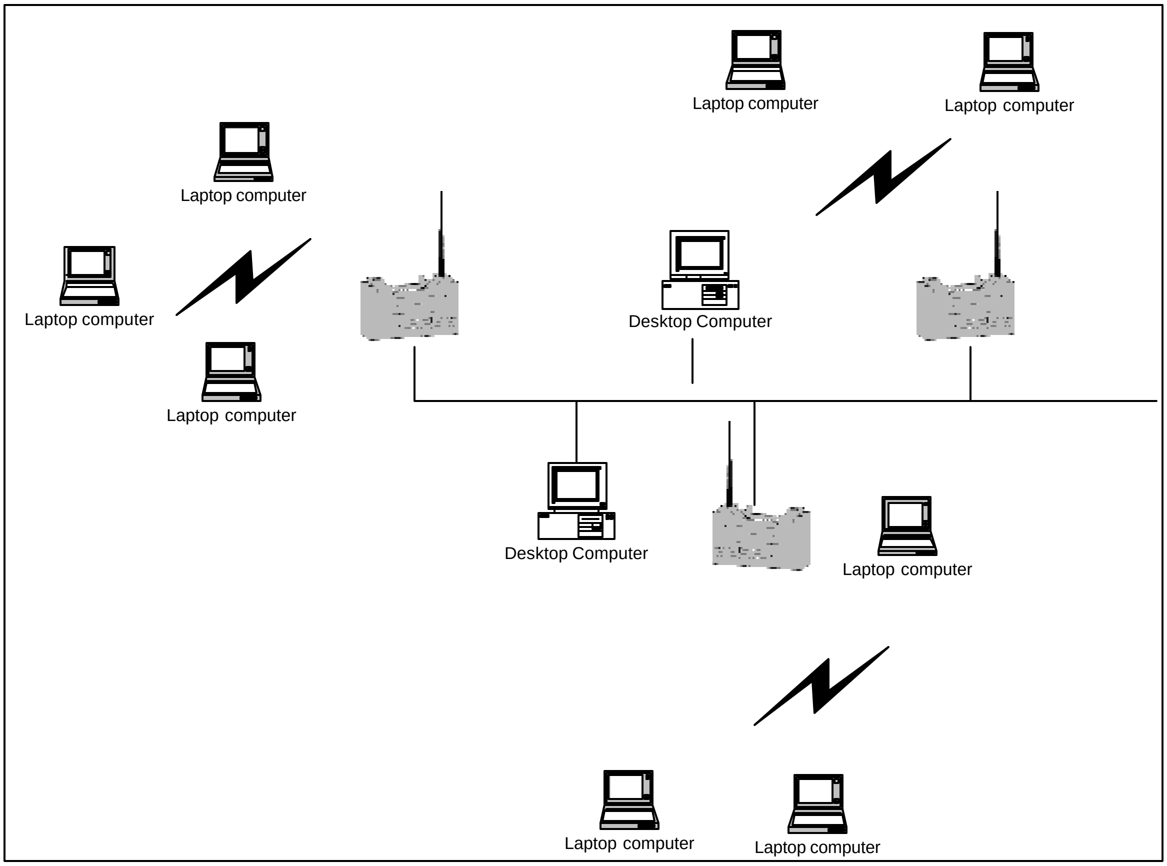


Figure 4.6. Infrastructure ESS Topology.

A Management Information Base (MIB) is normally provided by the manufacturer of the device in order to communicate with the physical layer primitives. The communication may be encapsulated in a driver and/or by using the Simple Network Management Protocol (SNMP). The architecture is shown in Figure 4.3. The most important services are authentication, association, and encryption. Theses service units are transmitted using one of three different types of frames: control, management, and data frames. A client must be configured with the same Service Set Identifier (SSID) and optional Wired Equivalent Privacy (WEP) key in order to connect to another wireless device. The SSID is user/network administrator defined value that is anywhere 0-32 characters long that identifies one or more Access Points (AP) or similar devices. An AP can be set in one of two modes concerning the broadcasting of the SSID. If it is in broadcast mode then any client who has their SSID set to blank or "any" will get a response from the AP. The other mode is called closed mode and requires the client to have the same SSID setting as the AP in order to get a response. Not all AP vendors support the option of closed mode. The WEP key is an encryption and authentication option that has the aim of making a wireless communication have the same security as if it were a wired connection. It uses a RC4 bit stream cipher. Its goal is to provide authentication as well as data encryption.

There are four modes of using WEP:

- Open Authentication, No Data Encryption
- Shared Key Authentication, No Data Encryption
- Open Authentication, Data Encryption
- Shared Key Authentication, Data Encryption

Not all AP vendors support all modes. Small Office Home Office (SOHO) vendors such as Linksys and Dlink have a limited capability offering only two or three modes. Most high end enterprise vendors such as Cisco, Agere, Symbol, and Enterasys provide for all four forms. Specific vulnerabilities of WEP will be discussed in the next chapter. Open authentication means WEP is not used for authentication purposes. Shared key means before a client can be authenticated an AP sends a random text string to a client and will only authenticate the user if it returns the string encrypted properly with the shared WEP key. Data encryption option obviously determines whether that the data is encrypted using WEP.

There are three states that any wireless client can be in: Unauthenticated/Unassociated, Authenticated/Unassociated, and Authenticated/Associated. A client that wants to connect to a wireless network must first authenticate by having the device set with the proper SSID and WEP key. Once it has authenticated it is then associated. Associated state means that it can send and receive past the access point to the network as if it were physically connected to it. Figure 4.7 shows the relationship between state variables and the wireless services.

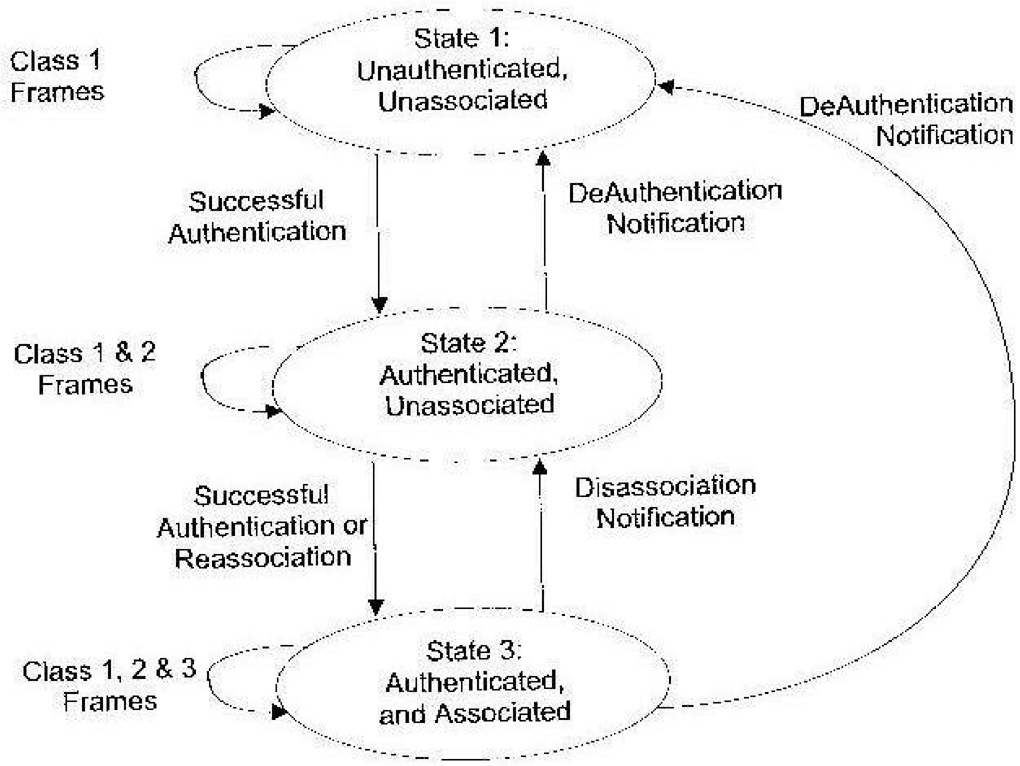


Figure 4.7. Relationship between State Variables and Services [14].

G. THE 802.11 FREQUENCY SPECTRUM

802.11b works in the 2.4 GHz frequency domain, a frequency region requiring no license from the FCC to operate. Although IEEE defined 14 channels in the specification, only 11 may legally be applied to wireless LANs in the US. Out of the 14 only three are non-overlapping: channels 1, 6, and 11.

This is important for two reasons: interference and wireless Access Point (AP) placement. When two or more wireless networks transmit on overlapping channels (for example channels 1 and 2) data rates are reduced due to packet collisions. Figure 4.8 shows how multiple wireless LANs can coexist without frequency induced collisions. The size of each cell is dependent on the amount of power, antenna gain, and environmental factors described in Chapter II. 802.11a which has eight non-overlapping channels vice three allows for a more flexible design.

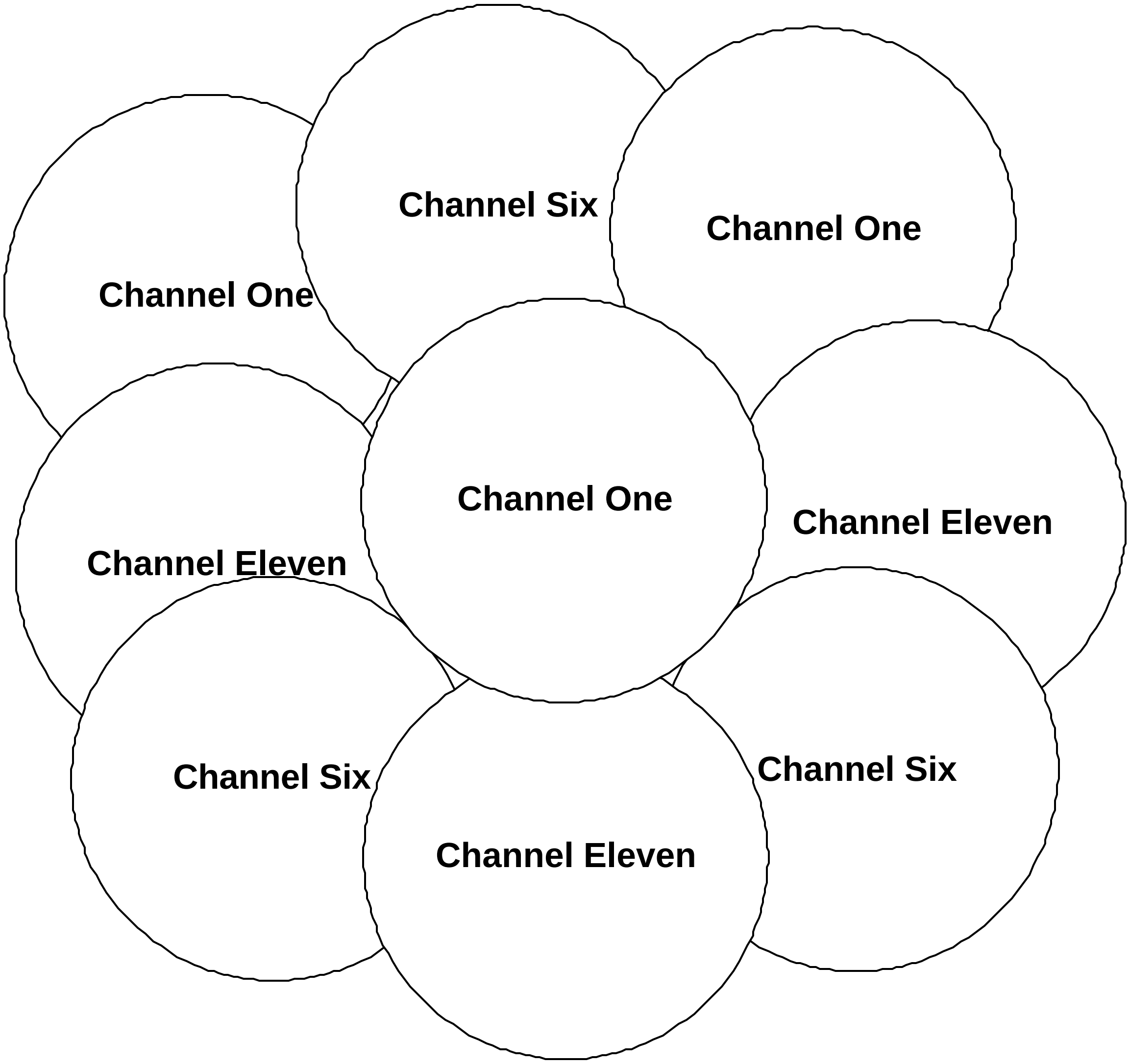


Figure 4.8. 802.11b Channel Optimization.

H. WIRELESS SIGNAL INTERFERENCE

Because the ISM band is unregulated there are many devices that may potentially interfere with 802.11b networks. A sample list of interfering products is listed below:

- Microwave ovens
- Cordless phones
- Home TV re-transmitters
- Remote control devices
- Bluetooth devices
- Other 802.11b devices

It is recommended when installing and using Wireless LAN devices that potential interference items within your wireless LAN work area are identified, removed and/or reconfigured.

I. WECA, WIFI, AND THE UNIVERSITY OF NEW HAMPSHIRE INTEROPERABILITY LAB

The relationship between the FCC and the IEEE needs to be defined. The FCC enforces the laws and defines the regulations for the proper allocation and use of the spectrum within the US territory. The IEEE defines the standards and makes recommendations to industry on the best standard for production. Nevertheless, the problem of interoperability between vendors emerged because of a lack of multi-vendor interoperability body. In 1999 the following companies got together to resolve this problem: 3Com, Aironet (later purchased by Cisco), Intersil, Lucent Technologies, Nokia, and Symbol Technologies. They decided to form a multi-vendor certification lab under an organization called the Wireless Ethernet Compatibility Alliance (WECA) This lab is called the Agilent's Interoperability Certification Lab (ICL). Vendors send their wireless products to undergo interoperability testing as defined in the IEEE 802.11b specification. If the product passes the test they are given a Wireless Fidelity (WI-FI) certification. WECA now has over 140 companies in their membership. It has decided to increase its certification to include 802.11a products and was originally going to use the label of WIFI-5 for the 5 GHz range that 802.11a operates in, but opted at the last minute to use the same WIFI certification symbol for both 802.11b and 802.11a devices and discontinued the WIFI-5 label. WECA has recently decided to change its name to WI-FI as well. The success of WECA has caused some confusion between the difference between IEEE 802.11 and WI-FI. More information on WECA can be found at http://www.wirelessethernet.org.

In 1988, the University of New Hampshire (UNH) started creating a cooperative research and development laboratory to improve the effectiveness of distributed and wireless computing. This structure has become known as the Interoperability Lab, or in the vernacular of computing acronyms, the IOL. The IOL is involved in research and development work, but is mainly used for interoperability and standards conformance by a community of over 200 vendors. The Wireless Consortium branch of the IOL was formed in March of 1996. The Consortium was formed through the cooperative agreement of vendors interested in testing 802.11 wireless products. Consortium members agree to provide a platform representing their equipment at the IOL for at least 18 months. The requirement to leave a platform at the IOL allows the users of the lab to perform interoperability testing with current equipment throughout the year, and without having to make special legal arrangements with other players in the technology. One of the major benefits of consortium membership is: "the ability to test against other vendor's products in a neutral setting without having to incur the capital expense of setting up and operating individual vendor test facilities.” [15]. This approach is very influential on WECA.

J. SUMMARY

The history of the IEEE 802.11 standard and the purpose of the working groups is vital to grasp the capabilities and direction of wireless technologies. To understand the 802.11 specification, the Media Access Control (MAC) layer, the various physical layers and architectural topologies is crucial to building a successful wireless design. Knowledge of the 802.11 frequency spectrum and wireless signal interference issues are also crucial practical factors. Knowledge of the related organizations to include WECA, WI-FI, and the University of New Hampshire Interoperability Lab is vital to ensure system compatibility, interoperability and proper vendor selection.

THIS PAGE INTENTIONALLY LEFT BLANK

V. WIRELESS SECURITY ANALYSIS

A. INTRODUCTION

The focus of this chapter is to make apparent the fundamental security issues associated with 802.11 wireless technology and suggest an appropriate strategy. The flaws of Service Set Identifier (SSID), Wired Equivalent Privacy (WEP), and Media Access Control (MAC) Authentication are reviewed. The most popular network tools and analyzers that are used by IT administrators and hackers were tested on the Naval Postgraduate School wireless LAN. The tools tested were Netstumbler, Airsnort, Ethereal, Airmagnet, and VXsniffer. External 802.11 security solutions such as 802.1X and VPN are suggested. Wireless Intrusion Detection Systems (IDS) and existing Federal Government policy are also reviewed. The final section of the chapter provides an improved wireless network architecture that counters all known threats as of September 2002.

B. SECURITY FUNDAMENTALS

Information system security is based on confidentiality, integrity, and availability also known as the CIA model. The purpose of confidentiality is to ensure that a sender's message is delivered to its intended recipient without the contents of the message revealed to anyone not specified by the sender. Integrity's focus is to ensure that a message that is sent is not advertently or inadvertently modified while it is being transported from sender to receiver. CRC (Cyclic Redundancy Check) and checksum algorithms are sent along with the data during a transmission to prevent unauthorized changes. This is a critical requirement during financial transactions. Changing the amount of financial deposit can cause havoc to any organization. A would-be hacker would love to change a $10 deposit to a $100k deposit. Availability's focus is to ensure that a system is accessible to authorized users and not available to unauthorized users in a reliable fashion.

Another popular model is the AAA model which stands for Authentication, Authorization and Accounting. Authentication is to validate a user or equipment against a database for access to a system. Authorization is the next step. Its function is to grant permissions based on a policy profile for the authenticated user. For example, the Chief Financial Officer will have greater access than a clerk. These profiles may be unique for an individual or for a group. At a university, students, staff and faculty will have different authorization privileges and these privileges can be specified in their profile. Accounting is the ability to track previous transactions. This takes place by logging activity. The AAA and CIA models clearly apply to a successful wireless LAN implementation. The 802.11 specification uses three elements for authentication and authorization: the SSID, the WEP key and MAC address. The chapter's discussion includes how the CIA and AAA models map to the 802.11 wireless medium, the vulnerabilities in the 802.11 design, and the tools and solutions to make 802.11 reasonably secure. Actual scan results of the NPS campus are used for analysis and the chapter concludes with an improved network architecture.

C. SERVICE SET IDENTIFIER (SSID)

For a wireless client to connect to a network the SSID and the WEP key (if used) needs to be known. In most cases, it is extremely important that one not set their SSID to beaconing. The only exception is if the Network Administrator wants the SSID to be easily identified. Public access networks are the notable exception. Otherwise it is recommended that beaconing be turned off. Beaconing SSIDs can easily be seen by freeware programs such as Netstumbler, Kismet, Aerosol, WEP Crack, and Airsnort. Netstumbler has been the most popular program because it can be run on Windows platforms. These freeware programs have induced a phenomenon of detecting and mapping wireless access points for sport, called "war driving", where thousands of access points have been mapped and reported on the internet. Figure 5.1 is an example of Netstumbler mapping. Some war drivers have also subscribed to the behavior of "war chalking". War chalking is based on a symbology used in the 1920s and 1930s that vagrants and hobos have used to identify people and places that give out free food. A hobo might chalk a special symbol near a place for free lunch. War chalking in a similar fashion uses symbols to identify wireless internet access and indicates whether they are beaconing their SSID and if they are using WEP or not. Figure 5.2 shows the symbology of war chalking. An open node means that the wireless LAN is beaconing their SSID and not using WEP encryption. A closed node means the wireless LAN is not beaconing their SSID, and WEP node means they are using WEP encryption.

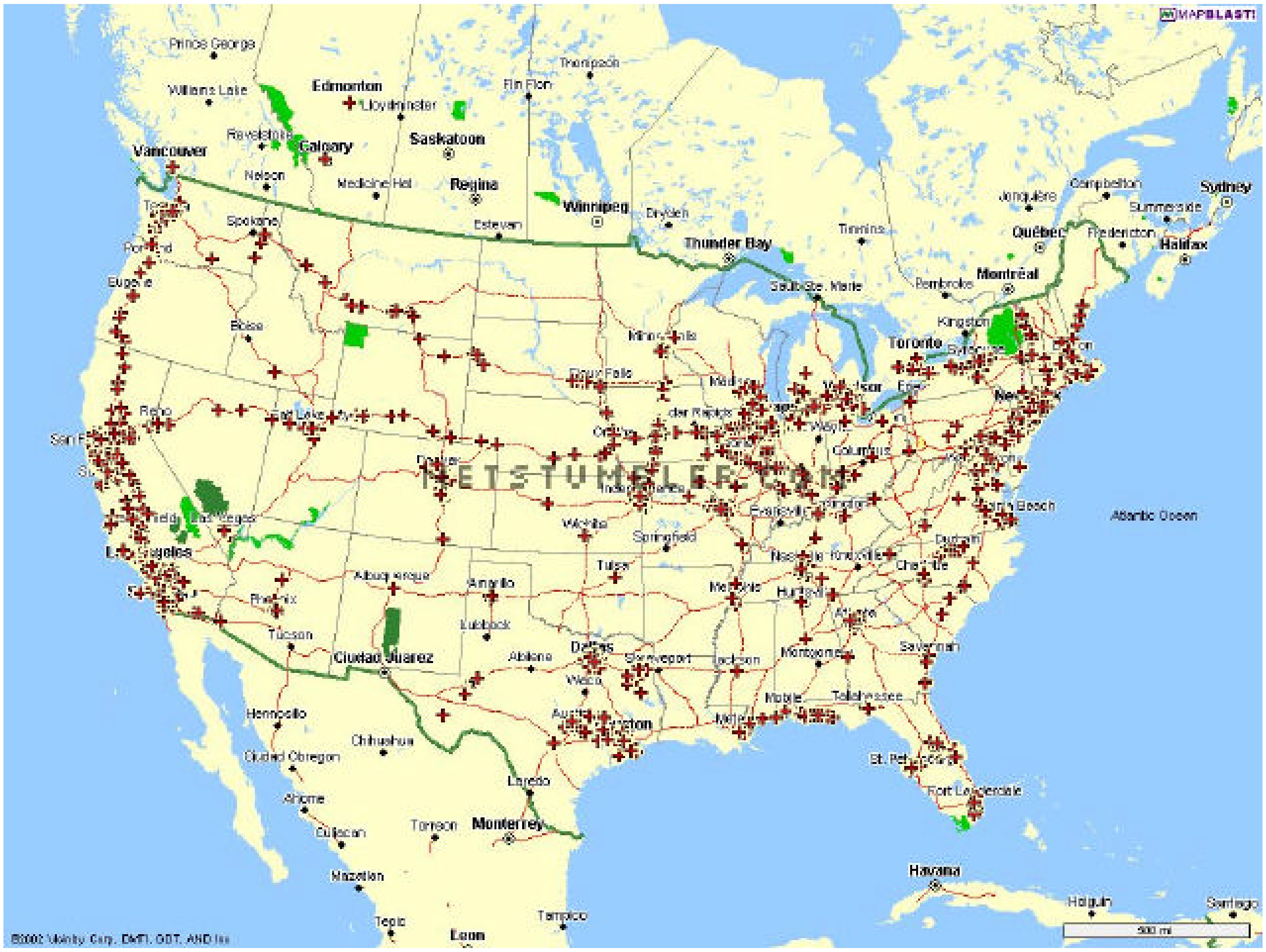


Figure 5.1. A Netstumbler Mapping of Access Points [16].

Setting SSID to non-beaconing and activating WEP encryption should be the first measures for wireless security to be enforced for basic security. Hackers prefer to go after easy targets. **Non SSID beaconing and WEP encryption will prevent many tools from even knowing one is using a wireless LAN, and thus delay/dissuade/prevent low to mid grade hackers from accessing your network.** Figures 5.3 and 5.4 show how to configure access points for WEP and non-SSID beaconing.

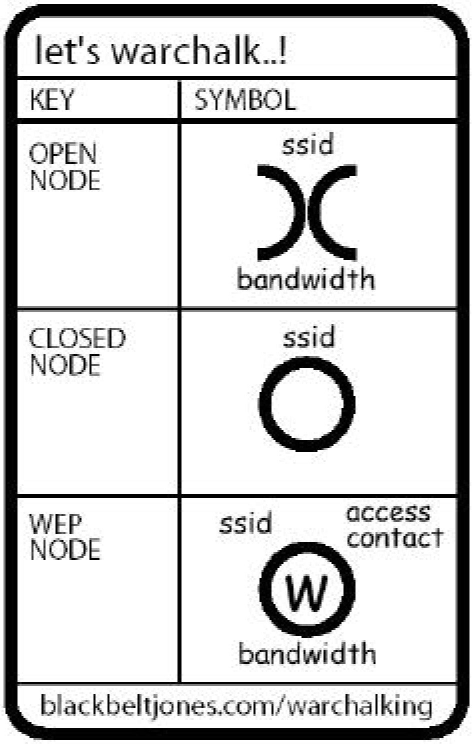
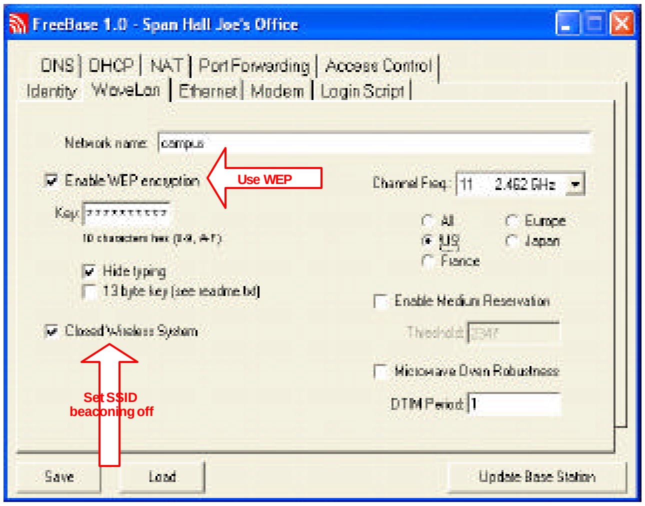


Figure 5.2. War Chalking Symbology [17].



Network name: campus

☑ Enable WEP encryption

Use WEP

Key: **********

10 characters hex (0-9, A-F)

☑ Hide typing

□ 13 byte key (see readme.txt)

☑ Closed Wireless System

Set SSID beaconing off

Channel Freq: 11 2.462 GHz

○ All ○ Europe
● US ○ Japan
○ France

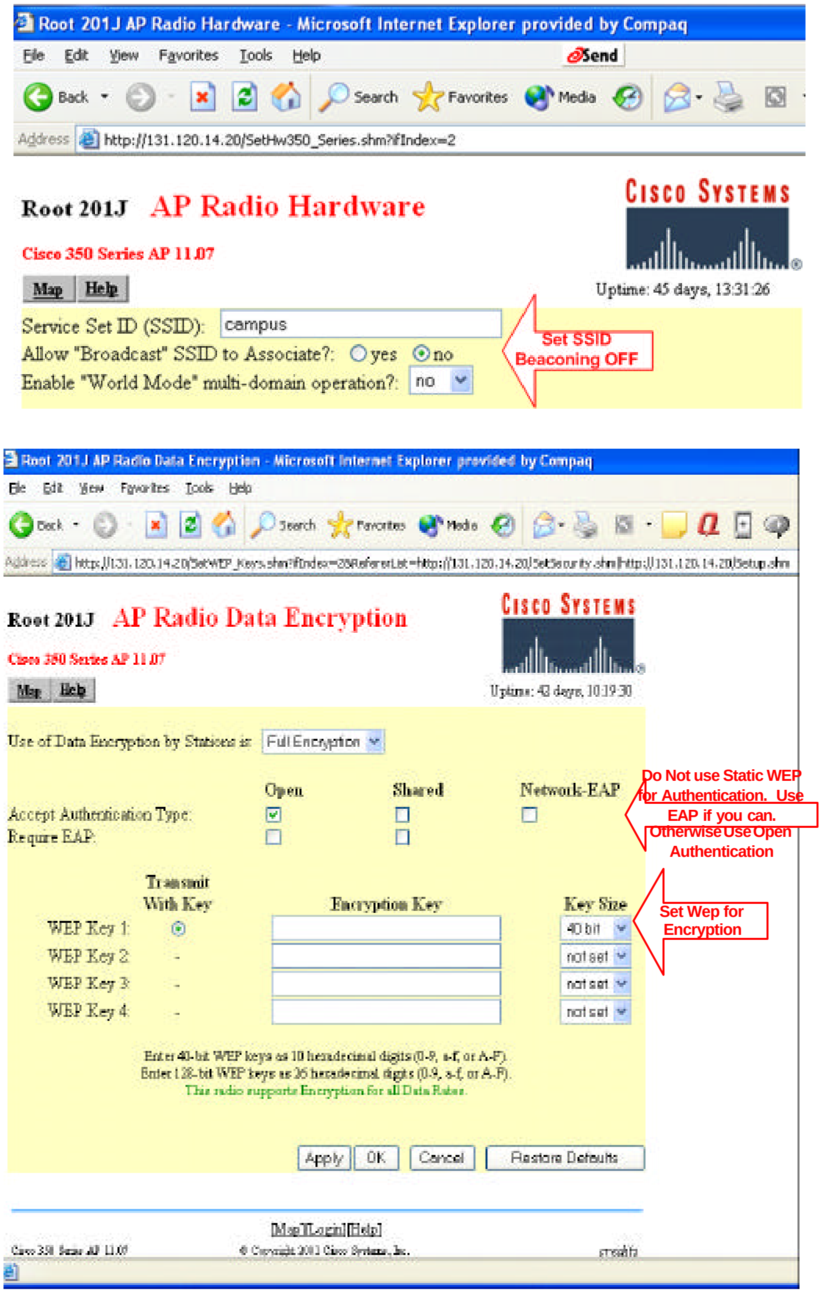
□ Enable Medium Reservation

Threshold: 2347

□ Microwave Oven Robustness

DTIM Period: 1

Figure 5.3. FreeBase Configuration Program Configuring an Apple Airport. (Lucent OEM) to Turn Off SSID Beaconing and Allowing for WEP Encryption [18].


Root 201J AP Radio Hardware - Microsoft Internet Explorer provided by Compaq
File Edit View Favorites Tools Help
Send
Back Search Favorites Media
Address
Cisco Systems
Map Help
Set SSID Beaconing OFF
Root 201J AP Radio Data Encryption - Microsoft Internet Explorer provided by Compaq
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Cisco Systems
Map Help
Do Not use Static WEP for Authentication. Use EAP if you can. Otherwise Use Open Authentication
Set Wep for Encryption
Apply OK Cancel Restore Defaults
[Map][Login][Help]

http://131.120.14.20/SetHw350_Series.shm?ifIndex=2

Root 201J AP Radio Hardware

Cisco 350 Series AP 11.07

Uptime: 45 days, 13:31:26

Service Set ID (SSID): campus

Allow "Broadcast" SSID to Associate?: ○ yes ● no

Enable "World Mode" multi-domain operation?: no

http://131.120.14.20/SetWEP_Keys.shm?ifIndex=2&ReferrerList=http://131.120.14.20/SetSecurity.shm|http://131.120.14.20/Setup.shm

Root 201J AP Radio Data Encryption

Cisco 350 Series AP 11.07

Uptime: 42 days, 10:19:30

Use of Data Encryption by Stations is: Full Encryption

	Open	Shared	Network-EAP
Accept Authentication Type:	☑	□	□
Require EAP:	□	□	

	Transmit With Key	Encryption Key	Key Size
WEP Key 1:	●		40 bit
WEP Key 2:	-		not set
WEP Key 3:	-		not set
WEP Key 4:	-		not set

Enter 40-bit WEP keys as 10 hexadecimal digits (0-9, a-f, or A-F).
Enter 128-bit WEP keys as 26 hexadecimal digits (0-9, a-f, or A-F).
This radio supports Encryption for all Data Rates.

Cisco 350 Series AP 11.07 © Copyright 2001 Cisco Systems, Inc. credits

Figure 5.4. Web Configuration Screens for a Cisco 350 Access Point. (Turn Off SSID Beaconing, Enable WEP Encryption and Set WEP Authentication On, Off, and/or allow for EAP.)

The group Black Alchemy Weapons Lab has developed a freeware program called Fake AP. Fake AP runs on a Linux system and generates thousands of counterfeit beacon frames, thus making it appear as if there were numerous access points. As part of a honeypot or as an instrument of your site security plan, Fake AP confuses Wardrivers, NetStumblers, Script Kiddies, and other undesirables. What better place to hide a tree but in a forest. Fake Ap can be downloaded at http://www.blackalchemy.to/Projects/fakeap/fake-ap.html.

D. WIRED EQUIVALENT PRIVACY (WEP)

Wireless networks by their nature are accessible and hence more vulnerable than wired or optical networks because they transmit data in the air. What the IEEE 802.11 committee hoped for when designing the specification was to come up with a scheme that would provide the same protection as if the data was being transmitted in a wired medium. What they came up with was the Wired Equivalent Privacy (WEP) specification. The requirements they used for developing WEP were:

- Exportable under exiting US law at the time 1997
- Reasonably strong algorithm
- Efficient
- Optional
- Self-synchronizing (Certified Wireless Network Administrator by Planet3 Wireless, p. 261)

WEP is an RC4 64-bit stream cipher that the 802.11 committee intended to be used for both authentication and encryption. RC4 is a weak encryption and the designers knew this at the time of selection. Existing US encryption export laws restricted more advanced encrypted data algorithms. The 802.11 group felt that capturing foreign markets was more important then security. It was later discovered that there were even more significant flaws in the WEP design.

The most fundamental problem is when WEP is used for authentication. The process begins where the access point generates a random sequence of characters and sends them to a client requesting access to the wireless network. In order for the client to gain access to the network it must encrypt the string and send it as a response. The AP then decrypts the string, and if it matches its original transmission, the client is granted access. The problem with this method is that it allows a would-be hacker the possibility of intercepting both unencrypted challenge and the encrypted response. A hacker can then easily derive the WEP key from these two values. Secondly, a hacker might also begin a brute force or dictionary attack to derive the WEP key. A brute force attack is to try every combination of keys and a dictionary attack is to try variations of common words. The effectiveness of this attack is that the AP will respond immediately if the WEP key for authentication is correct or not. It is highly recommended that WEP not be used as the only means of authentication. By themselves WEP keys can be hacked in as little as 15 minutes if used for authentication. Bill Arbaugh's paper *Your 802.11 Wireless Network has no Clothes* [19] explains this vulnerability in greater detail. WEP keys are also used for data encryption. Unfortunately the WEP key can be reversed engineered by hackers if approximately 5-10 million packets can be intercepted even if WEP is used solely for encryption and not for authentication. On a heavily loaded network this might take several hours. On a lightly loaded network this traffic analysis might take up to a week. The vulnerability is based on statistical analysis due to the repetition of the initialization vectors. Fluhrer, Mantin, and Shamir's paper *Weakeness in the Key Scheduling Algorithm of RC4* [20] and Adam Stubblefield's *Using Fluhrer, Mantin, and Shamir Attack to break WEP* [21] explain this vulnerability in greater depth. Freeware Linux programs Airsnort and Wepcrack can be downloaded at http://airsnort.shmoo.com/ and http://sourceforge.net/projects/wepcrack to crack WEP using a Linux operating system. Lucent, Cisco and several other vendors have upgraded their firmware to prevent the exploitation of this vulnerability when using their cards. Nevertheless, if a hacker can mount an active attack using a non-upgraded firmware card, the WEP vulnerability still exists. Of course the 5-10 million packets of interception can then only work between an access point and a client with a non-upgraded firmware card. This may force a hacker to actively interact with a target network using a non-upgraded card. This would pose greater risk for the hacker because going active might reveal the hacker's position. So it is a good idea to upgrade your firmware so it will take longer for a hacker to crack the WEP key and increase the hacker's visibility.

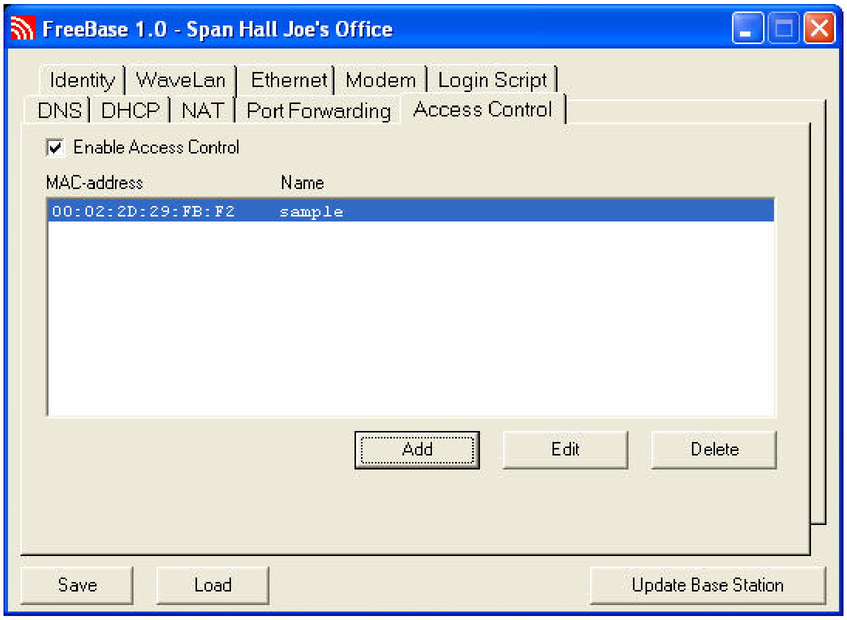
The length of the encryption in the 802.11 spec is 64 bits which includes a 24-bit initialization vector and a 40-bit encryption key. Most vendors have allowed for longer keys such 128-bit and 152-bit keys. They are also referred to 40, 104, and 128 bit keys because of the 24 bit IV is not counted. This has caused confusion, but they are in fact the same. Also according to Jessie Walker's paper *Unsafe at any key size; an analysis of* *the WEP encapsulation* [22], increasing the WEP key does nothing to increase WEP's resistance to attack because of how WEP uses cryptography, not the key size. Because the 128 and 152 WEP keys sizes are not specified in the 802.11 specification use of multiple vendors can cause interoperability problems. The long-term solution as expressed by the 802.11i group is to replace WEP with Advanced Encryption Standard (AES). In the mean time if no other encryption mechanisms are available, it is recommended to use WEP and upgrade the firmware on all access points and all user clients.

E. MEDIA ACCESS CONTROL (MAC) AUTHENTICATION

Although the 802.11 specification does not discuss MAC authentication, most wireless access point vendors provide it with their products as an additional security capability for authentication. A MAC address is a unique hardware identifier on every network card whether wired or wireless. It is assigned and burned into the card by the manufacturer. Depending on the manufacturer one can configure their access point to have a policy that grants and/or denies certain users based on their MAC addresses. This is beneficial. However, there are several problems and vulnerabilities with MAC authentication

- Equipment rather than users is authenticated and therefore stolen equipment might allow for unauthorized users access
- MAC addresses are easily intercepted and can be forged by hackers for unauthorized access. This act is usually called MAC spoofing.
- MAC addresses are difficult to manage on a large scale (such as a campus or enterprise) because they require network administrators to maintain authorization lists for every access point listing every authorized piece of hardware.

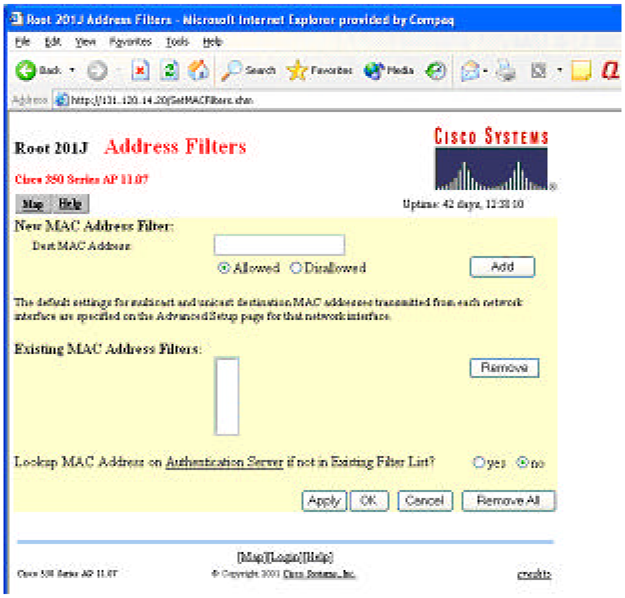
Figures 5.5 and 5.6 show how to enable MAC authentication as a means of access control.



☑ Enable Access Control

MAC-address	Name
00:02:2D:29:FB:F2	sample

Figure 5.5. MAC Access Control Configuration Screen for an Apple Airport (Lucent OEM) Using FreeBase.


Root 201J Address Filters - Microsoft Internet Explorer provided by Compaq
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://131.120.14.20/SetMACFilters.shm
Cisco Systems
Map Help
Add
Remove
Apply
OK
Cancel
Remove All
[Map][Login][Help]
credits

Root 201J Address Filters

Cisco 350 Series AP 11.07

Uptime: 42 days, 12:38:10

New MAC Address Filter:

Dest MAC Address:

● Allowed ○ Disallowed

The default settings for multicast and unicast destination MAC addresses transmitted from each network interface are specified on the Advanced Setup page for that network interface.

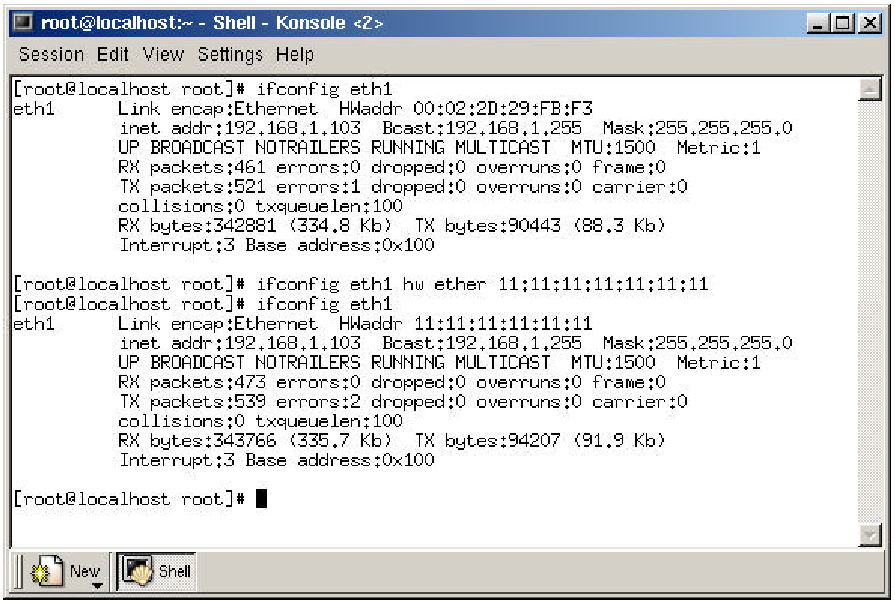
Existing MAC Address Filters:

Lookup MAC Address on Authentication Server if not in Existing Filter List? ○ yes ● no

Cisco 350 Series AP 11.07 © Copyright 2001 Cisco Systems, Inc.

Figure 5.6. MAC Access Control Configuration Screen for a Cisco 350.

Under the Linux operating system the command "`ifconfig ethXX hw ether xx:xx:xx:xx:xx:xx`” allows for the changing/spoofing of Mac Addresses. Figure 5.7 demonstrates the changing of the MAC address from “00:02:2D:29:FB:F3” to “11:11:11:11:11:11”.


root@localhost:~ - Shell - Konsole <2>
Session Edit View Settings Help
New
Shell

```
[root@localhost root]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:02:2D:29:FB:F3
          inet addr:192.168.1.103  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:461 errors:0 dropped:0 overruns:0 frame:0
          TX packets:521 errors:1 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:342881 (334.8 Kb)  TX bytes:90443 (88.3 Kb)
          Interrupt:3 Base address:0x100

[root@localhost root]# ifconfig eth1 hw ether 11:11:11:11:11:11
[root@localhost root]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 11:11:11:11:11:11
          inet addr:192.168.1.103  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST NOTRAILERS RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:473 errors:0 dropped:0 overruns:0 frame:0
          TX packets:539 errors:2 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:343766 (335.7 Kb)  TX bytes:94207 (91.9 Kb)
          Interrupt:3 Base address:0x100

[root@localhost root]# █
```

Figure 5.7. An Example of MAC Spoofing in the Linux Operating System.

F. WIRELESS TOOLS AND CAMPUS ASSESSMENT

This section explains the most popular tools used for wireless assessment. The NPS campus was used as the area for monitoring. Only passive monitoring methods were used and no data was decrypted. The software tools examined include Netstumbler, Mini-Stumbler, Airsnort, Airmagnet, Ethereal, and Vxsniffer. Netstumbler is by far the most popular and is responsible for the term “war driving”. Netstumbler is extremely easy to use and will run on Windows XP, Windows 2000, Windows 9X and has been ported to the PocketPC operating system under the name Mini-Stumbler. According to the author of the program, Marius Milner, Netstumbler should be used by:

1) Security folks checking that their corporate LAN isn't wide open

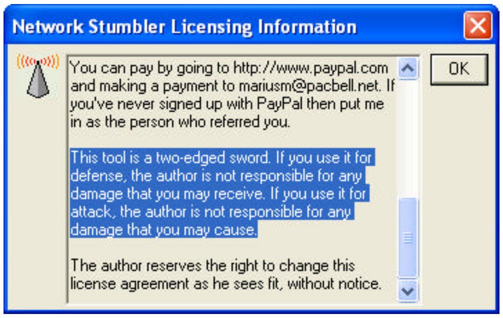
2) Systems admins checking coverage of their Wireless LAN

3) Gatherers of demographic information about 802.11 popularity

4) Drive-by snoopers

5) Overly curious bystanders [23].

Marius does provide a warning in the license window provided in Figure 5.8.



Network Stumbler Licensing Information

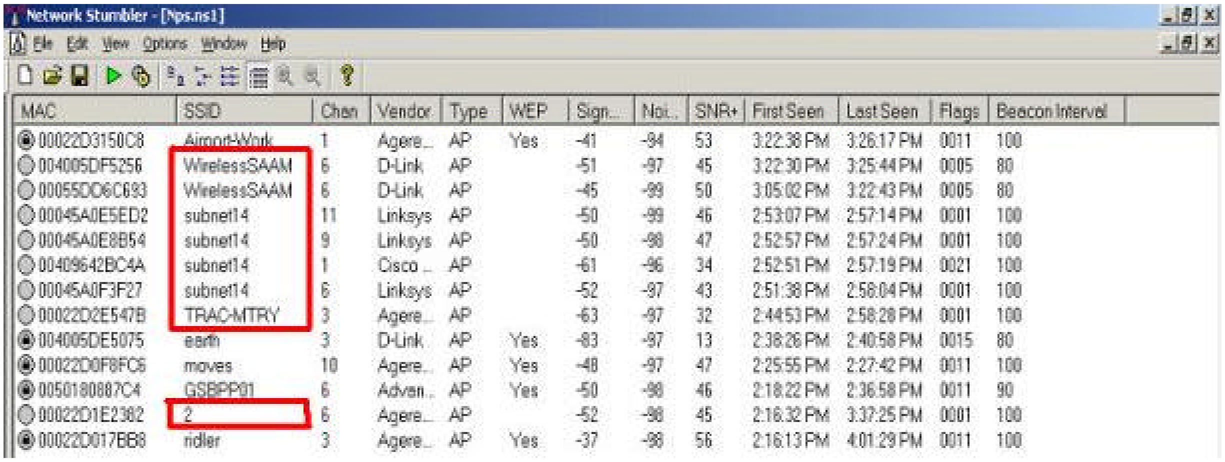
You can pay by going to http://www.paypal.com and making a payment to mariusm@pacbell.net. If you've never signed up with PayPal then put me in as the person who referred you.

