



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

A Case Study of Wireless Integration into an Enterprise Network

by

Donna L. Miller
Timothy E. Levin
Cynthia Irvine

January 2005

Approved for public release; distribution is unlimited.

Prepared for: Federal Aviation Administration

This Page Intentionally Blank

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Rear Admiral Patrick W. Dunne
Superintendent

R. Elster
Provost

This report was prepared by the Naval Postgraduate School Center for Information Systems Security Studies and Research (NPS CISR). Support for this work was provided by the Federal Aviation Administration.

Reproduction of all or part of this report is authorized.

This report was prepared by:

Donna L. Miller
Research Assistant

Timothy E. Levin
Associate Research Professor

Cynthia E. Irvine
Associate Professor

Reviewed by:

Neil C. Rowe
Professor
Department of Computer Science

Released by:

Peter J. Denning, Chair
Department of Computer Science

Leonard A. Ferrari
Associate Provost and
Dean of Research

This Page Intentionally 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 instructions, 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 31 January 2005	3. REPORT TYPE AND DATES COVERED Findings; 6/1/04 – 1/15/05	
4. TITLE AND SUBTITLE A Case Study of Wireless Integration into an Enterprise Network			5. FUNDING DTFAWA-04-X-00008	
6. AUTHOR(S) Donna L. Miller and Timothy E. Levin and Cynthia Irvine				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Center for Information Systems Security Studies and Research Naval Postgraduate School, 833 Dyer Road, Monterey, CA 93943			8. PERFORMING ORGANIZATION REPORT NUMBER NPS-CS-05-004	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Federal Aviation Administration 800 Independence Avenue, S.W., Room 602, Washington DC 20591POC:			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Federal Aviation Administration.				
12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words.) This report provides a high level recommendation for a wireless roll-out plan with wireless security policy applicable to the Federal Aviation Administration. We describe general information about wireless technology including the different wireless standards and security measures required to protect an entire network from its wireless components. We describe the history of the wireless roll-out process at Naval Postgraduate School with lessons learned. We describe a process to develop a wireless security policy for a major enterprise. We provide suggestions on development of a pertinent plan for wireless implementation. We offer an exemplar design process for implementation of a wireless network.				
14. SUBJECT TERMS IEEE 802.11, Wireless Security Policy, Wireless Implementation			15. NUMBER OF PAGES 87	
			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 Unclassified	

This Page Intentionally Blank

TABLE OF CONTENTS

I. INTRODUCTION	1
II. BACKGROUND	5
A. Introduction to IEEE 802.11	5
B. IEEE 802.11 WLAN Standards	8
1. IEEE 802.11b	9
2. IEEE 802.11a / IEEE 802.11h	9
3. IEEE 802.11g	11
4. IEEE 802.11b/a/g: Original Security Characteristics	12
5. IEEE 802.11i and Wireless Protected Access (WPA): Security Enhancements	15
C. IEEE 802.11 Threats, Vulnerabilities, and Countermeasures	21
III. NAVAL POSTGRADUATE SCHOOL WIRELESS CASE STUDY	29
A. Naval Postgraduate School Wireless Plan	29
1. The NPS Wireless Warrior Group	29
2. NPS Wireless Requirements	30
3. NPS Wireless Pilot Program	32
4. Current NPS WLAN Infrastructure	34
B. NPS Wireless Network Vulnerability Assessments	36
IV. FAA IT INFRASTRUCTURE	39
A. WJHTC Current IT Infrastructure	40
B. Wireless Deployment Considerations at FAA	40
V. WIRELESS POLICY RECOMMENDATION	43
A. Introduction	43
B. Wireless Security Policy	43
1. Considerations for Wireless Policy	44
C. Department of Transportation Wireless Standard Overview	49
D. DOD Directive 8100.2 Wireless Use	50
VI. RECOMMENDED WIRELESS ROLLOUT PLAN FOR FAA	53
A. Introduction	53
B. Policy	54
C. Define a General Plan of Action with Milestones	54
D. Determine the Requirements	55
E. The RF Site Survey	56
F. Design Considerations	58
G. Installation and User Registration	59
H. Security Maintenance of the Wireless Network	60
I. Conclusion	61
APPENDIX 1. AN EXAMPLE DESIGN FOR A SECURE WIRELESS LAN	65
A. Topology	68
LIST OF REFERENCES	71
INITIAL DISTRIBUTION LIST	75

LIST OF FIGURES

Figure II-1 OSI Model and IEEE 802.11	5
Figure II-2 Simple Illustration of Direct Sequence Spread Spectrum Process	7
Figure II-3 Direct Sequence Spread Spectrum channel description	8
Figure II-4 OFDM Channels.....	10
Figure II-5 802.11i/WPA Basics.....	17
Figure II-6 802.1X Basics.....	18
Figure II-3 802.1X Authentication Process	20
Figure III-1 AP Installation and Purchase Guideline.....	30
Figure III-2 NPS Wireless Survey	32
Figure III-3 Initial NPS WLAN Infrastructure	33
Figure III-4 Registering for Wireless Access Guidelines	34
Figure III-5 NPS Current WLAN Infrastructure	36
Figure III-6 NetStumbler Example	38
Figure IV-1 FAA Regional Locations	39
Figure IV-2 WJHTC IT Network Representation	41
Figure V-1 Example of a Segregated Wireless Network.....	46
Figure 1-1 A Generic Wireless Topology.....	65
Figure 1-2 IEEE 802.1X Technology	67
Figure 1-3 Exemplar WLAN Architecture	69

LIST OF TABLES

Table II-1 Comparison of 802.11b/a/g.....	12
Table III-1 WLAN Security Vendors and Security Solutions.....	35
Table III-2 Network Protocol Analyzer Tools.....	37
Table VI-1 Security Protocols	61
Table VI-2 WLAN Monitoring Tools.....	62
Table 1-1 IEEE 802.11 Standard Comparisons	66

ACRONYMS

AA – Authentication Agent
AAD – Additional Authentication Data
AES – Advanced Encryption Standard
AP – Access Point
ARP – Address Resolution Protocol
AS – Authentication Server
ASCII – American Standard Code for Information Interchange
BSS – Basic Service Sets
BPSK – Binary Phase Shift Keying
CA – Collision Avoidance
CCK – Complementary Code Keying
CCM – Counter Mode, Cipher-Block-Chaining Message Authentication Code
CCMP – Counter Mode, Cipher-Block-Chaining Message Authentication Code Protocol
CIO – Chief Information Officer
CRC – Cyclical Redundancy Check
CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD – Carrier Sense Multiple Access with Collision Detection
DAA – Designated Approving Authority
DBPSK – Differential Binary Phase Shift Keying
DFS – Dynamic Frequency Selection
DoD – Department of Defense
DOT – Department of Transportation
DMZ – Demilitarized Zone
DQPSK – Differential Quadrature Phase Shift Keying
DSSS – Direct Sequence Spread Spectrum
EAP – Extensible Authentication Protocol
EAPOL – Extensible Authentication Protocol over LAN
EAP-MD5 – Extensible Authentication Protocol Message Digest 5 Algorithm
EAP-TLS – Extensible Authentication Protocol Transport Layer Security
EAP-TTLS – Extensible Authentication Protocol Tunnel TLS
FAA – Federal Aviation Agency

FCC – Federal Communications Commission
FHSS – Frequency Hopping Spread Spectrum
FIPS – Federal Information Processing Standard
GHz – Giga Hertz
GIG – Global Information Grid
ICV – Integrity Check Value
IEEE – Institute of Electrical & Electronics Engineers
IR – Infrared
ISM – Industrial, Scientific, and Medical (refers to radio spectrum: bandwidth for wireless LAN Networks by FCC, 2.4-2.4835 GHz)
IT – Information Technology
ITACS – Information Technology and Communication Systems
IV – Initialization Vector
LAN – Local Area Network
LEAP – Lightweight Extensible Authentication Protocol
LLC – Logical Link Control
MAC – Medium Access Control
MAC – Message Authentication Code (refers to cryptographic use)
MAC OS – Macintosh Operating System
Mbps – Mega bits per second
MHz – Mega Hertz
MIC – Message Integrity Code
MMAC – Mike Monroney Aeronautical Center (refers to FAA facility)
NAS – Network Access Server
NIC – Network Interface Card
NIST – National Institute of Standards & Technology
NPS – Naval Postgraduate School
NSA – National Security Agency
OFDM – Orthogonal Frequency Division Multiplexing
OSI – Open System Interconnection
PKI – Public Key Infrastructure
QPSK – Quadrature Phase Shift Keying
PBCC – Packet Binary Convolutional Coding

PDA – Personal Digital Assistants

POA&M – Plan of Action & Milestones

RADIUS – Remote Authentication Dial-In User Server/Service

RC4 – Ron's Code 4 (refers to RSA Variable-Key-Size Encryption Algorithm by Ron Rivest)

RF – Radio Frequency

RSN – Robust Security Network

TSC – Sequence Counter

SSID – Service Set Identifiers

TK – Temporal Key

TKIP – Temporal Key Integrity Protocol

TPC – Transmitter Power Control

UDP – User Datagram Protocol

U-NII – Unlicensed National Information Infrastructure (refers to radio spectrum: bandwidth for wireless LAN Networks by FCC, 5.15-5.35 GHz and 5.75-5.825 GHz)

VPN – Virtual Private Network

WECA – Wireless Ethernet Compatibility Alliance

WEP – Wired Equivalent Privacy

WJHTC – William J. Hughes Technical Center (refers to FAA facility)

WLAN – Wireless Local Area Network

WPA – Wireless Protected Access

3DES – Triple Data Encryption Standard (168 Bit)

I. INTRODUCTION

The Federal Aviation Administration has issued a moratorium on the use of wireless technologies connecting to its internal IT infrastructure. Although, FAA employees would be able to take advantage of increased functionality and productivity provided by wireless connectivity, the FAA intends to develop a plan of action for securely rolling out wireless technology in its IT environment.

Wireless LAN (WLAN) technology is a fast growing field. Wireless networking provides an unparalleled mobility and freedom to users. In the past few years wireless technology has expanded into a “hotspot” custom. “Hotspots are public spaces like airports, hotel lobbies, or cafes, where people can log onto the Internet.” [1] In addition, major computer laptop manufacturers such as Intel and Dell are offering IEEE 802.11 products. [1, 2] It is obvious that people desire, and are increasingly utilizing, wireless technology.

Just as past computer improvements lead to the proliferation of home computing and the Internet, technical innovations coupled with the dropping costs of wireless-capable devices are leading to greater utilization of wireless technology. Although common WLAN clients today use laptops with PC cards “new technology innovations – smaller, lighter, and less power-hungry – are extending WLAN capabilities to PDAs, cell phone, and other mobile devices.” [3] The future of wireless devices seems limitless.

What's more, wireless technology is alluring to both the commercial and personal business markets. Wireless technology offers many tangible and intangible benefits to an existing network infrastructure with little financial outlay required for utilization. Convenience and productivity savings are key factors in the explosion of wireless products today. For example, a business or home office with wireless equipment requires minimal wiring, or rewiring for furniture repositioning, thus alleviating cost and recovering productivity time lost in the past to personnel relocations. The flexibility and ease of use for wireless technology within home and business environments is likely to only increase. [3]

Although the benefits to wireless technology are great, wireless equipment also brings an entirely new technology to the existing networking paradigm. Over the years, wired networking has prompted the evolution of many security practices to prevent unlawful or accidental information exposure. Yet, due to its nature, wireless technology exposes a realm of vulnerabilities not previously observed in wired networks. Thus, wireless technology requires security measures in addition to the existing wired network security models. These additional security measures must be factored into the overall wireless installation costs. The gravity of security risks introduced by wireless technology has resulted in a FAA moratorium on wireless use within its jurisdiction.

Wireless security concerns can never be removed completely but there are ways to greatly mitigate their shortcomings. First, wireless technology requires a stronger network security policy than is necessary for wired networks. Second, the organization must maintain highly trained IT security personnel with an understanding of wireless technology and security mechanisms required to protect against attacks. Third, all individuals of an organization must be taught about the security policy in order to diminish accidental wireless mistakes. And, most important, the policy must be enforced through consistent IT Department practices that maintain a level of confidence that policy is being adhered to by all personnel within the jurisdiction.

This report presents security information specific to wireless technology and general recommendations the FAA can follow in order to securely transition to the use of wireless technology. To establish a context for the recommendation, we first offer a brief overview of current wireless networking technologies and their security mechanisms provided by the IEEE 802.11 standards. The recommendation is presented in three phases. First, a case study of the Naval Postgraduate School's recent secure transition to wireless is described. This study provides lessons learned regarding the NPS effort to integrate wireless connectivity into its IT technologies. The second phase provides a survey and analysis of a subset of the FAA IT infrastructure, and of FAA goals for wireless connectivity. In the third phase the lessons learned from the case study form the basis for recommendations for wireless integrations into the FAA IT infrastructure.