This tool is a two-edged sword. If you use it for defense, the author is not responsible for any damage that you may receive. If you use it for attack, the author is not responsible for any damage that you may cause.

The author reserves the right to change this license agreement as he sees fit, without notice.

Figure 5.8. Netstumbler License Information.

The following results in Figure 5.9 were recorded with a laptop running Netstumbler at the Naval Postgraduate School.



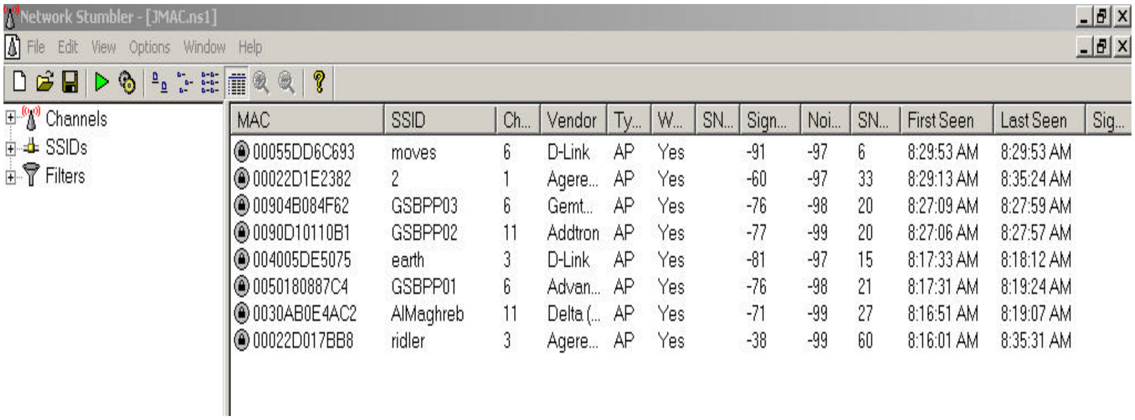
Network Stumbler - [Nps.ns1]

MAC	SSID	Chan	Vendor	Type	WEP	Sign...	Noi...	SNR+	First Seen	Last Seen	Flags	Beacon Interval
● 00022D3150C8	AirportWork	1	Agere...	AP	Yes	-41	-94	53	3:22:38 PM	3:26:17 PM	0011	100
○ 004005DF5256	WirelessSAAM	6	D-Link	AP		-51	-97	45	3:22:30 PM	3:25:44 PM	0005	80
○ 00055DD6C693	WirelessSAAM	6	D-Link	AP		-45	-99	50	3:05:02 PM	3:22:43 PM	0005	80
○ 00045A0E5ED2	subnet14	11	Linksys	AP		-50	-99	46	2:53:07 PM	2:57:14 PM	0001	100
○ 00045A0E8B54	subnet14	9	Linksys	AP		-50	-98	47	2:52:57 PM	2:57:24 PM	0001	100
○ 00409642BC4A	subnet14	1	Cisco ...	AP		-61	-96	34	2:52:51 PM	2:57:19 PM	0021	100
○ 00045A0F3F27	subnet14	6	Linksys	AP		-52	-97	43	2:51:38 PM	2:58:04 PM	0001	100
○ 00022D2E547B	TRAC-MTRY	3	Agere...	AP		-63	-97	32	2:44:53 PM	2:58:28 PM	0001	100
● 004005DE5075	earth	3	D-Link	AP	Yes	-83	-97	13	2:38:26 PM	2:40:58 PM	0015	80
● 00022D0F8FC6	moves	10	Agere...	AP	Yes	-48	-97	47	2:25:55 PM	2:27:42 PM	0011	100
● 0050180887C4	GSBPP01	6	Advan...	AP	Yes	-50	-98	46	2:18:22 PM	2:36:58 PM	0011	90
○ 00022D1E2382	2	6	Agere...	AP		-52	-98	45	2:16:32 PM	3:37:25 PM	0001	100
● 00022D017BB8	ridler	3	Agere...	AP	Yes	-37	-98	56	2:16:13 PM	4:01:29 PM	0011	100

Figure 5.9. Netstumbler Scan of the NPS Campus on 2/16/02.

Netstumbler identifies access points that are beaconing their SSIDs. From this information a user can deduce network card manufacturer, whether WEP encryption is used, and the MAC address of the card. Netstumbler can be defeated by turning beaconing off at the access point and by using WEP encryption. Some low end access points do not have the ability to turn off beaconing. The SSIDs that are circled in red are the most vulnerable because they are not using encryption and hacker might possibly use this wireless LAN as a point of entry to the wired infrastructure.

After drafting a local wireless policy (included in Appendix A) with the help of the NPS IT support staff and the wireless group an education campaign was begun to improve wireless security and usability. A couple of months later another scan of the campus was done with the following results in Figure 5.10:



MAC	SSID	Ch...	Vendor	Ty...	W...	SN...	Sign...	Noi...	SN...	First Seen	Last Seen	Sig...
00055DD6C693	moves	6	D-Link	AP	Yes		-91	-97	6	8:29:53 AM	8:29:53 AM	
00022D1E2382	2	1	Agere...	AP	Yes		-60	-97	33	8:29:13 AM	8:35:24 AM	
00904B084F62	GSBPP03	6	Gemt...	AP	Yes		-76	-98	20	8:27:09 AM	8:27:59 AM	
0090D10110B1	GSBPP02	11	Addtron	AP	Yes		-77	-99	20	8:27:06 AM	8:27:57 AM	
004005DE5075	earth	3	D-Link	AP	Yes		-81	-97	15	8:17:33 AM	8:18:12 AM	
0050180887C4	GSBPP01	6	Advan...	AP	Yes		-76	-98	21	8:17:31 AM	8:19:24 AM	
0030AB0E4AC2	AlMaghreb	11	Delta (...	AP	Yes		-71	-99	27	8:16:51 AM	8:19:07 AM	
00022D017BB8	ridler	3	Agere...	AP	Yes		-38	-99	60	8:16:01 AM	8:35:31 AM	

Figure 5.10. Netstumbler Scan of the NPS Campus on 5/16/02.

The number of APs that are beaconing have been reduced and all of them are using encryption. To ensure ongoing compliance monthly (or more frequent) scans are performed and published on the school's intranet with the aim of improving security and at the same time make it a learning experience.

On 8/24/02 a limited scan of the campus was performed using three additional tools Mini-stumbler (PocketPC port of Netstumbler), AirSnort and AirMagnet. The area that was monitored was the campus quadrangle and is shown in Figure 5.11. Three passes were run, one for each of the tools. Each pass lasted about 10 minutes consisting of a round trip from the Library to the roof of Spanagel Hall. No buildings were entered with the exception of Spanagel Hall and no amplifiers or external antennas were used with the wireless cards.

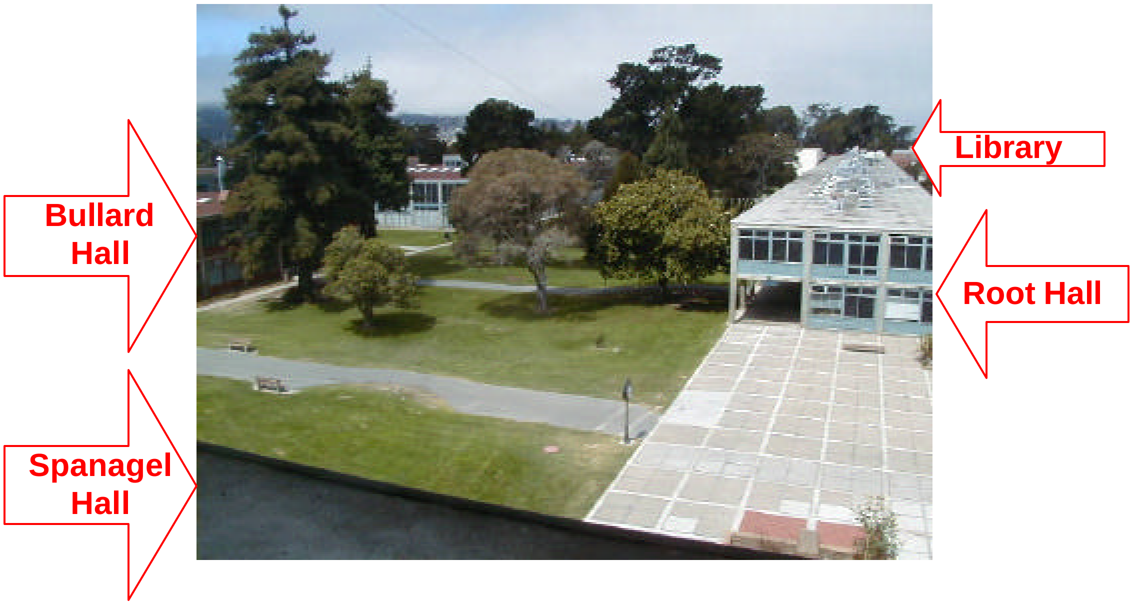
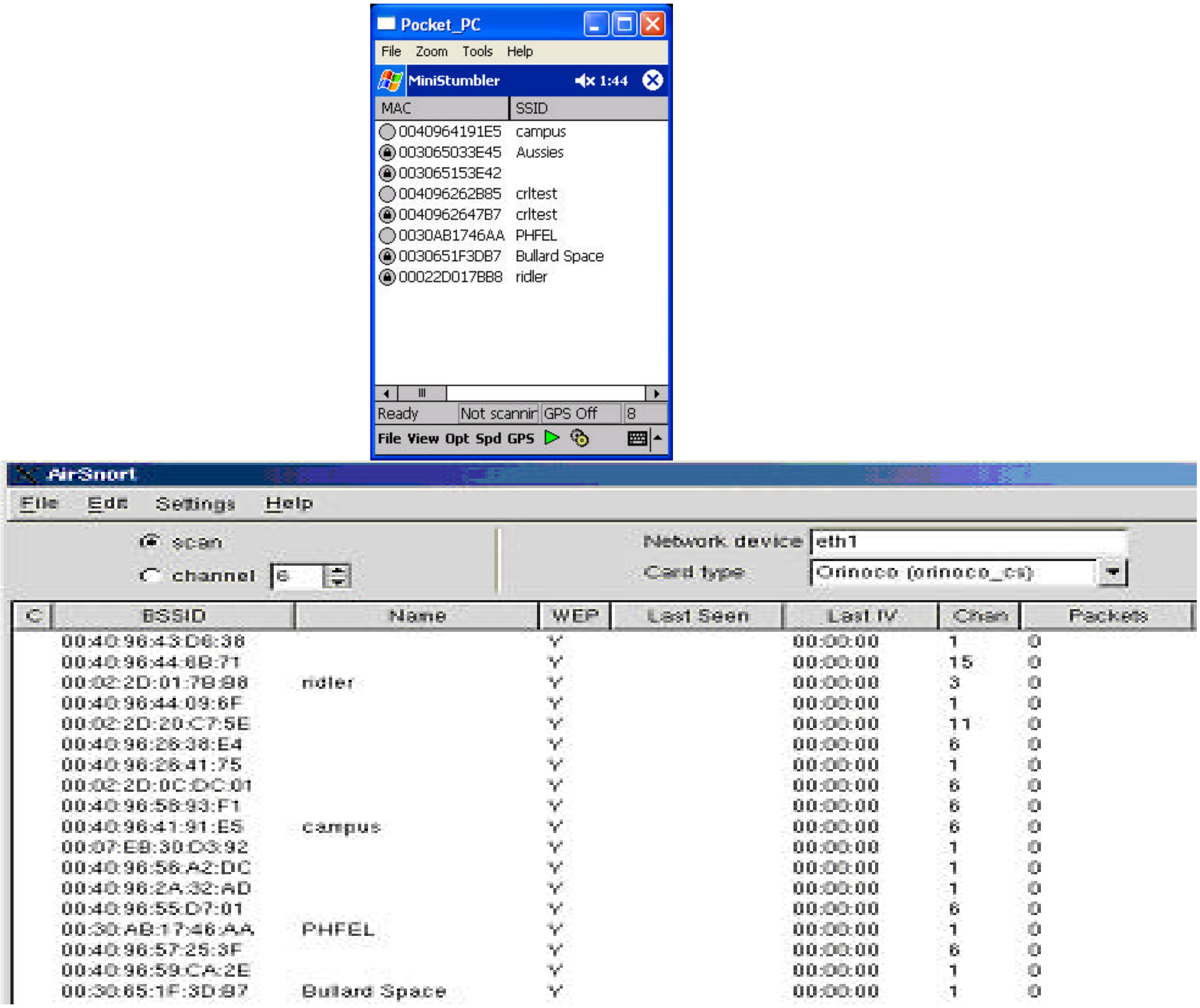


Figure 5.11. NPS Campus Quadrangle as seen from the Roof of Spanagel Hall.

Figure 5.12 shows the results from the Mini-stumbler and Air Snort scans. Both of these programs are freeware. Airsnort is a Linux application being used on a laptop. Airsnort has two additional capabilities over Mini/Netstumbler:

- The ability to see MAC address of wireless devices even if they are not beaconing their SSID
- The ability to crack WEP keys.

No attempt to crack the WEP key was made because it requires 5-10 million packets which might take over a week of constant collection. It is interesting to point out that Mini-Stumbler detected “crltest” and “Aussies” SSIDs where Airsnort did not. AirSnort did detect several device MAC addresses that were not beaconing. Mini-Stumbler was able to detect 8 devices and Airsnort was able to detect 18.



MAC	SSID
○ 0040964191E5	campus
● 003065033E45	Aussies
● 003065153E42	
○ 004096262B85	crltest
● 0040962647B7	crltest
○ 0030AB1746AA	PHFEL
● 0030651F3DB7	Bullard Space
● 00022D017BB8	ridler

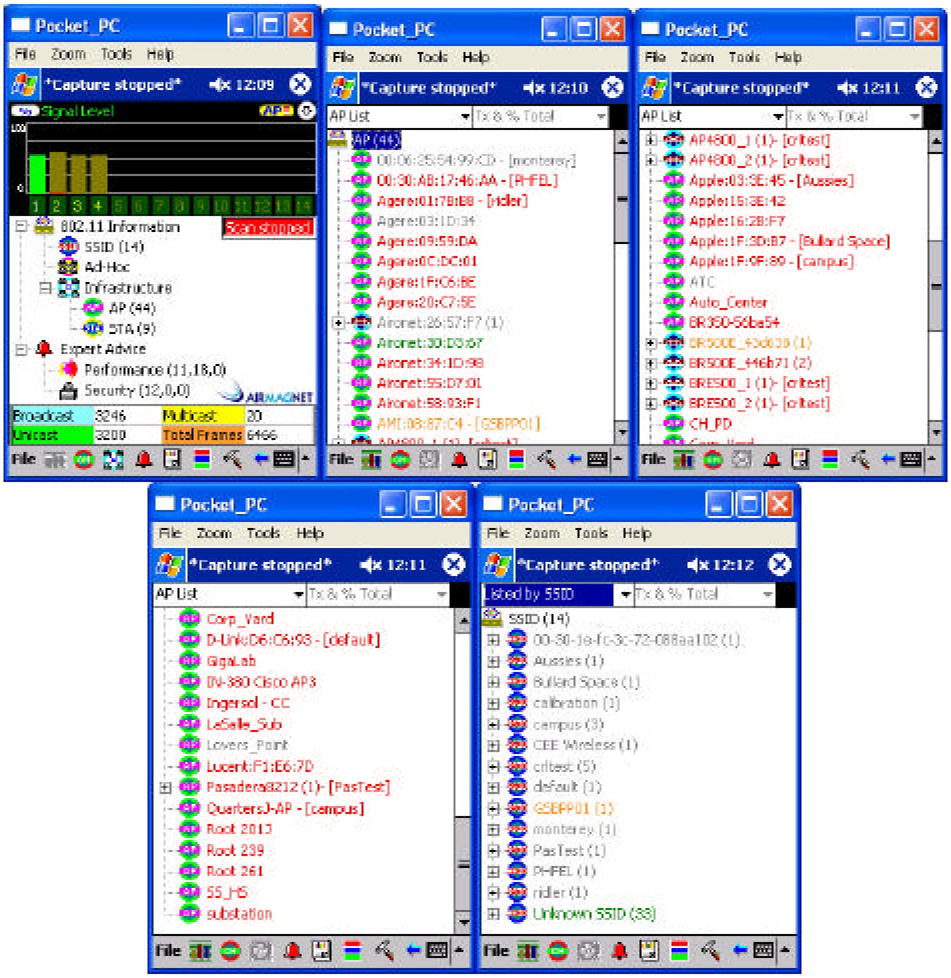
● scan
○ channel 6

Network device eth1
Card type Orinoco (orinoco_cs)

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets
	00:40:96:43:D6:38		Y		00:00:00	1	0
	00:40:96:44:6B:71		Y		00:00:00	15	0
	00:02:2D:01:7B:B8	ridler	Y		00:00:00	3	0
	00:40:96:44:09:6F		Y		00:00:00	1	0
	00:02:2D:20:C7:5E		Y		00:00:00	11	0
	00:40:96:26:38:E4		Y		00:00:00	6	0
	00:40:96:26:41:75		Y		00:00:00	1	0
	00:02:2D:0C:DC:01		Y		00:00:00	6	0
	00:40:96:58:93:F1		Y		00:00:00	6	0
	00:40:96:41:91:E5	campus	Y		00:00:00	6	0
	00:07:EB:30:D3:92		Y		00:00:00	1	0
	00:40:96:56:A2:DC		Y		00:00:00	1	0
	00:40:96:2A:32:AD		Y		00:00:00	1	0
	00:40:96:55:D7:01		Y		00:00:00	6	0
	00:30:AB:17:46:AA	PHFEL	Y		00:00:00	1	0
	00:40:96:57:25:3F		Y		00:00:00	6	0
	00:40:96:59:CA:2E		Y		00:00:00	1	0
	00:30:65:1F:3D:B7	Bullard Space	Y		00:00:00	1	0

Figure 5.12. Mini-Stumbler and Airsnort Scan of the NPS Quadrangle 8/24/02.

The third tool, Airmagnet, costs $2500 (http://www.airmagnet.com) and was on loan from Dean Au, the CEO of Airmagnet. Airmagnet runs only on a PocketPC that has a PCMCIA slot. It uses a modified Cisco 350 wireless card. It has the ability to see all wireless devices whether or not they are beaconing their SSID. It is also capable of detecting devices with greater precision, has sniffing and advanced security/performance analysis capability. Unlike Airsnort, it does not have the ability crack WEP. Figure 5.13 shows the result Airmagnet's 53 detections. Figure 5.14 shows the performance and security analysis. It identifies which APs are not using WEP and shows channel conflict that will degrade data rate performance. Table 5.1 shows the comparison results from the three tools. Other free tools such as Wepcrack, Kismet and Aerosol are available but were not tested. Additionally Sniffer technologies (http://www.sniffer.com/products/sniffer-wireless/), Berkley Veritronics Systems (http://www.bvsystems.com/Products/WLAN/WLAN.htm), and Wild Packets (http://www.wildpackets.com/) all sell commercial grade detection products similar to the ones tested here.



```
*Capture stopped*   12:09
802.11 Information          Scan stopped
  SSID (14)
  Ad-Hoc
  Infrastructure
    AP (44)
    STA (9)
Expert Advice
  Performance (11,18,0)
  Security (12,0,0)
Broadcast  3246    Multicast     20
Unicast    3200    Total Frames  6466
```

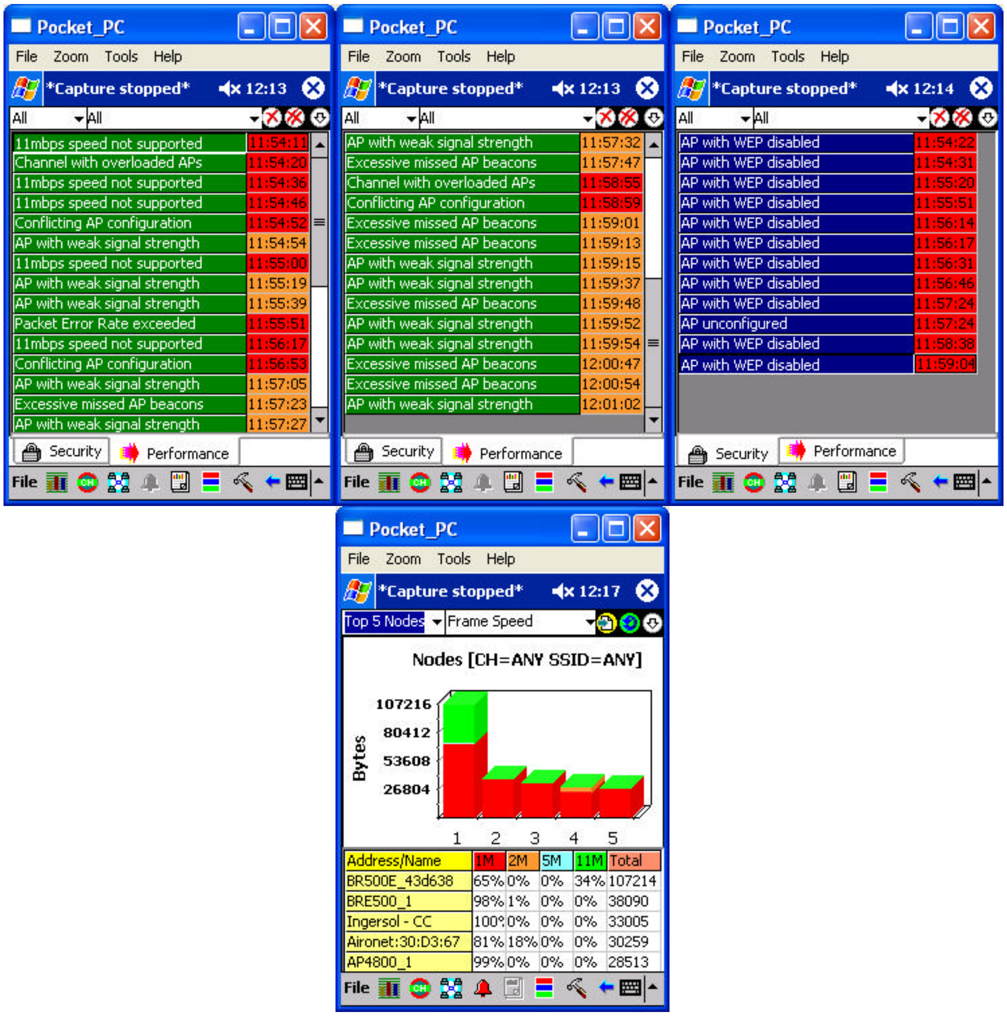
```
*Capture stopped*   12:10
AP List   Tx & % Total
AP (44)
  00:06:25:54:99:CD - [monterey]
  00:30:AB:17:46:AA - [PHFEL]
  Agere:01:78:B8 - [ridler]
  Agere:03:1D:34
  Agere:09:59:DA
  Agere:0C:DC:01
  Agere:1F:C6:BE
  Agere:20:C7:5E
+ Aironet:26:57:F7 (1)
  Aironet:30:D3:67
  Aironet:34:1D:98
  Aironet:55:D7:01
  Aironet:58:93:F1
  AMI:08:87:C4 - [GSBPP01]
```

```
*Capture stopped*   12:11
AP List   Tx & % Total
+ AP4800_1 (1)- [crltest]
+ AP4800_2 (1)- [crltest]
  Apple:03:3E:45 - [Aussies]
  Apple:15:3E:42
  Apple:16:28:F7
  Apple:1F:3D:87 - [Bullard Space]
  Apple:1F:9F:89 - [campus]
  ATC
  Auto_Center
  BR350-56ba54
+ BR500E_43d038 (1)
+ BR500E_446b71 (2)
+ BRE500_1 (1)- [crltest]
+ BRE500_2 (1)- [crltest]
  CH_PD
```

```
*Capture stopped*   12:11
AP List   Tx & % Total
  Corp_Yard
  D-Link:D6:C6:93 - [default]
  GigaLab
  IN-380 Cisco AP3
  Ingersol - CC
  LaSalle_Sub
  Lovers_Point
  Lucent:F1:E6:7D
+ Pasadera8212 (1)- [PasTest]
  QuartersJ-AP - [campus]
  Root 2013
  Root 239
  Root 261
  SS_HS
  substation
```

```
*Capture stopped*   12:12
Listed by SSID   Tx & % Total
SSID (14)
+ 00-30-1e-fc-3c-72-088aa102 (1)
+ Aussies (1)
+ Bullard Space (1)
+ calibration (1)
+ campus (3)
+ CEE Wireless (1)
+ crltest (5)
+ default (1)
+ GSBPP01 (1)
+ monterey (1)
+ PasTest (1)
+ PHFEL (1)
+ ridler (1)
+ Unknown SSID (33)
```

Figure 5.13.   Airmagnet's Scan Results of the NPS's Quad.



11mbps speed not supported	11:54:11
Channel with overloaded APs	11:54:20
11mbps speed not supported	11:54:36
11mbps speed not supported	11:54:46
Conflicting AP configuration	11:54:52
AP with weak signal strength	11:54:54
11mbps speed not supported	11:55:00
AP with weak signal strength	11:55:19
AP with weak signal strength	11:55:39
Packet Error Rate exceeded	11:55:51
11mbps speed not supported	11:56:17
Conflicting AP configuration	11:56:53
AP with weak signal strength	11:57:05
Excessive missed AP beacons	11:57:23
AP with weak signal strength	11:57:27

AP with weak signal strength	11:57:32
Excessive missed AP beacons	11:57:47
Channel with overloaded APs	11:58:55
Conflicting AP configuration	11:58:59
Excessive missed AP beacons	11:59:01
Excessive missed AP beacons	11:59:13
AP with weak signal strength	11:59:15
AP with weak signal strength	11:59:37
Excessive missed AP beacons	11:59:48
AP with weak signal strength	11:59:52
AP with weak signal strength	11:59:54
Excessive missed AP beacons	12:00:47
Excessive missed AP beacons	12:00:54
AP with weak signal strength	12:01:02

AP with WEP disabled	11:54:22
AP with WEP disabled	11:54:31
AP with WEP disabled	11:55:20
AP with WEP disabled	11:55:51
AP with WEP disabled	11:56:14
AP with WEP disabled	11:56:17
AP with WEP disabled	11:56:31
AP with WEP disabled	11:56:46
AP with WEP disabled	11:57:24
AP unconfigured	11:57:24
AP with WEP disabled	11:58:38
AP with WEP disabled	11:59:04

Address/Name	1M	2M	5M	11M	Total
BR500E_43d638	65%	0%	0%	34%	107214
BRE500_1	98%	1%	0%	0%	38090
Ingersol - CC	100°	0%	0%	0%	33005
Aironet:30:D3:67	81%	18%	0%	0%	30259
AP4800_1	99%	0%	0%	0%	28513

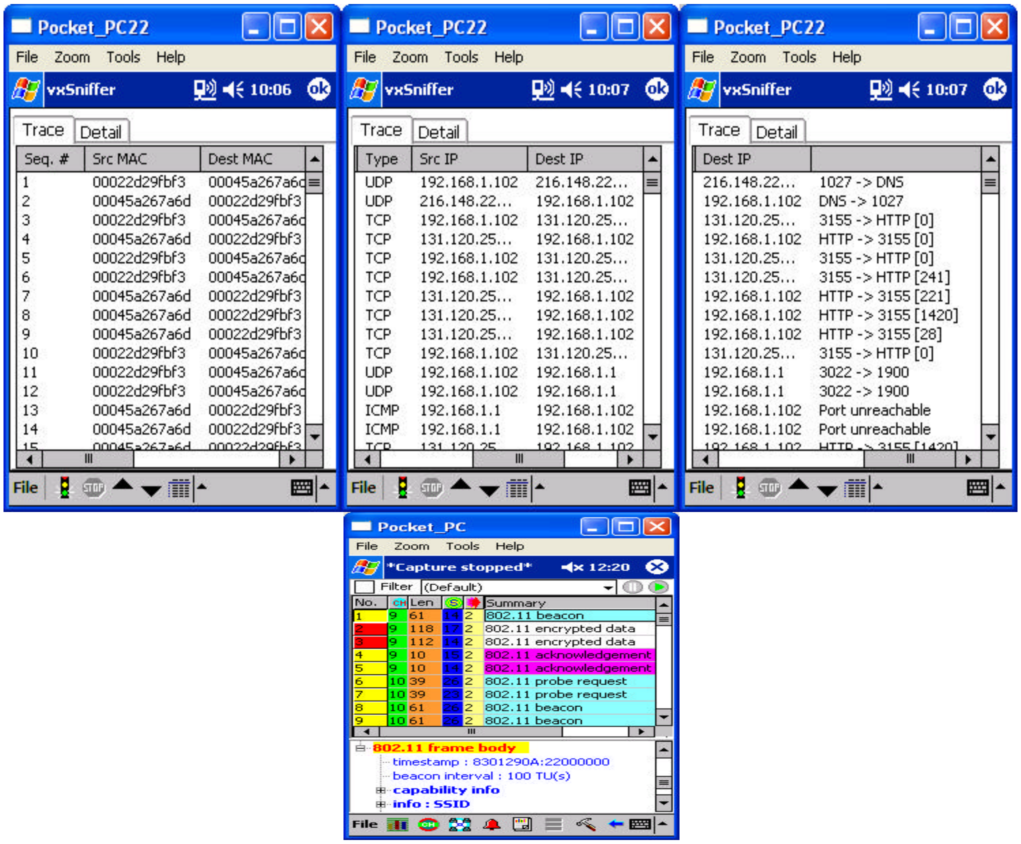
Figure 5.14. Airmagnet's Performance/Security Analysis.

Monitoring Tool	**# of Mac Addresses Detected**
Mini-Stumbler	8
AirSnort	18
Airmaganet	53

Table 5.1. Wireless Tool Comparisons.

G. NETWORK ANALYZERS

Network analyzers are the ideal tool to understand how protocols interact with each other in both wired and wireless networking. They are a fundamental teaching tool in the most basic networking classes. They are also perfectly suited to troubleshoot network and RF problems within a wireless network. They are also the hacker's best friend to eavesdrop or sniff traffic in order to obtain a MAC address for spoofing. Once an encryption key has been cracked a network monitor is capable of allowing a hacker to read the data frames. Under the 802.11 specification only the data frames are encrypted. If a wireless network is not configured to use any encryption or is reliant on WEP and WEP has been broken then a hacker is able to sniff passwords, credit card information, email, etc. If the hacker is unable to break the encryption key he or she will not be able to do this. That is why it is important to use some sort of dynamic key other than static WEP whether it be dynamic WEP, VPN, AES, 3DES, etc**.** Figure 5.15 shows two examples of wireless sniffers for the PocketPC: vxSniffer and Airmagnet. Vxsniffer is made by the Cambridge Computer Corporation (http://www.cam.com) and costs $59.95 but is free for a 30 day evaluation. Airmagnet already previously discussed has sniffer capability in addition to other site survey/war driving functionality.



Seq. #	Src MAC	Dest MAC
1	00022d29fbf3	00045a267a6d
2	00045a267a6d	00022d29fbf3
3	00022d29fbf3	00045a267a6d
4	00045a267a6d	00022d29fbf3
5	00022d29fbf3	00045a267a6d
6	00022d29fbf3	00045a267a6d
7	00045a267a6d	00022d29fbf3
8	00045a267a6d	00022d29fbf3
9	00045a267a6d	00022d29fbf3
10	00022d29fbf3	00045a267a6d
11	00022d29fbf3	00045a267a6d
12	00022d29fbf3	00045a267a6d
13	00045a267a6d	00022d29fbf3
14	00045a267a6d	00022d29fbf3

Type	Src IP	Dest IP
UDP	192.168.1.102	216.148.22...
UDP	216.148.22...	192.168.1.102
TCP	192.168.1.102	131.120.25...
TCP	131.120.25...	192.168.1.102
TCP	192.168.1.102	131.120.25...
TCP	192.168.1.102	131.120.25...
TCP	131.120.25...	192.168.1.102
TCP	131.120.25...	192.168.1.102
TCP	131.120.25...	192.168.1.102
TCP	192.168.1.102	131.120.25...
UDP	192.168.1.102	192.168.1.1
UDP	192.168.1.102	192.168.1.1
ICMP	192.168.1.1	192.168.1.102
ICMP	192.168.1.1	192.168.1.102

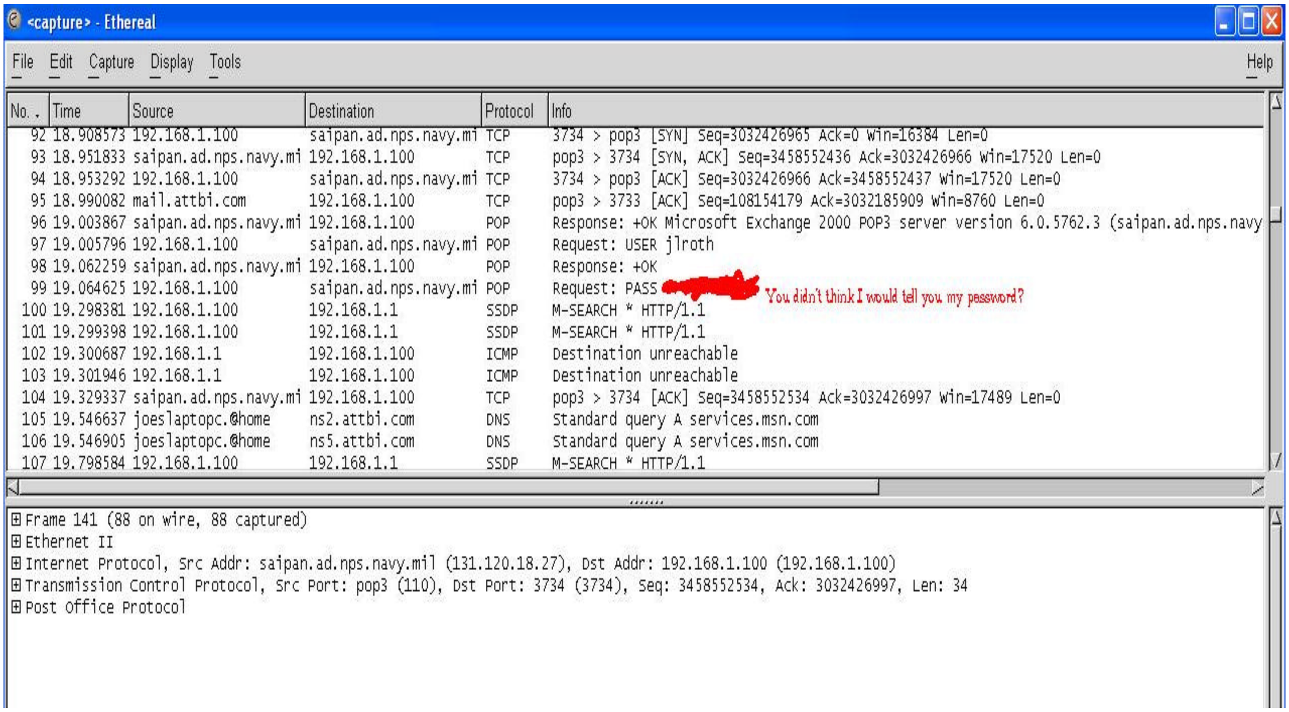
Dest IP	
216.148.22...	1027 -> DNS
192.168.1.102	DNS -> 1027
131.120.25...	3155 -> HTTP [0]
192.168.1.102	HTTP -> 3155 [0]
131.120.25...	3155 -> HTTP [0]
131.120.25...	3155 -> HTTP [241]
192.168.1.102	HTTP -> 3155 [221]
192.168.1.102	HTTP -> 3155 [1420]
192.168.1.102	HTTP -> 3155 [28]
131.120.25...	3155 -> HTTP [0]
192.168.1.1	3022 -> 1900
192.168.1.1	3022 -> 1900
192.168.1.102	Port unreachable
192.168.1.102	Port unreachable

No.	CH	Len	S		Summary
1	9	61	14	2	802.11 beacon
2	9	118	17	2	802.11 encrypted data
3	9	112	14	2	802.11 encrypted data
4	9	10	15	2	802.11 acknowledgement
5	9	10	14	2	802.11 acknowledgement
6	10	39	26	2	802.11 probe request
7	10	39	23	2	802.11 probe request
8	10	61	26	2	802.11 beacon
9	10	61	26	2	802.11 beacon

802.11 frame body
- timestamp : 8301290A:22000000
- beacon interval : 100 TU(s)
- capability info
- info : SSID

Figure 5.15. Examples of Two Wireless Sniffers vxSniffer (Top) and Airmagnet (Bottom).

Ethereal is one of the most popular network analyzers because it will run on most operating systems. It is free and can be downloaded at http://www.ethereal.com . As mentioned before if effective encryption is used then the only thing a sniffer will see is encrypted data. The management frames and control frames which never use encryption are still visible. Even if SSID beaconing is turned off, the SSID is broadcasted from an authorized client to an access point when it authenticates. The SSID might then be intercepted using network analyzer tools at that stage. The real threat to privacy is if no WEP is used or the WEP key is known. In a static WEP key LAN the WEP key is known by all its users. As an experiment, Ethereal was run on laptop against a wireless desktop on the same network that was checking its email via a home wireless network. WEP was enabled on the network. Because the eavesdropper already knew the WEP key all traffic on an access point might be intercepted in a shared static key WEP key implementation. Figure 5.16 shows the intercepted traffic of a POP3 mail server. The userid and password of Joe Roth is clearly revealed. The password has been crossed out because the author does not wish to be hacked.



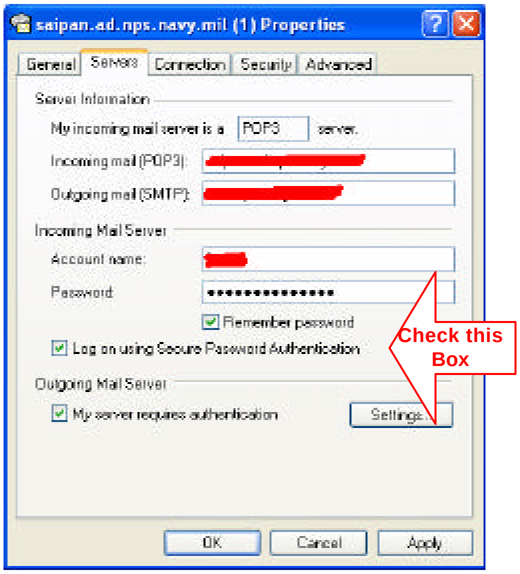
```
No. . Time      Source               Destination          Protocol Info
   92 18.908573 192.168.1.100        saipan.ad.nps.navy.mi TCP     3734 > pop3 [SYN] Seq=3032426965 Ack=0 Win=16384 Len=0
   93 18.951833 saipan.ad.nps.navy.mi 192.168.1.100       TCP      pop3 > 3734 [SYN, ACK] Seq=3458552436 Ack=3032426966 Win=17520 Len=0
   94 18.953292 192.168.1.100        saipan.ad.nps.navy.mi TCP     3734 > pop3 [ACK] Seq=3032426966 Ack=3458552437 Win=17520 Len=0
   95 18.990082 mail.attbi.com       192.168.1.100        TCP      pop3 > 3733 [ACK] Seq=108154179 Ack=3032185909 Win=8760 Len=0
   96 19.003867 saipan.ad.nps.navy.mi 192.168.1.100       POP      Response: +OK Microsoft Exchange 2000 POP3 server version 6.0.5762.3 (saipan.ad.nps.navy
   97 19.005796 192.168.1.100        saipan.ad.nps.navy.mi POP     Request: USER jlroth
   98 19.062259 saipan.ad.nps.navy.mi 192.168.1.100       POP      Response: +OK
   99 19.064625 192.168.1.100        saipan.ad.nps.navy.mi POP     Request: PASS [redacted]
  100 19.298381 192.168.1.100        192.168.1.1          SSDP     M-SEARCH * HTTP/1.1
  101 19.299398 192.168.1.100        192.168.1.1          SSDP     M-SEARCH * HTTP/1.1
  102 19.300687 192.168.1.1          192.168.1.100        ICMP     Destination unreachable
  103 19.301946 192.168.1.1          192.168.1.100        ICMP     Destination unreachable
  104 19.329337 saipan.ad.nps.navy.mi 192.168.1.100       TCP      pop3 > 3734 [ACK] Seq=3458552534 Ack=3032426997 Win=17489 Len=0
  105 19.546637 joeslaptopc.@home    ns2.attbi.com        DNS      Standard query A services.msn.com
  106 19.546905 joeslaptopc.@home    ns5.attbi.com        DNS      Standard query A services.msn.com
  107 19.798584 192.168.1.100        192.168.1.1          SSDP     M-SEARCH * HTTP/1.1
```

You didn't think I would tell you my password?

```
⊞ Frame 141 (88 on wire, 88 captured)
⊞ Ethernet II
⊞ Internet Protocol, Src Addr: saipan.ad.nps.navy.mil (131.120.18.27), Dst Addr: 192.168.1.100 (192.168.1.100)
⊞ Transmission Control Protocol, Src Port: pop3 (110), Dst Port: 3734 (3734), Seq: 3458552534, Ack: 3032426997, Len: 34
⊞ Post Office Protocol
```

Figure 5.16. Ethereal Interception of Login and Password Credentials via Wireless Sniffing.

The obvious question that needs to be asked is how can someone protect themselves if they use a wireless network that either does not use encryption or uses a static WEP key and does not wish to have their traffic read by either members of the network or from nonmembers of the network. The solution is application security. This means that applications must provide further security to encrypt and authenticate data. For example, Outlook Express has the option of encrypting the logon information. This is demonstrated in Figure 5.17.



My incoming mail server is a POP3 server.

Incoming mail (POP3): [redacted]

Outgoing mail (SMTP): [redacted]

Account name: [redacted]

Password: ***************

☑ Remember password

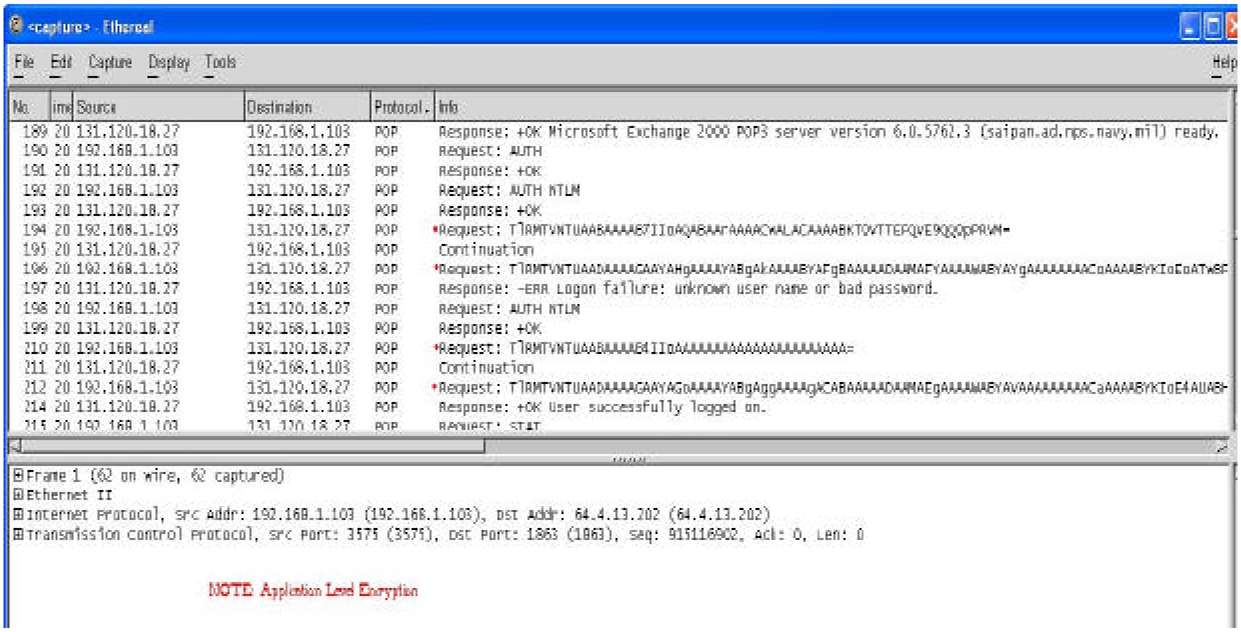
☑ Log on using Secure Password Authentication

☑ My server requires authentication

Check this Box

Figure 5.17. Enabling Secure Password Authentication in Microsoft Outlook Express.

Ethereal was run again and the results of the sniff are shown below in Figure 5.18. The userid and password are no longer visible. They have been replaced with an encrypted hash and therefore useless to the eavesdropper. In this example only the password is encrypted. Therefore, a Hacker might still read the contents of the email. It is recommended to use a more robust security application such as Pretty Good Privacy (PGP) or Secure Shell (SSH). These programs specialize in application security by encrypting all the application traffic. Free version of SSH and PGP can be downloaded at http://www.openssh.com and http://www.pgp.com.



```
No. ime Source           Destination     Protocol. Info
 189 20 131.120.18.27    192.168.1.103   POP     Response: +OK Microsoft Exchange 2000 POP3 server version 6.0.5762.3 (saipan.ad.nps.navy.mil) ready.
 190 20 192.168.1.103    131.120.18.27   POP     Request: AUTH
 191 20 131.120.18.27    192.168.1.103   POP     Response: +OK
 192 20 192.168.1.103    131.120.18.27   POP     Request: AUTH NTLM
 193 20 131.120.18.27    192.168.1.103   POP     Response: +OK
 194 20 192.168.1.103    131.120.18.27   POP    *Request: TlRMTVNTUAABAAAAB7IIoAQABAArAAAACwALACAAAABKTOVTTEFQVE9QQ0pPRVM=
 195 20 131.120.18.27    192.168.1.103   POP     Continuation
 196 20 192.168.1.103    131.120.18.27   POP    *Request: TlRMTVNTUAADAAAAGAAYAHgAAAAYABgAkAAAABYAFgBAAAAADAAMAFYAAAAWABYAYgAAAAAAAACoAAAABYKIoEoATwBF
 197 20 131.120.18.27    192.168.1.103   POP     Response: -ERR Logon failure: unknown user name or bad password.
 198 20 192.168.1.103    131.120.18.27   POP     Request: AUTH NTLM
 199 20 131.120.18.27    192.168.1.103   POP     Response: +OK
 210 20 192.168.1.103    131.120.18.27   POP    *Request: TlRMTVNTUAABAAAAB4IIoAAAAAAAAAAAAAAAAAAAAAA=
 211 20 131.120.18.27    192.168.1.103   POP     Continuation
 212 20 192.168.1.103    131.120.18.27   POP    *Request: TlRMTVNTUAADAAAAGAAYAGoAAAAYABgAggAAAAgACABAAAAADAAMAEgAAAAWABYAVAAAAAAAAACaAAAABYKIoE4AUABH
 214 20 131.120.18.27    192.168.1.103   POP     Response: +OK User successfully logged on.
 215 20 192.168.1.103    131.120.18.27   POP     Request: STAT

⊞Frame 1 (62 on wire, 62 captured)
⊞Ethernet II
⊞Internet Protocol, Src Addr: 192.168.1.103 (192.168.1.103), Dst Addr: 64.4.13.202 (64.4.13.202)
⊞Transmission Control Protocol, Src Port: 3575 (3575), Dst Port: 1863 (1863), Seq: 915116902, Ack: 0, Len: 0
```

NOTE: Application Level Encryption

Figure 5.18. Ethereal Interception of Encrypted Data.

Although there are problems with MAC authentication and WEP both provide some protection that ought to be retained as part of a "defense in depth" strategy. The NPS campus currently deploys these protections. Used together to protect a small office or home, the protection listed in Table 5.2 is sufficient concerning the effort and time it takes a hacker to crack a low-traffic low-value network.

Measure	**Security Effect**
Turn off SSID Beaconing	Minimize War Driving Threat
Enable WEP Encryption	Improve Data Confidentiality
Enable MAC Authentication	Minimize Unauthorized Equipment Network Access
Upgrade Wireless Card and AP Firmware	Minimize WEP Decryption Threat

Table 5.2. Wireless Security Practices for the Home or Small Office.

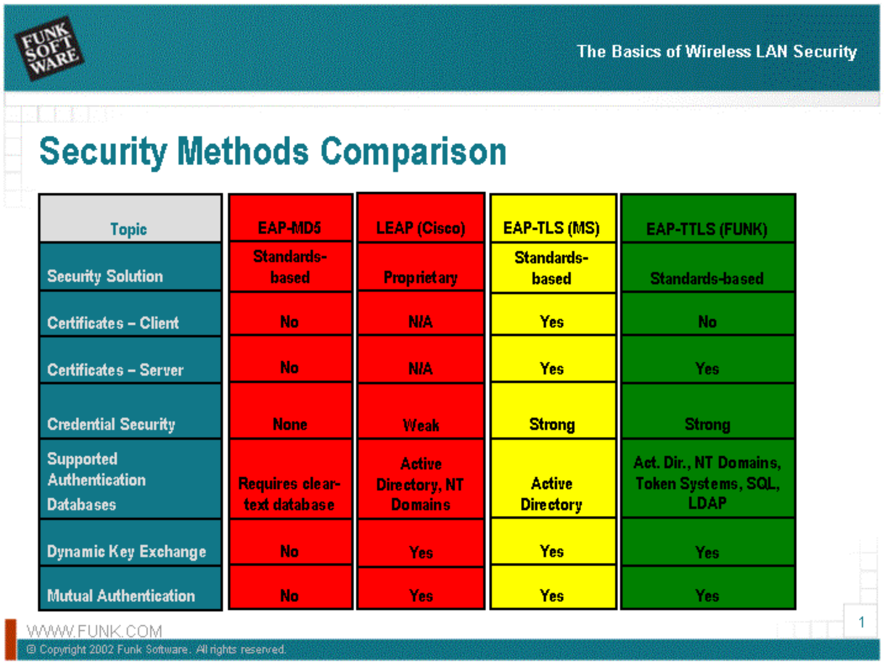
For mid-size and larger organizations a more enhanced security solution above and what is available in the 802.11 specification is of vital importance that addresses the addressees flaws of static WEP encryption and authentication. For any organization, a wireless security strategy is a necessity. The problem with static keys in general is that eventually a hacker will have enough encrypted data to be able to reverse engineer the key. The solution is to make the keys dynamic for each user's session and have the users be authenticated not their equipment.

H. FURTHER ESSENTIAL WIRELESS ENCRYPTION AND AUTHENTICATION

Existing wireless security for an enterprise is insufficient using the 802.11 specification alone. The scalability and security problems can be mitigated when used with an Extensible Authentication Server (EAP) and Remote Dial In User Service (RADIUS) Server. EAP is a security framework that compensates for the problems with WEP and MAC authentication by authenticating the user based on a combination of one or more characteristics password, token, and/or biometric reading. The 802.1X standard has the capability to authenticate users for access control and has the ability to deliver dynamic keys. The type of encryption algorithm the key uses is based on other protocols outside of the 802.1X specification. 802.11i working group is assuming the responsibility for the encryption algorithm. They have recommended AES as the long term encryption solution. In the meantime there are several 802.1X implementations that stay with WEP encryption.

Going beyond WEP requires additional hardware. The 802.1X and the 802.11i working groups want to provide seamless integration and security. Both IEEE groups realize that dynamic AES keys delivered through an improved authentication framework is the long term answer but getting industry to do it in a standard fashion will take time. Most authentication solutions only make the WEP key dynamic and require use of proprietary hardware. EAP/MD5 only allows for authentication and does not even have the capability for dynamic WEP keying. EAP/Cisco or LEAP requires network architecture to consist solely of Cisco LEAP compatible wireless cards and access points. The EAP/TLS authentication comes standard with Windows 2000 and Windows XP but requires that both the clients and the servers have certificates installed. This can be burdensome to network administrators. Funk and Certicom improved upon the capability of EAP/TLS and developed EAP/TTLS. EAP/TTLS has the same functionality as

EAP/TLS, but does not require client certificates, only server certificates. Figure 5.20 compares the most popular 802.1X implementations.



FUNK SOFTWARE

The Basics of Wireless LAN Security

Security Methods Comparison

Topic	EAP-MD5	LEAP (Cisco)	EAP-TLS (MS)	EAP-TTLS (FUNK)
Security Solution	Standards-based	Proprietary	Standards-based	Standards-based
Certificates – Client	No	N/A	Yes	No
Certificates – Server	No	N/A	Yes	Yes
Credential Security	None	Weak	Strong	Strong
Supported Authentication Databases	Requires clear-text database	Active Directory, NT Domains	Active Directory	Act. Dir., NT Domains, Token Systems, SQL, LDAP
Dynamic Key Exchange	No	Yes	Yes	Yes
Mutual Authentication	No	Yes	Yes	Yes

WWW.FUNK.COM

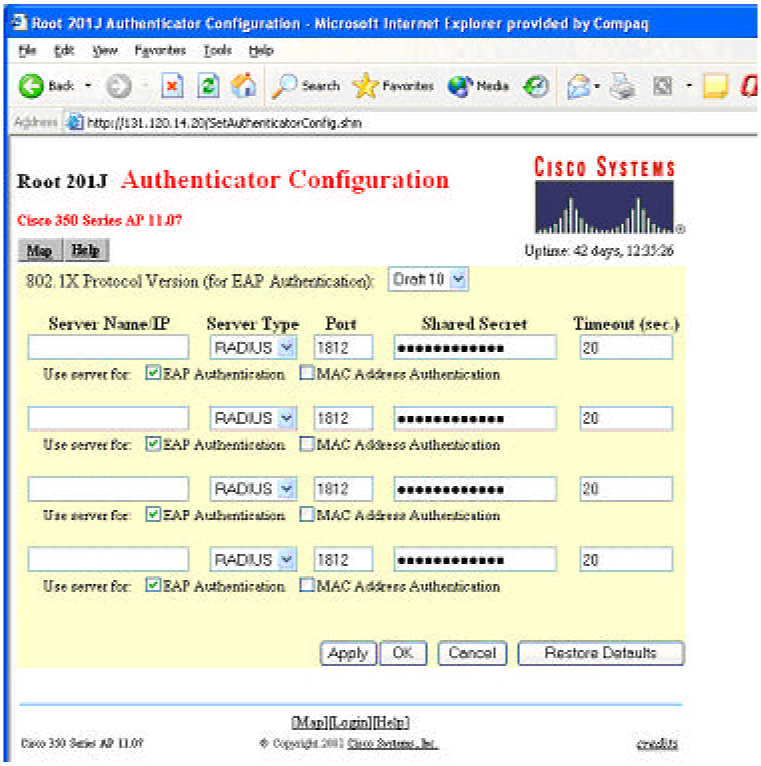
1

© Copyright 2002 Funk Software. All rights reserved.

Figure 5.19. A Comparison of the Different 802.1X Authentication Implementations [24].

Cisco and Microsoft recently announced support for another implementation of 802.1X called Protected-EAP or PEAP. Details of this joint venture are discussed in the April 2002 issue of Cisco's Packet magazine [25]. If this joint venture succeeds it will obviously emerge as the dominant authentication standard. University of Maryland Professor Bill Arbaugh wrote a paper *An initial security Analysis of the IEEE 802.1X standard* [26] that was critical of the 802.1X security capability. He claims it was susceptible to "man in the middle" attacks, session hijacking and is incapable of mutual authentication. A man in the middle attack is when a hacker tries to pose as an access point to collect information such as an SSID, WEP KEY, or IP address information. Additionally man in the middle attacks are capable of stealing a session from an weakly authenticated user. Arbaugh's review was of the first 802.1X implementation EAP/MD5. Newer version of 802.1X have solved these problems by allowing for mutual authentication and have prompted responses to Arbaugh paper from Cisco [27] and Funk [28].

Another solution is Cranite's Wireless Wall which uses EAP/TLS as its authentication protocol and implements its own encryption solution using AES. Fortresstech has a solution that implements its own proprietary authentication mechanism and uses AES and 3DES as it encryption mechanism. Reefedge is another competitor which uses a browser with Secure Socket Layer enabled for authentication and uses 3DES as its encryptio n method. Details of these products can be found at www.cranite.com, www.fortresstech.com, and www.reefedge.com respectively. Figure 5.20 shows an example of how to configure the Cisco 350 Access Point for 802.1X authentication. All the wireless solutions discussed so far have been for the delivery of layer 2 media access data link encryption keys. There are other solutions that can provide similar authentication and encryption.


Root 201J Authenticator Configuration - Microsoft Internet Explorer provided by Compaq
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Cisco Systems
Map Help
Apply OK Cancel Restore Defaults
[Map][Login][Help]
Cisco 350 Series AP 11.07
© Copyright 2001 Cisco Systems, Inc.
credits

http://131.120.14.20/SetAuthenticatorConfig.shm

Root 201J Authenticator Configuration

Cisco 350 Series AP 11.07

Uptime: 42 days, 12:35:26

802.1X Protocol Version (for EAP Authentication): Draft 10

Server Name/IP	Server Type	Port	Shared Secret	Timeout (sec.)
	RADIUS	1812	●●●●●●●●●●●●●	20
	RADIUS	1812	●●●●●●●●●●●●●	20
	RADIUS	1812	●●●●●●●●●●●●●	20
	RADIUS	1812	●●●●●●●●●●●●●	20

Use server for: ☑ EAP Authentication □ MAC Address Authentication

Use server for: ☑ EAP Authentication □ MAC Address Authentication

Use server for: ☑ EAP Authentication □ MAC Address Authentication

Use server for: ☑ EAP Authentication □ MAC Address Authentication

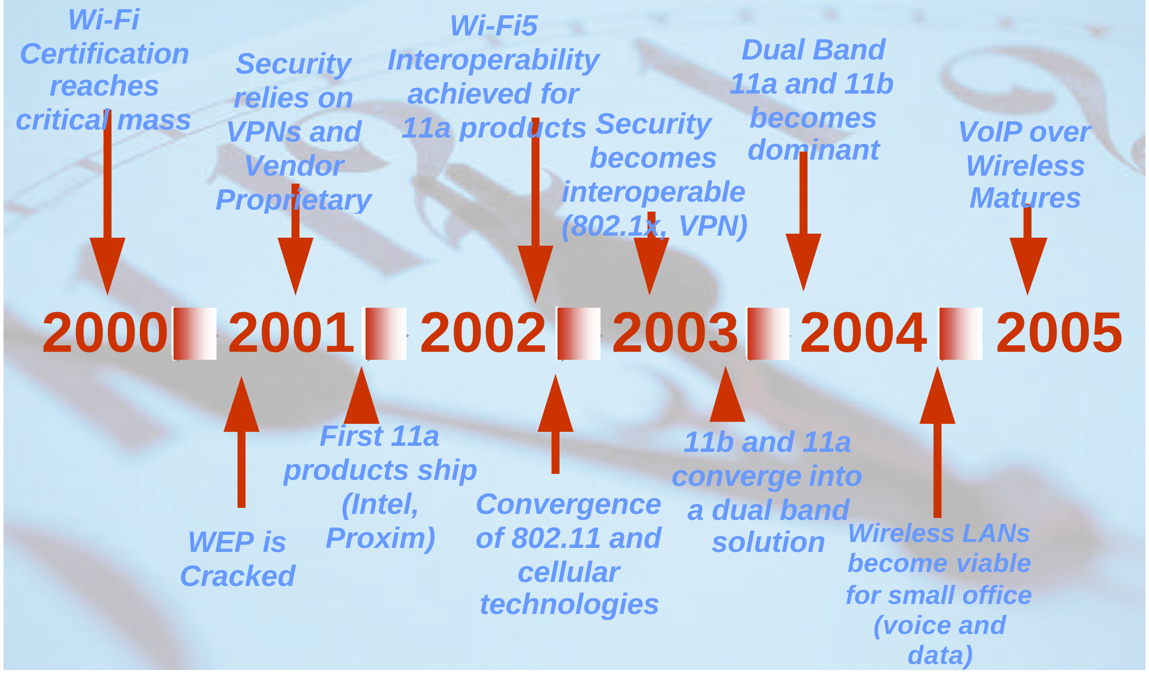
Figure 5.20. Cisco 350 802.1X Authentication Screen.

Other layer solutions such as Virtual Private Networks (VPN), Internet Protocol Security (IPSEC), and Secure Shell (SSH) provide equivalent security. In theory, because they are at higher layers they can run in concert with 802.1X, WEP, or other layer 2 encryption/authentication devices. In practice, multi-vendor security solutions often have interoperability problems. Tests were performed using the Cranite Wireless Wall product with a Symantec VPN, and it was quickly discovered that the two products were unable to operate in concert due to network card conflicts. Static WEP can work in conjunction with a VPN solution because static WEP communication is only between the client and the access point. In contrast, dynamic keying at layer two requires communication between the client and other servers.

Enterprises usually also have a requirement for a VPN to allow for remote users to access the internal network from the external internet. When designing a network having two different clients, one for wireless use and one for VPN use, can be burdensome and difficult to support. The disadvantage of using Layer 3 is that the IP addresses of devices can be exposed, and this is more susceptible to a denial of service/Address Resolution Protocol (ARP) Poisoning attack.

According to a leading information technology research and consulting firm, Metagroup 802.1X and VPN interoperability issues will be resolved by 2003 [29]. This is shown in Figure 5.21 Wireless Currently there is also a lack of standards concerning VPNs. This can cause interoperability problems in multi-vendor VPN client environment.

Wireless LAN Timelines



2000 2001 2002 2003 2004 2005

Wi-Fi Certification reaches critical mass

Security relies on VPNs and Vendor Proprietary

Wi-Fi5 Interoperability achieved for 11a products

Security becomes interoperable (802.1x, VPN)

Dual Band 11a and 11b becomes dominant

VoIP over Wireless Matures

WEP is Cracked

First 11a products ship (Intel, Proxim)

Convergence of 802.11 and cellular technologies

11b and 11a converge into a dual band solution

Wireless LANs become viable for small office (voice and data)

Figure 5.21. Projected Wireless LAN Progress.

I. ROGUE ACCESS POINTS AND INTRUSION DETECTION SYSTEMS

Keeping positive control of an organization's network is one of the most difficult tasks that IT managers face. Any employee is able to connect an improperly configured or unauthorized access point to circumvent the most securely managed infrastructure. Such unauthorized access point are called rogue access points. Several steps are necessary to prevent rogue APs:

- Have a strong security policy with ramifications for connecting an unauthorized Access Point
- Provide frequent training on wireless use, require for new users
- Provide adequately sanctioned wireless coverage to all users so there is no emergent demand for users to install their own equipment
- Perform frequent RF scans using tools like Airmagnet and Netstumbler
- Peform frequent wired scans to look for unauthorized equipment using SNMP sweeps or other discovery/mapping software like HP Openview

- Install wireless Intrusion Detection Software (IDS).

With the proliferation of wireless devices, a need has developed for a wireless Intrusion Detection System (IDS). Wireless IDSs can detect rogue access points as well as detect an attack on the wireless network including denial of service attack and man in the middle attacks and report them in real time. IDSs should be used for large scale deployments as another layer of defense. They do have the limitations of only being able to detect devices that use the 802.11 protocol. If a hacker were to install an AP that used their own protocol or used a less popular one such as HomeRF, Openair, Hyperlan, or an old proprietary wireless method, these devices are unlikely to be effective. Because 802.11 is so widespread and many hackers do not have access to non-802.11 or skill to create their own equipment using 802.11, IDSs still makes sense. During the recent August 2002 Hacker convention, Defcon, a popular Wireless IDS vendor, AirDefense installed their product at the convention. According to their press release their results are shown below in Table 5.3. A diagram of the AirDefense IDS is also shown in Figure 5.22.

AirDefense discovered 115 peer-to-peer ad hoc networks and identified 123 stations that launched a total of 807 attacks during the 2 hours.

Among the 807 attacks:

- 490 were wireless probes from tools such as Netstumbler, which were used to scan the network and determine who was most vulnerable to greater attacks;
- 190 were identity thefts, such as when Media Access Control (MAC) addresses and Service Set Identifiers (SSIDs) were spoofed to assume the identity of another user;
- 100 were varying forms of denial-of-dervice attacks that either (1) jammed the airwaves with noise to shut down an access point, (2) targeted specific stations by continually disconnecting them from an access point or (3) forced stations to route their traffic through other stations that ultimately did not connect back to the network; and
- 27 attacks came from out-of-specification management frames where hackers launched attacks that exploited 802.11 protocols to take over other stations and control the network.

Table 5.3. Air Defense Results from Defcon Convention in August 2002 [30].

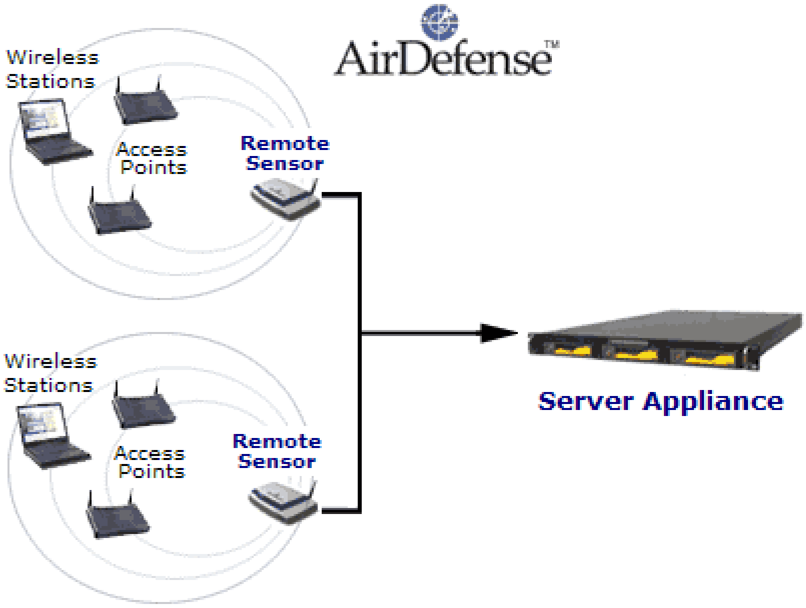


Figure 5.22. AirDefense Network Diagram Showing Security Sensors as Part of a Wireless LAN Installation

J. THE GOVERNMENT VIEW ON WIRELESS

NIST, the National Institute of Standards and Technology, a unit of the US Commerce Department together with the National Security Agency (NSA) have put out FIPS (Federal Information Processing Standards), a set of standards for information processing within government agencies concerning wireless encryption specifically, FIPS 197 and 140.

> The National Institute of Standards and Technology has recently announced the Secretary of Commerce's approval of the Advanced Encryption Standard (AES), which will provide agencies with a new encryption method designed to be secure for at least 20-30 years. Encryption (whether AES or another approved means such as Triple DES) is an important tool for protecting the confidentiality of disclosure-sensitive information entrusted to an agency's care [31].

FIPS Publication 197 [32] recommends that agencies use AES encryption for sensitive unclassified information regardless of whether it is on a wired or wireless LAN.

FIPS Publication 140 lists the security requirement for cryptographic modules and retains list of all products that have been certified. The FIPS specification can be found at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf and the list of certified FIPS 140 products can be found at http://csrc.nist.gov/cryptval/140-1/1401val.htm. This is important because many vendors claim to be certified but are not.

At the time of this writing the Department of Defense was drafting an instruction titled *Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG).* A copy of the 15 July 02 draft is included in Appendix B. The key parts concerning the use of unclassified information are listed in Section 4.1.1 and 4.1.2. The instruction requires strong PKI authentication and strong certified FIPS 140 AES or 3DES encryption for all unclassified wireless data traffic.

K. OVERALL RECOMMENDATIONS FOR NPS

The current NPS Wireless Network is shown in Figure 5.23. The existing security is insufficient because it uses MAC authentication and RC4 static WEP encryption. The Federal Government, industry and the IEEE 802.11i and 802.1X groups are starting to be in concert in addressing the shortcoming of the 802.11 specification with regards to security. Figure 5.24 is the recommended architecture for the Naval Postgraduate School. The exact type of equipment for the Access Control Server is not specified but needs to provide FIPS 140 compliant encryption and PKI authentication. Current solutions consist of only VPN and vendor proprietary implementations. Organizations that have many VPN remote access users that will also want to use wireless LANs should consider a VPN as the total combined solution. This will solve system integration and customer support issues. Organizations that do not have this characteristic have the option to explore 802.1X and proprietary solutions as long as they meet FIPS 140 criteria for encryption and PKI for authentication. A layered defense is the best defense.

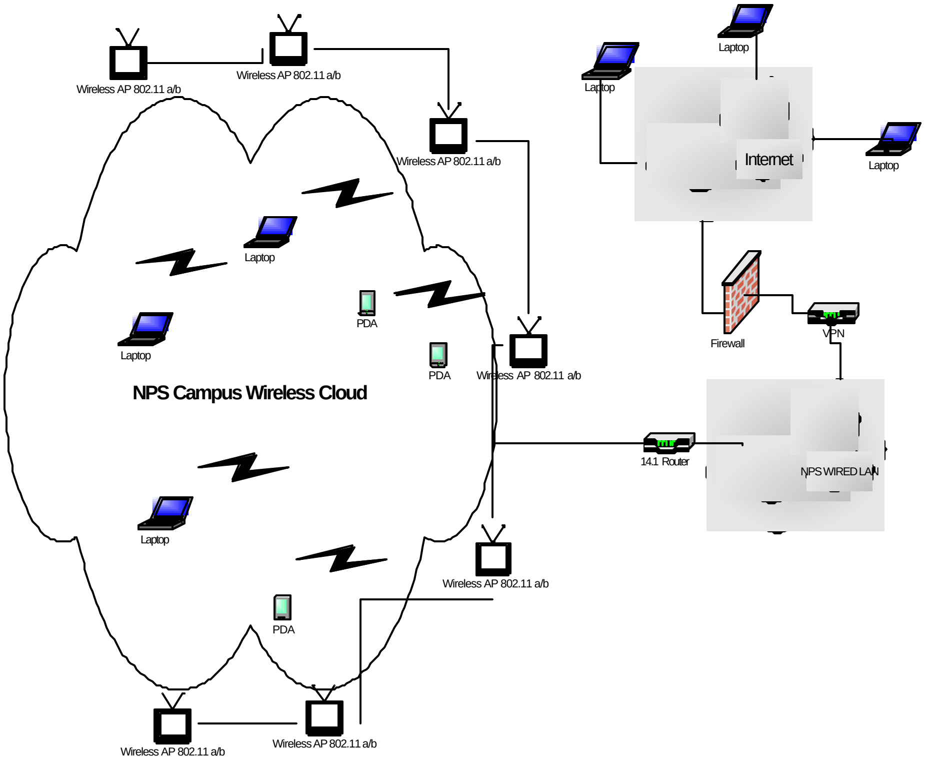


Figure 5.23. Current NPS Wireless Network Diagram as of August 2002.

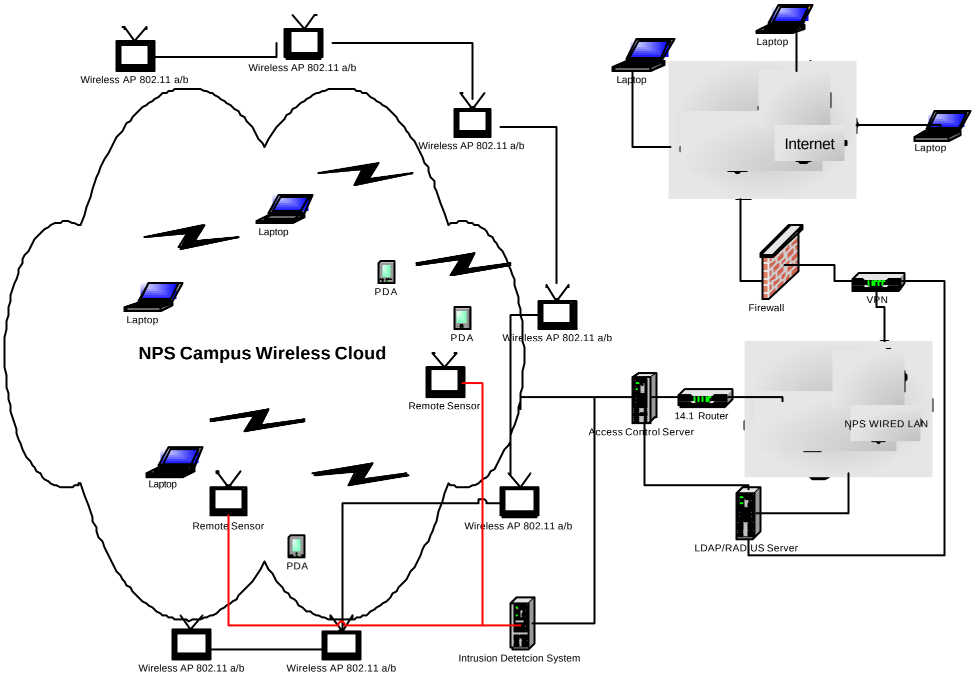


Figure 5.24. Recommended NPS Wireless Network.

L. SUMMARY

There are fundamental security issues associated with 802.11 wireless technology that require external non-802.11 defense protection. The flaws of Service Set Identifier (SSID), Wired Equivalent Privacy (WEP), and Media Access Control (MAC) authentication can all be overcome. Network tools and analyzers that are used by IT administrators and hackers such as Netstumbler, Airsnort, Ethereal, Airmagnet, and VXsniffer are demonstrated on the NPS campus for security assessment, detection of rogue access points and to heighten wireless security issues. External 802.11 security solutions such as 802.1X and VPNs augmented with Wireless Intrusion Detection Systems (IDS) that meet FIPS 140 encryption and PKI authentication standards is the best solution security solution for NPS or any large enterprise.

VI. SUPPORTABILITY, USABILITY, AND SECURITY (SUS) MODEL

A. INTRODUCTION

Too often decisions are made concerning the procurement and management of IT systems without a balanced approach. An overzealous IT security manager might lock down a system so hard that it is completely useless to its users. An organization that does not have a coordinated, centralized IT procurement process or strategy might purchase incompatible equipment. An organization that is too user centric may inadvertently provide security holes that might compromise sensitive data or allow the network to be degraded or compromised. A strategic model is needed for wireless LANs. The focus of this chapter is to synthesize a balanced model for the NPS wireless campus strategic plan.

B. DERIVATION AND EXPLANATION OF THE MODEL

A new approach to stategic management was developed in the early 1990's by Drs. Robert Kaplan (Harvard Business School http://www.hbs.harvard.edu) and David Norton (Balanced Scorecard Collaborative http://www.bscol.com). They named this system the 'balanced scorecard'. The Supportability, Usability, and Security (SUS) Model developed by the author of this thesis is based as an extension of this framework to help bring order and strategy to the decision making criteria and to derive a successful wireless design and implementation. Figure 6.1 shows the interlocking trinity of the model.

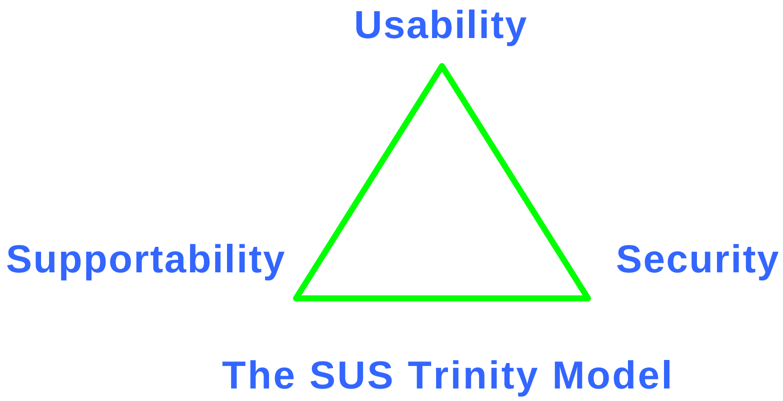


Figure 6.1. SUS Trinity Model.

What supportability means in a solution is that the design takes into account the amount of resources an organization has. Resources in terms of budget as well as in terms of manpower and the level of training must not be overlooked. Currently the IT support staff at NPS is undermanned and high wireless expertise is not present although it is developing at a high rate. The final implementation solution must take this into account. Specifically, whether to outsource the service or whether to man it using existing personnel can be a difficult decision. This is where a proper risk assessment must be done. A poorly trained and undermanned staff cannot easily support a complex system and this factor will determine if the operation will be successful or not.

What usability means is a desired end state where all users are able to seamlessly roam anywhere on the NPS campus and be connected to the network with your laptop or handheld device as if you were connected with a wired connection. Usability also means the architecture must support any 802.11 WI-FI client card on any operating system reliably. It is a paramount that the end user be able to use the device effectively and efficiently. That is the purpose for the system in the first place. That is why usability is at the top of the pyramid.

Although the fleet is standardized on IT-21 Microsoft operating systems and Intel equipment, NPS is a research institution and needs to be able to be more inclusive of not only Windows operating systems, but other OSs, such as Linux, MAC OS X, and even the PocketPC. This is vital for both research and the general freedom expected in an academic environment. A non-platform specific design is in keeping with one of the fundamental principles of software engineering: low coupling and high cohesion. Low coupling means flexible response in the support of a variety of end user platforms and operating systems. This is also in keeping with Admiral Cebrowski's notion of transformation from platform centric warfare into net centric warfare. High cohesion means a unified support architecture standards based with a limited vendor variety for ease of management and support.

What security means as the second criteria is that the default 802.11 wireless security is not secure. A detailed history of the 802.11 standard, vulnerabilities and developmental fixes is provided in Chapter V. 802.11 has been proven to be vulnerable without an external security enhancement. The IEEE 802.11 uses a weak RC4 encryption that was not designed with security in mind. It was designed with an interoperability focus and marketed for export to capture foreign markets in Europe and Asia. In addition to poor security design, the IEEE 802.11 specification was found to have additional security flaws [20]. The clear solution is to not rely on 802.11 security but add external proven enhanced security to it.

NPS has been visited by leading companies in Silicon Valley with enhanced security solutions: Reefedge, Cisco, Cranite, Funk, Bluesocket, Symbol and Fortresstech. The Federal Wireless Users Forum and the overarching DOD wireless policy (draft) provided in Appendix C have recommended that in order for wireless to be certified at the unclassified level, an organization needs to use the FIPS 140-1 standard. What security means is to use what the best Silicon Valley has to offer, tempered by existing DOD policy (approved and draft), incorporate private and public sector best practices, and use several different layers of security. This information also needs to be codified into a local policy and properly enforced.

Even if 802.11 wireless security concerns outweigh capability does not necessarily mean it must be banned. As mentioned earlier in the DOD model there is separation of technologies between the layers. This means even though the lower layers have security holes presently, one might still get great capability in an unclassified setting as well as the ability to further develop the applications to compensate for lower level security issues. Currently there is no one unique killer application for the wireless medium like there is for the wired world. The wired killer application is email and the web browser. The best way for the killer military wireless application to emerge is through controlled organizational exposure to the technology. If an application gets developed that is revolutionary, operational factors may insist on its deployment regardless of the security issues. The worst case is that the application will have the maturation factors through exposure to requirements such as human factors and system integration. It is effective use of time to develop these applications now so when the networks meet the security requirements the system might be effectively deployed.

C. SUMMARY

The SUS model provides the framework for better wireless networking. Every decision concerning implementation should involve the review of how can it be more usable, how can it be more secure, and how it can it be more supportable.

VII. NPS WIRELESS IMPLEMENTATION PLAN

A. INTRODUCTION

The Naval Postgraduate School (NPS) is the flagship postgraduate institution for the Navy/Marine Corps team, and indeed all of Department of Defense (DOD). The Superintendent of NPS, RADM Ellison, has stated that he wants NPS to be among the top ten postgraduate schools in the country. Wireless campuses are in keeping with almost every university in the country. Some of the more prominent include Carnegie Mellon University, Columbia, Drexel, MIT, Harvard, Wake Forest, American University, West Point, and many more. Wireless technology has a big place in meeting that goal, by providing the equipment and research capabilities NPS must have to lead the Navy into the future. Wireless can help make NPS a flagship institution in a bold fashion. The future of military networking is in the wireless domain, and NPS should focus resources to make wireless networking at NPS a reality.

1. Wireless Campus Mission

The Naval Postgraduate School, acting as the leading change agent for the next generation of Navy and Marine Corps leaders, must deploy and maintain an industry-standard wireless network in order to provide training and education in this critical enabling technology.

2. Wireless Campus Vision

The campus, by the end of First Quarter FY 2003, will have an industry-standard wireless network infrastructure in place to support the students, faculty, and staff in their research and educational endeavors. The final product is that any member of the NPS community can use a portable network device, such as a laptop or Personal Digital Assistant (PDA), and maintain a continuous broadband signal anywhere on campus in a reasonably secure fashion. The design is scalable and can be ported to base housing areas, other local Naval support facilities, and finally to the Fleet. The desired wireless portion of the network will seamlessly and securely extend the wired network. This connectivity will enable ubiquitous connectivity, resulting in large gains in individual access and productivity.

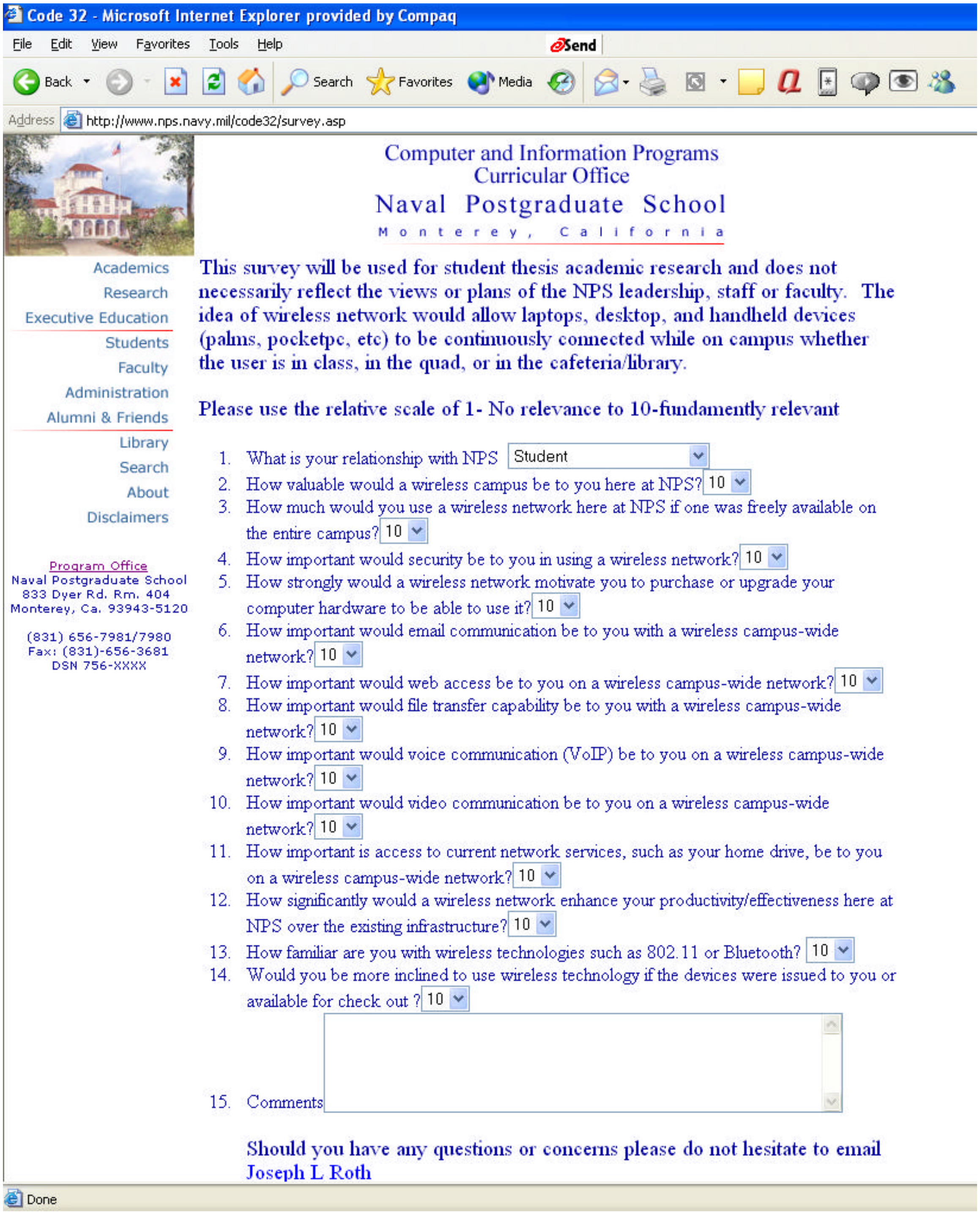
3. Mission of the Wireless Warrior Group

First, write an NPS wireless policy. Secondly lay the groundwork for the wireless transformation at the Naval Postgraduate School by eliciting and evaluating the specific requirements for wireless networking, and develop the wireless concept model for NPS. Third, provide wireless connectivity to the NPS Chapel and Religious Program Assistants with existing equipment, and at a lower cost than the cost of a wired installation. Finally, increase wireless coverage to as many as public on campus areas as possible.

4. Surveys

In order to derive the requirement two surveys were posted on the NPS intranet. The first was run from November 23 thru December 7th, 2001. The second was run August 28 thru September 6th, 2002. The survey was implemented using a web page that was connected to an Access database. Figure 7.1 shows the survey that was used in both occasions.

The participants were asked to rate their answers on scale from one to ten where one was not relevant and 10 was fundamentally relevant. Clearly these survey results, shown in Figure 7.2, support the collective belief that wireless adds value, productivity and usability to the NPS campus. It also shows there is strong desire for email, web access and file transfer. There is less concern for VOIP and Video. Security is the greatest concern of all participants. It is also interesting to note that 30 experimental access points were installed on campus during the period in between the two surveys. A formal NPS wireless policy was approved by the technology committee, and a special security subnet, was implemented for wireless use, Subnet 14. The second survey showed an increase in every area except security which showed a decrease. The greatest increase was question five, the willingness of NPS members to purchase or upgrade their personal equipment in order to use the school's wireless network. It is clear the more students, staff, and faculty that are exposed to wireless technology the more they want to use it, the more productive they feel, and the less they are concerned with security.



Computer and Information Programs
Curricular Office
Naval Postgraduate School
Monterey, California

Program Office
Naval Postgraduate School
833 Dyer Rd. Rm. 404
Monterey, Ca. 93943-5120

(831) 656-7981/7980
Fax: (831)-656-3681
DSN 756-XXXX

This survey will be used for student thesis academic research and does not necessarily reflect the views or plans of the NPS leadership, staff or faculty. The idea of wireless network would allow laptops, desktop, and handheld devices (palms, pocketpc, etc) to be continuously connected while on campus whether the user is in class, in the quad, or in the cafeteria/library.

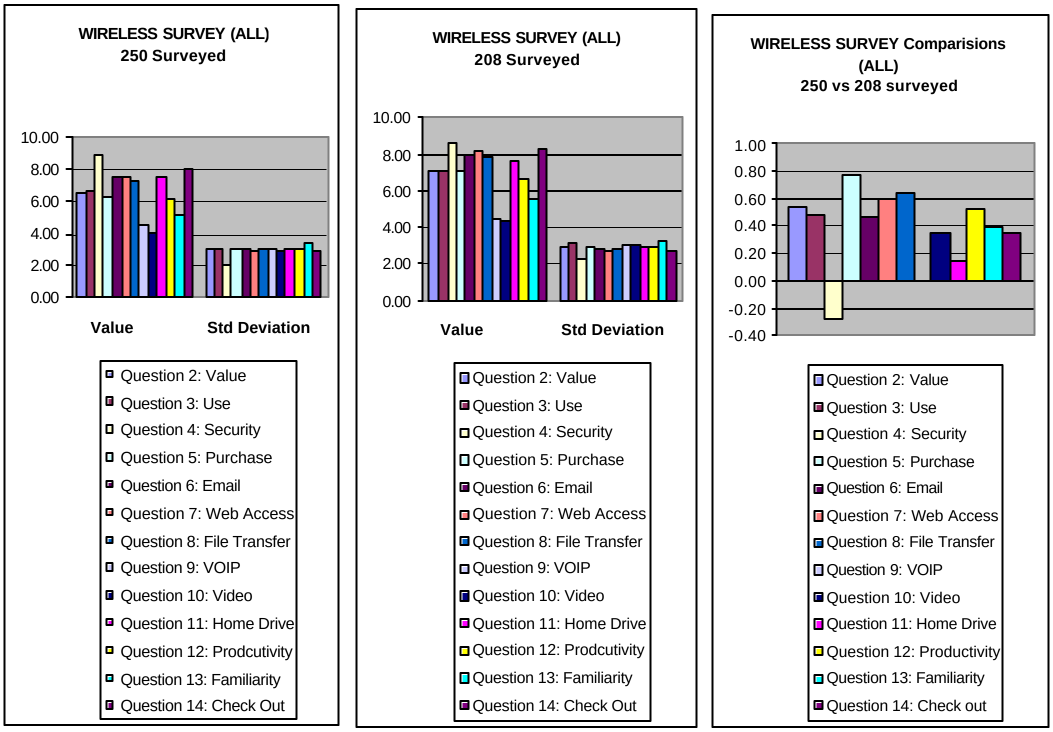
Please use the relative scale of 1- No relevance to 10-fundamently relevant

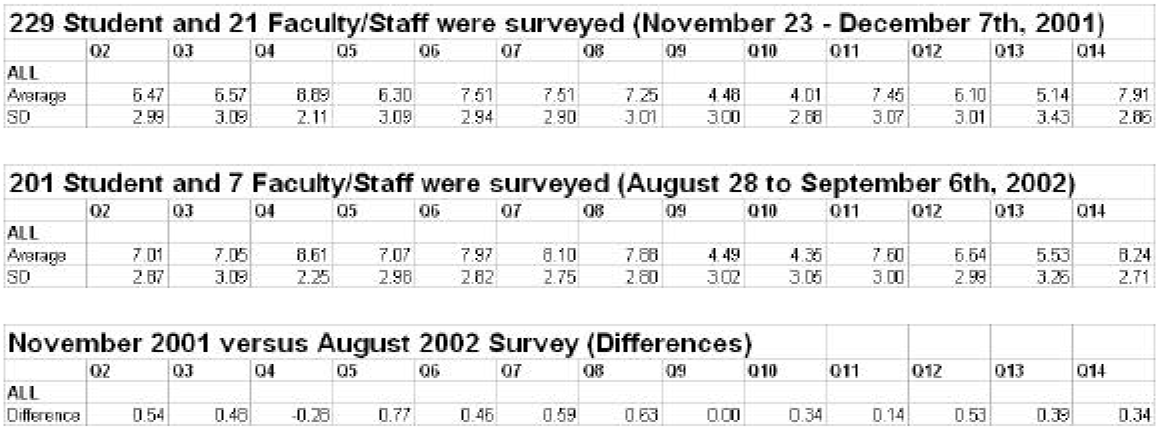
1. What is your relationship with NPS Student
2. How valuable would a wireless campus be to you here at NPS? 10
3. How much would you use a wireless network here at NPS if one was freely available on the entire campus? 10
4. How important would security be to you in using a wireless network? 10
5. How strongly would a wireless network motivate you to purchase or upgrade your computer hardware to be able to use it? 10
6. How important would email communication be to you with a wireless campus-wide network? 10
7. How important would web access be to you on a wireless campus-wide network? 10
8. How important would file transfer capability be to you with a wireless campus-wide network? 10
9. How important would voice communication (VoIP) be to you on a wireless campus-wide network? 10
10. How important would video communication be to you on a wireless campus-wide network? 10
11. How important is access to current network services, such as your home drive, be to you on a wireless campus-wide network? 10
12. How significantly would a wireless network enhance your productivity/effectiveness here at NPS over the existing infrastructure? 10
13. How familiar are you with wireless technologies such as 802.11 or Bluetooth? 10
14. Would you be more inclined to use wireless technology if the devices were issued to you or available for check out ? 10
15. Comments

Should you have any questions or concerns please do not hesitate to email Joseph L Roth

Figure 7.1. NPS Wireless Survey with the Questions Written by LT Andrew Weist.

Security is still the highest concern on both surveys, but familiarity and formal leadership involvement in the security process has reduced the collective hesitation. The raw data which includes comments and a more detailed breakdown of the survey responses is included in Appendix C.





229 Student and 21 Faculty/Staff were surveyed (November 23 - December 7th, 2001)													
	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
ALL													
Average	6.47	6.57	8.89	6.30	7.51	7.51	7.25	4.48	4.01	7.46	6.10	5.14	7.91
SD	2.99	3.09	2.11	3.09	2.94	2.90	3.01	3.00	2.88	3.07	3.01	3.43	2.86

201 Student and 7 Faculty/Staff were surveyed (August 28 to September 6th, 2002)													
	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
ALL													
Average	7.01	7.05	8.61	7.07	7.97	8.10	7.88	4.49	4.35	7.60	6.64	5.53	8.24
SD	2.87	3.09	2.25	2.98	2.82	2.75	2.80	3.02	3.06	3.00	2.99	3.26	2.71

November 2001 versus August 2002 Survey (Differences)													
	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
ALL													
Difference	0.54	0.48	-0.28	0.77	0.46	0.59	0.63	0.00	0.34	0.14	0.53	0.39	0.34

Figure 7.2. Results/Comparisons of the NPS Wireless Surveys of November 23, 2001 and August 28, 2002.

5. Assumptions

In order to complete requirement analysis, the following assumptions were made:

- Current and future technology will support wireless
- Wireless connectivity is worth pursuing
- Security and other issues have valid technical solutions (i.e., wireless is a viable networking technology)
- Wireless costs can be controlled
- Users will embrace wireless technology if it is made available

6. Stakeholders

a. Leadership

Because of the rigid hierarchical nature of the military, and the fact that NPS is a military institution, the primary stakeholder is the NPS leadership. This small group (the Superintendent, the Provost, and the Deputy Superintendent) determines the direction of the school and has responsibility for the apportionment and expenditure of allocated funds. Leadership goals are to deliver the best education possible while controlling costs. A stated goal of the leadership is to put the reputation of NPS among the top ten graduate institutions in the country. Leadership does not necessarily have any experience with wireless technology or competing technologies, but can be persuaded to pursue wireless if it will help them achieve their stated goals.

b. Administrators

Administrators form the remainder of the school leadership, and can be considered middle managers. They have influence with leadership, and can make suggestions, sit on committees, etc. This group may or may not have wireless experience, and what experience they do have comes from personal wireless experiments such as home wireless networks. Unless convinced otherwise, they may have “better uses” for wireless funding.

c. Network Managers

Network managers are responsible for the effective and secure operation of the campus network. This group has steadily been attrited from a high of 114 members to 58 today [33]. Funding has also been reduced, while requirements (mainly the amount of data and required network access of each user) have grown. On the other hand, the group has lived through almost daily increases in the capacity of equipment to handle information. This group is the most technically savvy of all stakeholders, and they see the value of wireless and in fact have made it a goal of their proposed future network. [34]. Network managers are generally in favor of wireless proposals.

d. Joint and International Services

As the resource provider (both funding and manpower) and ultimate consumer of NPS products (the students), the Navy-Marine Corps team has a vested interest in what occurs at NPS. The Army, Air Force, Coast Guard and international officers also make up a significant portion of the NPS population and for the most part contribute to the resourcing of the NPS institution. Although individuals in the sea, air, and land services may not be aware of the day-to-day operations at NPS, they deserve the best product that NPS can deliver. Furthermore, the fleet is always looking for better techniques to communicate in order to support their warfighting mission. Wireless technologies will be a solution, now and in the future, just as radio and satellite communications assist now.