The major goal of this report is to provide a high level recommendation for a wireless roll-out plan and wireless policy to the Federal Aviation Administration (FAA) by conducting a case study of the Naval Postgraduate School (NPS) wireless implementation plan. The FAA is interested in the Naval Postgraduate School's wireless roll-out experience and in the NPS lessons learned since the initial implementation of its wireless technology. The methods used to secure the NPS wireless network in accordance with local wireless policy and DoD Wireless Policy are of particular interest.

This report starts with general information about wireless technology including the different wireless standards and security measures needed to protect the entire network from its wireless components. The report then focuses on the roll-out of campus-wide wireless technology at NPS and the subsequent lessons learned. Based on the study of the NPS experience and of the FAA IT infrastructure, it concludes with recommendations to the FAA regarding its wireless policy, and for planning and roll out of a secure wireless infrastructure.

This Page Intentionally Blank

II. BACKGROUND

This chapter provides an overview of the IEEE 802.11 architectural standard, associated wireless security concepts, WLAN security weaknesses and associated mitigation techniques, and also includes an example design for a wireless LAN. This discussion is not a comprehensive description of IEEE 802.11 standard, but offers some background to assist with the decision making process.

A. Introduction to IEEE 802.11

In 1997, the Institute of Electrical and Electronics Engineers (IEEE) ratified the initial 802.11 standard. IEEE 802.11 standard defines the interface between a mobile host device and an access point (AP) within a wireless network. Figure II-1 displays the IEEE 802.11 standard in relation to the Physical and Data Link layers within the Open System Interconnection (OSI) Reference Model. The 802.11 standard involves the Physical layer and only a portion of the Data Link layer known as the Medium Access Control (MAC). The Data Link layer is split into two functional areas, the MAC and the Logical Link Control (LLC). The LLC is covered within the IEEE 802.2 standard. The LLC standard is capable of supporting several MAC options as depicted in Figure II-1.

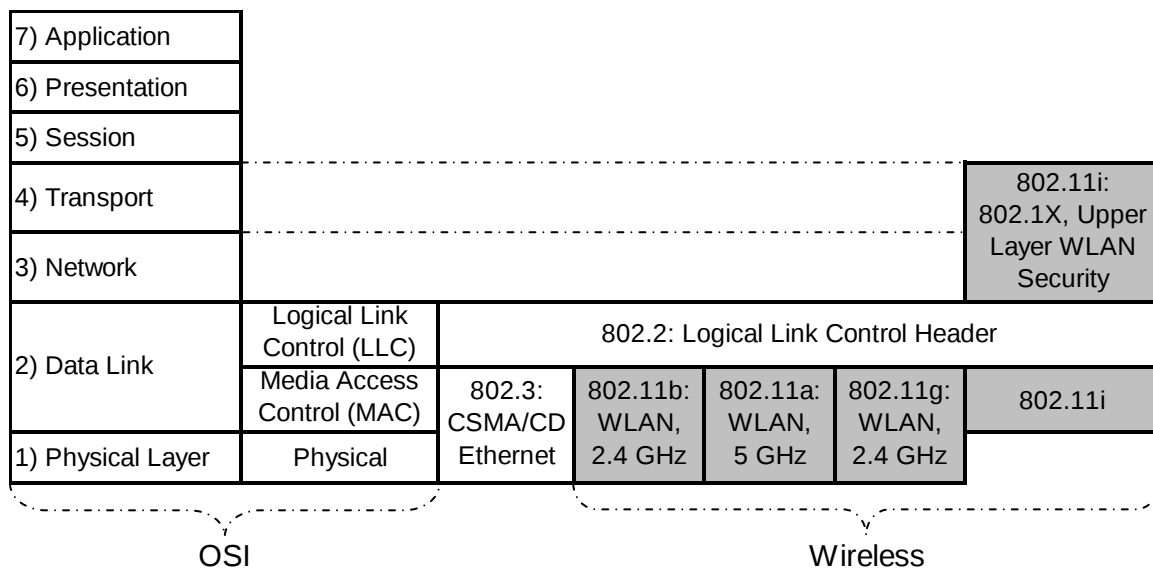


Figure II-1 OSI Model and IEEE 802.11 [4]

The Medium Access Control (MAC) Layer provides a variety of functions that support the operations of IEEE 802.11 wireless LANs. In a wireless network the main

function of the MAC Layer is to hide the unreliability of RF communication from the upper layers of the OSI mode. In a sense it manages and maintains communications between the mobile device network cards and APs by coordinating access to a shared RF channel and utilizing protocols to enhance both bursty and periodic communications over the wireless medium. Periodic communications are described as having a relatively constant amount of traffic over a long period where the bursty is described as having intermittent periods of large traffic amounts. It is important for wireless communication equipment to be a solution for both types of traffic.

There are several distinctive mechanisms established within the MAC Layer to manage the nuances of wireless communications. The discussion here is greatly simplified. A main concept within MAC is a coordination function that determines within a wireless channel when a station is permitted to transmit and receive data via the wireless medium. Each station on a wireless channel is given a transmission opportunity, a period of time that station has the chance to transmit on the wireless medium. Usually co-located with an AP, a point coordinator generates and transmits beacon frames at regular intervals. These beacon frames are sent for station synchronization and protocol information.

The 802.11 MAC Layer basic access mechanism is carrier sense multiple access with collision avoidance (CSMA/CA) with exponential back off. In other words each wireless device senses whether or not the channel it communicates on is busy, if it is busy and the device waits a random period of time before sensing again. If the channel is not busy it transmits the data. Since the wireless medium is not as reliable as over wire, collision avoidance (CA) is utilized instead of collision detection. The exponential back off refers to the process used after a transmission was unsuccessful. In exponential back off, the random period of time before sensing for retransmission is selected out of a window of time that is doubled each time the channel is detected to be busy. It prevents a situation where many hosts overload the channel during bursty traffic with many collisions.

The Physical layer is responsible for the physical transportation of the bits between adjacent systems over the RF channel, in other words between the portable or

mobile device and AP or between two portable or mobile devices. The protocol data unit for the physical layer consists of a preamble and a header, followed by the MAC data description abbreviated above. The header will be used by the receiver for detection and synchronization. When an AP has variable communications speeds the header will be sent at the slowest data rate to ensure furthest distance with propagation.

Initial design of the 802.11 depicts the physical layer transmitting in direct sequence spread spectrum (DSSS), frequency hopping spread spectrum (FHSS), or infrared (IR) and with a transmission rate of either 1 Mbps or 2 Mbps in the 2.4 GHz frequencies bandwidth. Before completion of the first standard it was evident that the bandwidth was unacceptable for use in the growing market. Of these original designs DSSS remains common within the 802.11 hardware today.

To modify the actual data from digital to RF waveforms for radio transfer, signal processing is needed. The signal processing steps performed are scrambling, spreading, and modulation. Figure II-2 Simple Illustration of Direct Sequence Spread Spectrum depicts a simple illustration of the process. Processing creates a resulting signal bandwidth of 22 MHz. Taking into consideration guard bands there are three distinct non-overlapping 22 MHz channels within the 2.4 - 2.4835 GHz range. The channels are centered at 2.412 GHz, 2.437 GHz, and 2.462 GHz as shown in Figure II-3. Although the maximum power allowed for transmissions is 1 Watt, many vendors have opted for a default 0.1 Watts as the transmit power level. The 802.11 WLAN enhancements associated with the OSI Physical layer are broken out in the next section.

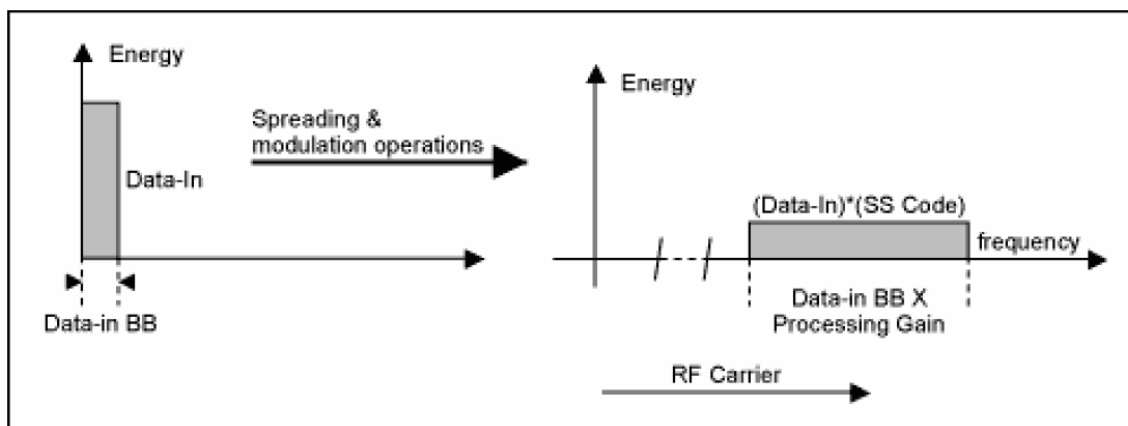
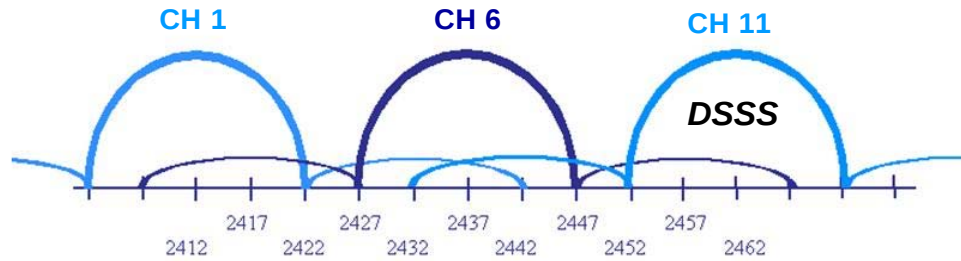


Figure II-2 Simple Illustration of Direct Sequence Spread Spectrum

Process [5]



Three non-overlapping channels in 2.4 – GHz band (20MHz Wide)

Figure II-3 Direct Sequence Spread Spectrum channel description [6]

The modulation supported in the original standard was differential phase-shift keying. The physical layer information uses differential binary phase shift keying (DBPSK) at 1 Mbps, the MAC information is sent using differential quadrature phase shift keying (DQPSK) for 2 Mbps. The binary phase shift uses no phase change for 0 and for 1 it uses a phase change of 180. A quadrature phase shift doubles the throughput by encoding 00 as no phase shift, 01 as 90 degree shift, 10 as 180 degree shift, and 11 as 270 degree shift. Enhancements to DSSS through new modulation techniques as well as the introduction of another physical layer design, orthogonal frequency division multiplexing (OFDM), is discussed in the next section, WLAN Standards. [7]

B. IEEE 802.11 WLAN Standards

It is important to remember that the 802.11 standard is work in progress. In the end, the commercial acceptance of any standard lies in the ability of manufacturers to provide equipment meeting the standard's objectives at a reasonable price and with ease of use to appeal to the consumer. Several individual groups within IEEE 802.11 have formed to focus on specific technologies within the general wireless standard. Each group, differentiated by a separate trailing letter, offers enhancements to the standard and protocol variations to support conformity issues. At a high description level these groups concentrate on the physical layer, security, and quality of services. Several vital standards within the 802.11 and the work of other still active groups are briefly discussed next in order to offer more clarity regarding the present status of wireless technology.

1. IEEE 802.11b

This is a physical layer enhancement. There are a large number of products on the market place today that meet this standard. Since it utilizes the initial 802.11 direct sequence spread spectrum (DSSS) technology and operates over the initial 2.4 to 2.4835 GHz frequency range it is discussed first.

In September 1999, the IEEE ratified the specification for IEEE 802.11b as an upgrade to the original 802.11. This standard increases the throughput from the original standard of 1 - 2 Mbps up to 5.5 - 11Mbps. The increase in throughput is due to the difference in modulation utilized. As described above, the older version utilized DBPSK and DQPSK. The newer 802.11b technology utilizes complementary code keying (CCK). CCK is a variation of an orthogonal keying modulation. The spreading is achieved by a spreading code with eight samples, each 8 chips obtained by using a quadrature phase shift key.