Another significant effect of this stakeholder is the regulation of all aspects of school life through the issuance of mandatory policies and procedures. In terms of wireless, these policies and procedures cover everything from contract management to security to personnel management, and significantly constrain leadership from doing whatever they want. On the other hand, there may be a certain limited amount of protection to the institution from following the rules.

e. Other Stakeholders

In the wireless domain, industry is a stakeholder. The NPS will not be developing or buying a GOTS solution to wireless, and is therefore constrained by the market. Other stakeholders are the regulatory agencies with which NPS must comply. The biggest example is the FCC.

f. Faculty/Staff

Faculty/staff are the group of users responsible for carrying out the educational mission of NPS. Faculty/staff are all subject matter experts in some field, not necessarily wireless, and benefit from the research tools aboard campus. Typically, faculty are required to generate income by conducting research on topics of interest to the Navy-Marine Corps team and the DOD. Faculty also have long experience with a plethora of projects, and may take a jaundiced view of new technology until it is "proven," a term which they themselves define (an example might be the early lack of support for the student-developed PYTHON administrative system).

Typically, faculty need reliable communications and access to world-wide resources. Faculty usually have offices with network connectivity on campus.

g. Infrastructure

The "infrastructure" are those users who make the school run. Examples are public works, the enlisted members, Code 05, leadership, etc. Needs run the gamut, but generally are the same as those of faculty. One particular need is to be able to access data about the campus from varied campus locations – for example, a PW electrician troubleshooting an electrical circuit may need access to detailed campus maps. Infrastructure can also be technical. The NPS backbone is being upgraded from ATM to gigabit Ethernet and modifications such as adding a wireless campus LAN needs to coexist without configuration management conflicts. It is vital that the wired and the wireless support groups orchestrate their efforts.

h. Students

Students are the final group of users, and also the largest. Students are comprised of members of all ranks below 0-6 from all four services, DOD civilians, and international students. Students typically do not have a fixed place such as an office on campus, and most students are housed in government-provided housing in either the former Fort Ord or La Mesa housing areas. Typical needs for students are to conduct research and class work from any place on or off campus in a compressed time period. Students have a widely varying understanding of wireless technology, but by their nature are inquisitive and demanding. Generally they will want high-speed connectivity, and are willing to invest their own money into wireless equipment, justifying it as "research."

i. Users Summary

In the wireless domain, there are few conflicts between the needs of the various user groups. The total number of users on campus is expected to be between 2000 and 3000 for the foreseeable future.

7. Derivation of Requirements - Why Wireless?

There are many benefits to the use of wireless networking:

- Mobility. NPS already has an effective wired network. Wireless networking will not replace this network, but will permit more users to access needed resources without being tied to a location. This ability to "take it with you" is the critical feature of wireless.
- Access. A robust wireless network can establish access where it was previously unavailable. This access can be established more cheaply than with a wired solution. The principal area considered here is in the housing areas.
- Availability. A wireless addition to the wired network increases network availability by reducing the risk of loss of connectivity. Multiple path redundancy is good.
- Bandwidth. Although wireless bandwidth is lower than in a wired solution, the use of 802.11a and b standards increases available bandwidth over other wireless solutions.
- Ease of Use. A wireless network brings networking to the user without a lot of complicated overhead or equipment.
- Use as an educational tool. As the future leaders of the Navy and Marine Corps, Naval Officers must become familiar with this technology. The military applications of wireless technology are obvious, and 802.11 technologies are evolutionary rather than revolutionary for the military.

8. Requirements Matrix

a. Geographic Coverage

The premise of this project is to provide a basic guide for the implementation of a wireless network for NPS and the surrounding relevant housing areas and facilities related to NPS. The selection of these facilities was made based upon their known interaction and relation with the mission of the Naval Postgraduate School and any areas not included are not specifically excluded from participation in the wireless LAN. The specific areas included were NPS campus, La Mesa housing area, and the Fort Ord military housing community. These locations capture the majority of all of the end users for the system as it is intended to be deployed. There is no provision for the access of faculty or student members that reside in private residences outside of these specific areas described in Table 7.1.

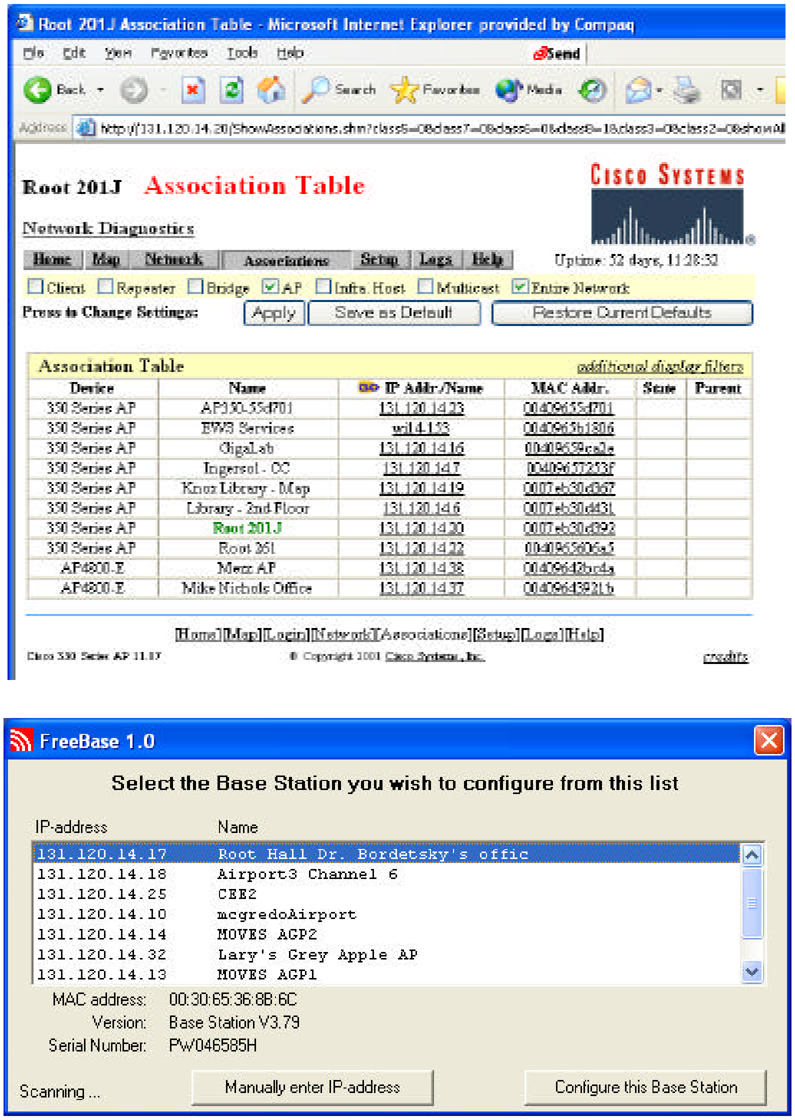
Geographic Coverage	The wireless system shall cover the entirety of the NPS campus with scalability increase capability to allow for LA Mesa and Fort Ord Coverage housing area coverage.
Hardware/Software	Systems chosen for this implementation shall be non-proprietary, interoperable, and conformal to accepted standards within industry. In the event there is no generally accepted standard then the system shall be standardized within the prevailing technology within The DOD and or governmental agencies.
Availability	Availability requirements for access to the wireless network shall be based on a dual threaded concept. Access points shall be located within the geographic areas of responsibility so as to provide a 50% overlap between access points and 99.99% availability. System availability shall be provisioned at minimum of 99.9%.
Security	Use FIPS 140 certified encryption(AES or 3DES) and PKI for authentication.
Quality of Service	Even though the 802.11 specification currently does not provide for QOS., the final goal is allow for 100% campus coverage with 802.11b and 802.11a encoding at 11 Mbps in the 2.4 GHz and 54 Mbps in the 5 GHz range. This will support constant email, web surfing, and limited audio/video streaming with roaming capability. QOS will be solved in the short term by providing a big pipe until the 802.11e working group provides QOS functionality in the wireless specification.
Bandwidth, Latency, and Packet Loss	Within the coverage area, data rates for individual users during peak hours and peak load periods shall be at a minimum of 56kbps regardless of data type or format. The network capacity shall be sufficient to support at a minimum 500 users simultaneously before there is a degradation of performance characteristics. System Latency should be no greater than 70 to 100 milliseconds and Packet Loss limited to no greater than 0.5%.
Scalability	The system chosen should be scalable to meet the requirements of a population of between 2000 and 3000 users. Provisioning for future access should include the housing areas where 75% of the homes occupied will demand access to the wireless network on a routine basis.

Table 7.1. Requirements Matrix.

.

b. Hardware/Software

The system is intended to provide wireless access to end users regardless of their platform type or operating system. Currently the NPS community uses PCs, PocketPCs, Apple Macintoshes and Linux systems. Client systems will have wireless cards from a multitude of vendors. The hardware and software selected to support the deployment of the wireless LAN are recommended to be non-proprietary and non-platform specific. Currently 802.11 vendor implementations have not allowed for 100% interoperability with regards to access points. The 802.11f working group is tackling this issue. In the mean time it is highly recommended that a sole source vendor be used for access point selection. There is often confusion between Small Office Home Office (SOHO) access points and enterprise access points. The big difference is price. SOHO APs cost around $200-300 and Enterprise APs cost around $800-1,000. SOHO APs are incapable of supporting large number of simultaneous users, do not have management software to interact with other APs, and have poor security functionality. The University of Akron, the world's largest university 802.11 network, has over 1200 Access Points. If they were to use a multi-vendor AP environment it would be unsupportable and highly insecure. By using a sole source enterprise access point vendor they are able to control all their APs from one web interface as well as perform security flash upgrades. SOHO APs often cannot be configured remotely and do not scale well for more than half dozen users. Poorly trained IT managers will use SOHO equipment for an enterprise installation because of the price differential. The savings will be short lived and the costs will reoccur in difficulty of configuration, security, and user dissatisfaction. The NPS community has pooled its gear which consists primarily of Cisco and Apple Access Points. The Cisco equipment is enterprise equipment and the Apple AP is of the SOHO variety. In order to remotely configure Apple devices on a PC, a shareware program called Freebase is used to manage the Apple Equipment. The Cisco and Apple (FreeBase) configurations screen are shown in Figure 7.3.


Root 201J Association Table - Microsoft Internet Explorer provided by Compaq
File Edit View Favorites Tools Help
Send
Back
Search
Favorites
Media
Address
http://131.120.14.20/ShowAssociations.shm?class5=0&class7=0&class6=0&class8=1&class3=0&class2=0&showAll
Cisco Systems

Root 201J Association Table

Network Diagnostics

Home | Map | Network | Associations | Setup | Logs | Help

Uptime: 52 days, 11:28:32

□ Client □ Repeater □ Bridge ☑ AP □ Infra. Host □ Multicast ☑ Entire Network

Press to Change Settings: Apply | Save as Default | Restore Current Defaults

Association Table — additional display filters

Device	Name	IP Addr./Name	MAC Addr.	State	Parent
350 Series AP	AP350-55d701	131.120.14.23	00409655d701		
350 Series AP	EWS Services	wil4.153	0040965b1806		
350 Series AP	GigaLab	131.120.14.16	00409659ca2e		
350 Series AP	Ingersol - CC	131.120.14.7	00409657253f		
350 Series AP	Knox Library - Map	131.120.14.19	0007eb30d367		
350 Series AP	Library - 2nd Floor	131.120.14.6	0007eb30d431		
350 Series AP	Root 201J	131.120.14.20	0007eb30d392		
350 Series AP	Root 261	131.120.14.22	0040965606a5		
AP4800-E	Merz AP	131.120.14.38	00409642bc4a		
AP4800-E	Mike Nichols Office	131.120.14.37	00409643921b		

[Home][Map][Login][Network][Associations][Setup][Logs][Help]

Cisco 350 Series AP 11.07 © Copyright 2001 Cisco Systems, Inc. credits

Select the Base Station you wish to configure from this list

IP-address	Name
131.120.14.17	Root Hall Dr. Bordetsky's offic
131.120.14.18	Airport3 Channel 6
131.120.14.25	CEE2
131.120.14.10	mcgredoAirport
131.120.14.14	MOVES AGP2
131.120.14.32	Lary's Grey Apple AP
131.120.14.13	MOVES AGP1

MAC address: 00:30:65:36:8B:6C
Version: Base Station V3.79
Serial Number: PW046585H

Scanning ...

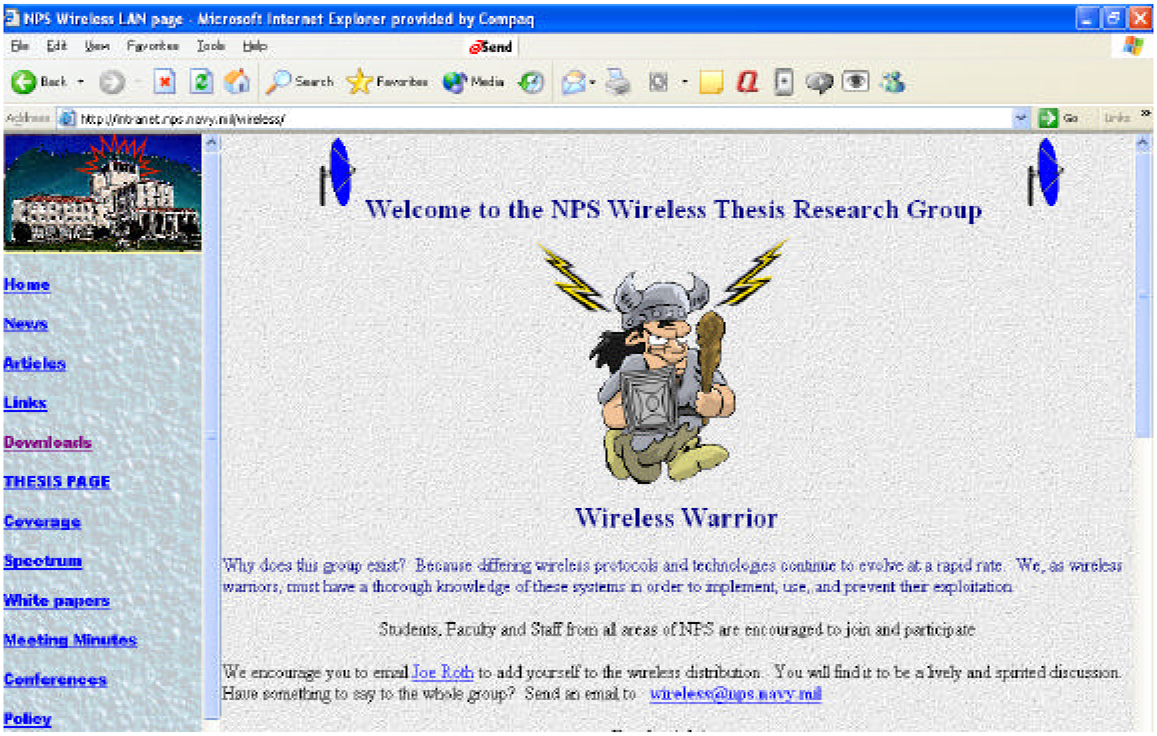
Figure 7.3. Enterprise and SOHO Access Point Configuration Screens.

All Access Point deployment and security enhancement must support any system regardless of their operating system or hardware platform. Specifically NPS needs to support at a minimum, the following operating system for wireless: Windows (9X, NT, 2K, XP, PocketPC), Apple (MAC OS X), and Linux (Redhat). Secondly, many users will have laptops with built in 802.11 cards from a variety of vendors so NPS must not design a solution that is not inclusive of all WI-FI certified client cards. The most famous software engineering axiom is high cohesion, low coupling. What high cohesion means in the wireless world is sole vendor enterprise grade access point selection. What low coupling means in the wireless domain is to support any client OS using any WIFI certified card.

9. Current Situation

a. Current Campus Wireless Initiatives

The wireless networking group is working hard to make wireless a reality. To that end, they have created the wireless webpage (see Figure 7.4) installed wireless where possible (see Figures 7.5 and 7.6), and developed appropriate policy to support the wireless systems on campus. It must be noted that wireless networks will exist on campus, whether the leadership wants them or not, barring draconian measures to eliminate them. If wireless is not supported, then “rogue” access points will exist, and be more of a hazard to the NPS network than would a regulated solution.


NPS Wireless LAN page - Microsoft Internet Explorer provided by Compaq
File Edit View Favorites Tools Help
Send
Back
Search
Favorites
Media
Address http://intranet.nps.navy.mil/wireless/
Go
Links
Home
News
Articles
Links
Downloads
THESIS PAGE
Coverage
Spectrum
White papers
Meeting Minutes
Conferences
Policy

Welcome to the NPS Wireless Thesis Research Group

Wireless Warrior

Why does this group exist? Because differing wireless protocols and technologies continue to evolve at a rapid rate. We, as wireless warriors, must have a thorough knowledge of these systems in order to implement, use, and prevent their exploitation.

Students, Faculty and Staff from all areas of NPS are encouraged to join and participate

We encourage you to email Joe Roth to add yourself to the wireless distribution. You will find it to be a lively and spirited discussion. Have something to say to the whole group? Send an email to wireless@nps.navy.mil

Figure 7.4. The NPS Wireless Thesis Research (Wireless Warrior) Web Page.

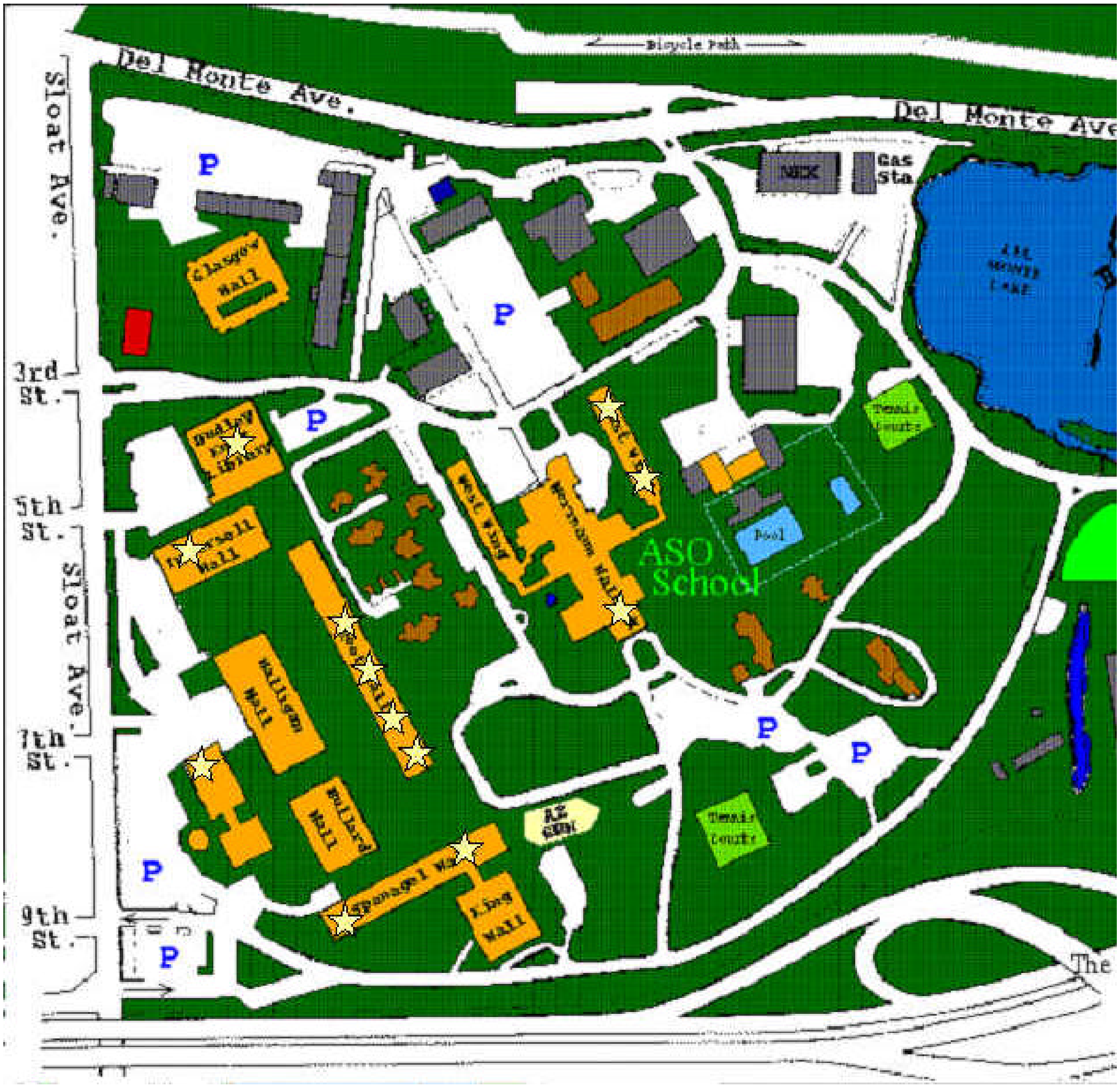


Figure 7.5 NPS Campus Wireless Access Points (September 2002).

Stars indicate the location of one or more wireless access points.

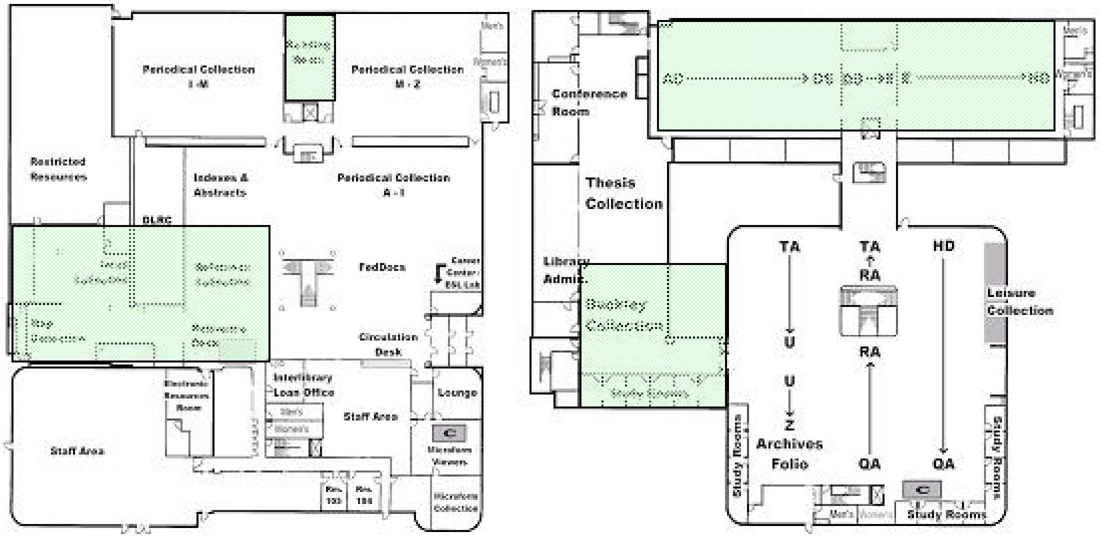
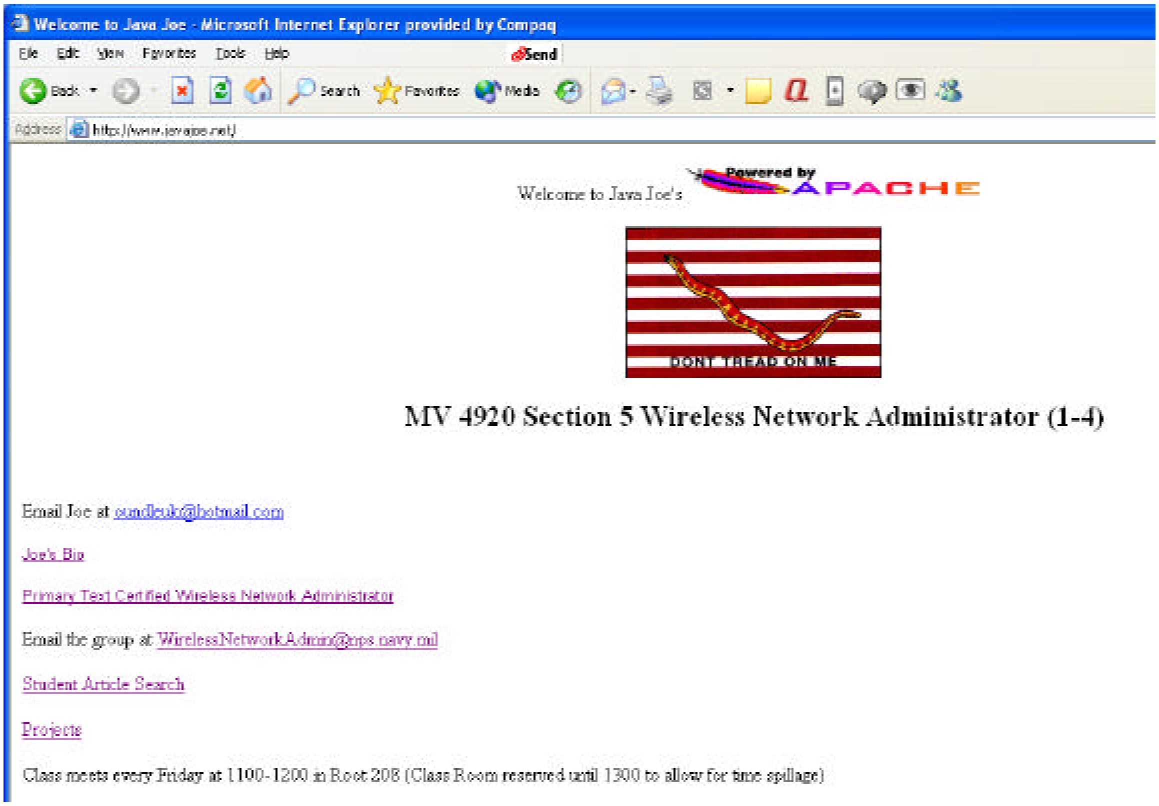


Figure 7.6. Dudley Knox Library Wireless Coverage.
Left (First Floor) and Right (Second Floor)

Another initiative of the wireless group was a three-day wireless networking conference from May 17-19, 2002 by a well-respected subject matter expert and noted wireless networking author, Jim Geier. The outline of his presentation is provided in Appendix D. A wireless network administrator class was also formed based on the industry vendor neutral Certified Wireless Network Administrator certification [35]. The class web page is shown below in Figure 7.7.


Welcome to Java Joe - Microsoft Internet Explorer provided by Compaq
File Edit View Favorites Tools Help
Send
Back
Search
Favorites
Media
Address
http://www.javajoe.net/
Powered by APACHE
DONT TREAD ON ME

Welcome to Java Joe's

MV 4920 Section 5 Wireless Network Administrator (1-4)

Email Joe at sundleuk@hotmail.com

Joe's Bio

Primary Text Certified Wireless Network Administrator

Email the group at WirelessNetworkAdmin@nps.navy.mil

Student Article Search

Projects

Class meets every Friday at 1100-1200 in Root 208 (Class Room reserved until 1300 to allow for time spillage)

Figure 7.7. MV 4920: Wireless Network Administrator Web Page (Http://javajoe.net).

Finally, this group provided wireless connectivity to the Chaplain assistants' offices in building 300. This small-scale project saved public works from having to dig a 30-meter cable path between this building and Herrmann Hall, an extremely expensive proposition that might likely have been low on the funding priority list. Figures 7.8 and 7.9 show the completed work.

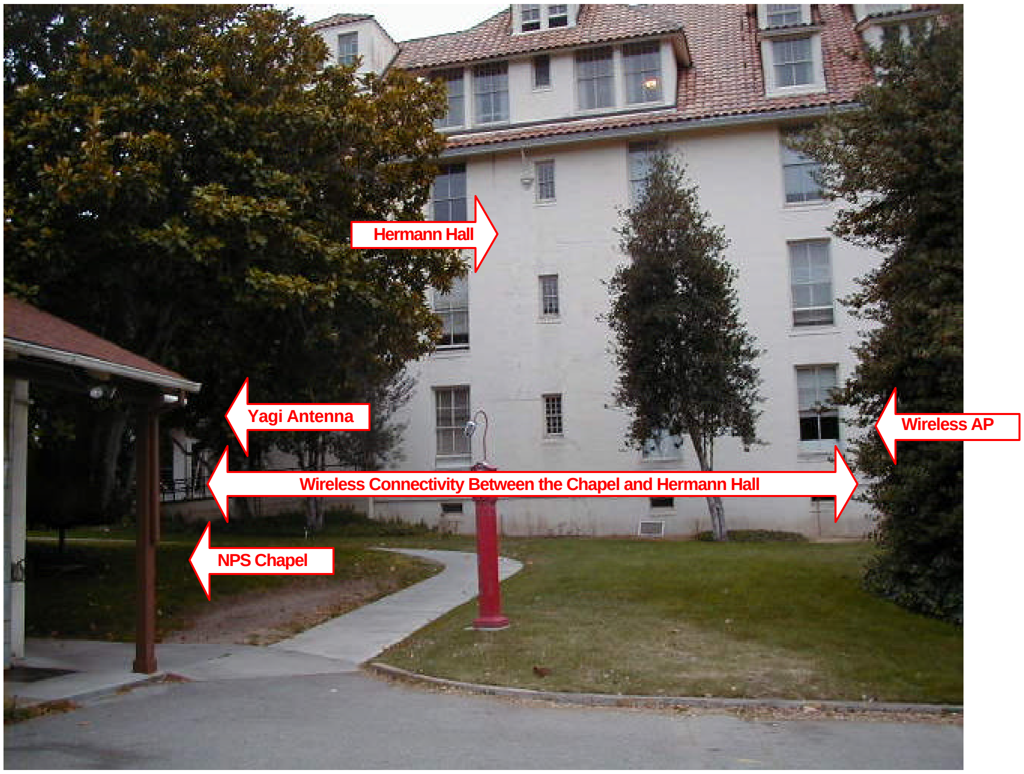


Figure 7.8. Chaplenet Wireless Link from the Chapel (Left) to Hermann Hall (Right).

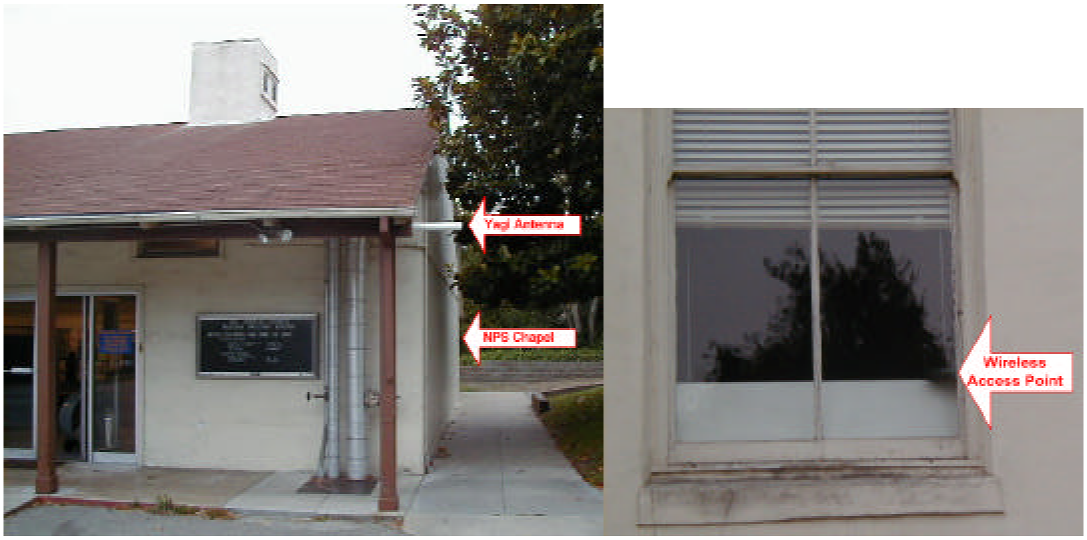


Figure 7.9. Chapel with Yagi (Left) and Hermann Hall Access Point (Right).

The total cost of the installation was $440. The equipment was donated by the wireless group and the Public Works time was already paid for so the cost to NPS was nothing. A more detailed breakdown is listed below in Table 7.2.

# of Items	Description	Unit Cost	Total Cost
2	Linksys WAP 11 Access Points	120	240
1	Yagi Antenna Kit	130	130
1	Cross over cable	10	10
1	Ethernet cable	10	10
0.5	Installation labor (hourly cost)	100	50
	Total		**$440**

Table 7.2. Chapelnet Wireless Link Costs.

The NPS quad was covered as a proof of concept using a modified low end Apple Airport connected to a high Yagi Antenna. Figure 7.10 shows the modification of the Apple Airport. Figure 7.11 shows the placement of the system on the fourth floor of Spanagel Hall for quad coverage.

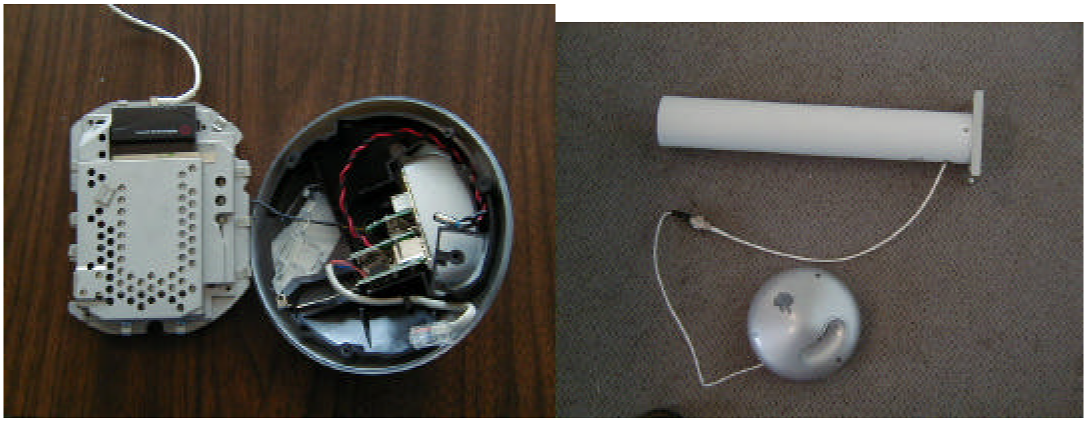


Figure 7.10. Modified Apple Airport Connected to a Yagi Antenna.

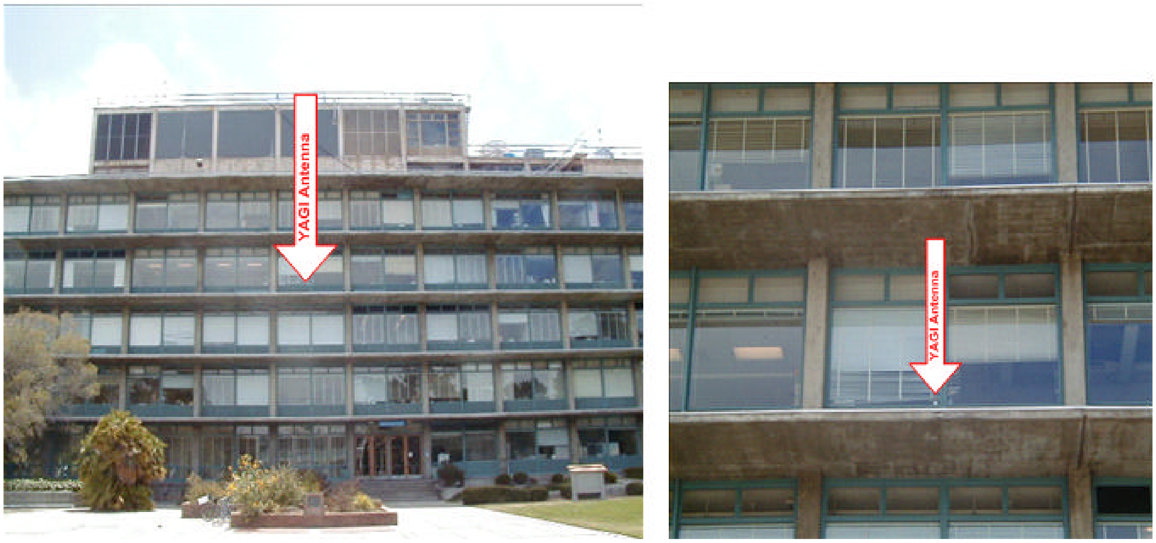


Figure 7.11. Wireless Yagi Covering the NPS Quad and Close-Up of Spanagel 402.

10. Proposed Wireless Expansion

a. NPS Outdoor Areas

Currently outdoor coverage of NPS is limited to the quad. The NPS police drive requirements for access outdoors beyond the quad. Access might benefit patrols throughout the base, as well as watchstanders at the gates. When the Threat Condition is high, different gates are often opened to mitigate security threats. This is an excellent example of how a wireless network is easily adaptable to changes in requirements. A costly underground wired installation for the Main Gate can be worthless if that particular gate is closed. However, wireless installations are not without their own issues. Because the outdoor NPS installation is similar to the proposed expansion at La Mesa, these issues will be discussed below.

b. La Mesa

Initially, the purpose of establishing a wireless network at La Mesa is to first provide network access for the police to expedite their data needs when they are patrolling the housing area. Ultimately, the wireless network shall provide access to all the residents of La Mesa as described in the requirements section above.

There are three main constraints for the wireless installation at La Mesa. There is a need for wired network access, adequate power, and line of sight (with acceptable obstructions).

- **Wired Network Access** – At present there are only three locations with wired access to the NPS network: The Tech Connection, The Housing Welcome Office, and the Family Service Center. All three locations are on the NPS ATM fiber backbone so bandwidth might not be an issue. However, if this network is to be used by all the residents of La Mesa, a study might be needed to determine the bandwidth usage implications of this action. Requiring a logon (authenticating NPGS domain users) is sufficient to manage bandwidth issues.
- **Power**– Power at La Mesa is provided by PG&E, but the entire area is all on a single meter. This is advantageous because power can be run to access points from any house or building in La Mesa without any billing issues. Installation of appropriate power receptacles at proposed AP sites is not thought to be an issue. The costs associated with this are included in the budgetary recommendations.
- **Line of Sight** – This may perhaps be one of the greatest challenges to provide wireless access in La Mesa. Most all of the streets in La Mesa have mature trees with many leaves, which can seriously affect the propagation of an 802.11 signal. Research from the University of Minnesota [36] indicates that typical outdoor installations can cover a few hundred meters due to tree, leaves, water etc. This strengthens the argument that a proper propagation study with professional tools is required. In addition it is imperative that the field portion of this study take place in the summer. Many accounts of wireless LAN signal degradation due to leaves that were not present during a winter setup have been documented on the Internet.

The main difficulty with La Mesa is that few locations have wired access. These locations essentially become hubs for wireless signals that must be propagated throughout the area. This can be done several ways:

- **Retransmission** – Retransmitting an 802.11 signal is generally not desirable because there is often throughput loss, but this is a viable solution to propagate access. The farthest street from wired access is no more than approximately 700 meters. Therefore, with one wireless repeater, it is theoretically possible to establish coverage with repeaters. However, once that distance has been reached, further retransmission along the streets will be necessary.
- **Elevated Retransmission** – Another alternative for the retransmission solution is to elevate the repeaters above the trees using telephone poles or some type of tower (there is already one antenna tower near the Housing Office). Directional Yagi antennas might be used to establish point-to-point connections. This reduces the number of repeaters necessary, thus reducing the hop count to end-users. The solution is not without problems. New towers may need to be constructed, frequency interface

with existing towers must be examined, and throughput may still be reduced due to the hops.

- **Fiber Backbone** – This is more of a worst-case alternative but viable nonetheless. Because La Mesa is on the ATM backbone, it might not be technically difficult to extend a fiber segment throughout the streets to provide network access for access points. Telephone poles can be the easiest, cheapest, and fastest way to run the fiber. In addition elevation is beneficial for connectivity to the access points. The main issue with this alternative is cost. There are approximately 8000 meters of road in La Mesa. Placing an access point every 300 meters requires only 27 access points, and the fiber itself is not cost prohibitive. The major cost involved will be the labor to string the fiber. Because of the cost, this solution may not be entirely desirable, but it might also be used in part to provide coverage in a problem area.

11. Costs

Wireless equipment is relatively cheap, and there are few infrastructure costs in getting the campus wireless network expanded as envisioned in the sections above. There are more costs associated with La Mesa, and each recommended option above might need to be studied for feasibility. Then a cost estimate might be made for that area. Estimated cost for the NPS base only campus is provided in Figure 7.12.

One Time Costs		
Per Access Point		
Equipment		$1,000.00
Installation		$1,000.00
Total		$2,000.00
Access Points Needed: 150		
Total for Equipment	$300,000.00	
Training		$50,000.00
Total One-Time Costs		$350,000.00
Annual Costs		
Life Cycle Maintenance	$50,000.00	

Figure 7.12. NPS Campus Wireless Cost Estimate.

An estimate of the cost savings from using the wireless network versus the expected costs for a wired network solution was not done. However, it is reasonable to expect that the savings is significant considering the size of the campus. The figures used were derived from a local market study for equipment and a study conducted by Carnegie-Mellon University [37] on the costs for their wireless equipment.. The costs listed are expected to be ceiling costs.

12. Areas for Further Research

- What is the maximum number of users per Access Point? How will that affect deployment?
- What are the true costs of extending the network to places like Fleet Numerical and the former Fort Ord?
- How will the Police and other emergency providers use the wireless network to access data?
- What other policies should be put in place to ensure security is properly implemented on campus and in the housing areas?

B. SUMMARY

Building a wireless campus successfully requires clear requirement definition, project management scheduling/planning, effective communication and technical skill. The wireless plan listed in this chapter is in keeping with the school's mission, vision and overall strategic plan. It has been validated by the NPS wireless group which consists of over 150 staff, students and faculty. All NPS stakeholders have been identified and canvassed for input and consensus has been reached. A requirements matrix is provided as well as an initial cost estimate. Once funding has been approved, the next step is to provide a timetable for procurement and installation.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. EXEMPLAR WIRELESS APPLICATIONS AND NETWORK MANAGEMENT TOOLS

A. INTRODUCTION

Computer users, network engineers, IT enthusiasts, and hackers all use tools to interact with wireless networks. No killer unique wireless application has yet emerged. The value of wireless networking as described in Chapter I is the ability to be mobile. The killer wireless application is to use your regular applications on the move. Email, browsing and net conferencing are what will attract users in the wired world and even more in the wireless world. Wireless can be used on just about any platform whether it be Windows, Linux, MAC, Palm, or PocketPC. If mobility is the key, than portability is the enabler. This chapter will give a basic overview of the most common tools used. The client hardware that was used was a Compaq Presario 2700T laptop (dual boot Windows XP Pro and Linux Redhat 7.3) with an Orinoco 802.11b wireless card, a Toshiba PocketPC(2002) e740 with a built in 802.11b wireless card and a Ipaq 3600 Pocket PC(2002) with a Cisco 802.11 wireless card and a Teletype GPS card. They are shown in Figures 8.1 and 8.2.

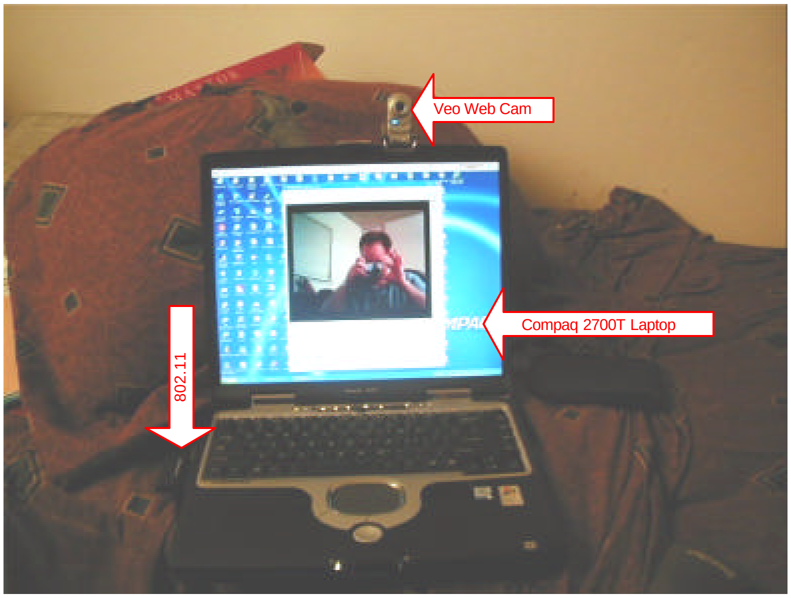


Figure 8.1. Compaq Laptop 2700T Presario with an Orinoco 802.11 Wireless Card and Veo Web Cam.

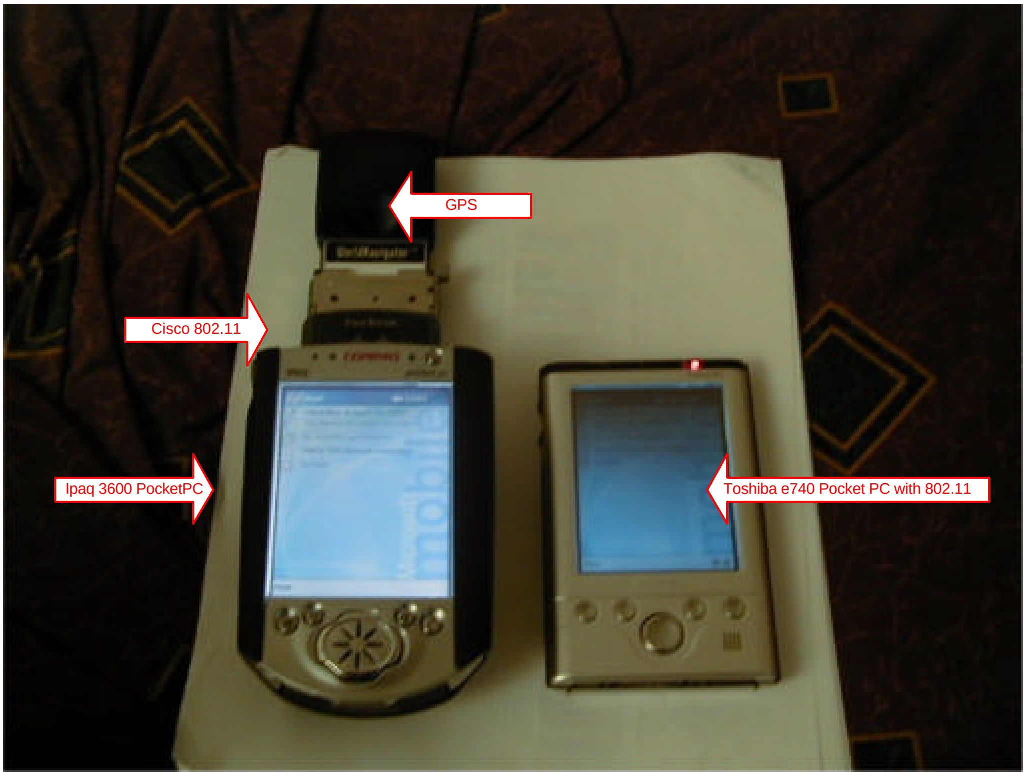
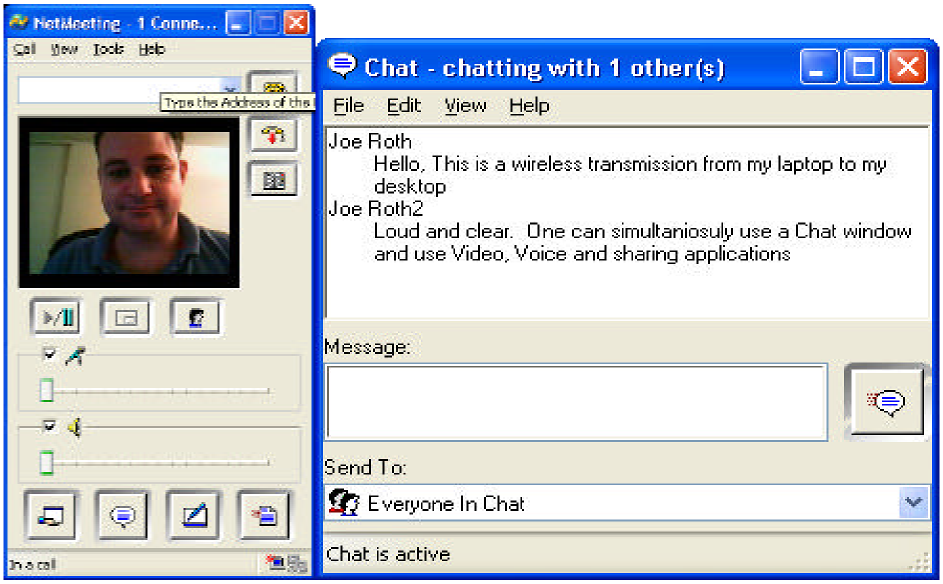


Figure 8.2. Two PocketPC Handheld Devices. Left: Compaq IPAQ with a Cisco 802.11b Card/Teletype GPS Card, Right: Toshiba e740 with Built In 802.11b.

NetMeeting is limited freeware that works on Windows 9x, NT, 2K, and XP platforms. It allows users who are wired or wireless to communicate through video, audio and text channels. It also has the ability to share applications across any network. Figure 8.3 is a demonstration across the network using video, audio, and text on NPS's wireless campus LAN. Microsoft Messenger combines NetMeeting, Hotmail and other applications as part of its initial .NET client package.

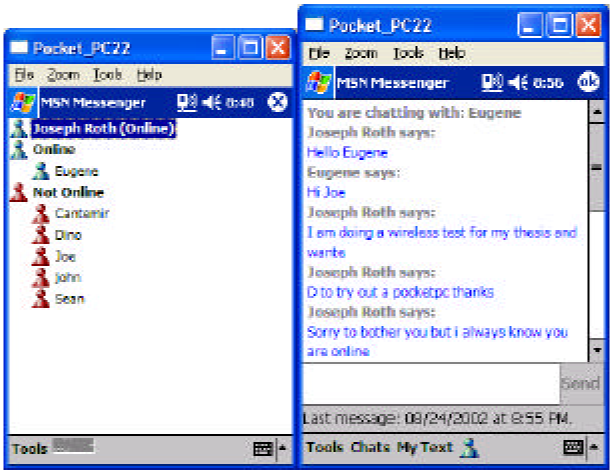


Joe Roth
Hello, This is a wireless transmission from my laptop to my desktop
Joe Roth2
Loud and clear. One can simultaniosuly use a Chat window and use Video, Voice and sharing applications

Chat is active

Figure 8.3. An Example of Wireless Video Conferencing and Chatting Between a Laptop and a Desktop using Microsoft's NetMeeting.

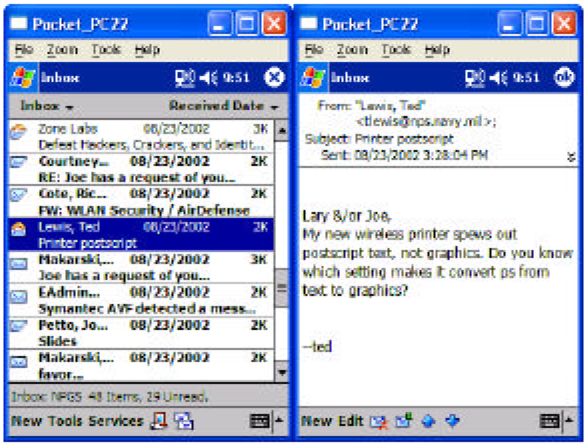
A light version of Microsoft Messenger works on the PocketPC that allows for chatting but does not yet support video. Figure 8.4 shows a brief conversation over the internet using a PocketPC via a wireless link. Pop3 email as well as web based mail can be used via wireless 802.11 PocketPC device and again is demonstrated in Figures 8.4 and 8.5. Internet web browsing is demonstrated in Figure 8.6 using a pocket explorer internet browser.



You are chatting with: Eugene
Joseph Roth says:
Hello Eugene
Eugene says:
Hi Joe
Joseph Roth says:
I am doing a wireless test for my thesis and wante
Joseph Roth says:
D to try out a pocketpc thanks
Joseph Roth says:
Sorry to bother you but i always know you are online

Last message: 08/24/2002 at 8:55 PM.

Figure 8.4. An Example of a Wireless PocketPC using Microsoft Messenger Across the Internet Between Joe Roth and Eugene Burakov.



Inbox	Received Date	
Zone Labs Defeat Hackers, Crackers, and Identit...	08/23/2002	3K
Courtney... RE: Joe has a request of you...	08/23/2002	2K
Cote, Ric... FW: WLAN Security / AirDefense	08/23/2002	2K
Lewis, Ted Printer postscript	08/23/2002	2K
Makarski,... Joe has a request of you...	08/23/2002	3K
EAdmin... Symantec AVF detected a mess...	08/23/2002	2K
Petto, Jo... Slides	08/23/2002	2K
Makarski,... favor...	08/23/2002	2K

Inbox: NPGS 48 Items, 29 Unread.

From: "Lewis, Ted"
<tlewis@nps.navy.mil>;
Subject: Printer postscript
Sent: 08/23/2002 3:28:04 PM

Lary &/or Joe,
My new wireless printer spews out postscript text, not graphics. Do you know which setting makes it convert ps from text to graphics?

--ted

Figure 8.5. An Example of a Wireless PocketPC using Microsoft Pocket Outlook Across the Internet.

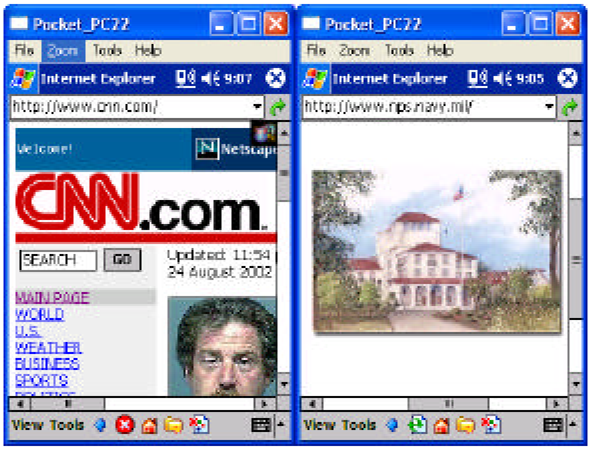
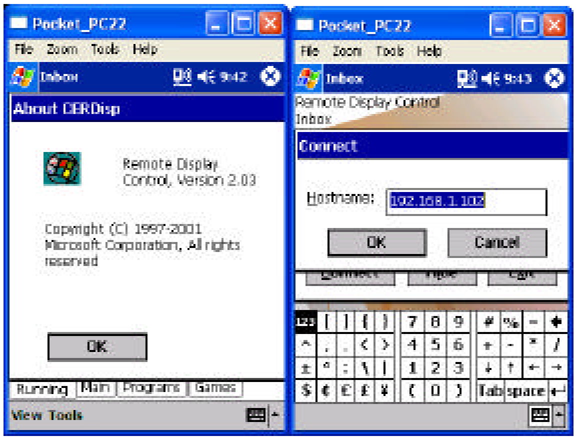


Figure 8.6. Two Examples of a Wireless PocketPC using Microsoft Pocket Internet Explorer.

Another collaborative tool is Microsoft's Remote Display. It allows a wireless-enabled PocketPc to connect and simultaneously be controlled and displayed on another PC. It is an ideal teaching device because an instructor could have a laptop connected to a projector and he or she could be running a remote display and be able to wirelessly demonstrate the functionality of a handheld to a classroom where normally the size of the handheld makes it impossible to demonstrate anything to more than one person at a time. All the screen shots of the PocketPC in this chapter were done using Remote Display. Figure 8.7 shows the configuration of remote display where the user enters the IP address of the laptop/desktop where the PocketPc will be transmitted to. Figure 8.8 shows the final affect where the web site http://javajoe.net is shown rendered on a PC, a PocketPC and again rendered in a remote display window. The PocketPC can be controlled directly at the PocketPC or on the remote display window running on the PC.



About CERDisp

Remote Display Control, Version 2.03

Copyright (C) 1997-2001 Microsoft Corporation, All rights reserved

OK

Connect

Hostname: 192.168.1.102

Figure 8.7. Remote Display Configuration Screens.

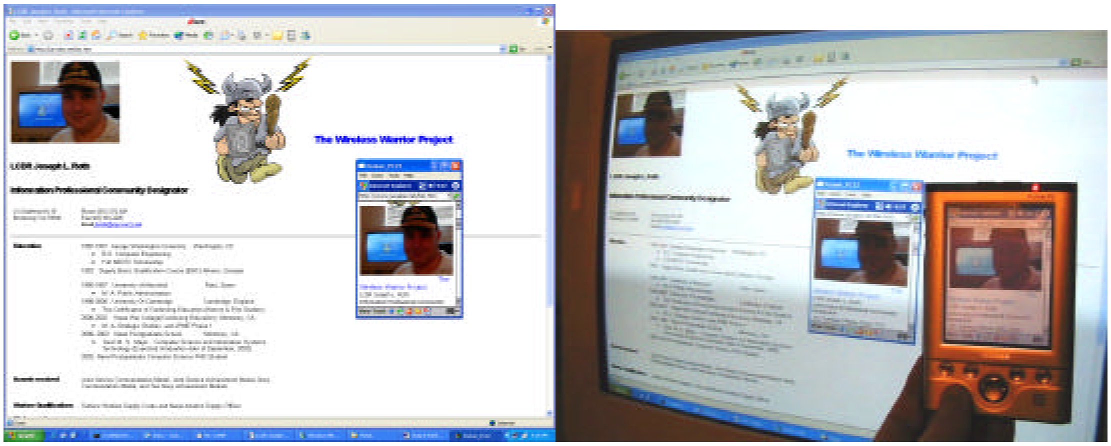


Figure 8.8. http://javajoe.net Shown on a Desktop, a PocketPC, and a Remote Display Window.

The dividing line between handheld and laptops devices is narrowing in the same fashion as laptops and desktops. Another example is Cortona's plug-in for X3D, the XML port of Virtual Reality Modeling Language (VRML). Figure 8.9 shows X3D Models of the USS Independence flight operations and of Herman Hall at the Naval Postgraduate School. These images were rendered live on a PocketPC and redisplayed via a wireless 802.11b network on a desktop using the remote display application.

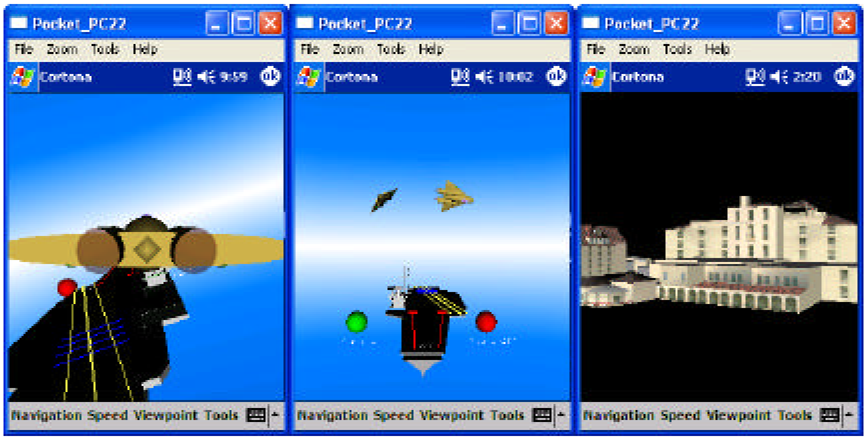
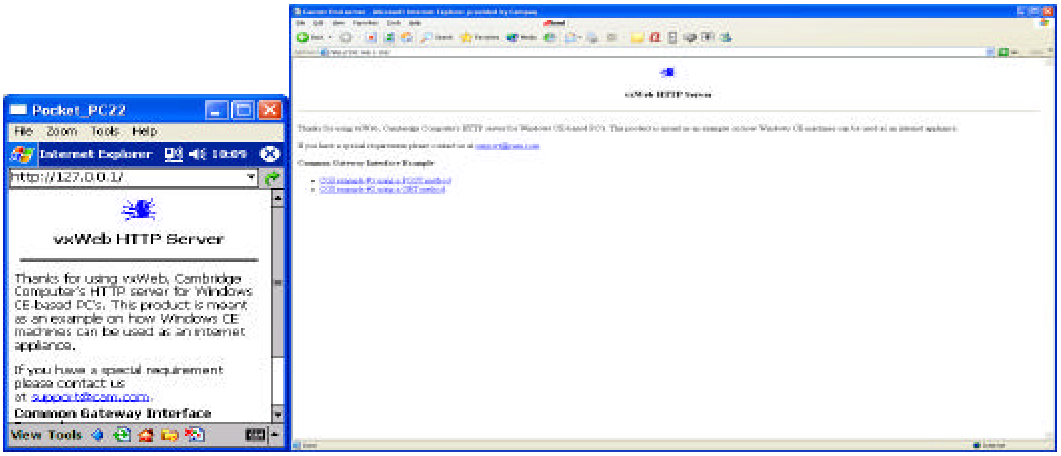


Figure 8.9. X3D Models of the USS Independence Flight Operation and the Naval Postgraduate School's Herrmann Hall
(Rendered on a PocketPC and Redisplayed wirelessly using Remote Display Configuration).
(The USS Independence Model was written by Joe Roth and the Hermann Hall Model was written by John Locke).

Wireless devices are not limited to client functionality. The Cambridge Computer Corporation (http://www.cam.com) makes a web server that runs on a PocketPC. This allows for a wireless portable web server on a handheld device. The military applications for such a device are endless, from remote sensors to biometric feedback on an individual. The hardware suite is cheap (under $700) and portable (under a pound). Its greatest limitation is battery life. It can function for 45 minutes with heavy wireless use and several hours with limited wireless use. A demonstration of the Vxweb web server is shown in Figure 8.10.



vxWeb HTTP Server

Thanks for using vxWeb, Cambridge Computer's HTTP server for Windows CE-based PC's. This product is meant as an example on how Windows CE machines can be used as an internet appliance.

If you have a special requirement please contact us at support@ccom.com.

Common Gateway Interface

Figure 8.10. Vxweb Web Server for the Pocket PC.

When the Vxweb server and the Remote Display Application are combined with wireless PocketPC with a web cam you have created a networked surveillance device that weighs less than 1 pound in weight and costs less than $800. The Vxweb server saves the image and can be served out to any user on its network. Figures 8.11 and 8.12 demonstrate this feat. These devices can also have GPS functionality which will help the user not only know where he or she is but also can be used in conjunction with 802.11b wireless link to report back the same information to others. Several experiments at NPS were conducted in February 2002 for a Limited Objective Experiment which examined how an anti-terrorist unit can collaborate using handheld and laptops devices with 802.11b and GPS features. Figure 8.13 shows the movements of an individual being tracked by GPS and that being relayed via 802.11 wireless network.

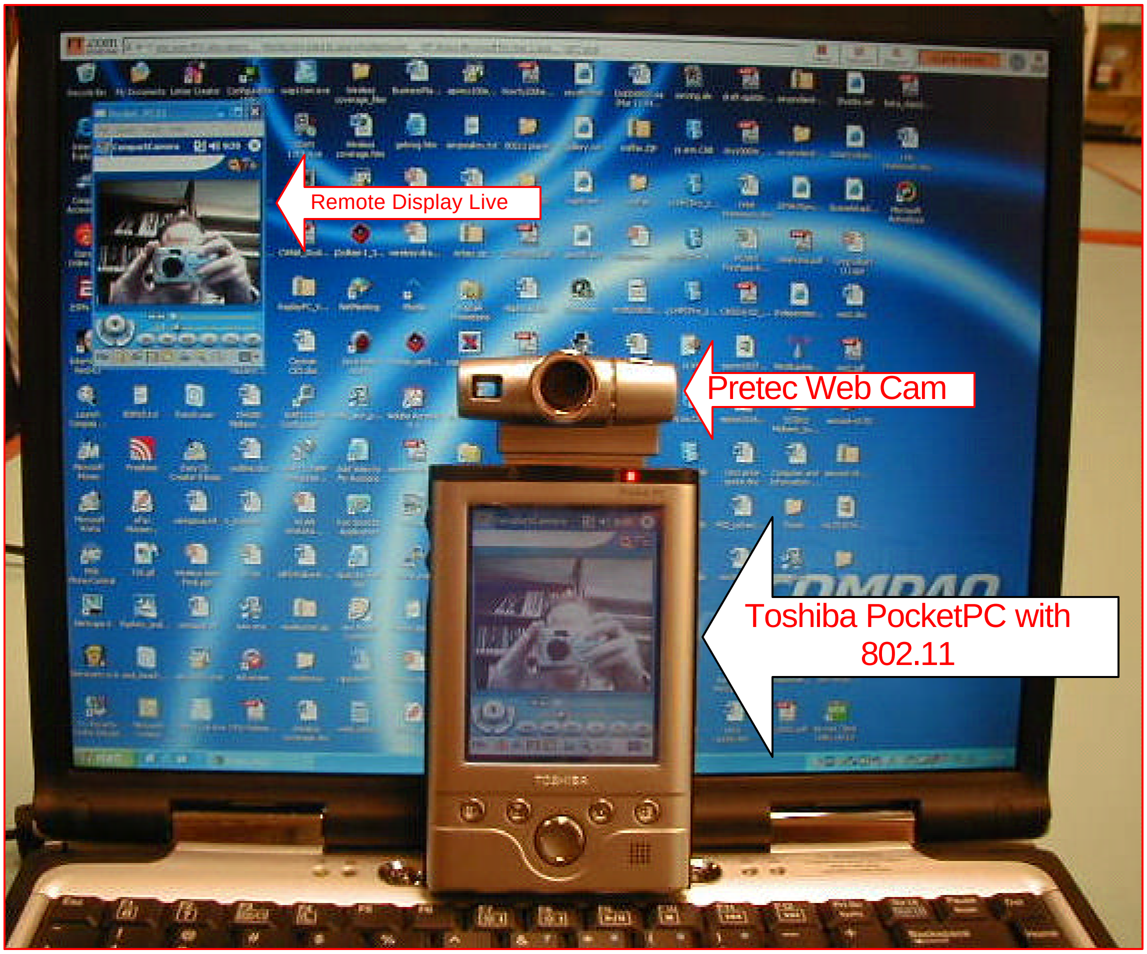


Figure 8.11. A Handheld Wireless Web Cam and Remote Display Application Exemplar.

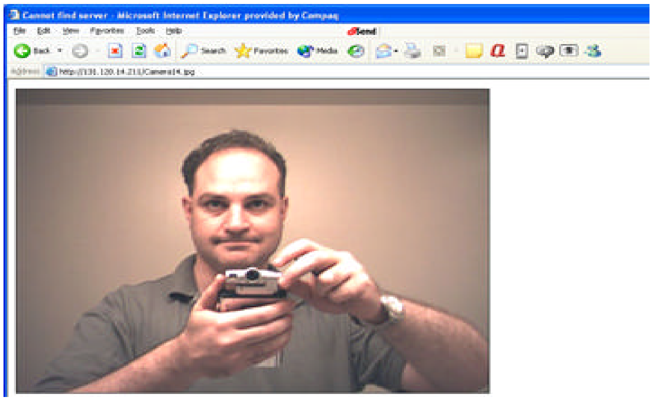
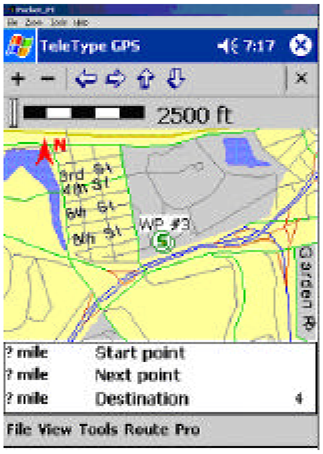

Cannot find server - Microsoft Internet Explorer provided by Compaq
File Edit View Favorites Tools Help
Send
Back
Search
Favorites
Media
Address
http://131.120.14.211/Camera14.jpg

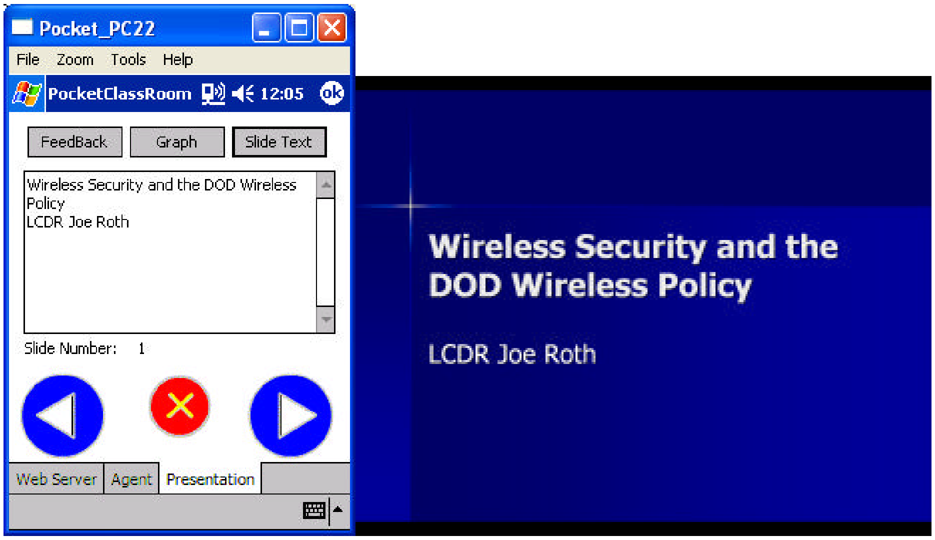
Figure 8.12. Wireless Live Images Served Out on a Wireless Handheld Web Cam Web Server Looking in the Mirror.



? mile Start point
? mile Next point
? mile Destination 4

Figure 8.13. A GPS Display of the Naval Postgraduate School Displayed on a PocketPC.

Another interesting development is the Pocket Classroom Project at Wake Forest University [38] Pocket Classroom is free software (for educational institutions) that allows a wireless PocketPC to control a desktop/laptop for the purpose of controlling power point presentation (See Figure 8.14). This is accomplished by running an agent on the laptop or desktop and selecting which power point file to run via a handheld device (See Figure 8.14).



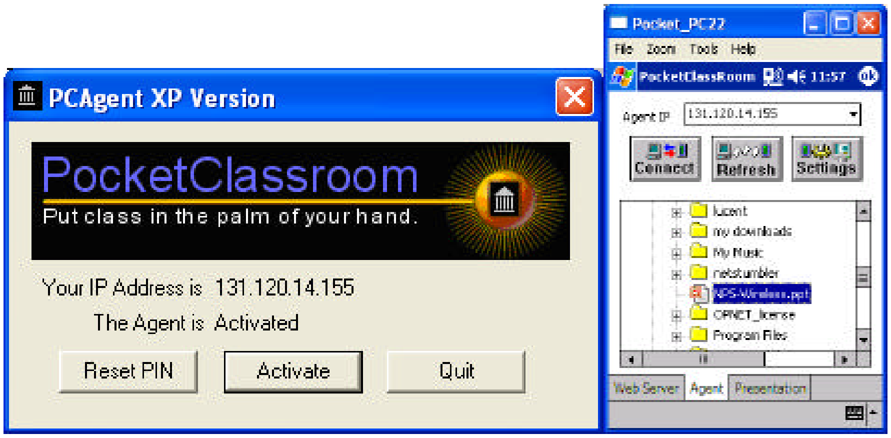
Wireless Security and the DOD Wireless Policy
LCDR Joe Roth

Slide Number: 1

Wireless Security and the DOD Wireless Policy

LCDR Joe Roth

Figure 8.14. Handheld PocketClassroom (Left) Wireless Controlling a Laptop/Desktop Running a Microsoft PowerPoint (Right).



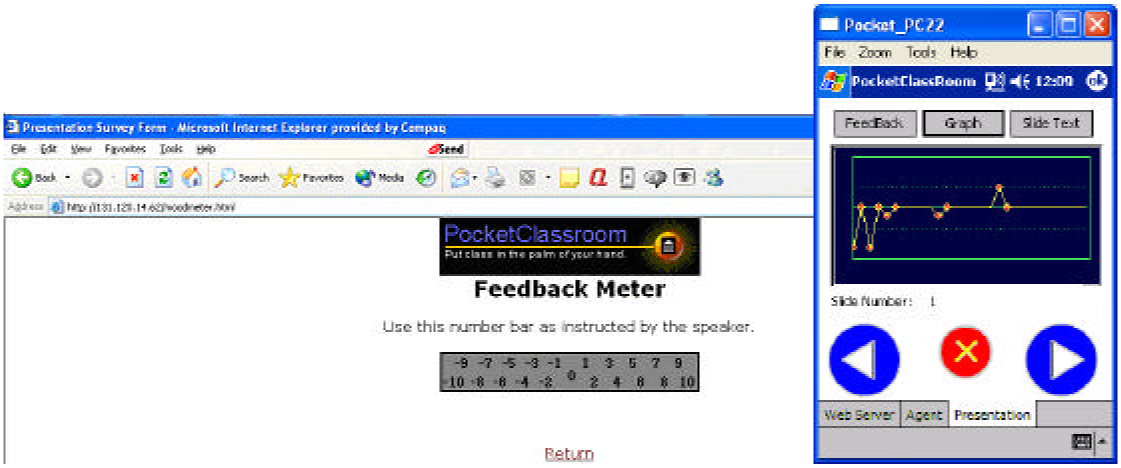
Your IP Address is 131.120.14.155

The Agent is Activated

Agent IP 131.120.14.155

Figure 8.15. The Pocket Classroom Desktop/Laptop Agent (Left) Being Controlled by a Pocket PC (Right).

It also is a handheld web server that establishes communication with the audience allowing students to send questions directly to the handheld device. It allows audience members to vote if they understand the subject on a scale from -10 to 10. They do this by using a web browser and typing in the IP address of the speaker's handheld. A live graph is also displayed on the handheld providing live aggregate feedback. (See Figure 8.16 below.)



http://131.120.14.62/woodmeter.html

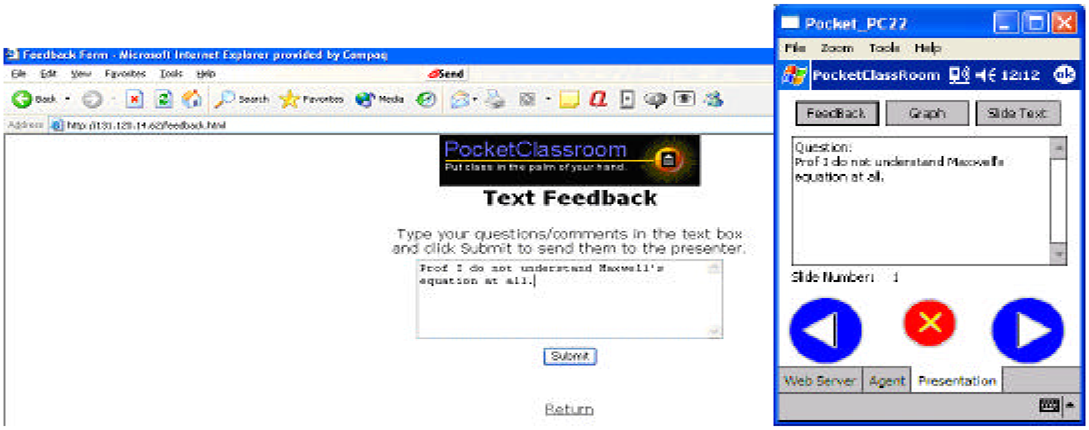
Feedback Meter

Use this number bar as instructed by the speaker.

Slide Number: 1

Figure 8.16. Show How Students Provide Live Numeric Feedback from -10 to 10 via a Web Browser (Left) and the Results are Displayed on the Instructor's Handheld (Right).

Audience members can also send text messages to the instructor so he can respond to them either at the point of receipt or later via email. Figure 8.17 demonstrates this.


Feedback Form - Microsoft Internet Explorer provided by Compaq
File Edit View Favorites Tools Help
Send
Back Search Favorites Media
Address http://131.128.14.62/feedback.html
PocketClassroom
Put class in the palm of your hand.
Submit
Return
Pocket_PC22
File Zoom Tools Help
PocketClassRoom 12:12 ok
FeedBack Graph Slide Text
Web Server Agent Presentation

Text Feedback

Type your questions/comments in the text box and click Submit to send them to the presenter.

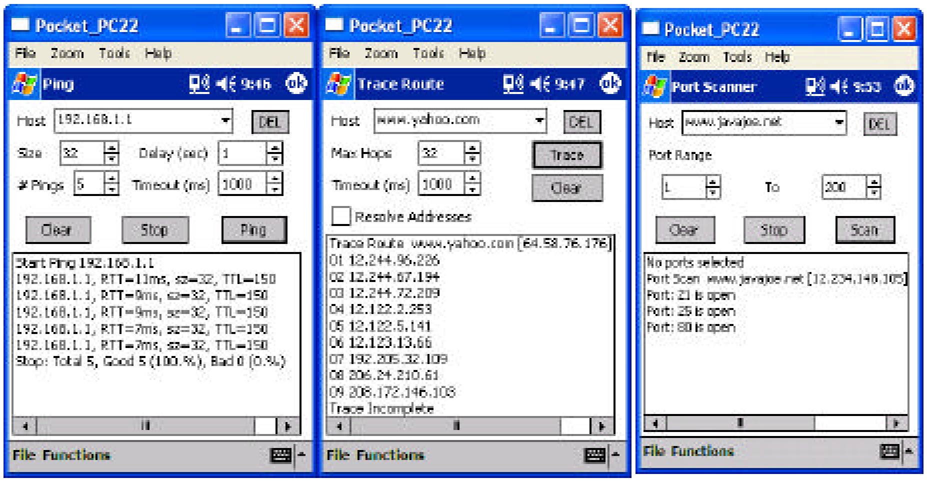
Prof I do not understand Maxwell's equation at all.

Question:
Prof I do not understand Maxwell's equation at all.

Slide Number: 1

Figure 8.17. Shows How a Student Provides Live Text Feedback via a Browser (Left) and Displayed on the Instructor’s Handheld Device (Right).

The basic network tools such as ping, traceroute, and port scan are built into most operating systems; unfortunately they are not included in the PocketPC operating system. Cambridge Corporation provides a utilities suite that does this for free called Vxutil and can be downloaded at http://www.cam.com. These are vital tools for any administrator to ensure their wireless LAN is working. Figure 8.18 shows these tools in action.



Host 192.168.1.1
Size 32 Delay (sec) 1
# Pings 5 Timeout (ms) 1000

```
Start Ping 192.168.1.1
192.168.1.1, RTT=11ms, sz=32, TTL=150
192.168.1.1, RTT=9ms, sz=32, TTL=150
192.168.1.1, RTT=9ms, sz=32, TTL=150
192.168.1.1, RTT=7ms, sz=32, TTL=150
192.168.1.1, RTT=7ms, sz=32, TTL=150
Stop: Total 5, Good 5 (100.%), Bad 0 (0.%)
```

Host www.yahoo.com
Max Hops 32
Timeout (ms) 1000
☐ Resolve Addresses

```
Trace Route www.yahoo.com [64.58.76.176]
01 12.244.96.226
02 12.244.67.194
03 12.244.72.209
04 12.122.2.253
05 12.122.5.141
06 12.123.13.66
07 192.205.32.109
08 206.24.210.61
09 208.172.146.103
Trace Incomplete
```

Host www.javajoe.net
Port Range
1 To 200

```
No ports selected
Port Scan www.javajoe.net [12.234.148.105]
Port: 21 is open
Port: 25 is open
Port: 80 is open
```

Figure 8.18. Vxutil Wireless Tools.

Another tool that helps one visualize the different types of traffic is called Etherape (http://etherape.sourceforge.net/). It is free but only runs on the Linux operating system. It is a great tool because it color codes the different types of traffic and varies the graphic in direct proportion to the amount of data. Figure 8.19 shows an example of a user surfing the web. The image on the left shows the network before the user clicks on a hyperlink and the image on the right shows after.

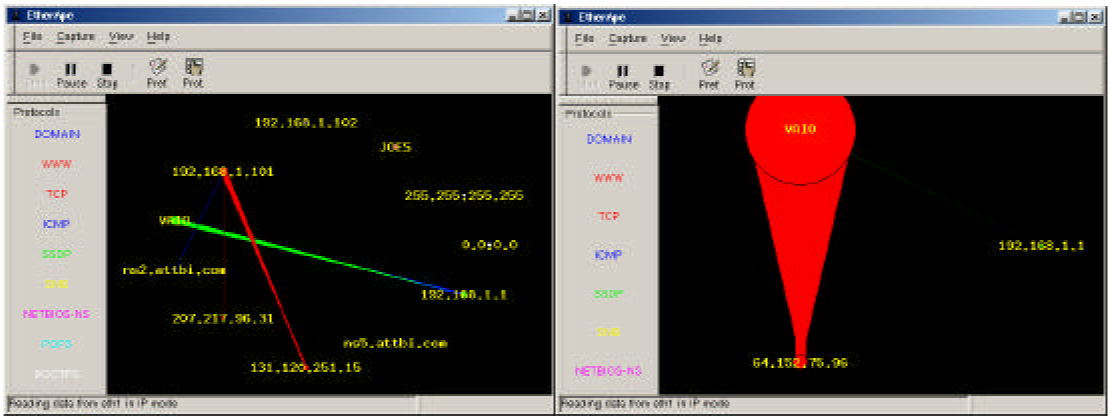


Figure 8.19. An Example of Etherape.

Etherape is a great teaching tool and could be used as monitoring device in a network operating center to get a general graphical feel for the amount and types of traffic on a network.

The premier wireless site survey tool is called Wireless Valley (http://www.wirelessvalley.com). It is a commercial grade software suite that does everything from design to site survey. An example of the more popular Wireless Valley products are Infielder and SiteFielder. Sample Screen shots are shown below in Figure 8.20 for 2d and 3d auto-mapping of wireless coverage.

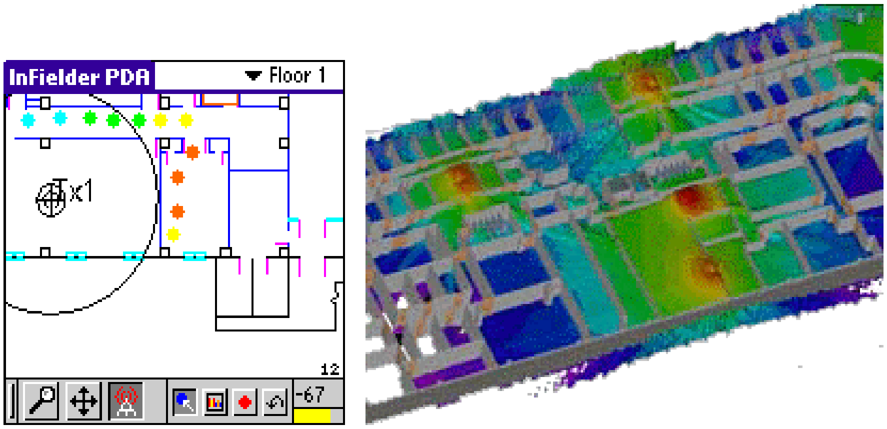
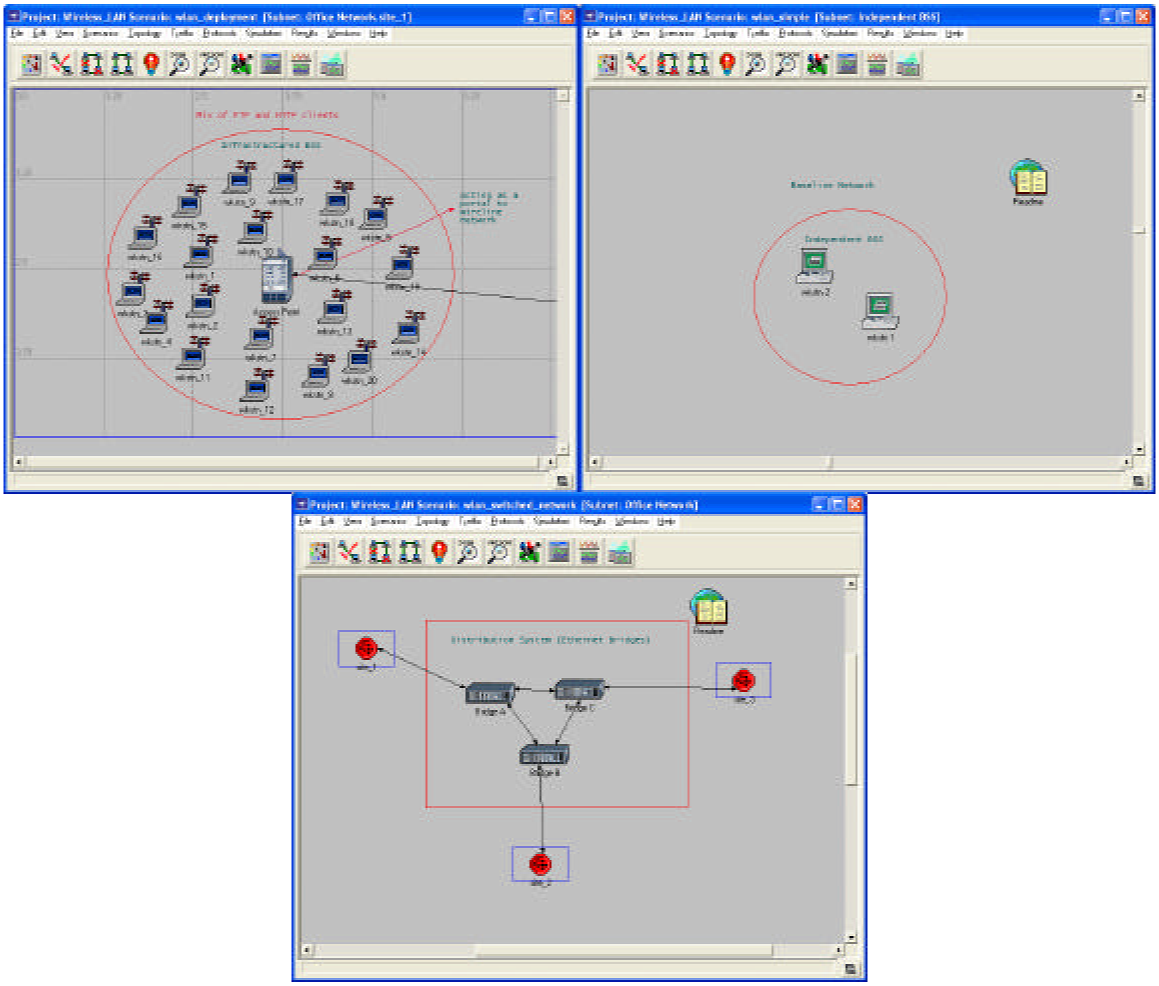


Figure 8.20. Wireless Valley's SiteFielder and Infielder.

Another great tool is Opnet (http://www.opnet.com). Opnet is a commercial grade modeling, simulation and traffic analysis software. It is geared primarily for wired networks but does have RF modules and has the basic 802.11 modules already built in. Opnet is extremely powerful and allows for developers to create new protocols. Figure 8.21 demonstrates several OPNET simulations of wireless networks.

B. SUMMARY

The power and extensibility of the functionality of small wireless devices are numerous. These devices are readily available as consumer electronics anywhere in the world. The military relevance is overwhelming. These devices (assuming battery life is improved) could be used to monitor a serviceman's biological reading for heartbeat and stress as well as provide a video/audio feedback to assist command and control situational awareness. If these devices were used in mass then data could be gathered on the stress levels of a battalion of marines during an amphibious assault or in combat. Historical metrics could be maintained and, where there are significant deviations, that could flag command elements to reinforce those areas. One can deploy an aerial



Project: Wireless_LAN Scenario: wlan_deployment [Subnet: Office Network.site_1]
File Edit View Scenarios Topology Traffic Protocols Simulation Results Windows Help
Mix of FTP and HTTP clients
Infrastructured BSS
Acting as a portal to wireline network
Access Point
Project: Wireless_LAN Scenario: wlan_simple [Subnet: Independent BSS]
File Edit View Scenarios Topology Traffic Protocols Simulation Results Windows Help
Baseline Network
Independent BSS
Readme
Project: Wireless_LAN Scenario: wlan_switched_network [Subnet: Office Network]
File Edit View Scenarios Topology Traffic Protocols Simulation Results Windows Help
Distribution System (Ethernet Bridges)
Bridge A
Bridge C
Bridge B
Readme

Figure 8.21. Opnet Running Three Wireless Simulations.

surveillance platform at minimal cost simply by attaching these devices to a small remote flying device. In summary, small wireless devices allow the ability to gather data and collaborate in real time cheaply. Email, voice, video, and collaborative applications can be done today. Due to the proliferation of wireless devices, the need for accurate modeling and simulation efforts is paramount. Build the wireless network at NPS and great applications will emerge including the realization of a net-centric warfare training environment.

IX. CONCLUSIONS AND RECOMMENDATIONS FOR FURTHER RESEARCH

A. CONCLUSIONS

It is clear that wireless technologies will be a part of everyone's life both in the civilian world as well as the military. The economic growth in a down economy of the 802.11 sector has shown its persistence for success. The students, staff and faculty of NPS have positively endorsed its use in two surveys. Every major university in America and most top international universities in the world have deployed 802.11 across their campuses including West Point. Throughout the third world people are moving from no telephones to roaming digital cell phones, and wireless data is following the same path. This great jump in capability has caused even a greater demand for wireless devices outside the US. This is driven based on the ability to skip several technological generations in one swoop (i.e., no telephone/data capability to a wireless roaming capability jump). The threat of being surpassed in terms technological advantage and wireless collaboration doctrine is real. Because the US has such a well-wired infrastructure wireless technology might not have the same revolutionary effect as in the rest of the world. In an extreme case, terrorists groups might use this low cost technological capability as an asymmetric strike communication capability. Wireless technology is the leveling playing field for our friends and foes. The only hope for US sustained advantage is through a commitment to build advanced mobile secure network infrastructures and collaborative application doctrine development. NPS is the ideal location for such an undertaking.

B. RECOMMENDATIONS FOR FURTHER RESEARCH

There are numerous areas where further research can be performed:

- Qualitative and quantitative research in discovering a numeric definition for the value of network mobility
- Antenna and power design and doctrine for the active control of wireless coverage
- Exploration of new wireless ultra-wide band technologies
- Explore / improve the 802.11 architecture to support improved Quality of Service functionality

- Determine appropriate security evaluation, training and implementation techniques in regards to emerging wireless technologies
- Catalog a knowledge base of specific applications/tools, wireless technology use, and security/supportability concerns across DOD
- Develop wireless network collaboration applications that serve real world purposes. It may consist of better ways to do supply inventories, better ways to teach, better ways to communicate from ship to ship, better ways to administer medical treatment, better ways to monitor the location and bio signs of soldier and sailors in the field, etc.

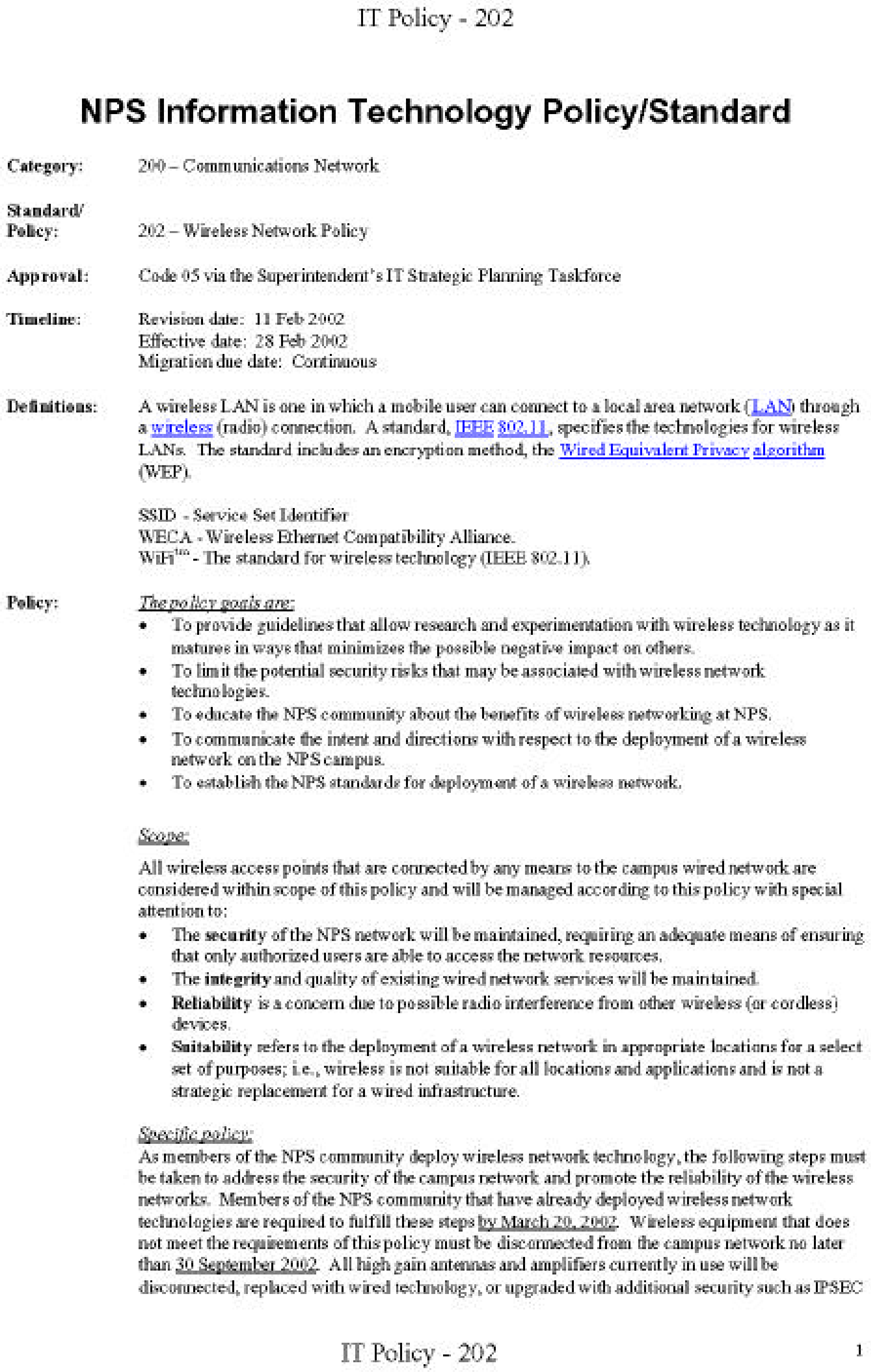
As military IT managers and Computer Scientists it is fundamental that military educational institutions embrace new technologies regardless of the apparent initial security risks associated with them. If new technologies are tested in an academic environment where it is part of everyone's daily production and communication then truths will emerge on supportability, usability, and security. Only then can impartial decisions be made on the proper deployment in non-academic environments. Labs need to be moved outside of the laboratory and testers need to be from diverse backgrounds. This is why wireless is the perfect fit for the NPS diverse campus. This is how we move into a net-centric learning environment. Few academic settings can boast of officers from every service, civil servants, international officers, and career academic faculty. Wireless networks at NPS build a fertile field for real academic achievement and exploration.