Today the four possible type modulations used and their associated data rates are: DBPSK for 1 Mbps, DQPSK for 2 Mbps, and CCK for both 5.5 Mbps and 11 Mbps. In place of CCK, packet binary convolutional coding (PBCC) can be utilized. It maintains the same 5.5 Mbps using bit to symbol mapping in binary phase shift key and 11 Mbps using bit to symbol mapping in quadrature phase shift key. After mapped through BPSK or QPSK the output goes through a cover sequence process before transmission.

The common range of operation for 802.11b is 150 feet for a floor divided into individual offices by concrete or sheet-rock, about 300 feet in semi-open indoor spaces such as offices partitioned into individual workspaces, and about 1000 feet in large open indoor areas. Disadvantages of 802.11b include interference from electronic products such as cordless phones and microwave ovens. [7]

2. IEEE 802.11a / IEEE 802.11h

This is also a physical layer enhancement. IEEE 802.11a provides significantly higher performance than 802.11b, at 54 Mbps. Unlike 802.11b, the 802.11a standard operates within the frequency range of 5.47 to 5.725 GHz and is not subject to

the same interference from other commercial electronic products. This higher frequency band allows significantly higher speeds of communication over the 2.4 GHz range.

802.11a technology utilizes orthogonal frequency division multiplexing (OFDM) instead of DSSS as in the 802.11b. In essence, OFDM process begins by splitting the input data into several parallel streams as shown in Figure II-4. Each of the streams of data is then modulated onto a separate carrier frequency. These individual carrier frequencies are transmitted in parallel as narrow subchannels. At the far end the subchannels are demodulated and recombined into a replica of the original input data. A spread spectrum technique is utilized to modulate each of the data streams onto the carrier frequencies. Because of their orthogonality the channels are overlapped, allowing greater efficiency. The orthogonal quality also allows for straightforward restructuring at the 802.11a receiver end.

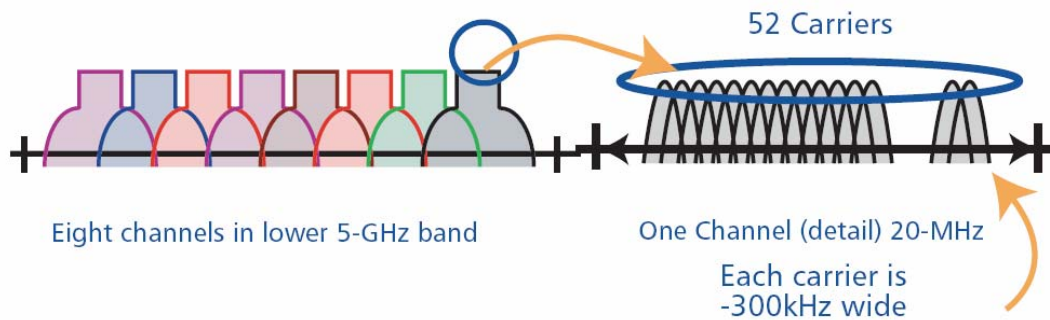


Figure II-4 OFDM Channels [6]

Disadvantages to OFDM include, 802.11a is not backward compatible with the 802.11b. Due to the higher frequency band the APs offer a smaller propagation coverage diameter, covering only about a quarter of the area of an 802.11b AP. Some 802.11a devices have a range of only 60 feet. The higher radio frequency also affects the coverage achievement making it more susceptible to walls and other environmental factors. Also, equipment for 802.11a is in general more expensive than for 802.11b. Today, commercially available APs can be purchased that transmit in both frequency ranges for forward compatibility with the 802.11g, but the cost is significantly higher than the 802.11a AP.

802.11h is a recently completed amendment to 802.11a that defines how 802.11a devices implement dynamic frequency selection (DFS) and transmitter power control (TPC). This was necessary to satisfy European regulations for 5 GHz band devices to implement DFS and TPC. Another reason for the amendment was compatibility with satellite communication systems and radars, the primary users of the Unlicensed National Information Infrastructure (U-NII) frequency band, of which the 802.11a is located within. The satellite and radar systems have the “right of way” requiring 802.11a owners to periodically test for the presence of radars and when detected must vacate the channel and transfer to another. [7]

3. IEEE 802.11g

Again, this is a physical layer enhancement. This standard was begun shortly after 802.11b and 802.11a were completed. The 802.11g has a performance capability of 54 Mbps similar to the 802.11a. Today 802.11g proprietary products can be purchased that support 108Mbps between the AP and host station. 802.11g operates within the 2.4 to 2.4835 GHz frequency range as the 802.11b standard. There are one mandatory and two optional physical layer mechanisms within the 802.11g. The mandatory mechanism is OFDM just as described with the 802.11a standard. In principle there are very few differences between the OFDM 802.11a and 802.11g. One difference is that the time required to complete the convolutional decoding of the OFDM is greater with the 802.11a. Therefore, the 802.11g is given an extra time period to equalize the two standards.

802.11g supports many different data rates. OFDM uses 6, 12, 24, 18, 36, and 54 Mbps. The optional CCK-OFDM provides the rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. The optional PBCC provides the rates of 22 and 33 Mbps. The selection of data rates is not specified within the standard and instead is left to the interpretation of the manufacturers.

802.11g APs are backward compatible with 802.11b APs. This backward compatibility with 802.11b is handled through the MAC layer, not the physical layer. On the negative side, because 802.11g operates at the same frequency as 802.11b, it is

subject to the same interferences from electronic devices such as cordless phones. Since the standard's approval in June 2003, 802.11g products are gaining momentum and will most likely become as widespread as 802.11b products. Table II-1 displays basic 802.11b/a/g characteristics. [7]

4. IEEE 802.11b/a/g: Original Security Characteristics

This section describes the security mechanisms included within the original 802.11b/a/g standards. In order to describe the security it is important to understand the basic concept behind a wireless connection. All wireless connection devices require hardware to support basic service sets (BSS). The BSS is the basic (wireless) network between two points: the host station and the Access Point (AP). The term host station will be used here to describe a host computer within a wireless network. Access Points (AP) are responsible for acquiring the wireless signal from the host station wireless device and managing traffic between the host station and the network it is wired to. In reality, the AP is connected to two networks simultaneously, the BSS with the host station(s) and the network it is attached to. Wireless APs require additional hardware and software compared to the host station wireless devices in order to support traffic management between the networks.

Physical Standard	Layer	Maximum Performance	Freq Range	Band	Technology	Backward Compatible:
802.11b		1 to 11Mb/s	2.4-2.4835 GHz	ISM	DSSS	
802.11a		54Mb/s	5.47-5.725 GHz	U-NII	OFDM	
802.11g		54Mb/s	2.4-2.4835 GHz	ISM	OFDM (mandatory)	802.11a*
802.11g		54Mb/s	2.4-2.4835 GHz	ISM	DSSS-OFDM	802.11b
802.11g		33Mb/s	2.4-2.4835 GHz	ISM	PBCC	

*compatible if AP broadcasts in both 2.4 GHz and 5 GHz ranges.

Table II-1 Comparison of 802.11b/a/g [7]

Scanning, authentication and association must take place in order to establish a wireless connection and exchange data. APs periodically transmit frames containing timing and network information that offer host stations the information they need to synchronize with an AP. The host station scans to discover BSSs available within their proximity. The host station then must authenticate to the AP. Authentication

verifies the host station's authorization to utilize the network through a difficult, but solvable security problem. The association is established after the host station has been authenticated. Data exchange occurs only after association is completed.

Ad Hoc and Infrastructure Modes

IEEE 802.11 defines two operating modes, ad hoc and infrastructure. In ad hoc mode, wireless clients correspond with each other directly without the use of a wireless AP. The wireless clients Network Interface Card (NIC) must be explicitly configured to use ad hoc mode. Note that a similar protocol standard, known as Bluetooth, is used for interconnection of personal digital assistants (PDA), cell phones and computers, operates in ad hoc mode. Dissimilar to ad hoc, infrastructure mode requires a wireless AP for all communications. The wireless client must communicate with the wireless AP in order to gain access to the resources of a wired network as well as the other hosts located on the wireless segment.

Authentication

Once the BSS is discovered, authentication must be completed before a connection can occur. Positive authentication leads to association, by which the host station becomes a member of the network. Note that if the host station is configured for ad hoc operation it can connect directly with other host stations configured similarly. If the host station is configured for infrastructure operation it requires connection to an available wireless AP.

The initial 802.11 1997 standard defined three types of authentication: open system, shared key, and upper layer. Although upper layer authentication is defined in the initial 802.11 standard, it is not offered within the original 802.11 security mechanisms. The open system operates on a two message exchange. The first message asserts identity and requests identity of the other party. The second message returns the result, success or failure. It trusts anyone, therefore, in practice it is not truly a security mechanism. Shared key authentication offers more.

The basic premise of shared key authentication is that each station requiring the connection must have a pre-shared secret key. In other words the key the

client uses for authentication and encryption of the data stream must be the same key that the AP uses. This equates to a symmetric as opposed to an asymmetric cipher key. In addition, this secret, symmetric key must be exchanged over a separate secure method in practice. The authentication challenge request is encrypted by the requesting end. At the receiving end the message is decrypted and, if it matches, then the key is accepted as the same and authentication is successful and association is established between the AP and host station.

On the other hand, there are several major disadvantages to shared key that have come to light since the original 802.11 was developed. Authentication is only one way: host to AP. In other words, genuine APs have some level of certainty that the hosts are authentic, but the hosts could unknowingly be associated to an AP that is not associated with the anticipated network. There is no key management associated with the original 802.11, and given U.S. government regulations for exporting technology the mandatory key size (when enabled) is held to a 40-bit size static key. A key is only secure as long as it has not been compromised and the static key requires regular and deliberate reconfiguration of host stations and wireless APs. If the key is compromised the network is left open to unauthorized users. In addition to this, all of the information required to construct a specific secret key can be found within the public domain of the network. 802.11i offers methods for wireless security that far surpass the original 802.11 standard. The next section covers 802.11i enhancements.

Tying theory into wireless hardware practice, the authentication methods introduced above utilize service set identifiers (SSID) and wired equivalent privacy (WEP). SSID operates as the open system portion of the authentication. Hosts are required to provide the name of the network SSID in their client settings in order to be allowed access to that specific AP. Newer 802.11 APs can be configured so they do not broadcast the SSID, but, by default APs broadcast the SSID. If an AP broadcasts its SSID, any client can detect the SSID through its own wireless hardware/software. WEP provides the shared key encryption and authentication for wireless communications. The default configuration of wireless APs are not WEP enabled. [7]

Privacy

WEP encryption is based on the stream cipher RC4 algorithm. The per-packet key is a combination of the private (shared) key and the random initialization vector (IV). The IV is a 24-bit field, which produces a 64-bit field when combined with the 40-bit key. The IV is created new for each packet but the private key remains the same. During the encryption process the new per-packet key is XORed with the plaintext. The decryption process is the reverse of this process. WEP does not offer data integrity keys. WEP can be configured to have an integrity check value (ICV) field within the plaintext, though. The ICV provides a 32-bit cyclical redundancy check (CRC) for each data frame sent. The result from the ICV is added to the end of each data frame.

WEP is particularly sensitive to passive attack. Due to the small key size of 40-bits a passive attacker can gain the private key information through a small amount of statistical analysis. An attacker can also create the data required to crack the key by sending text to another host station and then waiting to grab the cipher-text and compare to the original plain text message to discover the private key. Hence, WEP only provides security against casual monitoring. 802.11i and WPA were initiated to create more security for the 802.11 standards. [7]

5. IEEE 802.11i and Wireless Protected Access (WPA): Security Enhancements

The intent of the 802.11i is to offer security characteristics that correct vulnerabilities discovered over the years within the original 802.11 standard and to create a robust security network (RSN). The 802.11i standard was approved in June 2004 but has only partially migrated to consumer products through the actions of a related group known as the Wi-Fi Alliance. The Wi-Fi Alliance took action before the 802.11i standard was completed in order to address the most serious shortcomings of WEP, including weak encryption, small key lengths and lack of key distribution and management methods. Working closely with the 802.11i team the Wi-Fi Alliance developed an interim solution known as the WPA standard, released in late 2002. Note that the Wi-Fi Protected Access (WPA) is a subset of 802.11i and has recently been updated to reflect the official 802.11i release.

In general, IEEE 802.11i can be separated into two broad categories: those mechanisms that have hardware available commercially today, and futuristic mechanisms that require development of new wireless hardware offering the greatest security. 802.11i/WPA contains mutual authentication between the host station and AP in place of the original standard offering only one way authentication from host to the AP. The authentication is managed through upper layer security mechanisms instead of the shared key technology discussed earlier from the original 802.11 standard. In addition, the same key management algorithms are included within 802.11i and WPA, dynamic keys that are periodically refreshed as an alternative to the original 802.11 standard of static keys.