APPENDIX A. NPS IT POLICY 202 WIRELESS NETWORK POLICY

The beginnings of the NPS wireless policy started with the desire of the author of this thesis to build a campus wide wireless network in August 2001. After a thorough search there was no Navy or NPS policy on wireless LAN use. The Wireless Group was formed as a forum to discuss the security, management, and capability of the 802.11 technology and other wireless issues. An internal web site http://intranet.nps.navy.mil/wireless and mailing list wireless@nps.navy.mil was created to improve communication. A heated discussion on whether NPS should implement 802.11 on an enterprise level based on security versus and usability concerns. From these discussions that it became apparent that a local instruction was needed regardless of the scale of the wireless LAN.

LCDR Roth visited Carnegie Mellon University (CMU), the oldest and possibly the most successful wireless campus implementation. Informal interviews with CMU staff, faculty and students provided a knowledge foundation for NPS wireless policy and possible implementation. An internet search quickly showed that almost every major university had built a campus wireless LAN or was planning on building one in the next year. Many of them had their local policies posted to the internet. UC San Diego, UC Berkley, Northwestern, Cornell, Iowa State, Stanford and many other prominent university wireless policies were compiled and posted to the NPS wireless site for review. (http://intranet.nps.navy.mil/wireless/other_university_wireless_policy.htm).

In January, 2002 a draft NPS policy letter consisting of the best of breed from other universities was submitted to the NPS faculty, staff, and student body for comment. All comments were posted to the wireless site. The comments were compiled and briefed to the NPS Technology and Strategic Planning committees. Changes were incorporated and the final policy was submitted in February 2002 to the NPS leadership for approval. The NPS wireless policy is provided in this appendix and is posted on the wireless site http://intranet.nps.navy.mil/wireless.



NPS Information Technology Policy/Standard

Category: 200 – Communications Network

Standard/ Policy: 202 – Wireless Network Policy

Approval: Code 05 via the Superintendent's IT Strategic Planning Taskforce

Timeline:
Revision date: 11 Feb 2002
Effective date: 28 Feb 2002
Migration due date: Continuous

Definitions: A wireless LAN is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. A standard, IEEE 802.11, specifies the technologies for wireless LANs. The standard includes an encryption method, the Wired Equivalent Privacy algorithm (WEP).

SSID - Service Set Identifier
WECA - Wireless Ethernet Compatibility Alliance.
WiFi^{tm} - The standard for wireless technology (IEEE 802.11).

Policy: *The policy goals are:*

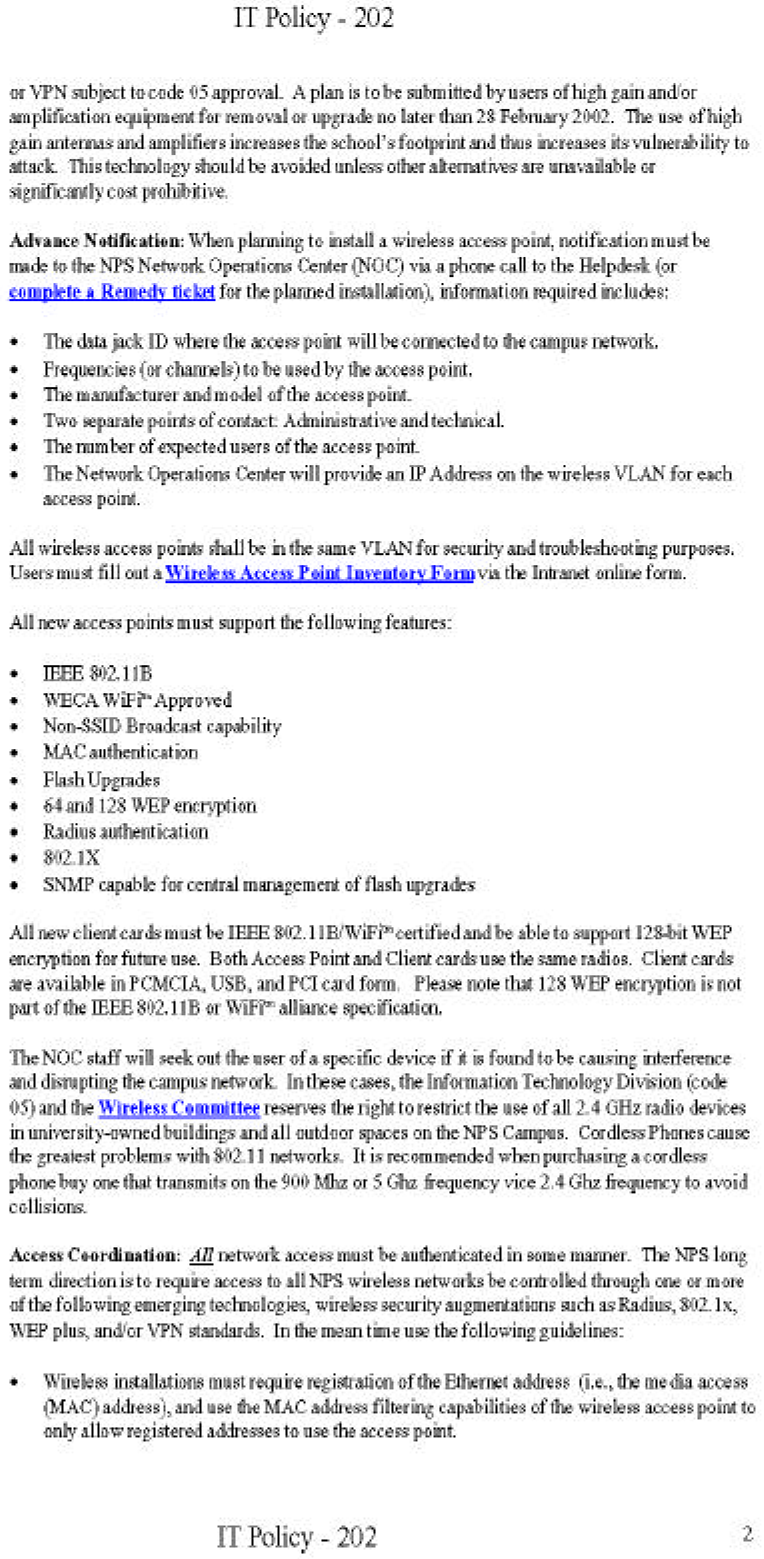
- To provide guidelines that allow research and experimentation with wireless technology as it matures in ways that minimizes the possible negative impact on others.
- To limit the potential security risks that may be associated with wireless network technologies.
- To educate the NPS community about the benefits of wireless networking at NPS.
- To communicate the intent and directions with respect to the deployment of a wireless network on the NPS campus.
- To establish the NPS standards for deployment of a wireless network.

Scope:

All wireless access points that are connected by any means to the campus wired network are considered within scope of this policy and will be managed according to this policy with special attention to:

- The **security** of the NPS network will be maintained, requiring an adequate means of ensuring that only authorized users are able to access the network resources.
- The **integrity** and quality of existing wired network services will be maintained.
- **Reliability** is a concern due to possible radio interference from other wireless (or cordless) devices.
- **Suitability** refers to the deployment of a wireless network in appropriate locations for a select set of purposes; i.e., wireless is not suitable for all locations and applications and is not a strategic replacement for a wired infrastructure.

Specific policy:
As members of the NPS community deploy wireless network technology, the following steps must be taken to address the security of the campus network and promote the reliability of the wireless networks. Members of the NPS community that have already deployed wireless network technologies are required to fulfill these steps by March 20, 2002. Wireless equipment that does not meet the requirements of this policy must be disconnected from the campus network no later than 30 September 2002. All high gain antennas and amplifiers currently in use will be disconnected, replaced with wired technology, or upgraded with additional security such as IPSEC



or VPN subject to code 05 approval. A plan is to be submitted by users of high gain and/or amplification equipment for removal or upgrade no later than 28 February 2002. The use of high gain antennas and amplifiers increases the school's footprint and thus increases its vulnerability to attack. This technology should be avoided unless other alternatives are unavailable or significantly cost prohibitive.

Advance Notification: When planning to install a wireless access point, notification must be made to the NPS Network Operations Center (NOC) via a phone call to the Helpdesk (or **complete a Remedy ticket** for the planned installation), information required includes:

- The data jack ID where the access point will be connected to the campus network.
- Frequencies (or channels) to be used by the access point.
- The manufacturer and model of the access point.
- Two separate points of contact: Administrative and technical.
- The number of expected users of the access point.
- The Network Operations Center will provide an IP Address on the wireless VLAN for each access point.

All wireless access points shall be in the same VLAN for security and troubleshooting purposes. Users must fill out a **Wireless Access Point Inventory Form** via the Intranet online form.

All new access points must support the following features:

- IEEE 802.11B
- WECA WiFi™ Approved
- Non-SSID Broadcast capability
- MAC authentication
- Flash Upgrades
- 64 and 128 WEP encryption
- Radius authentication
- 802.1X
- SNMP capable for central management of flash upgrades

All new client cards must be IEEE 802.11B/WiFi™ certified and be able to support 128-bit WEP encryption for future use. Both Access Point and Client cards use the same radios. Client cards are available in PCMCIA, USB, and PCI card form. Please note that 128 WEP encryption is not part of the IEEE 802.11B or WiFi™ alliance specification.

The NOC staff will seek out the user of a specific device if it is found to be causing interference and disrupting the campus network. In these cases, the Information Technology Division (code 05) and the **Wireless Committee** reserves the right to restrict the use of all 2.4 GHz radio devices in university-owned buildings and all outdoor spaces on the NPS Campus. Cordless Phones cause the greatest problems with 802.11 networks. It is recommended when purchasing a cordless phone buy one that transmits on the 900 Mhz or 5 Ghz frequency vice 2.4 Ghz frequency to avoid collisions.

Access Coordination: ***All*** network access must be authenticated in some manner. The NPS long term direction is to require access to all NPS wireless networks be controlled through one or more of the following emerging technologies, wireless security augmentations such as Radius, 802.1x, WEP plus, and/or VPN standards. In the mean time use the following guidelines:

- Wireless installations must require registration of the Ethernet address (i.e., the media access (MAC) address), and use the MAC address filtering capabilities of the wireless access point to only allow registered addresses to use the access point.

- Users must use WEP (Wired Equivalent Privacy) keys to limit the number of people that have unencrypted access to the network. The keys must be kept as a shared secret. Members of the NPS community must inform users how to properly configure WEP. The 64-bit version of WEP should be used in the short term to support legacy systems. When funding becomes available for a campus wide implementation 128 encryption with dynamic keys will be universally installed.

Encryption: All wireless installations must turn on the Wired Equivalent Privacy (WEP) feature in an effort to protect user data. WEP should not be considered a complete protection, as it can be deciphered quickly and easily using the commonly available hacking tools. In the near future, dynamic WEP unique session key assignment will be used to provide additional security of user data as mentioned before as a wireless security augmentation. The NPS ISSM will assign and distribute a centrally managed WEP Key.

Network Name: The NOC will assign a network name, SSID code and WEP key. The SSID and WEP key will be the same for all access point to allow for campus roaming and security standardization. The SSID will be set in non-broadcast mode as security measure.

Notice of Service Activation: Departments must notify the NOC when an access point is placed in service or taken out of service. Notification should be made through the online Remedy system at **http://intranet.nps.navy.mil/Code05/New05/remedyldr.htm** or by phoning the help desk at extension 1046.

Large Scale Deployments: Departments with a large-scale installation of more than 50 users must arrange a meeting with the NOC Manager at x3698, to discuss additional issues that must be taken into account to maximize the potential for success.

Applications that use NetBEUI or Apple Talk to access resources will, instead, have to use IP to access those resources. For most modern applications this is not a problem, but some reconfiguration may be required.

Shared Resources: Shared resources such as printers, servers, scanners, etc. should be placed on the wired network to allow for most efficient and reliable access.

Placement of equipment: All wireless equipment must be placed in locations and set to frequencies that coordinate reasonably with campus network mechanisms. While the 802.11 standard has 12 channels only three channels do not overlap: channels 1, 6, and 11. Channels 1 and 6 will be used for common access campus wide infrastructure and channel 11 will be reserved for research. All stations need to be locked down or placed in a protected closet to prevent theft. Customized antennae to provide required coverage of surrounding areas may be needed. These adjustments are the most difficult aspect of deploying wireless base stations and should be carefully coordinated through the NOC. Technical design meetings are crucial and should focus on coverage and not capacity.

Personally owned wireless access points **WILL NOT** be connected to the NPS network. Users are expected to abide by the user agreement and conduct themselves in a proper fashion. If a user wishes to connect to the network using their personal system (Laptop, desktop, handheld device, etc.) they must provide the details of their system to the help desk. Details must include, at least, the following information: Manufacturer, Operating System and MAC Address.

Standard: The FCC authorizes unlicensed spectrum at the 902-928Mhz, 2.400-2483.5Ghz and 5725-5850 GHz frequency ranges. Unlicensed spectrum is also called the Industrial, Scientific, and Medical band or ISM for short. This means anyone can transmit and receive at these frequency ranges without a license as long as the devices transmits under one watt. Consumer electronic devices such as cordless phones and wireless camera will transmit at one of these frequency ranges. All devices are required to be labeled with their frequency transmission characteristics on the device. 900 Mhz and 2.4 GHz frequencies are by far the most common. Cell phones transmit on licensed frequencies and are not limited to the 1-watt limit. The following wireless ISM frequency standards are the most common 802.11, 802.11b, 802.11A, HiperLan, HomeRF, and Bluetooth (802.15). The 802.11 specification transmits at 2.4 GHz, 802.11b standard transmits on the 2.4 GHz frequency, the 802.11a transmits on the 5 GHz frequency, HiperLan (European technology) transmits on the 5 GHz. frequency and Bluetooth (802.15) spec transmits at 2.4 GHz.

Guidelines: The campus network is a shared resource in which one individual's actions can adversely affect the network performance of others. The intent of this policy is to provide guidance and documentation on how to best use wireless technologies at the Naval Postgraduate School in the framework of the larger campus network. Failure to follow these guidelines and procedures may result in degraded network service, the loss of network connectivity and/or resources wasted to correct problems.

It is expected that general access equipment will be placed at the invitation of the management of a department, so there should be little chance of disruption of an on-going activity. However, in multi-department buildings, one department may ask to add the building to the general access network when there is a private network in place. In such cases, this policy requires that the private network be adjusted so that it does not interfere with the general access network or that it is incorporated into the general access network as part of the general infrastructure.

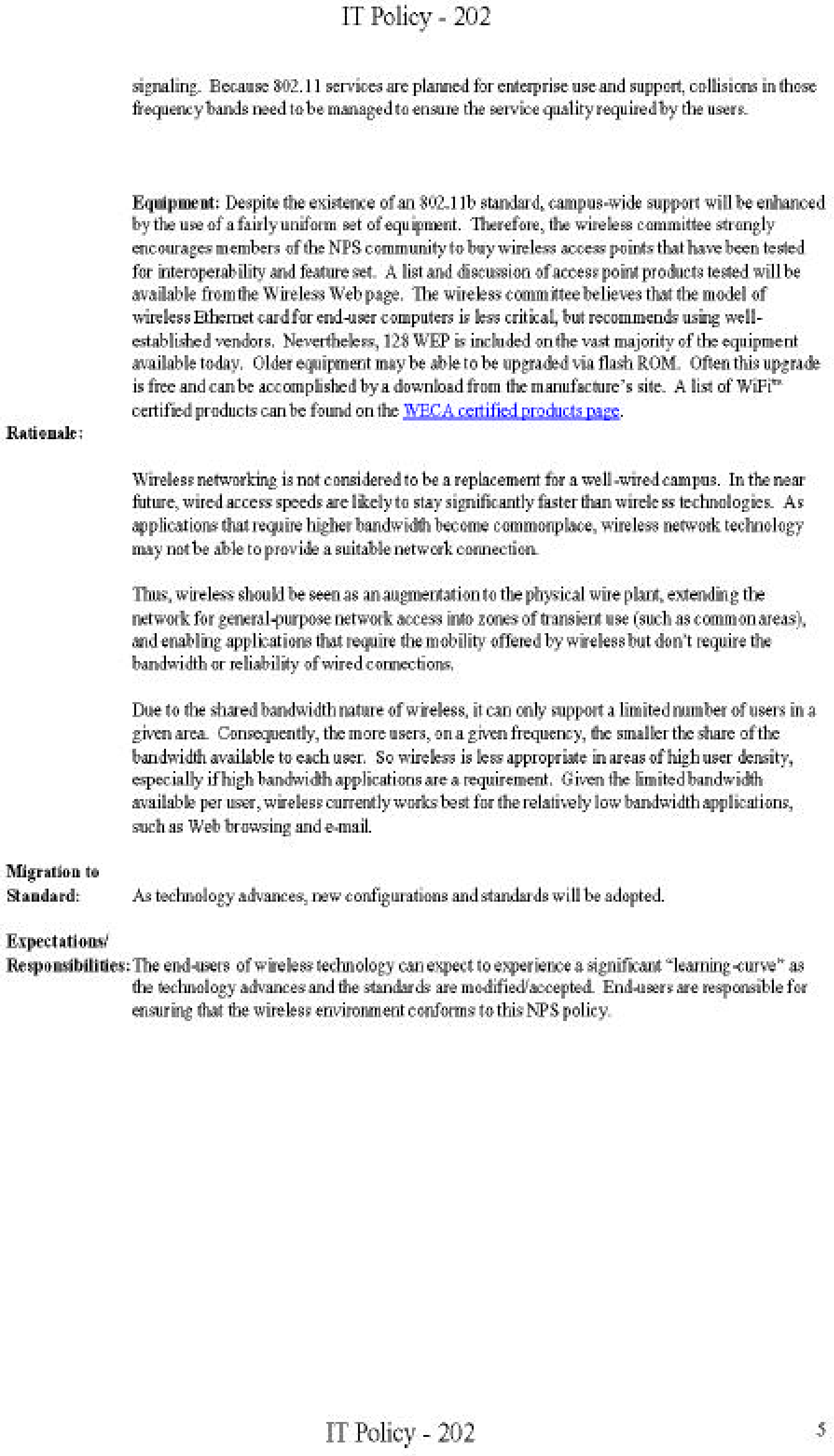
Transition: As technology advances, new configurations and standards will be adopted.

Technical Considerations: Other wireless technologies such as IEEE 802.11a, Home RF, Bluetooth and legacy wireless equipment exist. At this time, they will **NOT** be supported for any enterprise installation. The reason for this is as follows:

- 802.11A and HiperLan 2 despite having higher data rates do not enjoy the range of 802.11B and have not been as thoroughly tested for enterprise installations. Secondly 802.11A and HyperLan 2 function at the 5Ghz frequency and are incompatible with 802.11b equipment.
- Home RF and Bluetooth have slower data rates, shorter ranges and are incompatible with 802.11b. They transmit on the same 2.4 Ghz frequency and may cause collisions with an 802.11b network.

This is not to say that these devices will not be allowed. They will be allowed in research and test labs but users will need to go directly to the vendors for technical support. The Bluetooth focus has changed from a wireless local area network to the smaller ad hoc personal area networks. Bluetooth devices are used as cable replacement for PDAs, printers, and cell phones. Great effort is being invested by industry to ensure these devices can coexist with 802.11b equipment. As with the 802.11b devices all 802.11a, HomeRF and Hiperlan devices are required to be registered with the Network Operating Center (NOC). Bluetooth is more of a communication standard for peripheral devices and will not be required to be registered. The 802.11g standard, which expects to have products by 2003, is claming to be backwards compatible with 802.11b and enjoys similar data rates with 802.11A and HiperLan without the range limitations. If the 802.11g lives up to its claims it has the best hope of being the upgrade for an 802.11b enterprise network.

Frequency collisions: Members of the NPS community should be aware that the FCC does not license use of the frequencies used by 802.11b wireless Ethernet, and therefore other devices that use the same frequencies may disrupt wireless communications. The frequencies used by the 802.11b standard are in the unlicensed 2.4 GHz Industrial, Scientific and Medical (ISM) band. Future implementations of other 802.11 standards are planned for other unlicensed bands. Other devices that also use these unlicensed bands include but are not limited to cordless telephones, cameras, microwave ovens, cordless speakers, sprinkler control systems, and traffic light



IT Policy - 202

signaling. Because 802.11 services are planned for enterprise use and support, collisions in these frequency bands need to be managed to ensure the service quality required by the users.

Equipment: Despite the existence of an 802.11b standard, campus-wide support will be enhanced by the use of a fairly uniform set of equipment. Therefore, the wireless committee strongly encourages members of the NPS community to buy wireless access points that have been tested for interoperability and feature set. A list and discussion of access point products tested will be available from the Wireless Web page. The wireless committee believes that the model of wireless Ethernet card for end-user computers is less critical, but recommends using well-established vendors. Nevertheless, 128 WEP is included on the vast majority of the equipment available today. Older equipment may be able to be upgraded via flash ROM. Often this upgrade is free and can be accomplished by a download from the manufacture's site. A list of WiFi™ certified products can be found on the WECA certified products page.

Rationale:

Wireless networking is not considered to be a replacement for a well-wired campus. In the near future, wired access speeds are likely to stay significantly faster than wireless technologies. As applications that require higher bandwidth become commonplace, wireless network technology may not be able to provide a suitable network connection.

Thus, wireless should be seen as an augmentation to the physical wire plant, extending the network for general-purpose network access into zones of transient use (such as common areas), and enabling applications that require the mobility offered by wireless but don't require the bandwidth or reliability of wired connections.

Due to the shared bandwidth nature of wireless, it can only support a limited number of users in a given area. Consequently, the more users, on a given frequency, the smaller the share of the bandwidth available to each user. So wireless is less appropriate in areas of high user density, especially if high bandwidth applications are a requirement. Given the limited bandwidth available per user, wireless currently works best for the relatively low bandwidth applications, such as Web browsing and e-mail.

Migration to Standard: As technology advances, new configurations and standards will be adopted.

Expectations/ Responsibilities: The end-users of wireless technology can expect to experience a significant "learning-curve" as the technology advances and the standards are modified/accepted. End-users are responsible for ensuring that the wireless environment conforms to this NPS policy.

IT Policy - 202 5

APPENDIX B. DOD 8100.bb (SD106 COORDINATION DRAFT 15 JULY)

Currently the Office of the Secretary of Defense (OSD) is drafting a wireless policy for the whole of the Department of Defense. It is important that every military command align their long term procurement and operational IT strategies with senior leadership goals. Coordination with OSD has allowed NPS to focus its security solutions in concert with their draft regulation. Although this policy has not been signed, it is expected to be approved in its current form by Fall 2002.

The keys points of the policy are:

- **Classified Information**
  - Must use Type-One encryption
  - Must have Designated Approval Authority (DAA) approval
  - Must use PKI for Identification & Authentication
- **Unclassified Information**
  - Must use, as a minimum, FIPS 140-1/2 encryption
  - Must use PKI for I&A

Department of Defense

DIRECTIVE

Number 8100.bb
Month Day, 2002

ASD (C3I)/DoD CIO

SUBJECT: Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid (GIG)

References:

(a) DoD Directive 8100.aa, “Global Information Grid Overarching Policy”
(b) Director of Central Intelligence Directive 6/3, Protecting Sensitive Compartmented Information within Information Systems, and its supplemental manual, 05 Jun 99
(c) DoD Directive 8500.aa “Information Assurance”
(d) DoDD 5200.40, Defense Information Technology Security Certification and Accreditation Process (DITSCAP) 30 December 1997 (supplemented by DoD 8510.01-M, Applications Manual, Jul 2000)
(e) Through (n), see enclosure 1

1. PURPOSE

This Directive:

1.1. Establishes the policy for the use of commercial wireless devices, services, and technologies in the DoD Global Information Grid environment (reference (a)).

1.2. Directs the development of a knowledge management (KM) process to promote the sharing of wireless technology capabilities, vulnerabilities, and vulnerability mitigation strategies throughout the Department.

1.3. Promotes joint interoperability through the use of open standards throughout the DoD for wireless services, devices, and technological implementations, and the knowledge management process by all DoD components.

2. APPLICABILITY AND SCOPE

This Directive:

2.1. Applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Defense Agencies, and DoD Field Activities, and all other organizational entities of the Department of Defense (hereafter referred to collectively as the "DoD Components").

2.2. Applies to all DoD personnel, contractors, and visitors that have access to either DoD facilities or information.

2.3. Applies to all commercial wireless devices, services, and technologies, including voice and data capabilities, that operate either as part of the DoD networked Global Information Grid (GIG), or as part of DoD non-GIG IT (stand-alone) systems. This includes, but is not limited to: commercial wireless networks and portable electronic devices (PEDs), such as laptop computers with wireless capability, cellular/Personal Communications System (PCS) devices, land mobile radios (LMR), mobile satellite systems (MSS), audio/video recording devices, scanning devices, remote sensors, messaging devices, personal digital assistants (PDAs) and any other wireless devices capable of storing, processing, or transmitting information.

2.4. Does not apply to information systems to which DCID 6/3 (reference (b)) applies, i.e. Sensitive Compartmented Information and special access programs for intelligence under the purview of the Director of Central Intelligence (DCI).

2.5. Does not apply to receive-only pagers, Global Positioning System (GPS) receivers, hearing aids, pacemakers, other implanted medical devices, and personal life support systems.

3. DEFINITIONS

Terms used in this issuance are defined in Enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Wireless devices, services and technologies that are integrated or connected to DoD networks are considered part of those networks, and must comply with DoD Directive 8500.aa (reference (c)) and be certified and accredited in accordance with DoD Instruction 5200.40 (reference (d)). In addition:

4.1.1. Strong authentication, non-repudiation, and personal identification is required for access to a DoD information system (IS) in accordance with the DoD PKI implementation guidance provided by the ASD(C3I)/DoD CIO. Identification and Authentication (I&A) measures shall be implemented at both the device and network level. Voice does not require DoD PKI I&A.

4.1.2. Encryption of unclassified information for transmission to and from wireless devices is required. At a minimum, data encryption must be implemented end-to-end over an assured channel and shall be validated under the Cryptographic Module Validation Program as meeting requirements for FIPS PUB 140-1 or FIPS PUB 140-2, Overall Level 1 ((Triple- Data Encryption Standard (TDES) or Advanced Encryption Standard (AES)) standard (reference (e&f)). Encrypting unclassified voice is desirable but voice does not require encryption unless used to access a voice recognition / synthesis driven data application (e.g., VoiceXML). Individual exceptions may be granted on a case-by-case basis. PEDs shall use file system encryption (where applicable).

4.1.3. Wireless devices shall not be used for storing, processing, or transmitting classified information without explicit approval of the information system designated approving authority (DAA). If approved by the DAA then only assured channels employing NSA approved, Type-1 end-to-end encryption shall be used to transmit classified information. Classified data stored on PDA's must be encrypted using NSA approved Type 1 encryption.

4.1.4. Measures shall be taken to mitigate denial of service attacks. These measures shall address not only threats from the outside, but potential interference from friendly sources. Other risk mitigation strategies including virus protection, mobile code restrictions, and other preventive measures shall be incorporated in all wireless information systems as specified in Enclosure 3.

4.1.5. Introduction of wireless technologies in DoD information systems, including those creating an external interface to non-DoD systems (or allowing use of DoD wireless devices on non-DoD wireless networks) can have a significant adverse affect on the security posture of the information system and requires security review and documentation in accordance with paragraph E3.6.4.2 of DoD Instruction 5200.40 (reference (d)).

4.2. Wireless devices shall not be operated inside a permanent, temporary, or mobile Sensitive Compartmented Information Facility (SCIF) IAW DoD 5105.21-M-1 (reference (g)) unless, as a minimum, the device's wireless port (IR, RF, audio or video recording) is inoperable. An IR or RF capable port shall have its transmit capability disabled. Audio/ video recording devices shall also be disabled.

4.3. Wireless RF technologies/devices used for storing, processing, and/or transmitting unclassified information shall not be used in areas where classified information is stored, processed, or transmitted unless a minimum separation distance is maintained between the unclassified wireless processing device and the classified processing device. The separation distance shall be as determined by the cognizant DAA.

4.4. When wireless technology is used to support joint operations, the infrastructures and devices shall be required to be interoperable and support the interoperability profiles in Enclosure 3. Exceptions are authorized for activities evaluating new technologies (e.g. JWID, JEFX, ACTDs).

4.5. DoD Components shall insure spectrum supportability guidance is obtained from the Military Communications Electronics Board prior to assuming contractual obligations for the full-scale development, production, or procurement of wireless devices/systems, including FCC designated Industrial, Scientific, and Medical (ISM) spectrum devices, in accordance with DoDD 4650.1, (reference (h)). For OCONUS, ISM spectrum devices must be host nation approved for use.

4.6. Establishment of a DoD wireless KM process is required. The goal is increased sharing of DoD wireless expertise to include information on vulnerability assessments, best practices and procedures for wireless device configurations and connections.

4.6.1. The KM process shall be utilized by DAAs to help determine acceptable uses of wireless devices and employ appropriate mitigating actions.

4.6.2. Individual DAAs shall submit alternative mitigating techniques for inclusion in the KM database. The KM process shall also be used to coordinate, prioritize and avoid duplication of vulnerability assessments of wireless devices by DoD Components.

4.6.3. Enclosure 3 establishes minimum requirements, used as initial information in the KM process, to help mitigate known vulnerabilities of wireless technologies.

5. RESPONSIBILITIES

5.1.The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)), as the DoD CIO, shall:

5.1.1. Monitor and provide oversight and policy development of all DoD wireless activities.

5.1.2. Establish a formal coordination process with the Intelligence Community (IC) CIO to ensure proper protection of IC information within the DoD information systems employing wireless technologies.

5.1.3. Ensure information interoperability of wireless capabilities in support of Joint operations.

5.1.4. Direct the development of acquisition strategies and assess potential architectures (e.g. wireless application frameworks) to minimize cost of wireless development, services and systems, achieve economies of scale, and promote interoperability and security.

5.1.5. Direct the development and implementation of a DoD wireless KM process to promote increased sharing of DoD wireless information.

5.1.6. On a case by case basis, when requested by the individual Head of a DoD component, evaluate and approve specific implementation timelines for this directive.

5.2. The Director, Defense Intelligence Agency (DIA), shall:

5.2.1. Provide finished intelligence on wireless technologies, including threat assessments, to DoD Components.

5.3. The Director, National Security Agency (NSA), shall:

5.3.1. Implement an IA intelligence capability responsive to wireless requirements of the DoD.

5.3.2. Provide finished intelligence on wireless technologies, including threat assessments, to DoD Components

5.3.3. Serve as the DoD focal point for INFOSEC wireless technologies research and development (R&D) in support of IA requirements to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques.

5.4. The Director, Defense Security Service (DSS), shall

5.4.1. Include monitoring and assessment of wireless information system security practices and conduct regular inspections of DoD contractors processing classified information in accordance with DoD Manual 5220.22-M (reference (i)).

5.5. The Chairman of the Joint Chiefs of Staff shall:

5.5.1. Ensure that Combatant Commanders adequately review and confirm the security and sufficiency of wireless-related interoperability in the generation of requirements for information systems using wireless capabilities supporting Joint operations.

5.5.2. Develop, coordinate, and promulgate wireless policies and procedures applicable to Joint operations.

5.6. The Commander-in-Chief, Joint Forces Command (USJFCOM) shall:

5.6.1. As the joint force integrator, review and confirm the sufficiency of wireless-related interoperability key performance parameters and information exchange requirements for all capstone requirements documents and operational requirements documents.

5.7. The Commander-in-Chief , US Space Command (USSPACECOM) shall:

5.7.1. Develop defensive actions necessary to deter or defeat unauthorized wireless activity up to and including computer network attacks against DoD computer networks and to minimize damage from such activities.

5.8.The OSD Principal Staff Assistants (PSAs) shall:

5.8.1. Ensure end-to-end protection and joint interoperability in their functional areas by guiding inve stments and other actions relating to wireless technologies.

5.8.2. Ensure wireless requirements for information systems and functional applications developed under their cognizance are fully coordinated at the DoD cross-Component level.

5.9. The Heads of the DoD Components shall:

5.9.1. Ensure use of the wireless KM process when evaluating potential wireless solutions.

5.9.2. Ensure that activities evaluating wireless technology provide feedback to the wireless KM process concerning strengths, weaknesses, vulnerabilities, mitigation techniques, etc.

5.9.3. Acquire PKI- enabled systems IAW guidance provided by the ASD(C3I)/DoD CIO.

5.9.4. Ensure that appointed DAAs, in accordance with the DITSCAP:

5.9.4.1.Control wireless access to IS under their cognizance to ensure that the wireless systems (including external interfaces to commercial wireless services) do not introduce wireless vulnerabilities that undermine the assurance of the other interconnected systems and that increase community risk.

5.9.4.2.Include intrusion detection methodologies in the wireless portions of their systems.

5.9.5. Incorporate wireless topics into annual IA training.

5.10. The Director, Defense Information Systems Agency (DISA)shall:

5.10.1. Incorporate wireless considerations in its DoD-wide information assurance initiatives such as computer emergency response, vulnerability alerting, enterprise anti-virus and file system/ data store encryption software.

5.10.2. Provide finished intelligence on wireless technologies, including threat assessments, to DoD Components

5.10.3. Provide analytical and standards support to the DoD related to employment of wireless devices. Provide interoperability testing for wireless devices and operational support for spectrum deconfliction and interference resolution.

5.10.4. Provide Mobile Satellite Services to the DoD, as designated by reference (j).

5.10.5. Insure that wireless capabilities are appropriately integrated into the DISN.

5.10.6. Promote research and development of spectrum efficient technologies.

6. EFFECTIVE DATE

This directive is effective immediately.

Enclosures – 3
1. References
2. Definitions
3. Mitigating Actions Against Wireless System Vulnerabilities

E1. ENCLOSURE 1

REFERENCES CONTINUED

(e) Federal Information Processing Standard (FIPS) 140-1, 11 Jan 1994
(f) Federal Information Processing Standard (FIPS) 140-2, 25 May 2001
(g) DoD 5105.21-M-1, SCI Administrative Security Manual, September 18, 2001
(h) DoDD 4650.1, Management and Use of the Radio Frequency Spectrum, June 24, 1987
(i) DoDD Manual 5220.22M, National Industry Security Program Operating Manual, January 1995
(j) DoD Policy on Procurement of MSS, August 29, 2001
(k) NSTISSI No. 4009 rev 1, January 1999
(l) Policy for Land Mobile Radio Systems, August 1, 2001
(m) NTIA Manual of Regulations & Procedures for Federal Radio Frequency Management, January 2000 Edition with 2001 Revisions
(n) Federal Communications Commission CFR, Title 47, Part 15

E2. ENCLOSURE 2

DEFINITIONS

E2.1. Assured Channel. A network communication link that is protected by a security protocol providing authentication, confidentiality and data integrity, and employs US Government approved cryptographic technologies whenever cryptographic means are utilized. The following protocols and mechanisms are sufficient to meet the requirements of authentication, confidentiality and data integrity protection for an assured channel: the Secret Internet Protocol Router Network (SIPRNET); Internet Protocol Security (IPSec); Secure Sockets Layer (SSL)v3; Transport Layer Security (TLS); Secure Multipurpose Internet Mail Extension (S/MIME) and systems using NSA-approved high assurance guards with link encryption methodology.

E2.2. Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (reference (k)).

E2.3. Community Risk. A combination of: 1) the likelihood that a threat will occur within an interacting population; 2) the likelihood that a threat occurrence will result in an adverse impact to some or all members of that populace; and 3) the severity of the resulting impact.

E2.4. Component Heads. For purposes of this policy guidance, the Component Heads include: the Office of the Secretary of Defense Principal Staff Assistants, the Secretaries of the Military Departments, the Chairman of the Joint Chiefs of Staff, the Commanders of the Combatant Commands, the Directors of the Defense Agencies and DoD Field Activities, and the Inspector General of the Department of Defense and all other organizational entities of the Department of Defense.

E2.5. Designated Approving Authority (DAA). The official designated by the local authority, which has the power to decide on accepting the security safeguards prescribed for an information system NSTISSI No. 4009 (reference (k)).

E2.6. DoD Information Technology Security Certification and Accreditation Process. (DITSCAP). The standard DoD approach for identifying information security requirements, providing security solutions, and managing information technology system security. (DoD Instruction 5200.40 (reference (d))

E2.7. End-to-End. IS from the end user device up to the security border of a DoD network or between two user devices connected by a DoD / non-DoD network (to include the wireless infrastructure's air interface).

E2.8. External Interfaces. Interfaces that include commercial systems (such as a cellular/PCS or pager network not under control of the DAA) which may carry traffic between systems under control of the DAA (the DoD IS and a DoD wireless device).

E2.9. Federal Information Processing Standards (FIPS). The National Institute of Standards and Technology (NIST) Federal Information Processing Standards validation program.

E2.10. Global Information Grid (GIG).

(A) The globally interconnected, end-to-end set of information capabilities associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems as defined in section 5142 of the Clinger-Cohen Act of 1996.

(B) Includes any system, equipment, software, or service that meets one or more of the following criteria:

(1) Transmits information to, receive information from, routes information among, or interchanges information among other equipment, software and services.

(2) Provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software and services

(3) Processes data or information for use by other equipment, software and services

(C) Non GIG IT – Stand-alone, self-contained, or embedded IT that is not or will not be connected to the enterprise network.

E2.11. Identification & Authentication (I&A). Process of accepting a claimed identity and establishing the validity of that claimed identity.

E2.12. Information Assurance (IA). Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

E2.13. Information System (IS). The entire infrastructure, organization, personnel, and components for the collection, processing, storage, transmission, display, dissemination, and disposition of information.

E2.14. Information Technology Systems (ITS). An assembly of computer hardware, software, firmware, or any combination of these, configured to accomplish specific information-handling operations, such as communication, computation, dissemination, processing, and storage of information.

E2.15. Land Mobile Radio (LMR). A radio, which operates in a frequency band, designated for mobile communications by the US National Table of Frequency Allocations. LMRs are typically line-of-sight, handheld or vehicular radios providing netted two-way or trunked, voice and data communications.

E2.16. Mobile Satellite Service (MSS). Satellite-based services provided by existing and emerging commercial communications providers through mobile terminals.

E2.17. Personal Digital Assistant (PDA). A generic term for a class of small, easily carried electronic devices used to store and retrieve information.

E2.18. Portable Electronic Device (PED). Any non-stationary electronic apparatus with the capability of recording, storing, and/or transmitting information. This definition includes, but is not limited to PDA, cellular/PCS phones, two-way pagers, e-mail devices, audio/video recording devices, and hand-held/laptop computers.

E2.19. Public Key Infrastructure (PKI). That portion of the security management infrastructure dedicated to the management of encryption keys and certificates used by public key-based security services. A PKI is a credentials service; it associates user and entity identities with public keys. A well-run PKI is the foundation on which the trustworthiness of public key-based security mechanisms rests.

E2.20. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence. (DCID 6/3, reference (b))

E2.21. Synchronize. The process of communicating with a host or another PED to upload, download, merge, or swap information (Hot-Synch).

E2.22. Wide Area Network (WAN). A system that provides regional, national, or global communication coverage.

E2.23. Wireless. Technology that permits the active transfer of information involving emanation of energy between separated points without physical connection. Currently wireless technologies use infrared (IR), acoustic, radio frequency (RF), and optical but, as technology evolves, wireless could include other methods of transmission. .

E2.24. Wireless Application Protocol (WAP). An open, global specification that allows mobile users with wireless devices to access and interact with information and services.

E2.25. Wired Equivalent Privacy (WEP). An algorithm, part of the 802.11 standard, which is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network; this function is not an explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP.

E2.26. Wireless Personal Area Network (WPAN). A system that provides electromagnetic communication connectivity over a few yards. Currently it uses either radio or infrared technology.

E3. ENCLOSURE 3

MITIGATING ACTIONS AGAINST WIRELESS SYSTEM VULNERABILITIES

Knowledge Management shall identify vulnerabilities and security concerns related to wireless implementations that DAAs shall evaluate in their system accreditation deliberations and decisions. This enclosure contains representative vulnerabilities and minimum required mitigations. As more information is obtained on emerging commercial implementations and associated vulnerabilities, new mitigation requirements will be added. This is not an exhaustive list of wireless vulnerabilities and mitigation techniques but should be considered initial information in support of the knowledge management process.

E3.1. Wireless Personal Area Networks (WPAN)

E3.1.1. For classified information WPAN technologies (including IR, Bluetooth, Ultra wideband, 802.11) shall use NSA approved Type 1 encryption end-to-end per Section 4.1.3.

E3.1.2. WPAN technologies shall not be utilized for transmitting unclassified information unless the data is encrypted per Section 4.1.2. Current Bluetooth security would therefore be considered unacceptable because current implementations do not use FIPS PUB140-1/2-validated cryptographic modules. With IR, Bluetooth or an 802.11 peer, ad hoc networking may occur without the user's knowledge therefore DAAs shall disable or remove WPAN capability from a device unless FIPS PUB140-1/2-validated cryptographic modules are implemented.

E3.1.3. WPAN technologies are being included in laptops, cell phones, and other devices (microwave ovens, refrigerators, watches, etc.). DoD Components shall actively screen for these devises per section E3.8.

E3.2. Wireless Local Area Network (WLAN)

E3.2.1. For classified information WLANs shall use NSA approved Type 1 devices with data encrypted end-to-end per paragraph 4.1.3.

E3.2.2. WLAN technologies shall not be utilized for transmitting unclassified information unless the data is encrypted per Section 4.1.2. The wired equivalent privacy (WEP) security protocol built into the current 802.11 standard for wireless LANs does not use use FIPS PUB140-1/2-validated cryptographic modules and has been found by the cryptographic community to have fundamental flaws.

E3.2.3. When unclassified WLANs are used to support Joint operations hardware or software IPSec virtual private network (VPN) technology shall be used that meet the following interoperability profile:

1. DoD PKI x.509v3 certificates (per Section 4.1.1 Identification and Authentication).
2. FIPS PUB140-1/2-validated cryptographic modules (per Section 4.1.2.).
3. WEP and MAC address filtering shall be disabled.
4. IPSec (International Computer Security Association Labs 1.0B) certified for IPSec interoperability supporting the following protocols:
   a) IKE Phase 1 aggressive mode
      1) Group 2 DH-1024, TripleDES CBC, SHA-1
      2) Group 7 ECDH-163, TripleDES CBC, SHA-1 (only if available, not required by ICSA 1.0B)
      3) Other groups are allowed as long as Group 2 and Group 7 (group 7 only if available) are present
   b) IKE Phase 2 Tunneling mode ESP, SHA-1, TripleDES
   c) Extended Authentication (XAUTH) supporting DoD PKI x.509v3 certificates
5. In addition, WLAN cards and appropriate software drivers interoperable with the specific WLAN frequency and protocol equipment used must be installed on the wireless device. Additional IPSec VPN client configuration may be necessary for authentication and loading of the 'IPSec policy' that satisfies the interoperability profile above.

E3.2.4. Wireless Access Points (APs) shall only be placed in an isolated sub-network or Virtual LAN (VLAN) logically separated from the DoD network by a VPN (NSA Type I encrypted wireless APs are not required to use a VPN), yet physically located within the local DoD network security boundary. However, management interfaces shall be electronically secured with a strong password

E3.2.5. Connection, for initial configuration and system management purposes, to wireless APs shall be via a console connection or a wired connection. Wireless APs shall never be configured over the air interface.

E3.2.6. HyperText Transfer Protocol (HTTP), TFTP, Telnet and SNMP management interfaces shall be turned off after initial configuration in E3.2.5 unless managed remotely via a secure mechanism such as SSL or VLAN tagging to prevent an unauthorized client from accessing the WLAN AP management interface. If managed from a remote interface, select the most secure mechanism and turn off all the unused management ports.

E3.2.7. VPNs shall not be configured to allow split tunneling (allowing the VPN client to access the protected DoD network and a public network at the same time).

E3.3. Land Mobile Radio (LMR) – Use of LMR shall also be in accordance with the LMR policy in reference (l).

E3.4. Mobile Satellite Service (MSS) – Use of MSS shall also be in accordance with the MSS policy in Reference (j).

E3.5. Portable Electronic Devices (PEDs) - (Including PDAs, cellular/PCS phones, messaging devices, audio/video recording devices, scanners, and hand-held/laptop computers).

E3.5.1. PEDs shall not be used to store, process, and/or transmit classifiedor unclassified information unless adequate security mechanisms are provided to protect the information from compromise as prescribed in 4.1.2 and 4.1.3. Note: The detection segment of a PED (e.g., the laser beam between a laser disk and its reader head, between a bar code and the scanner head, or RF energy directed at a passive RF device (paper label tags) or the RF energy directed/ bounced back from the active RF device to the reader/ interrogator) does not require encryption.

E3.5.2. Wirele ss solutions could create backdoors into DoD networks. If a device receives information via a wireless technology and that device allows that information to be placed directly into the DoD networks at the workstation level, then all perimeters and host-based security devices have been bypassed.

E3.5.2.1. Therefore PEDs that are connected directly to a DoD wired network (e.g., via a hot synch connection to a workstation) shall not be permitted to operate wirelessly at the same time.

E3.5.2.2. Adhoc connections using an IR, Bluetooth or 802.11 peer could be used to pass malicious code into the device while it wasn't in the cradle. The device could then be commanded to extract information from the DoD network when it is placed in the cradle for later recovery.

E3.5.2.3. PEDs shall not be connected via hot synch to a workstation in a SCIF(per section 4.2.). This could enable malicious code on the PED to command recording devices on the workstation to capture and transfer classified information to the PED for later recovery. Unless, as a minimum, the device's wireless port (IR, RF, audio or video recording) capability has been rendered completely inoperable. An IR or RF capable port shall have its transmit capability disabled. Audio/ video recording devices shall also be disabled. Turning off a device may not prevent remote activation on a device having a sleep mode

E3.5.2.4. Mobile code shall not down loaded from non-DoD sources. Downloading of mobile code shall only be allowed from trusted DoD sources over assured channels.

E3.5.3. The use of DoD-approved anti-virus software on PEDs and workstations that are used to synchronize/transmit data is mandatory. Where antivirus software is not yet available for a device, disabling the synchronization capability or providing server based antivirus protection is required. To ensure consistent levels of protection required against viruses, it is required to maintain up-to-date signature files that are used to profile and identify viruses, worms and malicious code as approved by the DAA. The network infrastructure shall accommodate anti-virus software updates for all applicable PEDs and their supporting desktops at a site maintained by DISA.

E3.5.4. PEDs are easily lost or stolen. To protect against loss of sensitive information the use of DoD-approved file system/ data store encryption software on PEDs is mandatory. Encryption software for applicable PEDs, shall be available at a site maintained by DISA.

E3.5.5. PEDs with classified or unclassified information shall be capable of being erased/zeroized/overwritten. If PEDs that were used to store, process, and/or transmit classified or unclassified information are deemed no longer needed, and cannot be erased/zeroized/overwritten to the satisfaction of the DAA, it shall be physically destroyed in a manner that ensures that stored data is not recoverable.