The 2002 WPA standard focused on enhancing WEP through use of the temporal key integrity protocol (TKIP). IEEE 802.11i includes this TKIP as an optional but preferably temporary solution. Note that the TKIP is similar to the original WEP in that it utilizes the RC4 algorithm. Some equipment is available today under the “WI-FI” standard logo that supports the TKIP solution. This mechanism has been offered as the interim solution to major WEP shortcomings.

The more secure encapsulation mechanism developed through 802.11i/WPA is known as counter mode, cipher-block-chaining message authentication code protocol (CCMP). CCMP is enhanced from the stream cipher of the original 802.11 standard, but uses Advanced Encryption Standard (AES) instead of RC4. This technology is presently unavailable on the commercial market, but no doubt will shortly make an appearance.

Authentication: Upper Layer Functions

The 802.11i/WPA standard introduces upper layer functions through three components that are located outside the original standard itself. They are the IEEE 802.1X Port, the Authentication Agent (AA), and the Authentication Server (AS), as shown in Figure II-5 802.11i/WPA Basics. Note by using an 802.1X Port, the 802.11i utilizes the 802.1X standard for authentication and technically falls outside the 802.11 which is only a physical and MAC layer standard. 802.1X provides both authentication and key management. A wireless system deploying this upper layer suite is normally identified as a Wireless Protected Access (WPA) network.

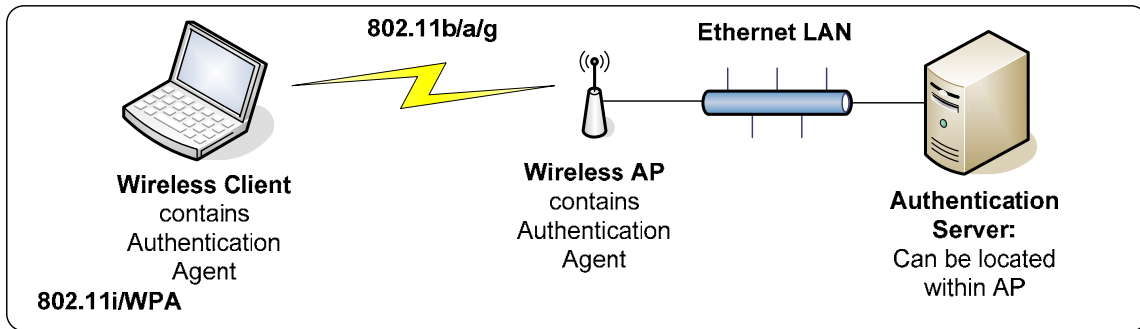


Figure II-5 802.11i/WPA Basics [7]

The 802.1X Port resides directly above the MAC layer of the 802.11. All traffic going through the MAC goes through the 802.1X Port. The second component, the AA resides above the 802.1X Port on each host station and within the AS on the network. The AA provides for authentication and key management utilizing protocols above the 802.11 and 802.1X to provide its services. The third component, the AS, resides within the network that participates in the authentication of all wireless host stations and APs. The AS communicates with the AA on each host station and the AP providing the information every station requires to authenticate every other station. Together these components determine when to allow traffic across an 802.11 wireless link as described next.

802.1X is a standard specifically developed for port-based network access control. It is based on the extensible authentication protocol (EAP). EAP is defined by RFC 2284 [8]. The EAP method describes three entities within the wireless network: supplicant, authenticator, and authentication server (AS) as described in Figure II-6 802.1X Basics. The 802.1X port within a system will be either a supplicant or authenticator. Any port established for access to network services takes on the supplicant role. The port allowing services to be accessed takes on the authenticator role. The authenticator utilizes the AS, which performs the actual authentication function. Note as stated above it is actually the AA of each supplicant and authenticator that communicates with the AS by exchanging EAP messages. In order to provide robust security the requirement is that both supplicant and authenticator authenticate each other before association and actual communication begins. Note that the AS may be co-located within the same system as the authenticator or it may be an external server.

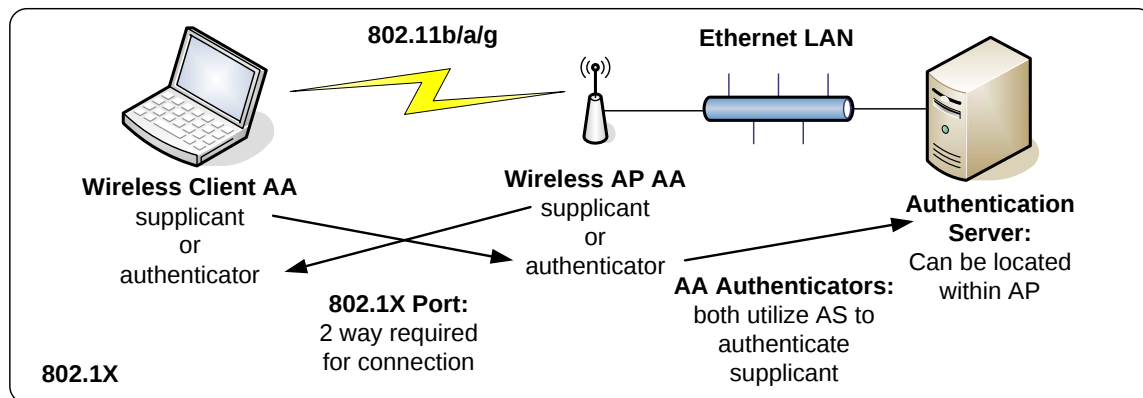


Figure II-6 802.1X Basics [7]

802.11i does not specify that EAP is mandatory. But, it is specified that the chosen 802.1X protocol must support an authentication algorithm that performs mutual authentication and key management based on the authentication. There are several 802.1X extensible authentication protocols used in commercial products. The following is a brief description of the four commonly used EAP methods:

- EAP-MD5 relies on and MD5 hash to pass authentication information for username and password to the RADIUS (Remote Authentication Dial-In User Server/Service) as the Authentication server. Since EAP-MD5 offers no other features over the standard IEEE 802.1X, EAP-MD5 is considered the least secure of all the common EAP standards. EAP-MD5 offers no key management or dynamic WEP key generation.
- LEAP (Lightweight EAP) is a proprietary standard developed by CISCO to be used in conjunction with 802.1X. LEAP accepts the username and password from the wireless client and transmits them to the RADIUS as the authentication server. LEAP conducts mutual authentication between the client and the server. LEAP also generates a unique WEP key for each client. Also LEAP requires the client to periodically log in for prevention of replay attacks.
- EAP-TLS (Transport Layer Security) outlined in RFC 2716 [9] defines the use of X.509, certificates to handle authentication. EAP-TLS relies on security in the transport layer to pass Public Key Infrastructure (PKI) information to EAP. EAP-TLS supports mutual authentication and generates dynamic one-time WEP key.
- EAP-TTLS (Tunnel TLS) is a proprietary product developed by FUNK SOFTWARE as an alternative for EAP-TLS. EAP-TTLS requires the user to provide username and password. The server authenticates to the user by certificates similar to EAP-TLS. [10]

In comparison with the 802.11i, the WPA standard more specifically delineates the incorporation of the 802.1X with the EAP protocol and specifies Radius technology

as the authentication server. RADIUS is a protocol that uses UDP packets to carry authentication and configuration information between the network access server (NAS) and the RADIUS Server. The authentication is based on the username, password, and, optionally, challenge-response. If the authentication is successful, the RADIUS server sends configuration information to the client. There are multiple RADIUS implementations including freeware as well as vendor-specific.

Figure II-3 displays the sequence of events that occur when a wireless client authenticates using 802.1X EAP-TLS. Two digital certificates are exchanged: one for the RADIUS server and one for the wireless client. The authenticator denies the wireless client access to network until authentication has succeeded and dynamic WEP keys have been established. [10]

Privacy

A message integrity code (MIC) introduced through the 802.11i/WPA standard is a data authenticity mechanism that proves more effective than the integrity check value (ICV) within the original 802.11 standard. The MIC is used within both temporary key integrity protocol (TKIP) and counter-cipher-block chaining medium access control protocol (CCMP). The MIC is a tag computed using a keyed cryptographic function. This tag is transported over an unprotected channel with the data it is associated with. The receiver verifies its value using the same key and cryptographic function used to encode it. The MIC is susceptible to brute force attacks, so each MIC failure is assumed to be an attack. The host station and AP are required to re-key after the first attack. Any station, host station or AP will stop all communications for 60 seconds on a second attack.

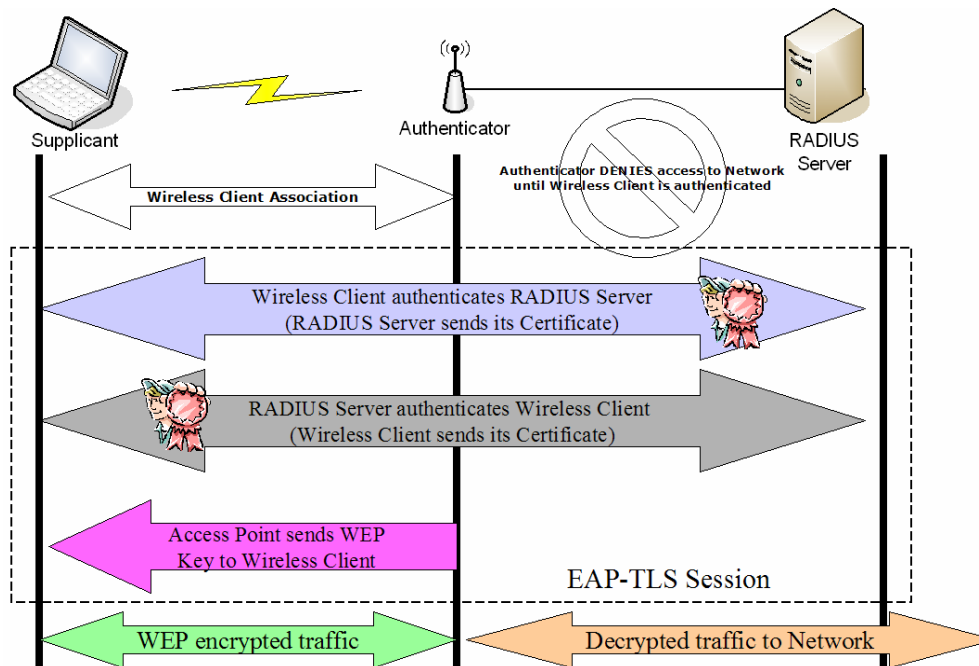


Figure II-3 802.1X Authentication Process [11]

Figure II-3 illustrates the steps described below:

- ①Wireless client Association—this is the start of the EAP exchange. Wireless client access is blocked until the client is authenticated. Server requests identity of client.
- ②The wireless client sends the certificate to the server. The server verifies the client certificate for validity. The client requests identity of server.
- ③The server sends the certificate to the wireless client. Wireless client verifies the server certificates.
- ④The server notifies the AP to either allow the client to connect into the network or deny the wireless client connection. If the client is allowed connection, a dynamic WEP key is generated and sent to the wireless client for encryption. [11]

TKIP was specifically designed for existing hardware devices supporting WEP. When utilized, TKIP elevates the privacy of an existing WEP wireless system. TKIP increases security by adding dynamic key management to replace the static key of WEP, and the 64-bit message integrity check (MIC). Given the size of the MIC, it provides protection against message forgery. TKIP also offers a TKIP sequence counter

(TSC) within the IV that drops packets delivered out of order as a form of replay protection. TKIP also uses a cryptographic mixing function to combine TSC, a temporal key, and the target address into the cryptographic key. Prior to 802.11i/WPA, WEP did not encrypt the IV at all, thus TKIP is less prone to attack.

Counter mode, cipher block chaining-message authentication code protocol (CCMP) provides all four security services: authentication, confidentiality, integrity, and replay protection. The CCMP is new to wireless technology through the 802.11i and, as stated earlier, requires new hardware development. It utilizes the AES encryption algorithm with a 128-bit key. CCMP combines counter mode (for confidentiality) and cipher lock chaining message authentication code (for authentication and integrity). A temporal key (TK) and pseudo-randomly generated number, or nonce, is required for each communication session. Also, additional authentication data (AAD) from the MAC header is included to provide extra integrity (MAC fields that vary are excluded). The MIC, described above, is included within the CCM process of encapsulation. Replay protection is incorporated into the process at the end of decapsulation when the receiver extracts the packet number for verification. As with TKIP, CCM provides for dynamic key management with the cryptographic keys. A fresh, never used, key is required at the start of each new session between AP and host station.

During the authentication process, as the host station and AP go into the association phase, the negotiation of the security parameters take place. The key exchange required for privacy takes place after mutual 802.1X authentication takes place. As described in the authentication section there are several handshakes between the supplicant, authentication agent, and authentication server. These are necessary to indicate that the link has been secured by the keys and allow normal data traffic. The handshake is performed using EAPOL (EAP over LAN). With CCMP the MAC is configured to discard data received over an association that is unprotected by the encapsulation algorithm. This is necessary or plaintext traffic could traverse the network with impunity. [7]

C. IEEE 802.11 Threats, Vulnerabilities, and Countermeasures

Threats are events or activities that have the potential to cause harm to information systems or networks. The term “threat” can apply to a myriad of events or activities, including environmental disasters, but here our interest in threat is on those threats associated specifically with wireless technology. In contrast, where threat implies an event or activity, “vulnerability” describes a weakness in, or absence of, precautions, exposing a potential for a threat to occur. In the past several years, we have seen vulnerabilities in wireless technologies that have lead to network attacks.

Wireless Threats

Wireless threats due to outsider attack are considered either passive or active. Passive threats are associated with attackers gaining access to an asset but not modifying its content. Active threats are associated with attackers gaining access to an asset and modifying its content.

Many wireless threats come from internal personnel, accidentally or intentionally. Often individual wireless users do not understand the danger they create merely by attaching an AP to a wired network. For instance, unauthorized APs can be easily deployed by anyone with access to a network connection, anywhere within the organization. These individuals may or may not be aware of the security policy and they may assume that a simple AP device could not increase the vulnerability of the overall network.

In addition, incorrectly configured APs offer a similar security threat. An AP out of the box in default mode works with no encryption and is commonly configured to openly broadcast SSIDs to authorized users. In some cases honest network administrators have incorrectly used SSIDs as passwords to verify authorized users. In this case a broadcast configured AP with no encryption activated would provide intruders with the “password” to operate on the organization network.

Authorized users can also threaten the availability of the network with abuses that drain connection speeds, consume bandwidth, and hinder a wireless LAN's overall performance. A few users who clog the network by trading MP3 files can affect the productivity of everyone on the wireless network. This affects all users of a network. These types of issues can be more difficult to identify and narrow down.

Overall, careless and deceitful actions by both loyal and disgruntled employees cause security threats and performance issues to wireless networks. These risks are only intensified by blatantly unauthorized APs, improper security measures, and network abuses present. This can occur with or without an organizational wireless policy in place.

Many of the threats described above are mitigated through sound security practices. Consistent, robust security practices are conveyed through a well prepared security policy. This greatly lowers a chance for a catastrophic active threat attack within the wireless network.

Wireless Vulnerabilities

It is common knowledge today that wireless technology includes numerous weaknesses. Wireless vulnerabilities stem from the general nature of wireless propagation as well as the protection mechanisms established to secure the data passing over a wireless network. The original definition of security within the 802.11 standard, Wired Equivalent Privacy (WEP) has been proven to contain weaknesses, making it inadequate for protecting networks containing sensitive information. Since the awareness of WEP vulnerabilities there has been a rush to mitigate the vulnerability associated with wireless security.

The intent of 802.11i/WPA is to alleviate most, if not all, of the original 802.11 standard vulnerabilities. When the mandatory CCMP 802.11i standard is implemented correctly, it will create a robust security system with wireless technology. It must be understood that the CCMP within 802.11i is new and complex, requiring a greater understanding of networking and security mechanisms within upper layers of the OSI model.

Additionally, a prepackaged solution for the CCMP 802.11i/WPA standard is not commercially available yet, although the optional TKIP 802.11i standard is presently offered on the market. Several companies such as Cisco, 3Com and Lucent have developed 802.1X EAP protocols and authentication servers compatible with the TKIP 802.11i/WPA standard. These that can be considered safe alternatives to the original WEP until the most robust CCMP 802.11i/WPA hardware is commercially available.

Although the 802.11i alleviates many existing vulnerabilities it is important to recognize the more serious weaknesses associated with WEP. The following sections describe existing security vulnerabilities with the original 802.11 security and suggested options available today to mitigate the risk.

WEP authentication: *Vulnerability*

WEP does not offer two-way authentication. WEP instead provides a method for authenticating host station machines through wireless to APs. There is no process for the AP to authenticate itself to the host station. The host stations can not have reasonable assurance that the wireless AP they are connected to is legitimate component of the organizational network. [7]

WEP authentication: *Solution*

The most robust option in this case would be to adopt the 2002 WPA standard that utilizes the 802.1X upper layer security suite. The utilization of the Authentication Server removes the authentication burden from the host station or the AP and places it in a separate entity within the network. As described in the 802.11i section for authentication, WPA offers a true two-way authentication. It requires a high level of IT competence to set up and operate.

A second option would be to purchase a vendor solution for a VPN that utilizes fairly secure encryption, such as IPsec. The VPN would force the two-way authentication before connection is established. Also, the AP and router on the wired side of the network would be configured to drop packets not configured for the proper IPsec connection.

Key management: WEP key management: *Vulnerability*

Key management is not specified in the WEP standard. This causes major threats to a wireless network from weak policy procedures. In order to use WEP within a network the WEP key must be manually distributed and individually programmed into APs and host stations throughout the group of wireless users. This manual management burden is intensified as the wireless APs are increased within an organization to support a greater audience.

Several weak key management policies can result in the introduction of vulnerabilities. Weak policy, vulnerability no. 1: Since manual WEP configuration can be burdensome sometimes WEP on each AP is disabled and the APs broadcast in the clear for ease of use. Weak policy, vulnerability no. 2: It can be a natural progression to lighten the management responsibilities by selecting one WEP key to share between all nodes and users of the network. Weak policy, vulnerability no. 3: Since synchronizing the change of keys is tedious and difficult, keys are seldom changed. Overall, without interoperable key management, keys will tend to be long-lived and of poor quality. [12]

Key management: WEP key management: *Solution*

The best option is to develop a comprehensive policy for wireless equipment and verify policy is obeyed. The policy must impose all the security requirements for APs and host stations. The IT department must document all personnel with authorization to access the wireless LAN, information on the specific computer used for access, private key information for APs, and when information is changed the files must be updated. For added security the policy should include written policy for the network security personnel to verify compliance on a regular basis.

Key management: WEP key size: *Vulnerability*

The original 802.11 standard specifies a 40-bit key size. The 802.11 standard was written in 1997. At that time it was expected a 40-bit key would be sufficient to protect against casual spying. In the past few years this 40-bit key has been cited as a huge weakness of wireless hardware.

It is known that an attacker that has access to both encrypted and plain text will be capable of deciphering the RC4 encryption stream, thus having the ability to decipher all future encrypted packets. Since the 40-bit key size is inadequate any attacker able to monitor traffic and can send traffic to induce a standard response from the intended victim, such as a ping reply. The attacker will then have enough information to recover the original cipher stream.

In response to this 40-bit key weakness, vendors today have implemented a configuration option that requires a key size of 104 bits. It is designated as a "128-bit"

WEP key. Selecting the WEP “128 bit” encryption option requires a 13 ASCII or 26 hexadecimal digit character key. In comparison the 40-bit WEP selection requires an 8 ASCII or 16 hexadecimal digit character key. As would be expected, the 104-bit keys are more resistant to brute-force attacks. But, it does not greatly increase the overall security of WEP. It can be cracked by passive sniffing of network packets given a persistent individual. In addition, WEP must still be enabled on the equipment when installed. [12]

Key management: *Solution*

Today’s best option is to purchase the temporal key integrity protocol (TKIP) upgraded wireless equipment present within the 802.11b/a/g equipment. This equipment is 2002 WPA compliant and offers the highest form of wireless security on the market today. It will provide interim strengthening corrections for WEP through the TKIP and also offers two-way authentication between AP and host stations. It must be noted that it proves weak against forgery and man-in-the-middle attacks.

Initialization Vector is too small: *Vulnerability*

WEP’s associated RC4 encryption key includes a 24-bit initialization vector (IV). The encryption key is constant for each encrypted packet and the IV is used to further differentiate the individual packet transmissions through the 802.11 concatenation process. Note the IV is sent in the clear with each packet. Several attacks are possible through the small size of the IV and the astronomical number of packets sent over the network for daily communications.

The IV size of 24 bits provides for a possible 16,777,216 different RC4 cipher streams for a given WEP key. The same plaintext encrypted with the same key will always result in the same ciphertext. Thus, when an IV is used more than once with a given RC4 cipher stream it creates a linear encryption pattern that can be computed through statistical analysis. In addition, IVs can be created that are weaker in nature and expose the RC4 cipher stream to a greater extent, thus limiting the true number of true IV choices. [12]

Initialization Vector is too small: *Solution*

Purchase of the temporal key integrity protocol (TKIP) upgraded wireless equipment present within the 802.11b/a/g equipment will protect against this weakness. The 2002 WPA compliant wireless equipment provides strengthening corrections for WEP. It must be noted that WPA proves weak against forgery and man in the middle attacks.

Integrity Check Value algorithm not secure: *Vulnerability*

The WEP integrity check value (ICV), based on CRC-32 (cyclic redundancy check) is intended to detect random errors within transmissions. The intent behind CRC is to offer redundant frame information in order for the receiver to verify data has not changed over the transmission. ICV is not associated with cryptographic security and is incapable of protection against malicious inaccuracies.

For instance, in a bit-flipping and replay attack an attacker can utilize the linear nature of ICV in order to flip bits and recalculate the new ICV CRC-32. This modified packet, even though it has not been deciphered by the attacker, is then sent through an AP with a known IV. The AP will forward the modified packet through given that the ICV is correct. A layer 3 device from the network will produce a rejection since the packet is not truly valid. The rejection will be sent back through the AP to the attacker. Since the rejection is predictable the attacker can compare the prediction with the encrypted response and derive the cipher stream of the RC4 key. [12]

Integrity Check Value algorithm not secure: *Solution*

TKIP and the future CCMP offer a Message Integrity Code (MIC) along with a slightly different procedure protecting against retransmission attacks. Therefore, TKIP-upgraded wireless equipment within the 802.11b/a/g (2002 WPA compliant) equipment will prevent ICV vulnerabilities found in WEP. [12]

MAC Address filtering as sole wireless security measure: *Vulnerability*

In the rush to move away from WEP and its supposed weakness, many organizations have implemented Media Access Control (MAC) filtering as the sole wireless AP security measure. By definition, each MAC Addresses is globally unique.

Users not explicitly authorized by their MAC Address from becoming associated with the network would be rejected by the AP.

Although this seems a reasonable concept, MAC filtering proves ineffective against unauthorized intrusions from MAC Address spoofing. An attacker possessing hardware and software capable of sniffing a wireless network can easily capture all packets between nearby APs and their host stations. This captured data contains all information required to connect to the wireless LAN. MAC Address spoofing software is also readily available to anyone with internet access. The spoofing software allows the user to easily rewrite normal address resolution protocol (ARP) packets with an authorized MAC Address instead of the MAC Address configured into the attacker's host Network Interface Card (NIC). [13]

MAC Address filtering as sole wireless security measure: *Solution*

An option is to purchase the temporal key integrity protocol (TKIP) upgraded wireless equipment present within the 802.11b/a/g (2002 WPA compliant) equipment that supports MAC filtering in addition to the WPA. When used together, they form a fairly effective security solution. It is important to activate the WPA since MAC Address filtering alone is easily overcome by spoofing. It is also important to practice other sound security practices with WPA.

III. NAVAL POSTGRADUATE SCHOOL WIRELESS CASE STUDY

A. Naval Postgraduate School Wireless Plan

In early 2001, Naval Postgraduate School (NPS) planned to extend its wired network with an industry-standard wireless local area network by the fall of 2002. The goal was to have a wireless infrastructure to support multiple platforms (e.g., Personal Digital Assistance (PDA), and laptops) and multiple operating systems (e.g., Microsoft Windows, MAC OS, and Linux). Also NPS wanted the wireless infrastructure to be scalable, seamless, and reasonably secured, despite the fear, uncertainty, and doubts regarding wireless vulnerabilities. [14] In practice, this ambitious endeavor exceeded their ability to rollout a secure wireless infrastructure as planned. Although constrained by budget, leadership pressure, and perceived urgency for wireless functionality, the NPS IT department put together a wireless security solution utilizing currently available industry capabilities. Early in the wireless planning, the NPS Wireless Warrior Group was established and tasked to write the NPS Wireless Policy, conduct surveys, determine wireless requirements, analyze the wireless networks, and assist in the roll out of wireless at NPS. This group is still function in an advisory role today.