E3.5.6. PEDs that support the wireless application protocol (WAP) and utilize commercial wireless network providers are at risk for information compromise. Data shall not be transmitted in this situation unless it can be ensured that data is encrypted end-to-end using a FIPS PUB 140-1/2-Level 1 approved encryption algorithm. The WAP standard is evolving to support data confidentiality requirements through the use of PKI digital certificates and by allowing customers to run their own WAP gateways for secure, direct connections to DoD application platforms.

E3.6. Cellular/PCS & wireless email devices

E3.6.1. Cellular/PCS& wireless email devices are subject to several vulnerabilities (e.g. interception, scanning, remote command to transmit mode, etc). Therefore cellular/PCS & wireless email devices that are used to transmit unclassified and/or classified information shall only be used when specifically approved by the DAA. Cellular/PCS and wireless email devices shall not be allowed into a SCIF (per section 4.2) unless the transmit capability is rendered completely inoperable while in the SCIF. Turning off a Cellular/PCS & wireless email device may not prevent remote activation on a device having a sleep mode.

E3.6.2. Information transmission devices with a connection to a commercial wireless infrastructure (e.g. cellular/PCS, pagers) are particularly vulnerable to probability of intercept/detection and/or traffic profiling because the radio link is exposed for several miles and due to commercial network management intrusion attacks. Therefore, these devices and network management systems (e.g. geo-location, subscriber identification) must be protected or operational procedure established to mitigate against these risks.

E3.7. Spectrum

E3.7.1. Licensed (Other than ISM) devices: The DoD is required to obtain radio frequency guidance prior to contractual obligations for full-scale implementation. A DD Form 1494 is necessary to submit for spectrum certification. This process reviews the equipment's characteristics for supportability and conformance to the national frequency allocation tables in the NTIA manual (reference(m)). Wireless devices intended for use outside the United States and Possessions (OUS&P) require host nation approval. Each country has its unique frequency allocation tables. Coordination and approval must be done with each country where use is intended (i.e. a military frequency allocated in the United States is not recognized as an allocated frequency for the same use in other countries). The DD Form 1494 is required for this approval. A frequency assignment is necessary once the spectrum certification is complete. This process gives the authority to transmit on a specific frequency within set parameters such as power level, antenna gain, and location.

E3.7.2. Non-licensed (ISM) devices: Non-licensed devices must conform to the FCC, Part 15 rules (reference (n)) and are exempt from the spectrum certification and frequency assignment process when used in the US&P. However, a DD Form 1494 may be required by the cognizant Frequency Management Officer (FMO). Any change or modification to a non-licensed Part 15 device, such as boosting the power, invalidates the conformance with Part 15, thus the user must apply for spectrum certification. Users of non-licensed devices that intend for use OUS&P must submit a DD Form 1494 for host nation coordination/approval. DoD activities will not indiscriminately use non-licensed devices for critical tactical or strategic command and control applications essential for mission success, protection of human life, or protection of high-value assets. Non-licensed devices must accept interference from any other federal, non-federal, or civilian electronic system, and therefore offer no protection of spectrum use in support of operational requirements. If non-licensed devices cause interference to a licensed user, the non-licensed user must cease operation. It is recommended that licensed devices be considered as the primary equipment.

E3.8. Intrusion Detection and Electromagnetic Sensing

The wireless systems shall also be subject to active penetration and other forms of testing such as electromagnetic sensing in accordance with DoD policy and restrictions (reference (i)). Active electromagnetic sensing at DoD or contractor premises to detect/prevent unauthorized access of DoD information systems shall be periodically performed by the cognizant DAA and Defense Security Service (DSS) office to ensure compliance with the DITSCAP ongoing accreditation agreement (reference (d)). Electromagnetic sensing shall be used to detect unauthorized Wireless LANs, unauthorized or improperly secured Bluetooth transmitters, or other security breaching backdoors to DoD information systems.

E3.9. User Responsibilities

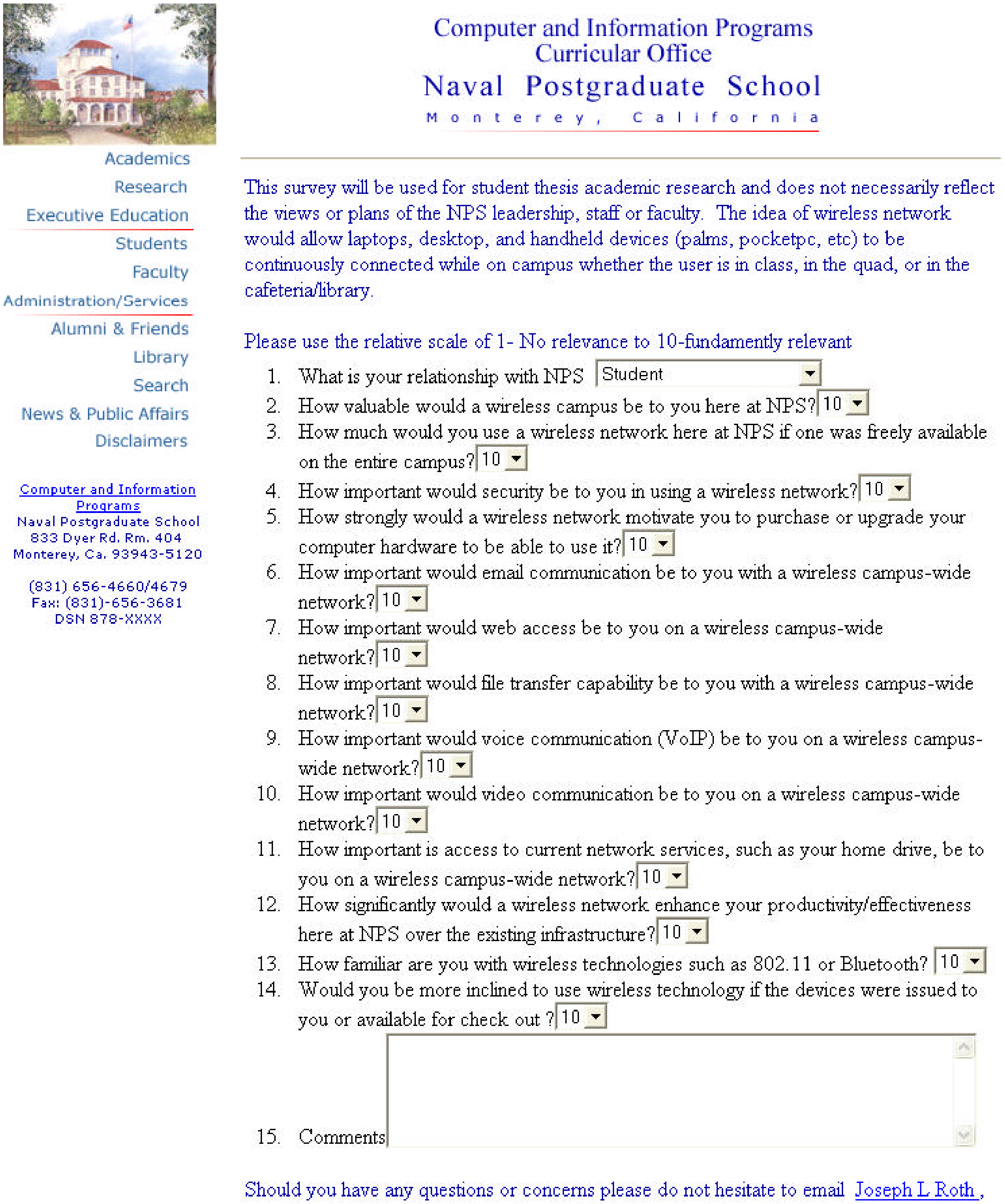
E3.9.1. Users shall immediately report lost or stolen wireless devices to the DAA regardless of the classification of its information content.

E3.9.2. User justification includes mission requirements, government availability, and rationale of how duty position will be enhanced. Users must sign a PED usage statement signifying complete understanding of the procedures established by the local DAA for government-furnished PEDs, visitors and/or privately owned PEDs connecting to DoD networks.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. NPS WIRELESS SURVEY SUMMARY AND RAW DATA

Two online surveys were performed in November 2001 (250 responses) and again in August 2002 (208 responses). Participants were asked to rate each category on a relative individual scale from 1 to 10 where 1 one was not relevant and 10 fundamentally relevant. Participants were given the opportunity to post comments at the end of the survey. The comments combined with the numerical data helped focus the implementation and wireless policy planning process on the important issues.



Computer and Information Programs
Naval Postgraduate School
833 Dyer Rd. Rm. 404
Monterey, Ca. 93943-5120

(831) 656-4660/4679
Fax: (831)-656-3681
DSN 878-XXXX

Computer and Information Programs
Curricular Office
Naval Postgraduate School
Monterey, California

This survey will be used for student thesis academic research and does not necessarily reflect the views or plans of the NPS leadership, staff or faculty. The idea of wireless network would allow laptops, desktop, and handheld devices (palms, pocketpc, etc) to be continuously connected while on campus whether the user is in class, in the quad, or in the cafeteria/library.

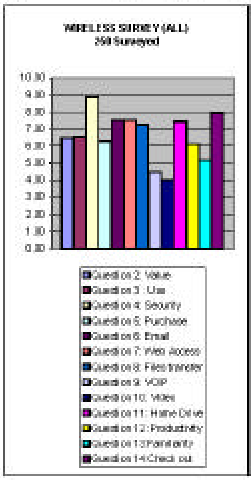
Please use the relative scale of 1- No relevance to 10-fundamently relevant

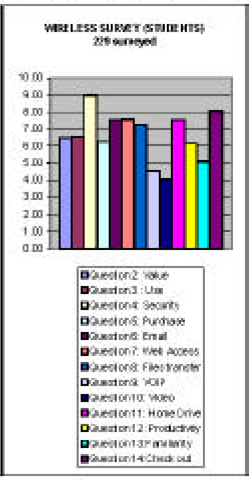
1. What is your relationship with NPS Student
2. How valuable would a wireless campus be to you here at NPS? 10
3. How much would you use a wireless network here at NPS if one was freely available on the entire campus? 10
4. How important would security be to you in using a wireless network? 10
5. How strongly would a wireless network motivate you to purchase or upgrade your computer hardware to be able to use it? 10
6. How important would email communication be to you with a wireless campus-wide network? 10
7. How important would web access be to you on a wireless campus-wide network? 10
8. How important would file transfer capability be to you with a wireless campus-wide network? 10
9. How important would voice communication (VoIP) be to you on a wireless campus-wide network? 10
10. How important would video communication be to you on a wireless campus-wide network? 10
11. How important is access to current network services, such as your home drive, be to you on a wireless campus-wide network? 10
12. How significantly would a wireless network enhance your productivity/effectiveness here at NPS over the existing infrastructure? 10
13. How familiar are you with wireless technologies such as 802.11 or Bluetooth? 10
14. Would you be more inclined to use wireless technology if the devices were issued to you or available for check out ? 10
15. Comments

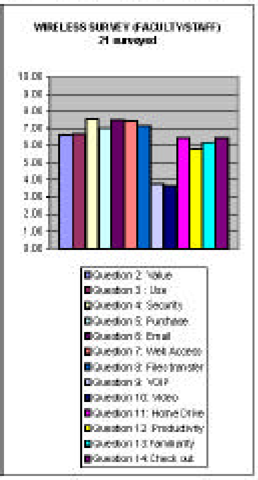
Should you have any questions or concerns please do not hesitate to email Joseph L Roth ,

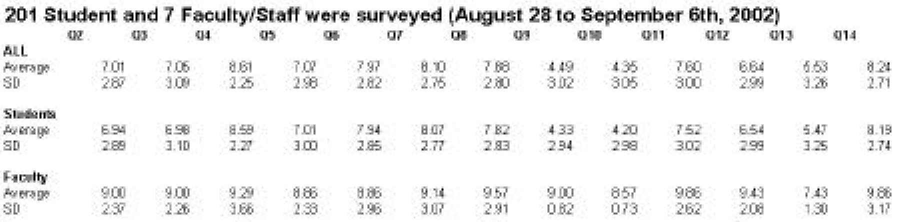
229 Student and 21 Faculty/Staff were surveyed (November 23 - December 7th, 2001)

	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
ALL													
Average	6.47	6.57	8.89	6.30	7.61	7.61	7.25	4.48	4.01	7.45	6.10	5.14	7.91
SD	2.99	3.09	2.11	3.09	2.94	2.90	3.01	3.00	2.88	3.07	3.01	3.43	2.86
Students													
Average	6.47	6.55	9.00	6.25	7.55	7.57	7.28	4.54	4.03	7.54	6.14	5.08	8.06
SD	5.66	5.66	0.00	4.95	4.95	4.95	4.95	4.95	4.95	4.95	5.66	1.41	2.12
Faculty/Staff													
Average	6.62	6.67	7.57	7.00	7.48	7.43	7.14	3.76	3.67	6.48	5.81	6.19	6.43
SD	2.89	3.09	3.22	3.13	3.03	3.06	2.97	2.70	2.82	3.52	2.91	3.39	3.63



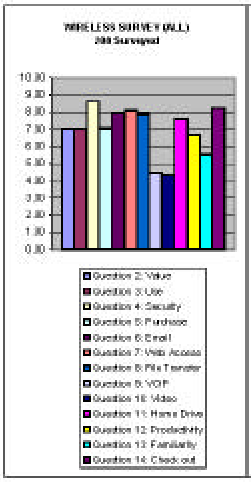


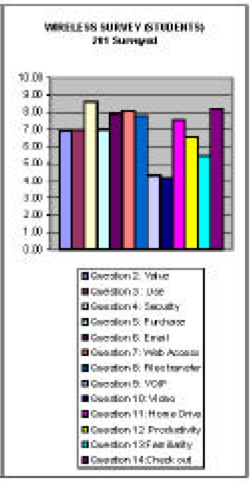


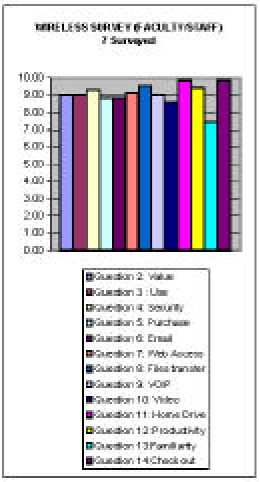


201 Student and 7 Faculty/Staff were surveyed (August 28 to September 6th, 2002)

	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
ALL													
Average	7.01	7.06	8.61	7.07	7.97	8.10	7.88	4.49	4.35	7.60	6.64	6.53	8.24
SD	2.67	3.09	2.25	2.98	2.82	2.75	2.80	3.02	3.05	3.00	2.99	3.26	2.71
Students													
Average	6.94	6.98	8.59	7.01	7.94	8.07	7.82	4.33	4.20	7.52	6.54	5.47	8.19
SD	2.89	3.10	2.27	3.00	2.85	2.77	2.83	2.94	2.98	3.02	2.99	3.25	2.74
Faculty													
Average	9.00	9.00	9.29	8.86	8.86	9.14	9.57	9.00	8.57	9.86	9.43	7.43	9.86
SD	2.37	2.26	3.66	2.33	2.96	3.07	2.91	0.82	0.73	2.62	2.08	1.30	3.17

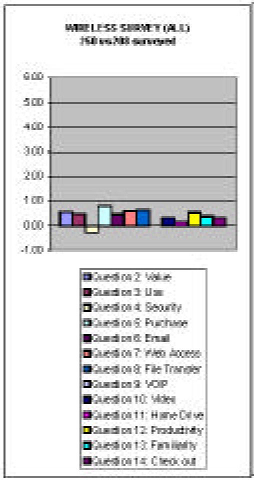


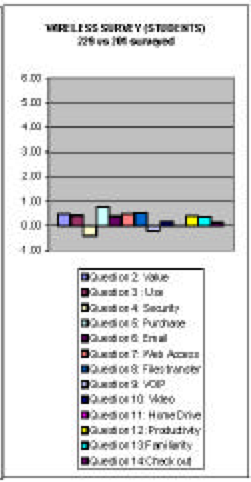


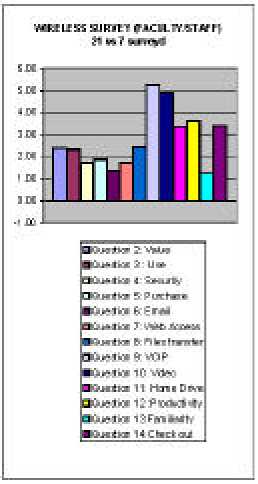


November 2001 versus August 2002 Survey (Differences)

	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14
ALL													
Difference	0.54	0.48	-0.28	0.77	0.46	0.59	0.63	0.00	0.34	0.14	0.53	0.39	0.34
Students													
Difference	0.47	0.43	-0.41	0.75	0.39	0.49	0.54	-0.21	0.17	-0.02	0.40	0.38	0.13
Faculty													
Difference	2.38	2.33	1.71	1.86	1.38	1.71	2.43	5.24	4.90	3.38	3.62	1.24	3.43







A. RAW DATA NOVEMBER 23, 2001

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	This is a test
Student	4	5	6	8	10	10	10	6	5	10	10	10	10	Cool technology!!!
Faculty	8	8	10	9	3	7	8	8	3	8	7	1	7	One vision of use - every classroom becomes computer "lab" capable.
Student	8	8	10	8	9	7	7	8	1	8	9	5	10	
Student	8	10	8	9	10	10	10	5	5	10	8	8	9	very interesting survey. the voice and image transfer may not be needed at all stations. but at the main entrances of buildings they may be useful. can the image and voice transfer be implemented using current network? ozkan knatemir 1lt Turkish Army
Student	8	7	5	8	7	7	7	7	2	7	5	10	10	
Student	8	8	8	8	9	10	9	7	7	9	8	8	8	
Student	3	5	5	3	3	6	6	3	3	5	2	2	7	
Student	7	7	10	5	10	10	4	4	4	10	7	7	10	
Student	3	1	10	1	4	1	10	1	1	2	1	3	10	
Student	3	3	10	3	5	5	5	5	5	5	10	10	5	I think that a wireless campus is a wonderful idea but not a practical one here at NPS. If it is a test bed for an actual fleet implementation then I would see some practicality in it. I myself do not have any application for this but other curriculums may have some.
Student	10	10	10	10	10	10	10	10	10	10	10	1	10	It may seems like I haven't read any of the questions, but I have indeed. Actually, I find extremely important any kind of improvement in network concepts, but I'm not a professional of this area (I have a BS in Chemical Engineering and I'll pursue a MSc in Engeneering Acoustics). I hope I was able to contribute. Thank you.
Student	10	10	7	8	10	10	6	6	4	10	10	7	9	
Student	10	10	10	9	10	10	10	5	5	10	10	6	10	
Student	10	10	8	8	10	10	5	3	2	7	9	7	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	10	10	10	8	10	10	10	10	10	10	10	8	10	The more we advance in wireless, as with any other leading edge technology, here on campus the more competitive we are in those technologies. It just makes good sense to embrace such a quickly advancing field. We are YEARS behind our state-sponsored organization counterparts elsewhere in the world regarding wireless communications implementation. Let us get back on track. Very Respectfully, LT Bry Carter
Student	3	2	10	1	5	5	3	2	1	5	2	4	4	From what I've heard, wireless networks pose more security hazards than benefits. I think any finances allocated for such a project would be better spent on upgrading or adding to labs & network infrastructure & security already in place. Most people seem to have PCs anyway - not laptops, so aside from a handful of laptops & PDAs, the whole wireless thing would be largely pointless. Besides, most people spend too much time checking email as it is. Good luck ~
Faculty	6	6	10	6	10	10	10	2	2	2	3	10	10	
Faculty	10	10	8	10	6	10	4	1	1	8	10	10	1	
Faculty	10	10	10	7	10	10	6	7	7	10	7	10	5	
Student	5	4	7	8	6	5	7	4	4	7	4	6	7	
Student	3	3	8	5	8	8	9	3	5	9	5	2	9	
Student	10	10	10	8	10	10	10	10	8	10	10	10	10	
Student	7	7	10	7	6	8	8	4	4	10	7	8	10	
Faculty	1	1	10	5	5	5	5	2	2	2	1	1	10	Joe, We should talk about survey design. R, P
Faculty	10	10	9	10	10	7	10	1	1	10	9	2	1	Great Thesis!
Student	1	1	10	1	1	5	1	1	1	1	1	10	1	I have done extensive research of the 802.11b standard and I know that it is an unsecure link. I do not think that we should use any type of wireless link due to security. If you put in a wireless connection, just assume that you have allowed everyone access to your network. Most hackers can get into an encrypted wirless network in under 30 minutes and you will never know they are there.

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	6	8	10	5	7	5	6	2	4	6	7	3	10	
Student	7	3	10	7	6	6	7	2	2	9	3	1	9	
Student	7	7	10	7	8	10	10	8	9	9	7	4	7	Although I'm not very familiar with wirelell technology, I'm very interested and will become more familiar.
Student	1	1	1	1	1	1	10	1	1	1	1	1	1	
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	
Student	7	2	10	3	9	9	8	4	4	10	2	7	10	Wireless might be good if laptops were available for use. I don't see much need though with the lab computers provided in the Mechanical Engineering dept. Most of our classes have no online content, or require much online interaction therefore for our dept. course are more engineering design sofware intensive might not benefit so much from wireless.
Student	5	1	10	3	2	5	3	1	1	3	1	1	2	
Student	10	10	10	10	10	10	10	10	10	10	10	7	10	Great idea.
Student	8	8	10	9	9	8	7	3	3	9	8	4	8	
Student	5	5	10	5	7	5	3	5	3	5	5	1	10	Most of these numbers would be much larger if a wireless lan access could be extended into the housing areas. Most of my writing, research etc I do from home on my computer and not at school.
Student	1	2	10	3	6	3	6	1	1	8	7	2	8	
Student	8	8	9	6	6	8	2	2	1	6	7	8	8	
Student	10	8	10	10	10	10	10	5	7	10	8	7	10	
Student	10	10	10	10	10	10	10	2	5	5	10	3	10	
Student	1	3	10	6	6	6	10	7	6	7	7	1	8	
Student	5	3	10	7	5	7	3	1	1	6	5	1	10	
Student	4	7	10	8	10	10	10	8	6	10	7	1	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	10	10	10	10	10	10	10	4	4	10	8	9	10	As one who is currently usinga wirelesss network within our lab/office confinement I do need to state that there are some very inherent flaws which we have come to notice. These flaws can be anywhere from the computer trying to access the net to run applications versus the hard drive,or simple inabiloity to access the net due to weather or amount of traffic within the office and outside (this was a major one to find out about!) So it seems that although a wireless network may be a VERY good idea there are of course glitches.
Student	4	4	7	7	10	10	1	1	1	10	5	5	8	
Student	8	8	10	8	8	10	10	3	4	5	7	2	7	
Staff	6	6	9	3	8	4	8	6	10	9	6	3	7	
Student	2	2	9	5	7	3	5	3	1	5	2	1	7	
Student	3	4	3	7	2	2	2	1	1	6	1	2	2	
Student	10	10	10	7	10	10	10	10	10	10	10	1	7	
Student	3	3	10	1	1	4	4	1	1	8	3	1	8	Not sure wireless is worth the security risk with so many labs available for students. Also, in order to really sue wireless you need a laptop, $ out of reach
Student	5	3	7	5	10	10	10	3	3	10	4	1	10	You don't know what you don't know- hard to judge the utility of a wireless network without having used one. I suppose one good use woulld be to do research in the library while connected - frees you up to search the stacks.
Student	7	7	10	8	8	7	7	7	7	7	7	10	7	My main concern would be the obvious, security. A weak physical layer would make NPS's LAN very vulnerable, if it is not already.
Student	1	1	10	1	1	1	1	1	1	1	1	1	1	I assume a 1 is on the "not" end of the scale?
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	
Student	3	5	10	3	10	10	4	1	1	10	5	1	7	
Student	3	3	10	3	8	8	8	6	5	9	5	1	10	
Student	8	10	10	7	10	10	7	5	3	8	7	7	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	8	8	8	5	10	10	10	5	5	8	5	1	10	I'm a lo-tech, national security curriculum kind of guy, but technology is very relevant, especially if we go to a walking campus with limited student study facilities.
Student	2	2	10	5	3	3	6	1	1	6	1	1	10	
Student	5	5	10	5	10	10	10	3	3	1	3	1	10	
Student	8	8	7	6	10	10	10	4	4	10	6	1	8	For me, problems with network access revolve more around network slowdown than access to a machine.
Student	10	10	10	10	10	10	7	5	5	10	10	2	10	I sincerely hope you are successful in getting a wireless network here at the school. For an institution that is on the cutting edge of technology, we shouldn't be without one. Plus, I am getting tired of having to find a 10baseT connection.
Student	5	5	8	5	5	5	5	2	1	10	5	1	8	Hello guys, I'm not highly interested in having a wireless network at NPS (could be fun though), but I wish you good luck for your thesis. Christian
Student	10	10	10	10	8	9	9	7	7	8	10	6	10	It would be a great enhancement if this is implemented. But, the standard of the wireless modem should be that of COTS.
Faculty	10	10	10	10	10	10	10	10	10	10	10	3	10	Let's go wireless! We need this technology in field operations and so we had better get started in working with it at NPS. The Security Building program has research projects already started that are building on a wireless system.
Student	7	9	7	4	10	8	4	1	1	10	8	9	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	7	6	10	6	6	6	7	3	3	7	6	5	10	I'm not sure which classes you have taken or why you have picked a 10-point scale for your study. Most research shows that a five5 or seven point scale provides much better results as people can way a middle point much easier. E.G. people prefer a strongly agree, agree, unknown/indifferent, disagree, strongly disagree to having to agree or disagree by some level. The small difference between a four and a five on a ten point scale cause more thought on the scale then the answer then does the difference on a seven or five point scale.
Student	7	8	8	6	10	6	9	7	5	9	8	8	8	
Student	3	3	10	1	4	1	1	1	1	1	2	8	7	A wireless network would work well in a place like the library where you can sit and study, check email and look up information you may need when the limited computers there are unavailable without getting up. Beyond this purpose, I see little to no value in being able to sit down with a laptop anywhere in the vicinity of the NPS campus and connect to the NPS servers. We are already fighting a tough battle to keep our networks secure and this would serve to open an unnecessary portal that would make the battle even harder and more taxing on the limited personnel available to manage it.
Student	3	6	9	1	10	10	10	2	2	10	3	2	3	The security concerns of using a wireless network (as so eloquently demonstrated by our last SGL speaker) seem to outweigh the relatively marginal benefit over our current hard-wired infrastructure.
Student	8	10	10	8	10	10	9	8	8	10	10	1	9	
Staff	9	9	10	8	8	8	10	6	5	8	7	7	10	
Student	3	7	10	7	9	9	10	5	6	9	3	1	10	
Student	2	5	10	3	8	7	9	2	1	9	4	6	7	
Student	6	8	10	7	8	7	8	6	5	8	6	2	10	
Student	8	3	10	1	10	10	10	5	5	5	6	2	2	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Faculty	5	5	4	6	3	3	3	2	3	4	5	8	2	My interest in a wireless LAN on campus is less for the infrastructure (I'd probably use it sparingly and the wired network, if properly managed would do most of what I need). But interest is more on exposing students to the technology for pedagogical reasons.
Student	8	9	9	8	10	10	4	8	9	8	7	8	10	
Student	10	10	10	10	10	10	10	5	10	7	10	9	8	It's a good future to see all of the student carry only handheld devices and get the connection everywhere in the campus.
Student	10	10	8	10	10	7	5	2	2	9	10	10	10	IT support would also be a big issue. Perhaps looking at Carnegie Mellon's infrastructure would be good. BTW- great idea!
Student	10	10	10	7	10	10	3	1	1	1	10	8	3	As you may know, WEP for 802.11b networks has been recently been shown to be a weak encryption algorithm and can be relatively easily exploited using tools such as Airsnort. Recommend you look at additional security features such as IPSec and VPN to encrypt the signal and directional antennas for limiting the broadcast.
Student	10	10	10	7	7	9	6	3	1	10	5	3	10	
Faculty	6	7	10	7	10	10	10	3	3	8	5	1	7	You fellows need to work on your survey methodology for some of the answers do not fit the metrics. Also, of what importance is "relevance" to potential behaviors. Tsk-tsk: behaviorialist social scientists would warn you to beware making over-reaching conclusions on the basis of relevance. Jon Czarnecki, NWC, faculty
Faculty	7	7	9	8	7	8	7	3	7	7	6	5	6	
Student	6	7	10	4	2	8	10	2	2	8	4	5	9	
Student	10	10	10	10	10	10	10	10	5	4	4	8	10	
Student	8	8	10	7	8	7	9	6	5	9	7	10	8	Only serious concern for a wireless network is the security. As of yet I have been very unimpressed with wireless security measures, and the possibility of an outside user getting into the NPS system is that much more

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
														likely.
Student	5	6	9	6	7	7	6	6	6	5	4	1	7	
Student	1	1	1	1	2	2	1	1	1	2	1	1	1	I am not convinced that wireless communication offer adequate security as of yet for a campus wide use.
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	
Faculty	4	2	6	1	2	3	5	4	1	3	2	8	1	
Student	7	7	9	8	8	7	8	2	2	10	6	5	7	
Student	8	10	10	5	10	10	10	6	7	10	5	3	10	
Student	8	6	10	8	7	7	7	5	5	7	6	4	10	
Student	3	3	10	2	2	2	2	2	2	2	2	5	2	
Student	8	8	9	9	7	6	7	5	5	5	9	7	7	
Student	7	7	3	8	7	9	8	2	2	6	6	1	8	The main issue for me is not availability or convenience, but the quality of the network. Even if I can work from my study carol or elsewhere, as long as Kiska is down or slow, I gain nothing. Please fix Kiska first!
Student	10	10	10	10	10	10	10	3	3	10	4	10	10	
Student	1	1	10	1	1	1	1	1	1	1	1	7	6	
Student	3	1	10	1	1	1	1	1	1	1	1	8	1	Wireless for every person is nothing more than a toy. The cost and the security concerns can not be offset by the perceived value of not being "inconvenienced" by wires. Wireless does not solve any problems that cannot be handled by simply planning ahead a little bit. Wireless to cover an expanse where running a wire is not feasable or very expensive is quite different then browsing the web in the quad just because its cool. Some vital function of NPS will eventually depend on wireless and so all students will be required to make use of the system. This side-effect usage is the only way I see myself becoming involved in such a superfluous venture.
Faculty	6	10	3	8	10	10	10	6	2	10	6	5	3	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	10	10	10	10	10	10	10	7	7	10	8	9	10	I already have a Macintosh configured with an Airport (802.11) Card and use a wireless network at home. Having one at school would mean I don't have to carry an ethernet cable with my laptop. email: rlphilli@nps.navy.mil
Student	3	3	10	3	10	10	10	5	5	2	5	10	10	There are hugh security issues here that need to be overcome before I would recommend the installation of 802.11 hardware. Passwords would be sent freely over the airwaves. You need to ensure that there is a strong, strong, strong NPS security policy put into place. You may want to consider changing passwords more frequently than the current policy. Good Luck!
Student	10	10	10	8	10	10	10	1	1	10	10	1	10	
Student	7	7	10	7	10	10	10	5	5	10	7	8	9	
Student	10	10	10	7	5	10	10	8	8	8	10	3	3	
Student	10	8	9	10	10	10	8	6	5	8	10	1	10	
Faculty	1	1	10	1	1	1	1	1	1	2	1	2	5	
Student	10	5	8	7	10	10	10	10	10	10	9	1	10	Drexel University in Phil. PA is completely wrieless, and has succeeded in innovating many services for their student population...a wireless network would greatly improve communication and flow of information.
Student	7	10	5	5	10	10	7	10	5	10	5	1	10	
Student	5	5	10	4	8	8	7	7	6	9	5	7	10	Don't have any devices that could utilize a wireless network, but I think it is a good idea.
Student	10	10	10	3	6	7	7	3	2	10	8	2	10	
Student	7	7	6	8	7	4	4	3	2	5	7	10	8	I think a wireless network in NPS is good mainly for educational reasons about the wireless technology. The provided scales represent the relevance today. In 3-4 years, VoIP and video communication via wireless networks will be very important.
Student	5	5	10	7	10	10	10	10	1	10	3	7	8	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	4	4	10	6	7	8	5	4	4	5	5	7	8	I am greatly concerned about the security of a wireless network (having recently read an article about "security experts" hacking into the databases of London Financial Institutes to prove how easily it could be done via wireless connections).
Student	3	1	8	5	5	3	8	1	1	5	7	1	10	Security concerns are of utmost importance (not for me in particular, but for the school as a whole). I have a friend working on a thesis that uses COTS hardware to sniff wireless packets. He's having good success with it, too...
Student	7	5	8	8	10	8	6	2	2	6	4	2	8	A lot of it depends on the instructors. I have had some who relied heavily on the intranet/internet for their course material--and others who didn't use them at all. #3 depends on a lot; I have neither a Palm nor a laptop, so it'd depend on how much it'd cost me, how close I was to graduation, etc. Good luck with your thesis!
Student	3	3	8	3	2	2	2	1	1	1	1	1	5	
Student	8	10	10	3	10	10	7	2	1	10	10	6	10	Institution of a student laptop-lease program with wireless capability would enhance the proposed wireless service. Otherwise it will only be used by those in locations not already wired for the LAN (few) and those with sufficient funds (or sponsors with sufficient funds) to purchase equipped laptops.
Student	10	10	10	10	10	10	10	5	5	10	7	5	10	
Faculty	8	7	10	8	10	10	10	5	5	10	7	7	10	
Student	5	5	7	6	4	4	9	3	1	7	7	1	8	
Student	7	10	10	3	7	6	4	3	1	8	6	2	10	
Student	7	7	9	8	7	7	7	7	7	7	7	5	8	
Student	5	9	10	10	10	10	10	1	1	10	5	8	10	Current Network is adequate, albeit ofen slow (ie MATLAB!!!) A wireless network would enable more office and cubicle computer work, but would not speed current network applications. The question to answer is; what is the value added for the cost required?
Student	10	10	10	10	10	6	10	6	6	10	6	7	8	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Staff	3	4	10	4	2	2	3	7	2	7	2	1	3	I use a laptop, a PDA, a desktop and a cell phone. I can access my e-mail at any computer on campus and have an office on campus. I have not seen the compelling argument for a wireless network so perhaps I don't know how much I need it...thanks.
Student	8	10	10	10	10	10	10	5	5	10	7	4	5	
Student	10	7	10	10	8	7	10	8	1	10	10	5	10	
Student	10	10	10	10	10	10	10	5	5	8	8	5	10	Your default values would seem to bias your results.
Student	7	7	9	7	5	7	8	6	7	9	7	1	9	
Student	7	7	9	7	5	7	8	6	7	9	7	1	9	
Student	7	10	9	10	8	10	10	7	6	9	9	8	10	CSUMB is currently testing this model. You may find some interesting feedback or lessons learned from them.
Student	10	10	10	10	10	10	10	8	4	10	10	10	10	I already have a Palm M505. I am just waiting for the wir eless infrastucture to catch up. Blue Tooth has been talked about for sometime and was already suppose to be here. However, there are few products available with bluetooth capabilities. I think the wireless LAN is more of a reality presently. I like the subject matter of your thesis and considered doing a similar thesis concerning integrated PDA's in Fleet Suppo Operations. Good Luck on your thesis. Rick Adside
Student	5	5	8	5	10	10	10	1	2	10	5	1	8	For me personally I don't do much work on the computer outside of my lab. I run very robust computer models. If a wireless network could duplicate the LAN we already have, be as secure as the LAN we already have, and offer mobility then we should look into switching over to it. But honestly I don't think it is cost efficient. LT Lind
Student	10	10	10	10	10	10	8	5	2	10	10	10	10	Wireless is great stuff but the security flaws are giving it a bad name
Student	7	7	10	8	10	5	8	10	5	8	7	10	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Faculty	5	9	1	9	9	2	2	2	2	2	5	5	9	Getting to wireless services at home (less than 1 mile from the campus) would allow me to review my e-mail from my easy chair in the morning. This at the same time I can not use the modem because of incoming calls.
Student	6	3	8	8	10	10	10	3	2	10	5	7	5	First need the laptop. Checking one in and out as needed would not be feasable since it would create more work than it would help.
Faculty	7	8	3	8	9	9	7	3	2	3	7	9	10	Less interested in security than in having it work. I tend not to roam all that much during the day--mostly to classes I teach. It would be more useful to students, who go to four or five classes a day, and in odd places, such as the library.
Student	10	10	10	10	10	10	10	10	10	10	10	1	10	
Student	8	6	10	8	10	10	10	6	6	10	10	5	10	
Student	5	5	10	2	10	10	10	5	1	10	6	7	5	
Student	8	8	9	7	10	10	10	3	3	10	7	8	10	This survey is very subjective, what is the difference between a 6 and a 7. I believe that I wireless network would be a valuable tool for staying connected to e-mail and having access to your files. It would be even more useful if I was issued a network card for my labtop. I don't see too many people purchasing there own equipment just to use the network.
Student	4	1	10	3	3	3	1	1	1	3	1	1	1	I don't like wireless stuff because you are broadcasting all your info to anyone within a radius that is larger than most people think. We have enough issues with the firwall.
Student	7	10	10	8	10	4	8	8	8	10	9	7	10	
Student	7	7	10	9	7	8	10	4	4	10	7	2	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	8	8	9	8	9	10	7	7	7	8	9	8	9	This is the way to go for the next lap. A lot of renowned universities has already embarked on such system as a more efficient means of communication including e-tutorials, e-lectures, throughout campus. Computers are purchased bulk at discounted rate and the school also allow laptops to be loan out ofr those who could not afford it. NPS should lived up to its goal to be at the forefront of technology.
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	You guys rock !!!! Where do I sign up? VR/Rob Rulof
Student	5	8	10	8	8	8	6	8	4	8	6	1	8	
Student	3	2	10	2	10	6	2	1	1	1	1	8	6	
Student	6	7	8	6	10	9	8	9	8	10	5	1	10	
Student	3	7	2	9	2	8	10	3	2	10	3	5	4	Wireless sounds like a good idea, but there are much more important things to be done at NPS. My priority for this is pretty low, given that there are computer labs in nearly every building.
Student	4	5	1	5	5	10	8	5	5	7	5	1	5	
Student	9	9	10	9	10	10	2	2	2	2	8	8	10	
Student	1	1	10	1	1	1	1	1	1	1	1	9	1	Since we are on a Military installation, Security should always be paramount. Proliferation of wireless connectivity would only serve to promote security violations and make all wireless communications vulnerable to concerned outsiders. Things as simple as email can provide a vast amount of intelligence to the "enemy." A wireless network on campus is a BAD-BAD-BAD idea without extreme measures taken to make it secure. We should never sacrifice our security for the mere sake of convenience.
Student	10	10	10	10	10	10	10	5	5	10	10	8	10	Sounds like a great idea, and as long as it is complient with 802.11, I'm ready to go now!
Student	9	10	10	9	10	10	10	7	8	10	7	8	10	
Student	10	10	10	5	9	10	10	2	2	5	10	7	10	
Student	2	2	10	2	3	1	2	3	2	7	3	8	6	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	5	4	8	1	1	1	6	1	3	1	1	1	1	
Student	2	3	8	3	2	1	6	5	1	5	3	1	8	It would be more helpful if effort could be put towards keeping the current network up more often and functioning smoothly than the quantum leap of developing a wireless network.
Student	10	10	10	1	10	10	10	1	5	10	10	10	10	
Student	10	1	10	5	10	10	10	10	10	10	10	10	10	
Student	7	7	9	8	9	9	10	4	5	10	8	2	9	Reliable access and security would be essential. Also, commonly available components, allowing the use of laptops, PDA's, etc with the network at a low cost would be important.
Student	3	4	7	2	6	5	1	1	1	2	2	2	3	Your survey is flawed. You can't have every response defaulted to "10." You need to modify each response so the default is a blank and will not register as a response if a number is not selected. Personally, they need to get the network fully functional before tackling another project. There are too many outages, freeze-ups, and too few IT personnel to maintain a wireless network as well. Nice toy, but unnecessary waste of dollars.
Student	7	7	8	7	7	10	7	4	6	9	7	9	8	Wireless access is valuable. However, wireless access without a backend network able to support the expected number of users is useless. Reliable service with a reasonable quality of service are essential if you expect people to use this network.
Student	1	1	10	1	8	8	10	5	3	1	1	1	1	
Student	2	6	10	4	9	9	9	2	2	9	2	10	10	WRT question 4, keeping the wireless network secure would be, in my mind, the most important aspect on a Government Wireless LAN. If security cannot be assured, then I would recommend against its implementation.

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	10	10	8	10	10	6	10	2	1	8	8	4	10	If the wireless network were available from local housing (La-Mesa & Ft Ord) It would be a real benefit and help me appreciably. If Web access were only available by a second network such as could be accessed via a different dial-up but from the same equipment then it would also be a real benefit and could keep some measure of security on the campus network. If the network were to exist I would gladly spend my own money in upgrading my personal computer equipment if the price of check-out equipment were keeping the school from implementing the network.
Student	10	10	10	5	10	10	10	10	10	10	10	10	10	
Faculty	2	2	10	1	7	7	5	1	1	1	1	10	1	
Student	5	5	8	10	7	7	7	6	6	3	6	5	7	
Student	1	2	10	2	10	10	10	2	2	10	2	10	10	
Student	7	8	8	10	8	10	7	5	5	8	6	6	8	It would be most useful for web/email access when desktops are not available. It would motivate me to purchase a Wireless card for my laptop if acess was avaialble.
Student	10	10	10	8	10	8	10	4	4	10	9	6	10	
Student	10	8	10	10	10	10	10	10	7	5	7	8	1	
Student	8	9	8	1	7	9	6	3	1	9	7	10	1	
Student	10	10	4	10	10	10	4	1	1	10	5	1	7	
Student	3	3	10	3	3	3	3	1	1	3	3	1	10	
Student	7	6	10	2	3	7	3	1	1	10	2	1	5	
Student	6	8	9	7	10	10	10	6	7	10	7	1	10	
Student	10	10	6	8	10	10	10	9	8	10	10	10	10	
Student	8	8	10	5	8	8	5	1	1	7	7	1	10	
Student	8	8	10	10	10	10	10	3	6	2	8	1	10	
Student	4	4	10	5	7	4	7	2	2	8	5	5	7	I know some about Bluetooth tech. but very little about 802.11. My interest is greatest if my PDA can intereact with the wireless campus-wide network.
Faculty	9	5	7	10	7	5	8	8	5	10	5	6	10	Being a relatively slow adapter of new technology, my responses may be a bit low. I feel there's already enough technology in my life as is. I could see getting excited though once the wireless system were in place.