1. The NPS Wireless Warrior Group

The Wireless Warrior Group is comprised of students, faculty, and staff members who have an interest in wireless technology. Their first assignment was to write the wireless policy. The NPS wireless policy derived from careful review and analysis of wireless policies of prominent campuses (e.g. such as Carnegie Mellon University (CMU), Columbia, Drexel, Massachusetts Institute of Technology (MIT), Harvard, Wake Forest, American University, West Point), as well as review of the draft version of the Department of Defense (DoD) “wireless use” policy that was recently approved in April 2004. From those policies and local security considerations, NPS derived its own wireless policy, IT 202, in February 2002.

The goals of the policy are to limit the potential wireless security risks, educate the users to the benefits of wireless, and to establish NPS wireless network standards. The policy also provides guidelines (see Figure III-1) for the registration and

purchase of new departmental wireless APs to ensure interoperability, security, and manageability.

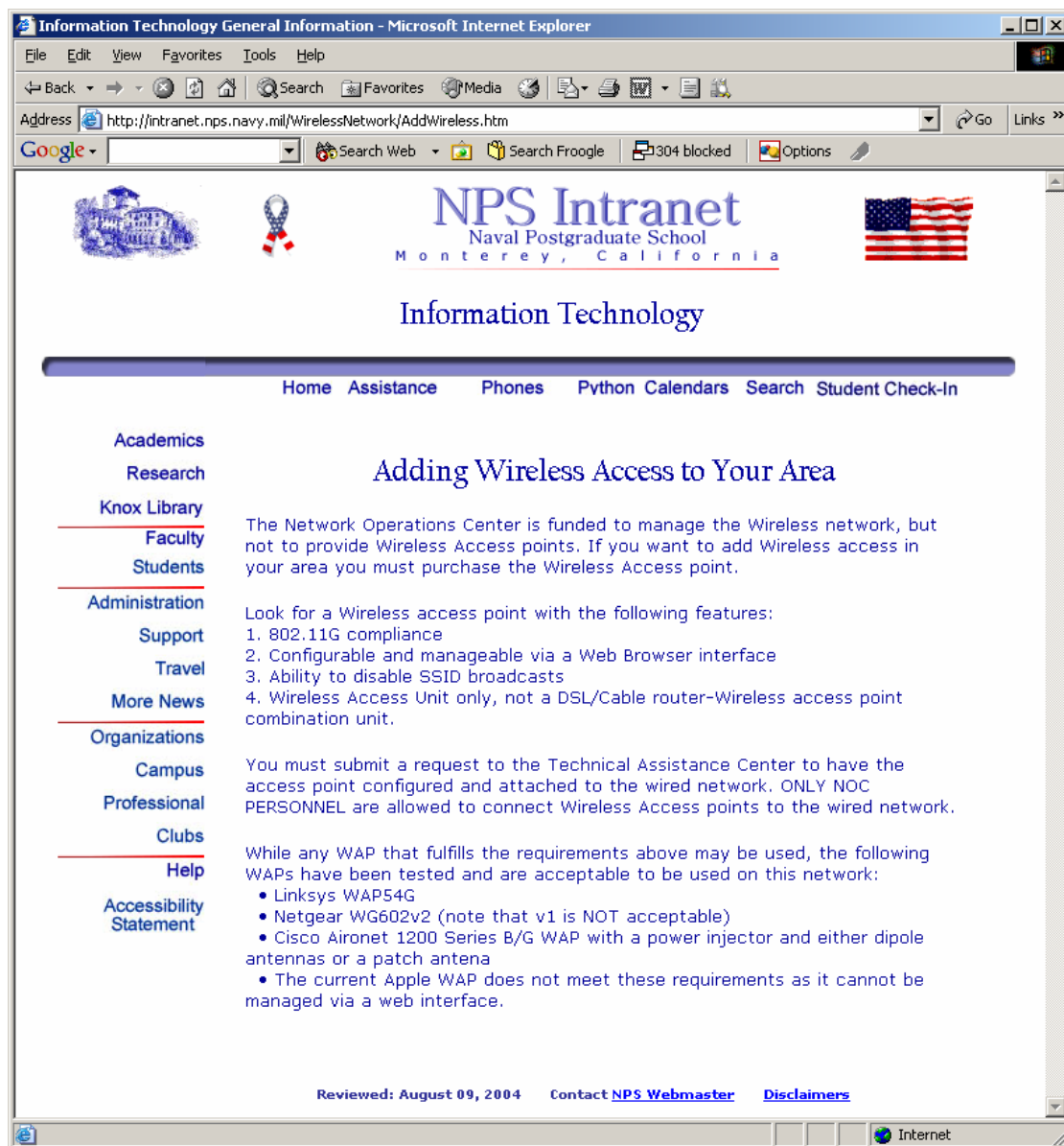


Figure III-1 AP Installation and Purchase Guideline [15]

2. NPS Wireless Requirements

While drafting the wireless policy, NPS conducted two identical on-line surveys (see Figure III-2). The first survey ran for 14 days from November 23 thru December 7th, 2001 with 250 individuals out of 1339 possible participating. Ten months later, the second survey ran for 10 days from August 28 thru September 6th, 2002 with

208 individuals out of 1285 possible participating. The results of the two surveys were almost identical.

Most of the participants believed that wireless would add value, productivity, and usability to their research and studies. The surveys also revealed the participants strong concern about wireless security, as well as a strong desire for wireless access to email, web, and file transfer functions.

The requirements for the NPS wireless implementation were derived from a variety of input, including the experience collected from other universities, NPS wireless meetings, DoD requirements, and the NPS user surveys. Major requirements are listed below [14]:

- For geographic coverage, NPS wireless system shall cover the entirety of the NPS campus
- For 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 La Mesa and Fort Ord military housing area.
- For hardware and software, NPS shall choose non-proprietary, interoperable systems that conform to accepted industry standards.
- For availability requirements NPS systems shall provide a 50% AP overlap with reference to projected propagation and 99.99% availability.
- For encryption and authentication, NPS systems should be FIPS 140 encryption certified (AES or 3DES) and extendable to include PKI for authentication.

Code 32 - Microsoft Internet Explorer provided by Compaq

File Edit View Favorites Tools Help

Address <http://www.nps.navy.mil/code32/survey.asp>



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

Academics
Research
Executive Education
Students
Faculty
Administration
Alumni & Friends
Library
Search
About
Disclaimers

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-fundamentally relevant

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

Should you have any questions or concerns please do not hesitate to email [Joseph L Roth](#)

Done

Figure III-2 NPS Wireless Survey [15]

3. NPS Wireless Pilot Program

In February 2002, with an approved wireless policy and a defined list of requirements, NPS rolled out a wireless pilot program with 30 APs installed throughout the campus. In September 2003, NPS enhanced its wireless security by requiring that the WEP key be changed quarterly, which is posted on a secure website on the NPS intranet. NPS also enhanced its wireless security by increasing the WEP key encryption from 64-

bit to 128-bit. Figure III-3 depicts an initial architecture of the NPS WLAN roll out as of August 2002. The security functions for this WLAN are provided by WEP at the AP.

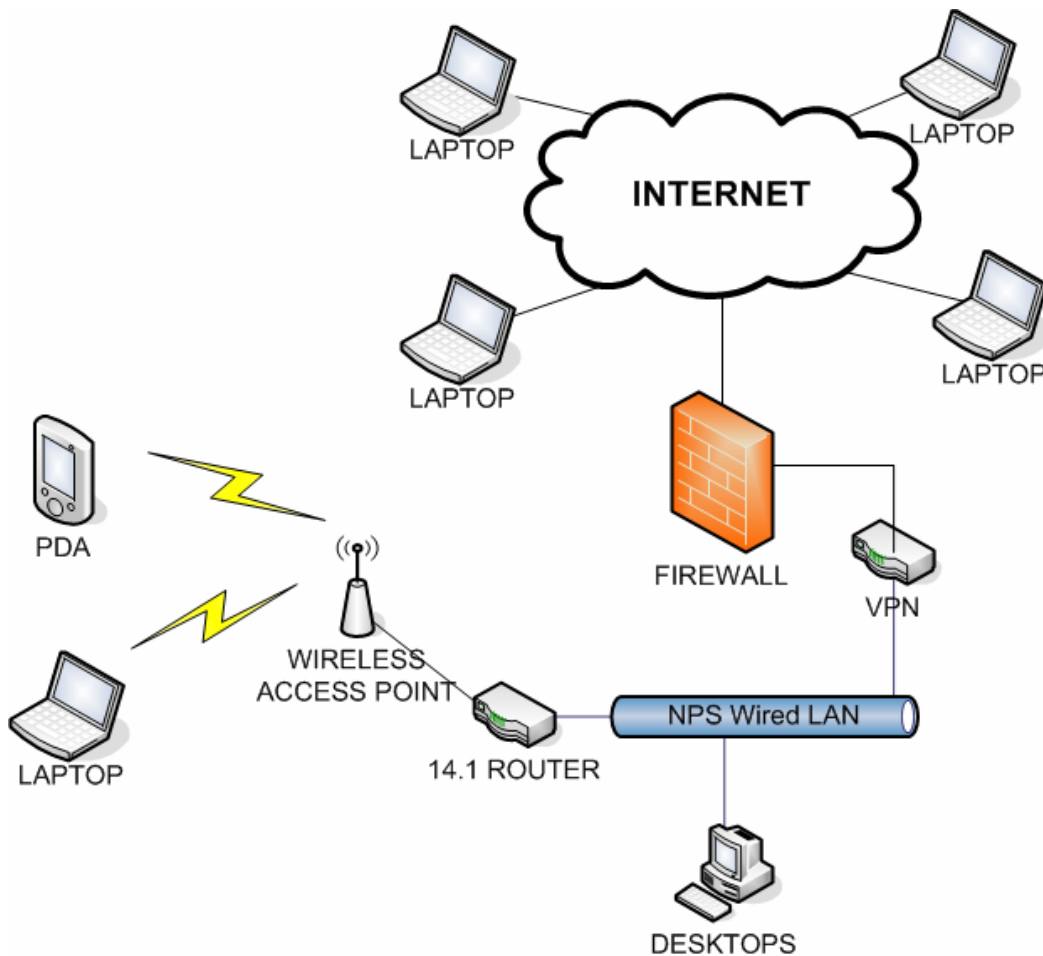


Figure III-3 Initial NPS WLAN Infrastructure [14]

In order to connect to the network, all wireless users must register their mobile devices with the campus-wide IT Management Department, ITACS (Figure III-4). All users must provide their laptop and wireless interface card MAC addresses to ITACS. These are required for audit purposes rather than for access control. ITACS verifies the users' devices for up-to-date patches, critical updates, and the latest virus definitions. If the system is not conformant, ITACS installs the latest patches, critical updates, and virus definitions. Once ITACS has hardened the device, the WEP key and SSID are installed. The user's *username* and *password* are logged into the LDAP server for the purpose of authentication. Also, the user *username* is added to the "wireless email" distribution list.

The original intent was that every quarter, wireless users will be sent an email notification with a link to a secure web site to retrieve the new WEP key and SSID. In conjunction with the new WEP key and SSID, all users are required to change their passwords according to network security policy. In actuality these quarterly requirements have not been implemented.

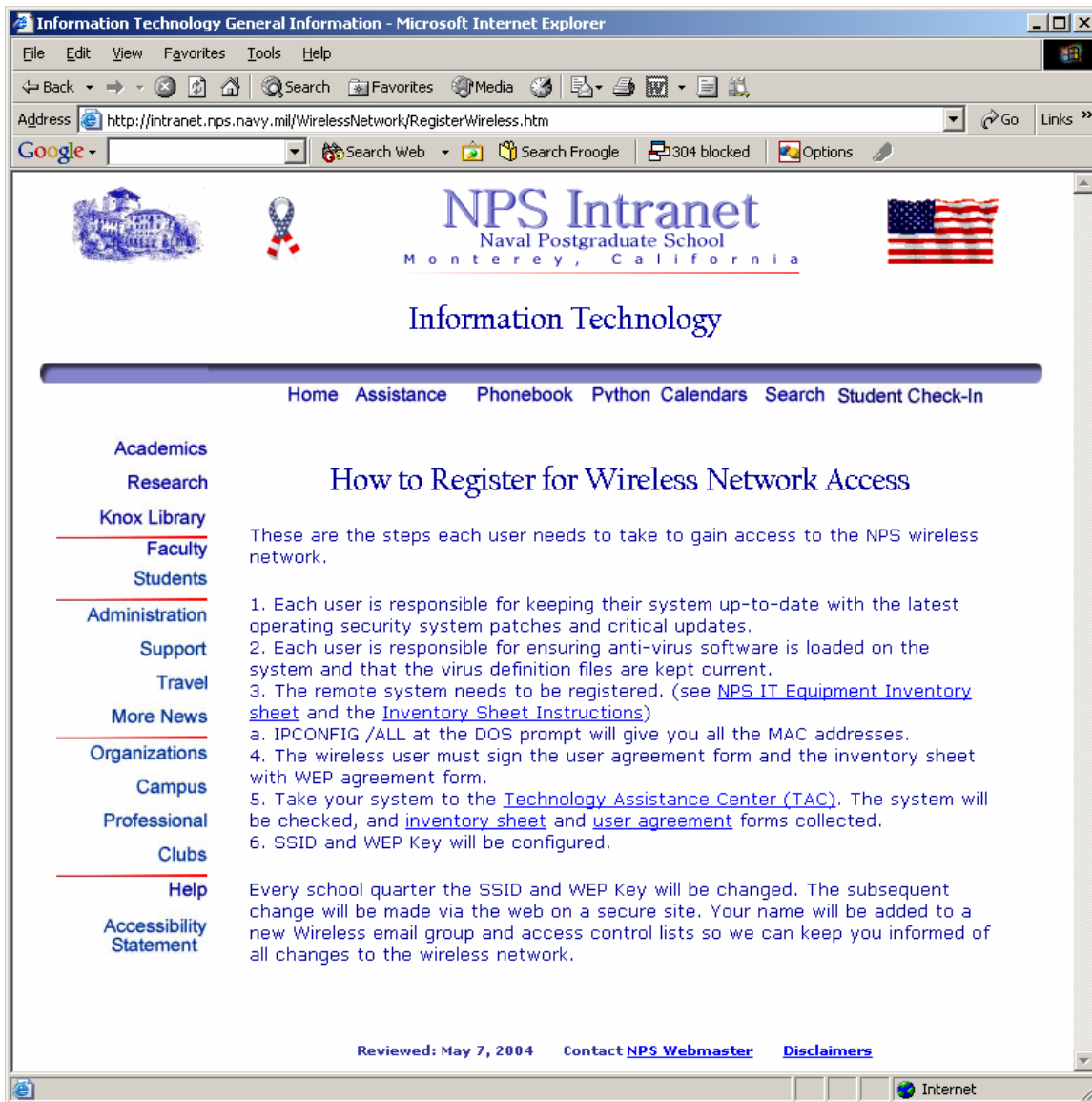


Figure III-4 Registering for Wireless Access Guidelines [15]

4. Current NPS WLAN Infrastructure

NPS examined several WLAN security solutions before selecting one (see Table III-1). CISCO offered 802.1X and LEAP authentication for their security solution,

but LEAP is a CISCO proprietary protocol. CRANITE offered EAP-TLS as its authentication protocol and a proprietary encryption solution using AES. Yet, EAP-TLS requires a PKI infrastructure and NPS decided PKI authentication was too burdensome for the client in the near term. FUNK offered EAP-TTLS as the authentication protocol and required IEEE 802.1X and RADIUS but NPS has chosen not to implement the IEEE 802.1X standard at this time. Finally, Fortresstech offered a proprietary authentication mechanism using an AES and 3DES encryption solution but once again NPS sought a non-proprietary solution. The ReefEdge product offered interoperability with the existing NPS IT infrastructure, involved no proprietary authentication or encryption scheme, and met the NPS IT budget.

Vendors	Security Solution
www.reefedge.com	Offers SSL authentication and 3DES encryption solution
www.cisco.com	Offers 802.1X and LEAP authentication
www.cranite.com	Uses EAP-TLS as its authentication protocol and implements a proprietary encryption solution using AES
www.funk.com	Offers EAP-TTLS (requires 802.1X and RADIUS)
www.fortresstech.com	Implements proprietary authentication mechanism and uses AES and 3DES encryption solution

Table III-1 WLAN Security Vendors and Security Solutions [14]

NPS relies on a username and password for its authentication method. Authentication of wireless users is accomplished between a Remote Authentication Dial-In User Service (RADIUS) server and the Lightweight Directory Access Control Protocol (LDAP) server. In order for wireless users to connect to the NPS network, the users need know the AP's SSID and the WEP key, both of which are posted on the NPS intranet website.

The NPS LAN infrastructure was enhanced by adding an Intrusion Detection System (IDS) and a RADIUS server, Figure III-5. The Intrusion Detection System is capable of real-time monitoring for rogue APs as well as for network attacks. Figure III-5 displays a conceptual interpretation of the NPS network.

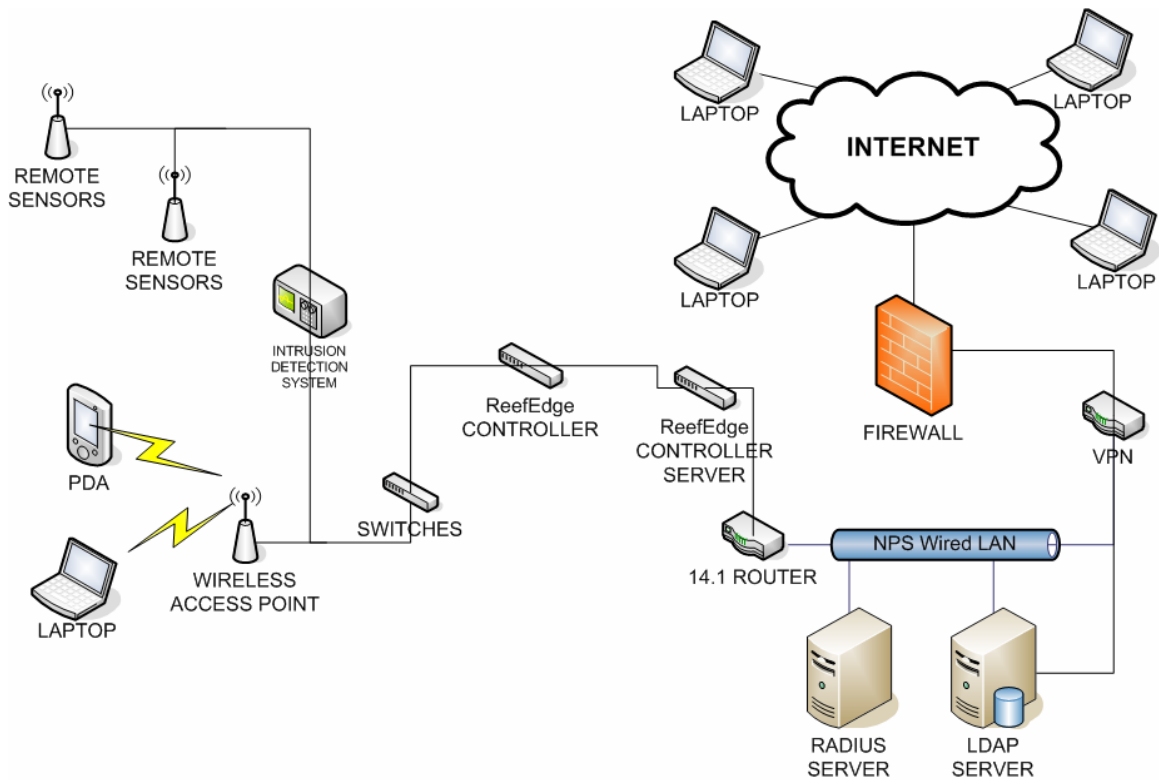


Figure III-5 NPS Current WLAN Infrastructure [14]

B. NPS WIRELESS NETWORK VULNERABILITY ASSESSMENTS

After NPS completed the initial wireless LAN implementation, it conducted three passive vulnerability assessments of the NPS wireless LAN using the network analysis tools shown in Table III-2.

On February 16, 2002 NPS conducted the first network analysis using NetStumbler. Some of the results are shown in Figure III-6. NetStumbler was able to capture the APs MAC addresses, identify beaconing APs SSIDs, and identify WEP enabled APs. The results of the passive monitoring revealed that for 8 out of 13 APs WEP was not enabled for one reason or another. All of the APs monitored were broadcasting their SSID.

The APs depicted in Figure III-6 that are blank under the WEP column are the most vulnerable APs since they did not have WEP encryption enabled. Without WEP enabled, an unauthorized person can connect to the internal network without WEP authentication. Note that the columns MAC address and SSID are obscured for privacy reasons.

Tools	Features
NetStumbler http://www.netstumbler.com	Identifies AP MAC addresses, SSID if broadcast, transmitting channel, manufacturer, status of WEP (on/off), etc
Mini-Stumbler http://www.netstumbler.com	Handheld PC version of NetStumbler
AirSnort http://airsnort.shmoo.com/	Same as NetStumbler plus the ability to break WEP
AirMagnet http://www.airmagnet.com/	Same as NetStumbler plus it detects the SSID even when not broadcast
Ethereal http://www.ethereal.com	Freeware network protocol analyzer for Unix and Windows. It allows examination of data from a live network or from a capture file on disk. Users can interactively browse the capture data, viewing summary and detailed information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session.
VxSniffer http://www.cam.com/vxsniffer.html	Eavesdrop to obtain MAC address for spoofing

Table III-2 Network Protocol Analyzer Tools [14]

After the first assessment, an education campaign was launched to raise and to improve wireless security awareness with the help of the NPS IT support staff. Three months after the vulnerability testing, NPS conducted the second vulnerability assessment, again with NetStumbler. This time, the results were much better. The number of broadcasting SSIDs was reduced and all were using WEP. It is apparent that, in order to reduce vulnerabilities, all wireless users need to be trained in wireless security measures and the requirements of the wireless policy.

Network Stumbler - [20020613130116.ns1]

MAC	SSID	Name	Ch...	Vendor	Type	WEP	SN...	Signal+	Noise-	SN...	Latitude
00:0E:32:55:55	default		7		AP			-76	-105	26	
00:1C:12:5D:A8	TNT		6	Agere (Lucent) WaveLAN	AP			-93	-98	4	
00:2D:38:9F:5B	CA255GROUP	APC...	11	Agere (Lucent) Orinoco	AP			-88	-105	15	
00:2D:44:A5:53	E1110GROUP		1	Agere (Lucent) Orinoco	AP	Yes		-92	-96	4	
00:1C:1F:55:52	idles		1	Agere (Lucent) WaveLAN	AP	Yes		-78	-103	21	
00:2D:02:79:E	CA922USA		9	Agere (Lucent) Orinoco	AP			-77	-104	27	
00:FE:70:56:3	Lanewd		6		AP			-80	-106	25	
00:2D:3A:C8:7	ES754GROUP		11	Agere (Lucent) Orinoco	AP			-82	-100	17	
00:1C:21:CF:5E	00000M4		7	Agere (Lucent) WaveLAN	AP			-90	-102	12	
0A:0B:02:31:04:A	NetAP-335		7		AP			-88	-102	11	
0A:0B:02:3C:05:6	5400T5754W54LA...		7		AP	Yes		-92	-103	11	
00:40:00:00:3E:A	default		7	Gemtek (D-Link)	AP			-84	-108	21	
00:2D:05:0D:18:4	WAFSTAR_11b		1	Agere (Lucent) Orinoco	AP	Yes		-93	-99	5	
00:FE:70:5A:C3	Lanewd		6		AP			-94	-106	12	
00:2D:05:0A:27:3	EB450GROUP		1	Agere (Lucent) Orinoco	AP	Yes		-87	-97	10	
00:2D:08:99:02	WaveLAN Network		3	Agere (Lucent) Orinoco	AP			-87	-105	16	
00:2D:08:96:25	WaveLAN Network		3	Agere (Lucent) Orinoco	AP			-93	-103	10	
00:2D:0A:72:71	wireless-LAN		7	Agere (Lucent) Orinoco	AP	Yes		-93	-96	3	
0A:0B:05:2C:46	JRSTATION		11	Cisco (Aironet)	AP	Yes		-80	-107	25	
00:70:10:55:49	tdRoutepu		1		AP			-87	-99	12	
00:2D:1E:11:52			11	Agere (Lucent) Orinoco	AP	Yes		-80	-104	20	
00:2D:1E:12:24			6	Agere (Lucent) Orinoco	AP	Yes		-82	-104	21	
00:74:00:07:1E:7	default		6		AP	Yes		-80	-106	26	
00:74:00:05:55:9	TME-NET		6		AP			-86	-101	15	
00:09:10:58:01	conega WL_PCC-11		1		AP			-83	-103	15	
0A:0B:05:44:0D	chinkatou		7	Cisco (Aironet)	AP	Yes		-89	-100	8	
00:FE:70:5A:FE	Lanewd		6		AP			-88	-105	17	
00:2D:08:9A:FC:D	00000AuTayo		5	Agere (Lucent) Orinoco	AP			-88	-98	10	
00:2D:08:9C:33	nechi		11	Agere (Lucent) Orinoco	AP	Yes		-93	-96	3	
0A:0B:02:4C:31:F	default		6		AP			-81	-105	24	
00:CC:11:22:FE	Geonixware		1		AP			-93	-98	5	
0A:0B:02:3C:D7:6	idles		7		AP			-83	-107	24	
0A:0B:02:31:ED:8	default		1		AP			-76	-104	21	
00:2D:3E:A8:54	00000GROUP		7	Agere (Lucent) Orinoco	AP			-87	-97	10	
0A:0B:02:39:4C:D	default		7		AP			-87	-105	18	
00:1C:05:0E:52:9	7C471AGROUP		1	Agere (Lucent) Orinoco	AP			-92	-93	1	

Ready Not scanning GPS: Disabled 106 / 106

Note: certain columns have been obscured purposely

Figure III-6 NetStumbler Example [14]

Three months later on August 2002, a third vulnerability assessment of NPS wireless network was conducted using the Pocket PC version MiniStumbler, AirSnort and AirMagnet tools. This time around MiniStumbler captured 8 MAC addresses, AirSnort captured 18 MAC addresses, and AirMagnet captured 53 MAC addresses.