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	8	8	10	1	5	5	5	3	2	8	3	3	3	
Student	10	10	6	9	10	10	7	1	1	5	9	8	9	Go Wireless!
Student	5	5	10	6	10	5	5	5	5	8	8	8	10	
Student	8	9	10	10	9	9	8	7	8	10	9	8	9	
Student	7	9	10	10	7	8	8	4	2	8	8	1	10	A wireless network would be a nice luxury but, not a necessity.
Student	3	2	10	3	2	2	2	2	2	2	2	7	3	
Student	3	5	10	7	5	5	7	4	4	8	5	3	5	
Student	8	8	10	6	7	8	8	8	5	7	6	9	10	SECURITY, SECURITY, SECURITY. If we're going wireless, first crack down on all the unsecure wireless access points currently on campus. We're practically offering free .mil access to anyone with a wireless card.
Student	5	5	5	6	10	10	10	4	4	10	8	8	10	
Student	1	3	10	2	2	2	3	1	1	2	2	1	2	
Student	7	7	10	5	9	10	5	4	3	10	7	1	6	
Student	10	10	10	10	5	10	7	4	2	7	5	7	10	It is hard to answer these questions objectively (is this a correct english word? - international student). Being interested in new techonolgy it is always easy to answer "yes" and "important" but the truth is that you probably could manage without a wireless network. The thing, in my opinion, is that a person that is interested in technology most likely will use the service and therefore he or she will be more productive. A person who doesn't have this interest will not find it very useful and will not be more productive due to the network.
Student	5	6	9	10	9	8	9	2	1	8	6	8	10	Such a WLAN should add a layer of I&A above the 802.11b standard, especially for personal info access. There really are plenty of PCs on campus for general work, so justifying the cost of implementing wandering access will require the ID of a "killer a

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	5	6	9	10	9	8	9	2	1	8	6	8	10	Such a WLAN should add a layer of I&A above the 802.11b standard, especially for personal info access. There really are plenty of PCs on campus for general work, so justifying the cost of implementing wandering access will require the ID of a "killer a
Student	5	2	10	3	2	3	3	2	1	10	1	4	1	I don't think I would use it. I don't anticipate purchasing a laptop so it would not be of much use to me. Additionally, I would be very c oncerned about security. Encryption degrades the speed considerably, and unless you intend to encrypt with some MIL Spec system (KY for or Freq hoping or something) the current COTS encryption is not that secure.
Student	6	3	2	7	4	7	2	1	1	1	4	10	10	
Staff	5	8	10	5	3	3	3	1	1	7	7	1	8	
Student	10	10	10	10	9	8	9	8	9	10	9	9	9	
Student	10	10	10	10	10	10	10	5	5	10	10	7	10	
Student	5	5	10	10	8	8	8	1	1	10	6	6	10	
Faculty	6	6	10	10	10	10	10	4	4	6	7	8	10	Security and transmission speed ar ethe biggest concerns for me.
Student	4	4	7	1	1	2	2	1	1	4	1	2	5	
Faculty	10	10	1	10	10	10	10	1	10	10	10	10	10	Reporting your results to Code 05 WILL INSURE that Code 05 blocks ALL on-campus wireless services, if the past is any guide. Sorry to see you doing this survey.
Student	10	5	10	5	10	10	10	3	3	10	7	7	10	
Student	10	10	10	7	10	10	10	10	5	10	7	1	9	
Student	10	10	10	10	10	10	10	7	5	10	10	10	10	My only concerns would be the INHERENT vulnerability the 802.11b standard brings to the network with respect to hacking (see Mel Yokoyama'swork).
Student	1	1	10	1	10	10	10	1	1	10	1	1	1	
Student	7	10	9	8	10	7	10	8	3	10	9	6	7	
Student	10	8	10	10	10	10	10	8	7	10	10	10	10	
Student	4	5	10	3	4	4	7	4	10	7	4	2	8	
Student	7	10	1	10	10	10	10	4	3	10	10	2	10	
Student	3	1	8	1	1	1	1	1	1	1	1	7	8	
Student	10	10	10	10	10	10	10	10	10	10	10	1	10	I don't know, but this technology sounds pretty intrusive to me, even

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
														though it may be fun and useful...
Student	10	10	7	8	10	10	10	10	10	10	10	10	10	This is a great idea
Student	3	2	10	1	2	1	1	3	1	1	1	10	9	
Student	3	7	10	8	8	8	8	3	3	10	1	9	7	A lot of functionality that I am looking for in any information technology on campus would not change fundamentally. I don't think that the availability of wireless technology (though it would be cool) is going to change the way I work using information technology. And my current work habits are adapted towards the use of wired technology.
Student	9	10	10	8	8	9	10	10	10	10	10	10	10	
Student	1	1	10	5	5	10	10	1	1	10	7	1	10	
Student	8	7	9	7	6	10	10	4	4	9	7	1	8	
Student	8	7	10	9	10	9	9	7	7	10	10	1	10	
Student	10	8	8	8	10	8	9	10	8	10	10	7	10	
Student	1	1	10	1	7	8	8	3	3	7	1	8	5	
Student	1	1	1	1	5	5	5	1	1	1	1	1	7	
Student	2	2	10	1	2	3	2	1	1	3	1	5	10	
Student	5	8	10	8	3	6	2	4	5	6	5	3	10	
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	
Student	10	10	10	8	7	7	7	10	6	10	8	8	10	I find it interesting that some NPS faculty expend significant effort to avoid change rather than embrace emerging technology for the benefit of the fleet.
Student	7	7	10	8	10	9	9	7	5	3	8	1	10	
Student	1	1	10	1	7	7	1	1	1	1	1	1	10	I don't have or want a laptop or other wireless technologies. Personally, I don't think that "being connected" is critical for effectiveness/productivity and in many cases it is a hinderance to critical thinking.
Student	5	5	10	1	5	10	7	1	1	10	8	10	5	
Student	1	1	10	1	1	1	1	1	1	1	1	1	3	I have no real need to be in instant communications with anyone. Empty nester; wife totally absorbed in Red Cross volunteer work. School is my work for the next two years.
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	
Student	10	8	10	8	10	10	10	5	5	8	8	1	8	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	3	5	9	4	6	5	3	2	2	10	5	5	10	Although I would not likely to use it now, the wireless network is a good direction of development in the future.
Student	5	5	10	5	5	5	9	2	5	10	5	6	9	
Student	10	10	5	10	10	10	10	10	6	10	7	7	10	
Student	3	5	10	3	5	5	3	1	1	3	5	3	3	
Student	10	10	10	8	10	5	7	10	7	10	8	7	10	
Student	8	9	8	4	6	6	7	3	2	8	8	2	10	
Faculty	8	6	8	3	8	9	9	5	5	10	8	9	7	
Student	2	1	9	1	7	7	3	1	1	7	1	1	5	As an NSA student, most of what I use the network for is either research or word processing. That should probably be taken into account when considering my answers.
Student	10	10	10	10	10	10	10	7	3	10	10	1	10	
Student	5	6	4	5	6	5	5	10	5	10	5	8	10	
Student	1	3	10	1	1	1	1	1	1	1	1	1	1	we're here to learn theory, not geek out on new toys. invest this into the fleet to support warfare and mission accomplishment. stick to the books here unless it's in your major.
Student	2	2	10	3	3	3	3	3	3	3	2	8	7	
Average	**6.47**	**6.57**	**8.89**	**6.30**	**7.51**	**7.51**	**7.25**	**4.48**	**4.01**	**7.45**	**6.10**	**5.14**	**7.91**	
SD	2.99	3.09	2.11	3.09	2.94	2.90	3.01	3.00	2.88	3.07	3.01	3.43	2.86	

B. RAW DATA AUGUST 28, 2002

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	Issued!
Student	10	10	10	8	10	10	8	2	2	10	8	1	10	
Student	6	8	10	7	10	10	10	4	4	7	8	7	7	I have a wireless network at home. The ability to move easily from one wireless network to another would be extremely helpful.
Student	7	10	8	5	10	8	4	4	2	10	6	6	10	
Student	8	8	10	10	10	10	10	5	5	8	8	8	10	
Student	7	10	10	7	7	8	8	6	6	8	8	10	10	Give em' Hell Joe...
Student	6	7	10	8	10	6	6	2	2	2	5	10	2	
Student	3	3	10	1	3	7	5	1	1	7	3	7	4	
Faculty	8	8	10	7	7	9	9	8	8	9	6	8	10	
Student	3	3	1	1	3	10	10	1	1	10	4	10	5	
Student	10	10	7	8	10	10	10	6	7	8	9	10	9	
Student	10	5	7	10	10	10	10	1	1	5	6	10	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	10	10	10	10	7	10	7	4	4	10	10	6	10	Regarding 14: I would love it if a wireless device like a laptop could be issued to me like many commands are doing with PDA's. Regarding the entire survey. I almost felt like I was not doing it correctly since I had so many 10's. But I reread all the questions, and I really do feel that strongly in favor of a campus-wide wireless network.
Student	1	1	5	7	8	10	10	3	3	8	3	1	8	
Student	10	10	1	1	10	10	10	10	10	10	10	1	10	
Student	10	10	10	10	10	10	10	8	8	10	10	9	10	Issuance of standard/strictly configured laptops should be considered for each student. The cost is quite minimal and the resources available would offset the cost (consider that each person will get ~$1K for book reimbursements ($125X8QTRS)... take this money and purchase laptops that are able to access 'softcopy' versions of the textbooks via the wireless network. This would be just one capability - but one that could justify alone a new way of thinking and computing) The additional capabilities associated with having a personal/portable computing environment is the difference in NPS being a leader vice a follower of IT integration/innovation. Security must be very carefully scrutinized. The current 128-bit encryption is way too inadequate to provide for the necessary security required to maintain wireless connectivity to home drives and other network resources. I am concerned that 3DES would be adequate. This is an area where NPS would benefit the most from developing its own standard for a high-

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
														level security solution for its wireless networks. Video and voice capabilities over a wireless network present new genres to the computing environment... however, I am willing to bet that most people would not utilize these to their potential and thus believe that they should not hold up the actually implementation - they are able to be added as the network becomes more mature and robust. 802.11a should be considered as the standard... the additional bandwidth capabilities would help ensure a delay in antiquity - and also make the network more capable of handling large file transfers. - Douglas K. Shamlin, LT, USNR
Student	6	8	8	10	6	7	6	1	1	10	4	1	10	I own a desktop at home and bring a Palm to school to take notes which I then hotsync when I return home. Short of hotsyncing, the current hard wired system provides the capability I need, though it would be incredibly convenient to be able to access all of that from my Palm. The ability to access my home computer is also of great interest. I'm not sure how much more productive it would make me to be able to access things via a wireless network though.
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	
Student	7	10	10	6	10	10	10	4	4	4	5	10	3	
Prefer to be Anonymous	8	10	10	10	10	10	10	10	10	10	10	10	10	As much as the convience of wireless would be a great asset, it is worthless, or even dangerous if not secured properly. The benefits do not out weigh the risks.
Student	10	10	10	10	9	9	10	8	6	10	8	8	10	
Student	10	10	7	10	10	10	10	2	2	10	8	6	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	7	7	5	7	8	8	6	4	4	8	7	1	5	Are you the person to contact if I want to go wireless? I just purchased a laptop and have my Sprint account taking wireless comms into consideration.
Student	1	1	10	1	1	1	1	1	1	1	1	10	1	
Student	9	10	10	7	8	9	8	7	8	9	9	3	9	
Student	7	7	10	8	10	10	9	2	1	10	5	1	8	
Student	10	10	10	10	10	10	10	10	10	10	10	1	10	
Student	10	8	10	8	10	10	10	10	5	8	7	7	10	Cost Benefit I'll take all of the tools you give me but what are my other options if you decide to spend the money elsewhere. I think I waste more time parking each day than I would gain from walking my lazy butt to a terminal or telephone.
Student	7	7	10	5	10	10	10	4	4	10	6	10	8	
Student	8	9	5	9	9	7	10	5	7	8	9	5	7	
Student	6	3	4	6	4	6	4	2	2	3	2	7	7	
Student	10	10	6	10	10	10	10	1	1	10	10	10	10	Wireless would be great! I have a wireless network at home with two desktops and one latop connected. It would be extremely valuable to have such connectivity available on campus.
Student	10	10	10	10	10	10	10	7	10	10	10	10	8	
Student	10	10	10	10	10	10	10	8	8	5	10	8	10	I feel the costs associated with implementing a wireless network to augment the existing LAN would be justified, especially in comparison to the costs associated with upgrading the existing LAN. I am somewhat aware of the security vulnerabilities associated with current wireless standards and protocols; however, I also believe there are excelletn solutions available to help mitigate these vulnerabilities. I would be very dissappointed to see wireless not used because of security concerns, wothout taking a serious look at these alternatives. (comments made by Major Woody Hesser, USMC, code 32

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
														(2d year IST student)
Student	5	10	10	8	6	7	6	2	1	6	6	9	10	Security is the biggest concern. We (NPS) should not sacrafice security for the sake of covenience. Wireless is very convenient, but I don't know that it is necessary here at NPS. However, we are a cutting edge institution that should lead the way in technology. I use wireless daily, but I don't know that every student here is as security concious as I am.
Student	6	7	8	7	10	1	1	1	1	1	6	8	10	
Student	10	10	10	10	10	10	10	10	10	10	10	6	10	Great way to use technology!
Student	5	10	10	8	6	7	6	2	1	6	6	9	10	Security is the biggest concern. We (NPS) should not sacrafice security for the sake of covenience. Wireless is very convenient, but I don't know that it is necessary here at NPS. However, we are a cutting edge institution that should lead the way in technology, so I'm not at all opposed to a wireless campus. I use wireless daily, but I don't know that every student here is as security concious as I'd like to think I am.

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	10	10	6	9	8	10	8	3	4	4	10	10	4	I am extremely interested in wireless technology. I have just purchased a new Sony Vaio with built in 802.11b technology.
Student	8	8	4	8	10	10	10	3	3	5	5	6	10	
Student	7	9	8	5	9	8	9	5	9	8	9	1	7	
Student	8	10	10	7	7	10	7	7	7	10	7	10	10	
Student	10	10	10	10	10	10	8	6	4	8	10	8	10	
Student	8	8	10	10	8	10	10	8	7	10	8	1	10	I am not familiar with wireless technology (#13), and I would gladly use it if it were issued (#14)
Student	2	2	8	1	10	10	10	1	1	10	1	2	2	
Student	8	10	10	7	6	8	10	3	3	8	10	7	10	I currently use wireless in the library and it is outstanding!
Student	5	5	10	5	7	7	7	7	4	3	5	3	7	I consider this a "Nice to have" but not required technology for NPS.
Student	3	5	10	7	8	7	6	5	5	10	5	4	10	
Student	7	9	8	10	6	10	7	3	2	6	7	1	7	New student in second week.
Student	10	7	7	10	10	10	10	5	7	10	10	10	10	I strongly support a wireless campus, to include the use of 2.5 & 3G wireless technology when on travel and doing field reasearch.
Student	10	10	10	10	10	10	10	10	10	10	10	6	10	I am using the wireless network on campus now and it is fantastic. My concern is that as more people migrate over to the wireless community that it will become as congested as the hard wired LAN is today. I fully support wireless and think is should become the standard on campus. Thanks to you Joe Roth.
Student	5	5	10	4	10	10	10	2	1	10	1	1	10	
Student	1	1	7	4	10	10	7	5	5	10	10	1	10	
Student	5	7	8	7	5	6	6	4	4	9	7	7	9	I'm a PhD student w/ a desk and a computer always tied to the network. I think a wireless campus network would be more important to the Masters population which have no "home work-area" to call their own.
Student	10	7	7	8	10	10	10	3	3	9	8	5	3	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	8	8	10	7	8	8	8	4	4	6	7	6	9	It would be great to have the flexibility of a wireless network. I would bring in my laptop and set it up in my study cubicle. At the present time, I wouldn't see audio or video capability as a necessity.
Student	10	10	10	10	10	10	10	3	5	10	8	2	10	
Student	1	3	2	1	1	3	1	2	1	1	1	4	2	
Student	7	4	8	6	9	6	6	3	4	10	5	6	7	
Student	6	10	10	7	10	8	10	5	5	10	1	7	10	I guess the answer on question 12 very much depend on the current work situation. As for me, I have access to a computer which means that I am not forced to use the lab computers or a private computer on campus.
Student	8	10	7	10	7	10	8	1	1	5	5	1	5	Current user here on campus.
Student	8	8	3	10	10	9	9	3	1	2	7	5	10	
Student	7	5	10	7	8	9	8	5	5	7	7	2	8	
Student	7	7	10	8	10	10	8	6	5	6	7	6	10	
Student	5	5	8	6	7	7	7	4	4	6	3	6	3	A wireless network not coupled with extensive training and a tangible increase in productivity would be a waste of taxpayer money. A more significant bottle neck to productivity is the preponderance of information and knowledge relegated only to tree kill (paper documents). Money would be better spent in digitization technology that may not only increase accessibility to resources on campus but also to operational forces.
Student	7	6	8	5	9	6	9	2	2	9	6	4	1	I am currently running a wireless network in my home (DSL router + 3 Desktops +1 Laptop). Availibility of a wireless network at NPS would increase the ease of file transfer and email access, but I imagine I would still be reliant on computer labs due to software availiability. (1st Quarter MOVES student)
Student	8	10	10	8	10	9	8	9	9	10	8	5	10	
Student	10	8	10	10	10	10	10	1	1	1	8	10	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	10	10	10	10	10	10	10	5	2	1	9	8	9	Joe, They need to put a wireless class into the CS curriculum. Scott.
Student	8	8	9	9	10	7	9	4	2	8	7	7	9	
Student	4	1	10	1	7	1	1	1	1	6	1	8	5	Outside of email access you are never that far away from a lab/classroom/LAN connection on such a small campus/facility. The number of students that have begun using laptops in the classrooms during class only have serverd as a distraction to other students between rebooting/startup sounds and using it 90% of the time to surf the web vice the intended purpose of following along in class. The unresolved security issues of protecting Privacy Act Information through a wireless connection is my greatest fear. Those that are responsible for instituting and installing this technology go forward and make claims that the information will be secure yet we find out in numerous instances that it is not, all too late after information has been compromised.
Student	4	2	10	2	8	10	10	1	2	10	3	2	6	
Student	3	1	10	1	10	10	7	1	1	10	3	10	3	I use wireless at home, but I am not certain I would take my laptop in. It would be easier to use my own instead of NPS computers though. Most wireless users have 802.11b right now, but if the trend is toward the 5Ghz frequency of 802.11a, would it be feasable to have a dual frequency system? I would encourage manadatory MAC address registration, if not even not broadcasting the network name. Thus, one would have to resister the MAC address and enter the name to use the network to be able to use it. I have a concern ith foreign student access

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
														however. You must separate them to a separate router somehow to disable them from accessing a .mil network other than NPS. Otherwise, they have access to the rest of the military that contains FOUO and restricted data.
Student	8	10	10	7	10	10	9	5	7	8	10	3	10	
Student	3	1	8	2	2	2	1	1	1	1	1	5	8	
Student	1	1	10	1	1	1	1	1	1	1	1	3	7	I am a technology junkie, but I do not understand the push for wireless technology. I have owned several pc's (I bought my first in 1985) and currently own two pc's and a laptop. My day to day activities rely heavily on email, the internet and on several computer applications. I have text messaging and web/email access on my cell phone and have never had a need to use them (other than for fun). Bluetooth technology is great if you want to get a dinner recipe off the web from a console on your refridgerator, but I view it as nothing more than an extravagant time wasting endevour.
Faculty	10	10	10	10	10	10	10	10	10	10	10	10	10	I am already wireless with The MOVES Institute. It works great!
Student	1	2	10	1	1	1	1	2	1	1	1	1	1	
Student	10	10	5	7	10	10	10	4	4	10	8	3	10	
Student	6	1	5	10	1	1	1	1	1	7	2	7	10	
Student	8	8	10	9	10	8	8	2	2	10	8	10	10	
Student	10	10	10	10	10	10	10	7	4	10	10	7	10	
Student	8	8	9	4	9	8	7	3	3	8	7	9	8	
Student	10	6	10	7	7	7	10	6	10	7	8	6	10	
Student	10	10	10	10	10	10	10	5	5	10	8	7	10	
Student	10	10	5	10	10	5	10	1	1	3	10	8	10	
Student	2	1	10	1	8	3	2	1	1	1	3	1	9	
Student	8	9	6	10	9	8	8	3	3	9	8	1	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	10	8	8	9	10	10	10	6	3	10	7	8	10	I think the wireless campus is a powerful and brilliant idea. The support for portable devices, like Palm, Pocket PC, Tablet PC, laptops is a key to improve the productivity of the students.
Student	7	9	10	8	10	9	8	3	4	8	4	6	5	
Student	5	5	10	5	10	10	10	5	5	10	5	1	10	
Student	10	10	10	10	10	10	8	5	5	10	8	8	10	
Student	10	9	7	9	10	10	10	2	3	10	7	5	9	If there is any current wireless network in the Campus, I would like to learn more about it! Is there any forum for this?
Student	7	10	5	9	10	10	10	2	2	10	6	6	10	
Student	10	6	8	8	10	10	10	3	2	9	7	9	7	I'm already using wireless, so the wording of the some questions on the survey (e.g., "more inclined" on 14) actually made me push my answers down.
Student	2	2	10	4	8	9	9	5	2	10	7	8	10	
Student	8	8	8	7	4	10	4	1	1	10	10	9	10	I am extremely displeased with the organizations support for students working in the NSA department. Thesis carrolls have been revoked and there is no place to spread out three or four books and a notepad while writing on a computer. This is not a luxury but a requirement to produce the type of work expected by professors in this curriculum and the facilities at NPS do not support the requirement. The only possible solution on the horizon is the implemenation of a wireless campus which would allow ample desk space in the library to become functional for laptop computing on the net.
Student	10	10	8	8	10	10	10	5	3	8	7	7	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	8	8	8	7	4	10	4	1	1	10	10	9	10	I am extremely displeased with the NPS's support for students working in the NSA department. Thesis carrolls have been revoked and there is no place to spread out three or four books and a notepad while writing on a computer. This is not a luxury but a requirement to produce the type of work expected by professors in this curriculum. The facilities at NPS do not support the requirement. The only possible solution on the horizon is the implemenation of a wireless campus which would allow ample desk space in the library to become functional for laptop computing on the net.
Student	1	1	5	3	10	10	10	1	1	10	1	5	1	
Student	8	8	10	10	10	8	10	6	6	10	10	1	10	If I knew that the technology was available to me, then I would become more familiar with it. The most important thing to me is being able to transfer large files of unclassified work from my network account to my personal computer so that I can work on it at home.
Student	10	10	10	10	10	10	10	5	7	10	9	8	10	
Student	10	10	7	10	10	10	9	3	3	3	10	7	10	Wireless is the way to go - get rid of all of the labs with aging and archaeic desktops and issue laptops to all students - no longer need network home drives
Student	5	5	10	7	7	7	7	3	3	5	3	8	7	SECURITY SECURITY SECURITY! We are not just another civilian campus; we are a military institution. I have yet to see a reasonable case made that the wireless network can be sufficiently secured considering the work we do here.
Student	6	7	9	7	7	10	9	3	3	9	7	2	8	
Student	10	10	8	9	8	9	8	7	10	9	10	9	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	4	4	9	3	3	2	4	2	2	3	6	8	7	The benefits of wireless are no different then the benefits of networks in general. If the school would use the infrastructure that is in place, wireless would be basically moot. All classrooms have wired drops, but only one drop per room is activated. By simply providing service to all the existing wired drops, I think we obtain the same benefits without all the concerns of wireless. I gave relatively high marks for wireless improving the current situtation, because the current situtation is a campus without access via the wired drops that already exist. I also gave high marks to the idea of checking out devices, because I think that is the direction the school should go. Checking out both computing and networking devices to students and doing away with the PC based labs would allow students to be more productive while allowing IT to avoid trying to be all things to all people through a single PC. The caviat is that an IT department of this sort would have to be staffed rather robustly, centrally organized but physically distributed and network access must be available to students where they can use it, such as classrooms and study areas. I also think that students should have offices, but that doesn't have much to do with wireless. I don't see much value for roaming the campus on a wireless network, except maybe to save the expense of installing wire. The problem with this statement is that it seems to me that the school has already installed the wire. I'll use wireless where there are no drops, but I prefer

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
														the cable. I see wireless as most valuable for point to point directional networking. George Lawler
Student	8	8	6	10	10	8	8	5	7	8	8	6	10	
Student	10	10	6	10	10	10	10	10	10	10	10	10	10	
Student	7	7	10	5	7	8	10	5	6	8	7	1	4	I am concerned about the security of wireless networks. I realize that virtually anyone can hack into our existing system, but I wonder if wireless creates additional security parameters that have not been identified.
Student	8	7	5	9	9	8	7	3	3	10	8	1	9	Good luck
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	
Student	5	5	10	6	10	10	10	4	10	10	4	1	10	
Student	8	7	8	9	7	6	8	7	4	9	6	7	10	
Student	5	5	10	8	8	8	5	4	5	8	7	2	8	Currently, I do not have the capability to utilize wireless technology. Having it made available would definitely be a factor in my next system upgrade.
Student	6	9	10	6	10	10	10	10	6	7	7	1	8	
Student	5	3	10	3	3	3	3	1	1	10	3	3	3	
Student	10	10	10	10	10	10	10	1	1	10	10	7	1	I am going to buy my own wireless card. After I spent money on a laptop the extra $45 is not going to kill me
Student	10	10	10	8	10	10	10	8	8	10	8	8	10	
Student	3	1	8	3	3	3	3	1	1	9	1	8	10	For those of us without laptops - wireless is a nice idea but the current infrastructure works fine. If there was a program to get a laptop when we arrived at the school then wireless would be a benefit. Just because we CAN make the campus completely wireless, does that mean we should?
Student	7	7	3	7	7	5	5	2	1	7	5	5	8	I would appreciate it if a wireless network were Macintosh-compatible.
Student	7	9	10	8	10	10	10	10	7	10	9	8	10	
Student	10	10	10	10	10	10	10	7	7	6	8	9	10	
Student	2	1	10	3	1	1	1	4	1	2	1	6	2	Wireless is not secure enough for use on military systems
Student	1	1	6	3	6	6	6	6	3	6	1	2	3	
Student	1	3	10	1	1	1	1	1	1	1	1	3	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	10	10	10	6	10	10	7	10	1	1	7	10	10	More inlclined if issued. Don't have to spend money.
Student	1	1	5	1	2	1	3	1	1	3	1	1	5	
Student	7	5	10	6	10	10	10	7	7	9	8	4	7	
Student	8	7	10	9	7	8	9	10	6	10	3	6	8	I don't believe ir or em data rates are fast enough to support most student driven applications on a wireless campus. If it takes five minutes to move a MATLAB file, I won't use wireless for anything more than an extension of my cell phone or PDA. I hardly use either device.
Student	1	1	1	1	1	1	1	1	1	1	1	1	10	I don't see the benefits of using a wireless network, since during the classs I pay attention to the class, off class there are a lot of computers in all buildings where I have acessed. I think that the wired system is working quite well, I don't agree with the increased costs of this change.
Student	7	8	9	7	6	7	7	6	4	6	7	7	10	
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	
Student	5	5	10	10	10	10	10	7	10	10	5	1	10	
Student	6	6	3	8	8	8	6	6	6	4	8	1	1	
Student	4	2	10	3	5	6	7	1	1	8	1	1	6	I admittedly do not know much about wireless networks, but I would worry about the susceptibility to security violations
Student	1	1	1	1	1	1	1	1	1	1	1	1	1	
Student	10	10	8	10	10	10	10	4	6	10	10	8	10	I think it would benefit the students, instructors and school if wireless networks were set up on campus and in housing areas and wireless cards were issued when you arrived as part of check-in
Student	9	8	10	10	10	10	7	2	2	2	8	8	8	Already using wireless that is available here. It has helped a lot in getting files e-mailed and checking information between classes.
Student	10	10	10	10	7	10	10	3	3	3	5	1	10	
Student	8	6	10	10	9	9	9	8	7	8	7	8	3	
Student	5	6	8	4	5	5	5	3	4	5	2	5	7	
Student	7	5	10	8	8	10	10	3	7	8	8	5	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	8	8	9	8	8	8	6	4	4	6	6	3	9	
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	
Student	9	10	10	10	10	10	10	10	10	10	10	2	10	
Student	7	7	10	10	10	8	7	10	8	10	8	1	10	
Student	10	10	7	10	8	10	10	6	6	9	10	3	10	Having just started here at NPS in the Information program I have already come to the conclusion that a wireless net would enhance learning many fold. For example, in the information class, instead of watching the professor play with the net and wondering why I here in class instead of at my COMPUTER trying to figure out the problems.
Student	1	1	10	6	10	10	10	1	1	10	5	8	10	
Student	10	10	10	10	10	10	10	3	4	9	10	7	10	Would love to help in anyway that I can with this project.
Student	7	4	10	7	8	7	7	1	1	10	6	7	10	
Student	5	5	10	5	10	5	5	10	10	5	5	1	5	Don't really know enough about wireless networks to trust them.
Student	5	5	10	8	10	9	7	4	2	7	5	5	10	
Student	9	9	10	8	7	7	10	6	6	10	9	4	10	
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	
Student	3	3	10	1	3	4	3	2	2	9	5	6	9	
Student	2	2	1	2	4	3	3	1	1	4	3	6	5	Wireless access is fine for those who would use it for military business, but I think it also gives some students too much flexibility in running their "personal business" which often seems to take priority over military business and would simply be another distraction in classes.
Student	10	10	7	10	10	10	10	10	10	10	10	1	10	
Student	10	10	5	10	10	10	10	5	5	10	10	7	1	I already have a laptop and a wireless card that I am using on the campus. The installation of WAPs has done more to enhance my productivity than anything else. I no longer need, or want, to use the labs. In fact, I haven't used a computer lab in over 6 months. A wireless network should be NPS's #1 IT goal!
Student	10	10	10	10	10	10	10	10	5	1	10	8	7	
Student	10	10	10	8	10	10	9	1	1	10	10	8	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	2	2	10	1	1	1	1	1	1	1	1	1	10	
Student	5	8	8	8	5	10	9	1	4	10	8	9	8	
Student	8	6	10	8	10	10	10	3	2	10	8	9	7	
Student	7	8	10	10	8	8	10	3	3	5	8	2	10	
Student	8	5	10	4	4	5	10	2	2	10	4	8	10	
Student	10	10	10	8	10	10	10	5	8	10	10	10	10	
Student	2	2	10	2	2	2	2	2	2	2	2	1	3	
Faculty	8	5	5	7	5	5	8	9	9	10	10	6	9	
Student	7	7	10	8	10	10	10	1	1	3	5	8	10	Nicely done Joe! r/ Rich Makarski
Student	4	3	10	2	2	2	2	1	1	1	1	1	1	Access while I'm driving? The roads are already unsafe as they are. There are so many computers available at NPS wireless seems an unnecessary luxary. Furthermore, if I understand this right, wireless is a bit more restrictive (speed, content) etc. than land line. Besides, when I am out of the office, I want to be out of the office. Don't put me on call 24 hours a day with wireless gadgets.
Student	5	7	10	7	10	10	10	10	7	5	6	1	10	
Student	7	9	10	10	8	10	10	3	3	9	10	2	10	
Student	4	6	9	7	5	7	5	6	5	5	6	6	7	
Student	4	4	10	4	1	9	9	1	1	10	5	1	10	
Student	10	10	10	9	10	10	10	1	6	10	10	10	10	
Staff	10	10	10	8	10	10	10	7	5	10	10	1	10	
Student	3	4	10	4	5	5	5	5	5	5	3	7	10	Sorry, but I do not see the need for wireless on the campus.
Student	5	5	5	4	4	3	3	3	10	3	3	1	4	
Student	10	10	10	10	10	10	10	5	5	10	10	8	10	having a Macintosh laptop (which comes almost standard with a wireless card), I exclusively use a wireless network at home and prefer to connect to a network without cables.
Student	8	8	5	6	9	10	10	6	5	10	7	7	6	If La Mesa were included, most of my answers would be near the top of the scale (10).
Student	10	10	10	10	10	10	10	10	10	10	10	10	10	
Student	10	10	8	10	10	10	10	3	3	8	9	6	10	
Student	7	8	10	5	5	5	9	1	1	10	8	2	5	
Student	4	5	7	4	5	8	7	3	5	5	6	1	9	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	10	10	10	8	1	10	5	5	7	8	10	9	9	Wireless networks can be very useful for those owning a laptop with wireless capability so they can connect anywhere inside the campus.
Student	7	7	10	8	9	10	7	3	3	10	5	1	10	
Student	8	9	8	8	10	10	8	1	1	10	8	5	10	Moving toward a wireless campus is a step in the right direction. Several universities throughout the country have done this with success. You could also possibly get more students and staff on the network if we could get a group discount on PDAs similar to the one we have with Dell. I would recommend tutorial type training sessions once the network is set up to demonstrate the capabilities of a wireless network.
Student	7	4	10	3	8	10	10	3	3	10	7	7	10	
Student	8	8	8	7	8	10	7	6	6	8	8	10	10	
Student	7	7	10	5	10	10	7	8	5	6	4	4	10	
Student	7	8	10	10	10	7	10	4	4	7	8	5	5	
Staff	10	10	10	10	10	10	10	9	8	10	10	7	10	Would connecting to the internet be faster? Wireless sounds very painless to me. No more tripping over wires.
Staff	9	10	10	10	10	10	10	10	10	10	10	10	10	
Student	3	3	10	5	10	5	10	1	1	5	1	1	10	
Student	8	8	10	9	10	10	10	5	1	10	7	1	10	
Student	1	2	10	3	3	10	2	1	1	10	1	1	10	I do most of my computing at home, which is not on or near campus. Although I have a laptop with me, I rarely bring it to campus. so, a campus-wide wireless network is of minimal use or value to me.
Student	1	1	2	1	1	1	2	1	1	1	1	2	2	
Student	8	10	10	8	10	7	10	7	8	10	10	6	6	
Student	10	10	10	10	10	10	10	9	8	10	10	5	10	
Student	5	1	5	1	10	5	10	1	1	6	7	1	10	

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
Student	7	10	10	10	10	8	8	4	4	8	5	4	10	I am currently a user of wireless web clipping and e-mail / instant messaging through my palm device. If a well-thought-out wireless network was available here on campus, I would invest in a new laptop, bluetooth technology and an air-card. It seems like a logical step and a nice upgrade to current capability. We'll need more picnic tables in the quad though -- more folks will be working outdoors!!! Thanks for asking. V/R, LCDR Herdlick
Student	10	10	10	10	10	10	10	1	1	10	10	10	10	I've heard of a concept where the campus would sub-custody laptops with wireless cards to students upon arriving at NPS (for the duration of their time at NPS) and do away with the campus computer labs, allowing the precious campus space to be redesignated for other use. This would provide the students and faculty with a campus-wide virtual lab and potentially make every classroom a computer lab. I've also heard there is reluctance among some faculty, staff and administrators because of potential problems with having computer avaiability in the classroom (e.g., students surfing the web & causing distraction, and/or professors looking at the back of laptops instead of the bright, shining faces of their students). In my view, this is a poor arguement for not moving forward with the technology at an academic institution like NPS. I've often made SOF comments at the close of each quarter that I wished many of the IST courses were taught in computer lab settings so the students could see programming langauge, database,

STATUS	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	Q14	COMMENTS
														active server page examples, etc., in real time vice the "Death by Viewgraph" method so enamored by today's standard. The courses don't always have an associated lab and even if they do, they don't help much if the student doesn't "SEE IT" or "GET IT" as it's being taught. I think the wireless constuct would go a long way toward overcoming this problem. LtCol Dave Overton, USMC
Student	3	3	10	1	5	5	5	6	4	5	1	1	5	
Student	5	5	10	5	10	10	10	5	5	10	5	3	10	
Student	10	10	10	10	10	10	10	10	10	10	10	5	10	PDA's!
Average	7.01	7.05	8.61	7.07	7.97	8.10	7.88	4.49	4.35	7.60	6.64	5.53	8.24	
Stand dev	2.87	3.09	2.25	2.98	2.82	2.75	2.80	3.02	3.05	3.00	2.99	3.26	2.71	
Previous Survey	6.47	6.57	8.89	6.30	7.51	7.51	7.25	4.48	4.01	7.45	6.10	5.14	7.91	
Difference	0.54	0.48	-0.28	0.77	0.46	0.59	0.63	0.00	0.34	0.14	0.53	0.39	0.34	

APPENDIX D. JAMES GEIER WIRELESS SHORT COURSE

The NPS Wireless Group presents a three day Wireless Technology seminar led by one of the top names in the wireless industry: **Jim Geier**

Concepts, Technologies, Security, 802.11 standards, and implementation methods

May 17-19 (0900-1700 Friday, Saturday, and Sunday)

Ingersol Hall Auditorium (1st Deck)

Click here for the outline

All three days are open to Students, Staff, and Faculty **free** of charge provided that you register by May 13, 2002.

Click here to register

Jim Geier is an independent consultant assisting firms with the development of wireless network products and integration of wireless networks into corporate information systems. His 20 years experience deals with the analysis, design, software development, installation, and support of numerous client/server and wireless network-based systems for retail, manufacturing, warehousing, healthcare, and airline industries throughout the world. Jim is author of three books: *Wireless LANs*, *Wireless Networking Handbook*, and *Network Reengineering,* as well as numerous articles.

Jim speaks regularly at seminars, conferences, and tradeshows. Jim is an active participant in the Wireless Ethernet Compatibility Alliance (WECA), responsible for certifying interoperability of 802.11 (Wi-Fi) wireless LANs. He served as Chairman of the Institute of Electrical and Electronic Engineers (IEEE) Computer Society, Dayton Section, and Chairman of the IEEE International Conference on Wireless LAN Implementation. He has been an active member of the IEEE 802.11 Working Group, responsible for developing international standards for wireless LANs.

Jim's education includes a bachelor's and master's degree in electrical engineering (with emphasis in computer networking and software development) and a master's degree in business administration.

Please send all questions and concerns to: LCDR Joe Roth

Wireless LAN Workshop

Day 1 – May 17, 2002

1. **Wireless LAN Markets and Applications**
   - Corporate Information Systems: Temporary offices, Ethernet replacement
   - Warehousing: Receiving, Shipping, Put away, Picking, Inventory Control, Work-in-Process
   - Retail: Pricing and Inventory Control
   - Healthcare: Electronic Patient Records, Narcotics Tracking, Asset Management
   - Education: Inter-building Communications, Wireless Computing in Classrooms
   - Hospitality: Meal Ordering, Guest Reception, Baggage Tracking
   - Home and Small Offices: Peripheral Sharing
   - Trends in the Wireless LAN Market
2. **Wireless LAN Benefits**
   - Efficiency and Accuracy do to Mobility and Real-time Access to Information
   - Easier and Less Expensive Installation in Difficult-to-Wire Areas
   - Increased Reliability Due to Fewer Wires and Connectors
   - *Discussion: Workshop participants will analyze the applications and benefits of wireless networks for their particular product or within their own company or customer environment.*
3. **Wireless LAN Implications**
   - RF Interference of Nearby Radio Signal Sources
   - Security Vulnerabilities
   - Limitations of Batteries
   - Non-interoperability of Proprietary Wireless LANs

- Difficulty in Planning the Number and Location of Wireless LAN Access Points
- Potential Incompatibilities across Multi-vendor Wireless LANs
- *Discussion: Workshop participants will analyze implications related to implementing wireless LANs for their particular product or within their own company or customer environment. The instructor will offer recommendations on resolving applicable issues.*

4. **Wireless LAN Technologies and Standards Overview**
   - Spread Spectrum (Frequency Hopping and Direct Sequence)
   - Orthogonal Frequency Division Multiplexing (OFDM)
   - Ultra Wideband Technologies
   - Infrared Wireless LANs
   - IEEE 802.11 vs. SWAP vs. HiperLAN vs. Bluetooth
   - IEEE 802.11a vs. 802.11b vs. 802.11g
5. **Wireless LAN Components and Operation**
   - Wireless Network Interface Cards and Access Points
   - Antennas: Omnidirectional vs. Highgain vs. Smart Antennas
   - End-User Devices: Scanners, Data Collectors, Handheld PCs, Palm-Based Computers
   - Wireless LAN Software: Terminal Emulation, Middleware, Client/Server Connectivity
   - Wireless LAN Product Vendors
   - *Discussion: The instructor will demonstrate how to interconnect and setup wireless LAN components and show how the components operate.*

Day 2 – May 18, 2002

6. **Wireless LAN Configurations**
   - Wireless LAN-based PC Clients Accessing an Enterprise System
   - RF Data Collection System
   - Corporate Wireless Information System
   - Public Wireless LAN Hotspot
   - Small Office / Home Wireless LAN
   - Inter-building Wireless Data Communications System
7. **Introduction to the IEEE 802.11 Wireless LAN Standard**
   - History of the 802.11 Standard
   - Primary 802.11 Features and Services
   - Physical Topologies and Logical Architectures
8. **Operation of the IEEE 802.11 Medium Access Control (MAC) Layer**
   - IEEE 802.11 MAC Layer Architecture
   - Distributed Coordination Function for Non-Deterministic Access (CSMA/CA)
   - Point Coordination Function for Time-Bounded Communications
   - Synchronization between End-User and Access Point Stations
   - Power Management Protocols
   - Authentication and Privacy Techniques (WEP, 802.1X, and 802.11i enhancements)
   - IEEE 802.11e QoS enhancements
   - Infrastructure Mode vs. Peer-to-Peer
   - MAC Frame Structure and Types
9. **Operation of the IEEE 802.11 Physical (PHY) Layers**
   - IEEE 802.11 PHY Layer Architecture
   - Differentiation between 802.11, 802.11a, 802.11b, and 802.11g PHY layers
   - Frequency Hopping Spread Spectrum (FHSS) Modulation Functions
   - Direct Sequence Spread Spectrum (DSSS) Modulation Functions

- Infrared (IR) Physical Layer Modulation Functions
- Orthogonal Frequency Division Multiplexing (OFDM) Modulation Functions
- *Discussion: Workshop participants will discuss which Physical Layer is best for satisfying needs for their particular product or their company or customer environment.*

10. Wireless LAN Product Design

- IEEE 802.11 Chip Set Vendors and Product Suppliers
- IEEE 802.11 Configuration Parameters and Design Tips
- MAC Software Licensing vs. Internal Development
- Compliance Certification Steps
- *Discussion: Workshop participants will discuss which approach and steps to take in order to develop a wireless LAN product.*

Day 3 – May 19, 2002

11. System Integration Techniques

- Terminal / Host Connectivity
- Client Server Connectivity
- Issues of TCP/IP over Wireless Networks
- Use of MobileIP for Solving IP Addressing Issues
- Wireless Middleware
- *Discussion: The workshop instructor and participants will discuss requirements for specific system solutions.*

12. Analyzing Requirements for a Wireless LAN Solution

- Eliciting Information and Identifying Applicable Requirements Types
- Defining Requirements that Satisfy Application Needs
- Performing a RF Site Survey to Determine the Number and Location of Access Points
- Analyzing the Feasibility of a Wireless LAN
- *Discussion: The workshop instructor and participants will discuss requirements for specific system solutions.*

13. Designing a Wireless LAN

- Identifying Technologies and Products that Best Meet Requirements
- Determining Optimum 802.11 Parameters and Options
- Assigning Access Point Channels
- Determining Throughput Requirements
- Wireless LAN Sizing and Collocation Techniques
- Verifying the Design Through Prototyping and Simulation
- *Discussion: The workshop instructor and participants will discuss the design of specific system solutions.*

14. Installing and Testing a Wireless LAN

- Installation Issues and Resolutions
- Installing Wireless NICs and Access Points
- Testing and Troubleshooting a Wireless LAN Installation

- *The workshop instructor and participants will discuss installation issues and resolutions for specific system solutions.*

15. **Securing a Wireless LAN**
    - 802.1X Operation
    - Authentication Methods (EAP-TLS, EAP-TTLS)
    - Access Controller Solutions
    - 802.11i Update
    - *The workshop instructor and participants will discuss security issues and resolutions for specific system solutions.*

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Mohler, M. *FORCEnet, the Catalyst Transforming the Navy, Connecting Technology Brief*. [http://www.it-umbrella.navy.mil/ct/spring/02/agenda/spring02-agenda-detailed.html]. May, 2002.

2. Cerf, V. and Kahn, R. *A Protocol for Packet Network Interconnection*. Institute of Electrical and Electronic Engineers (IEEE). May, 1974.

3. Gilder, *G. Metcalfe's Law and Legacy*. Forbes ASAP. [http://www.seas.upenn.edu/~gaj1/metgg.html]. September, 1993.

4. NOP Research Group. *Wireless LAN Productivity and Benefits: A Research Study*. [http://newsroom.cisco.com/dlls/tln/wlan/wlan_benefits.html]. November 2001.

5. Sage Research. *Wireless LANs: Improving Productivity and Quality of Life* [http://newsroom.cisco.com/dlls/sage_report.pdf]. May, 2001.

6. FCC. *Regulation Subpart C Section 15.247.* [http://ftp.fcc.gov/oet/info/rules/part15/part15_dec18_01.pdf]. December, 2001.

7. Sivowitch, E. *IEEE Milestones: Directive Shortwave Antenna 1924*. [http://www.ieee.org/organizations/history_center/milestones_photos/yagi.html]. March, 2002.

8. Flickenger, R. *Antenna on the Cheap (er, Chip)*, [http://www.oreillynet.com/cs/weblog/view/wlg/448]. July 2001.

9. Eckstrom, D Cornell Computer Science, *Low Cost 802.11A Directional Antenna using obsolete PrimeStar Dish.* [http://www5.cs.cornell.edu/%7Eeckstrom/802.11a/primestar/index.html]. June, 2002.

10. UMTS FORUM, *Long Term Potential Remains High For 3G Mobile Data Services*. [http://www.3gnewsroom.com/html/whitepapers/year_2002.shtml]. February, 2002

11. LaRocca, J. and LaRocca, R., *802.11 Demystified: Wi-Fi Made Easy*, McGraw-Hill, 2002.

12. Lawson, S. *WLAN Use Growing Fast, Researchers Say. Network World Fusion* [http://www.nwfusion.com/news/2002/0801wlan.html]. August, 2002.

13. Blunk, L. and Vollbrecht, J. *PPP Extensible Authentication Protocol (EAP) IETF RFC 2284.* [http://www.ietf.org/rfc/rfc2284.txt]. March, 1998.

14. O'Hara, B. and Petrick, A., *The IEEE 802.11 Handbook: A Designers Companion*, p. 16. IEEE Press, 1999.

15. UNH InterOperability Lab and the Wireless Consortium. [http://www.iol.unh.edu/consortiums/wireless]. September, 2002

16. Milner, M. *National Map Netstumbler.* [http://www.netstumbler.com/nation.php]. September, 2002.

17. Jones, B. *Collaboratively Creating a Hobo-Language for Free Wireless Networking.* [http://www.warchalking.org]. July, 2002.

18. Gongrijp, R. *FreeBase Free Windows Software to Configure the Apple AirPort Base Station.* [http://freebase.sourceforge.net]. September, 2000.

19. Arbaugh W. *Your 802.11 Wireless Network Has No Clothes.* [http://www.drizzle.com/~aboba/IEEE/wireless.pdf]. March, 2001.

20. Fluhrer, Mantin, and Shamir. *Weakeness in the Key Scheduling Algorithm of RC4* [http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf]. August, 2001.

21. Stubblefield, A. *Using Fluhrer, Mantin, and Shamir Attack to Break WEP.* [http://www.cs.rice.edu/~astubble/wep]. August, 2001.

22. Walker, J. *Unsafe at Any Key Size; An Analysis of the WEP Encapsulation,* [http://www.drizzle.com/~aboba/IEEE/0-362.zip]. October, 2000.

23. Milner, M. *Netstumbler FAQ.* [http://www.netstumbler.com/FAQ]. September, 2002.

24. FUNK.com. *A Comparison of the Different 802.1X Authentication Implementations.* [http://www.funk.com/radius/Solns/EAP_type_chart.gif]. September, 2002.

25. Cisco Systems. *Under the Hood: Wireless Authentication.* [http://www.cisco.com/warp/public/784/packet/exclusive/apr02.html]. April, 2002

26. Arbaugh W. *An Initial Security Analysis of the IEEE 802.1X Standard.* [http://www.cs.umd.edu/~waa/1x.pdf]. February, 2002.

27. Cisco Systems. *Cisco Aironet Response to University of Maryland's Paper, "An Initial Security Analysis of the IEEE 802.1x Standard".* [http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1680_pp.htm]. August, 2002.

28. Funk.com. *Comments on "An Initial Security Analysis of the IEEE 802.1X Standard"* [http://www.funk.com/radius/Solns/umdresp_wp.asp]. March, 2002.

29. Metagroup. *Wireless LANs.* Presentation Presented at the 802.11 Planet Conference in Philadelphia. May, 2002.

30. Air Defense. *Results from the Defcon Convention*. [http://www.airdefense.net]. August, 2002.

31. Office of Management and Budget. *OMB Guidance to Federal Agencies on Data Availability and Encryption* [http://csrc.nist.gov/policies/ombencryption-guidance.pdf]. January, 2002.

32. NIST. *FIPS Publication 197.* [http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf]. November, 2001.

33. NPS. *Draft NPS IT Strategic Plan,* [http://intranet.nps.navy.mil/Docs/ITStrategicPlan4-25.pdf , p. 3]. September, 2002.

34. NPS. *Draft NPS IT Strategic Plan,* [http://intranet.nps.navy.mil/Docs/ITStrategicPlan4-25.pdf, pp. 4, 8, and 12]. September, 2002.

35. Planet 3 Wireless, *Certified Wireless Network Administrator certification,* [http://www.cwne.com]. September, 2002.

36. Lopez. A. *Wireless LANs.* [http://www.cs.uni.edu/~fienup/mics_2002/proceedings/papers/alopez.pdf]. March, 2002.

37. Carnegie Mellon University. *Welcome to Wireless Andrew*. [http://www.cmu.edu/computing/wireless]. August, 2002.

38. Wake Forest University. *Pocket Classroom*. [http://pocketclassroom.wfu.edu]. June, 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

Akin, D., Sandlin, K., Turner, S., Nicholas, R., McCord, J., Jones, J., Brooks, S., Waldo, B., and Oxford, B., *Certified Wireless Network Administrator: Official Study Guide*, Planet 3 Wireless, 2002.

Barnes, C., Bautss, T., Lloyd, D., and Ouellet E., *Hack Proofing Your Wireless Network,* Syngress, 2002.

Bruce, W. and Gilster, R., *Wireless LANs End to End*, Hungry Minds, 2002.

Davis, H. and Mansfield, R., *The WI-FI Experience Everyone's Guide to 802.11b Wireless Networking*, QUE, 2002.

Gast, M. S., *802.11 Wireless Networks: The Definitive Guide*, O'Reilly Networking, 2002.

Geier, J., *Wireless LANs*, SAMs, 2001.

LaRocca, J. and LaRocca, R., *802.11 Demystified: Wi-Fi Made Easy*, McGraw-Hill, 2002.

Nichols, R. K. and Lekkas, P. C., *Wireless Security: Models, Threats, and Solutions,* McGraw-Hill, 2002.

O'Hara, B. and Petrick, A., *The IEEE 802.11 Handbook: A Designers Companion*, IEEE Press, 1999.

Ouellet, E., Padien, R., Pfund, A., and Fuller, R., *Building a Cisco Wireless LAN*, Syngress, 2002.

Stallings, W., *Wireless Communications and Networks*, Prentice Hall, 2001.

Terry, J. and Heiskala, J., *OFDM Wireless LANs: A Theoretical and Practical Guide,* SAMs, 2002.

Wheat, J., Hiser, R., Tucker J., Neely A., and McCullough A., *Designing a Wireless Network*, Syngress, 2002.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Don Brutzman
   Naval Postgraduate School
   Monterey, California

4. Dr. Alex Bordetsky
   Naval Postgraduate School
   Monterey, California

5. LCDR Joseph Roth
   Naval Postgraduate School
   Monterey, California

6. Dr. Christine Cermak
   Naval Postgraduate School
   Monterey, California

7. Dr. Dan Boger
   Naval Postgraduate School
   Monterey, California

8. Rex Buddenberg
   Naval Postgraduate School
   Monterey, California

9. Tom Halwachs
   Naval Postgraduate School
   Monterey, California

10. Jim Geier
    Wieless-Nets Ltd.
    Yellow Springs, Ohio

11. Carl Consumano
    Office of the Secretary of Defense OSD-C3I
    Washington, DC

12. Barry Frew
Naval Postgraduate School
Monterey, California

13. CAPT Frank Petho
Naval Postgraduate School
Monterey, California

14. VADM Dick Mayo
COMNAVNETWARCOM
Norfolk, Virginia