In the fall of 2003, NPS purchased the AirMagnet Distributed 4.0 system, which is an around the clock network protocol analyzer and monitor system. As of today, the system is running and provides a huge amount of network information. Unfortunately the NPS IT department does not have enough IT personnel to monitor and analyze all of the data collected by AirMagnet Distributed System. Network security for the NPS wireless network continues to be a delicate balancing act between updated technology and having a large enough, adequately trained manpower group to monitor and analyze the information and react to attacks in real time. [14]

IV. FAA IT INFRASTRUCTURE

The Federal Aviation Administration (FAA), which is responsible for the safety of civil aviation, provides a safe, secure, and efficient global airspace system that contributes to national security and the economy. The FAA is divided into nine regions with regional headquarters from Anchorage, Alaska to Atlanta, Georgia, see Figure IV-1. The agency's two largest Research and Development Center facilities are the FAA Mike Monroney Aeronautical Center (MMAC) at Oklahoma City, Oklahoma, and the William J. Hughes Technical Center (WJHTC) at Atlantic City, New Jersey.

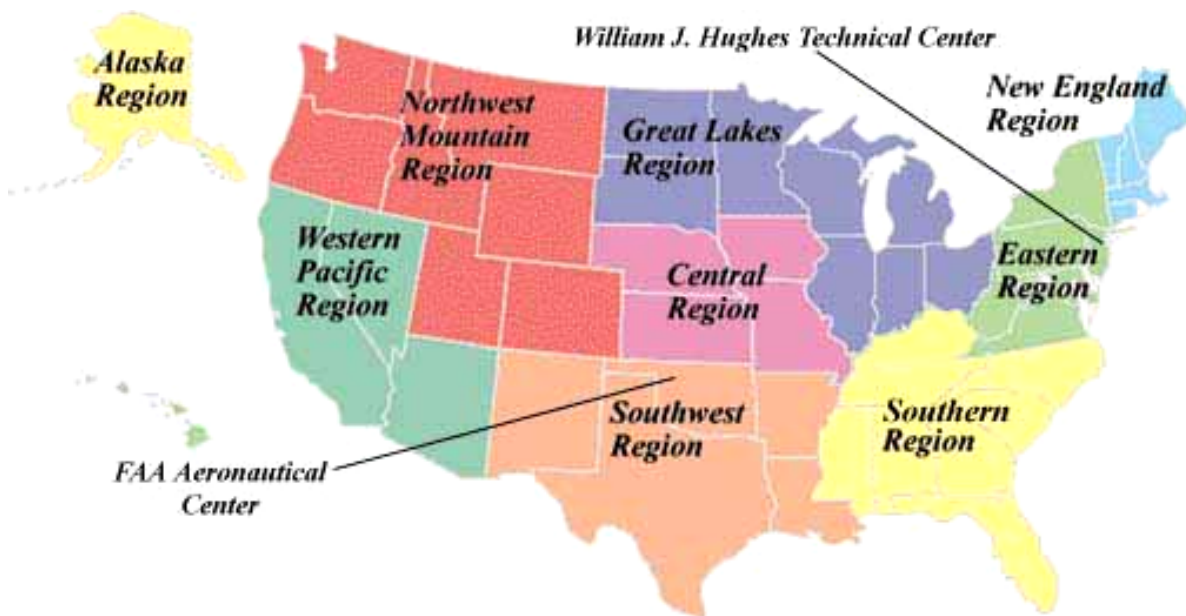


Figure IV-1 FAA Regional Locations [16]

The WJHTC is the model for analysis of the FAA IT infrastructure. The WJHTC is the FAA's vital research, development, test and evaluation facility. The aviation research focus is on air traffic management, communications, navigation and surveillance, airport and aircraft safety, and aviation security. Its unique facilities include: air traffic control laboratories and an air traffic simulation facility; a human factors laboratory; weather laboratories; a fleet of specially instrumented aircraft, ranging in size from small planes to helicopters and large transports; the world's largest full-scale aviation fire test facility; a chemistry laboratory; an impact test facility; radar test laboratories; the National Airport Pavement Test Facility; and an aviation security

laboratory. The WJHTC not only serves as a cornerstone for aviation advancements, but is also a key focal point for Homeland Security.

A. WJHTC Current IT Infrastructure

The WJHTC consists of over 15 internal offices from The Office of Enterprise Performance (ACF) that provides performance and financial planning, develops policies and strategies to the Information Security Group (ACB-250) that identifies, evaluates and proposes candidate technical security solutions for both existing (legacy) and future (acquisition) systems.

The WJHTC utilizes Windows 98, 2000, NT and XP (Professional) operating systems in support of operations, administration, and research. The network file server is supported by Novell NetWare and Microsoft Windows NT. For remote dial-in access to the Internet and access to e-mail while traveling, the WJHTC provides Mobile Citrix for their employees to stay connected to the office.

The example in Figure IV-2 offers a conceptual illustration of the internal network of the WHJTC. This model indicates the security posture of the WHJTC utilizing firewall, DMZ,outers, and switches. For security reasons, Figure IV-2 is only a representation of the WHJT Center internal network and not its actual layout.

B. Wireless Deployment Considerations at FAA

The foremost goal of the FAA with respect to wireless technology is to increase productivity in its processes and employees while maintaining security. This must be accomplished through a transition process that maintains a high security position. To meet this end the FAA transition process must be developed through careful consideration of any unique FAA mission needs in conjunction with commercial best practices and policy requirements.

There are unique requirements associated with wireless implementation that must be addressed by the FAA in order to support the transition to wireless technology. For instance, a comprehensive site survey for wireless hardware implementation will be necessary to ensure complete coverage within the designated area. The site survey must also document the capability required by the hardware to provide satisfactory density and network throughput for the targeted area and wireless host located within it. Another

requirement the FAA may choose to impose would be that WLAN technology be centrally managed to ensure the protection of the FAA's network resources.

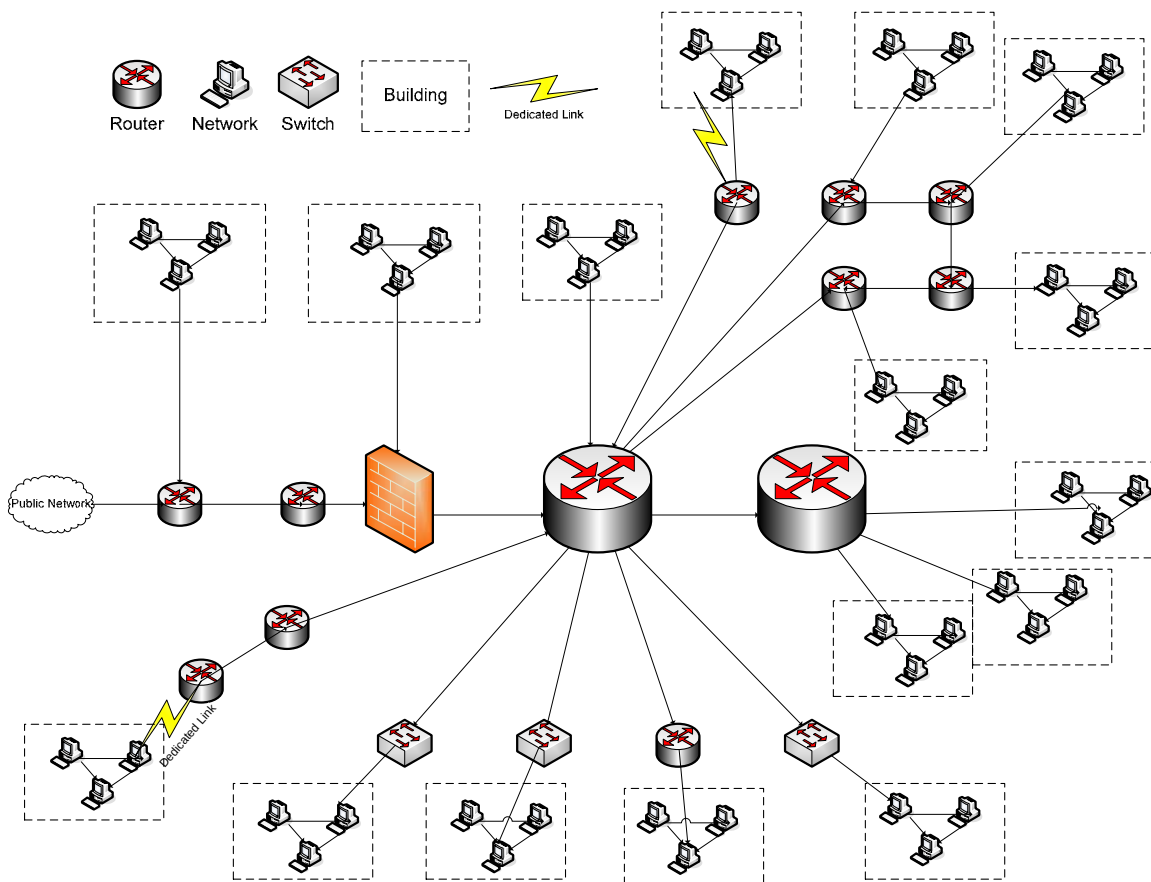


Figure IV-2 WJHTC IT Network Representation

In addition, customer support services will need to include wireless support, from technical to administrative issues. This may include creation and ongoing maintenance of wireless support web pages within the WHJTC web site. For example, the web space could provide policies, operational status of the FAA wireless infrastructure, reference materials and how-to guides.

Finally, it must be understood that specific implementations, as well as the scope and goals of wireless deployment at FAA, will need to be addressed by the FAA CIO. The CIO must decide how to strategically and efficiently utilize wireless technologies in accordance with the FAA's mission. The next chapter will explore wireless policy and best practices. It is an essential first step for the success of wireless initiatives.

This Page Intentionally Blank

V. WIRELESS POLICY RECOMMENDATION

A. Introduction

The FAA is presently under FAA Order 1370.82 Information Systems Security Program dated June 9, 2000. [17] In response to the United States Computer Security Act of 1987, this Order establishes the policy to ensure computer security implementation within the FAA and assigns organizational and management responsibilities. FAA Order 1370.86 AVR information Systems Security Protection dated March 1, 2001, establishes minimum requirements for Information Systems Security Protection and describes the implementation of security policy for the FAA. [18]

The focus of this chapter is to provide a foundation for development of an FAA wireless policy prior to wireless implementation. This document has described major technologies behind wireless communications, some of the threats and weaknesses with suggestions to mitigate them, and a selection of wireless tools for deployment. We have also described the deployment of wireless communications at NPS and the IT architecture at the FAA WHJT Center. This chapter describes the essential elements of a wireless security policy.

B. Wireless Security Policy

Development of a wireless policy, in addition to existing security policy, will greatly facilitate the introduction of wireless technology into an organization. Wireless defense mechanisms incorporate many existing IT security implementations, yet wireless technology, by its nature, increases the requirement for new protection techniques. By developing a wireless policy, an organization is actively contributing to its computer security. Development of the wireless policy as a prerequisite to wireless implementation offers a well-organized evolution to the process of introducing wireless technology.

In general, a security policy must be understandable, realistic, consistent, enforceable, visible, flexible, and it must be periodically reviewed as described below:

- *Understandable* — The policy must be easy for users to comply with. Stay away from ambiguous terms to prevent users from misinterpretation.
- *Realistic* — Understand the organizational priorities for securing its data and the amount of communications required by its personnel to share the data. It

is important the policy meet business, technological and security needs simultaneously. A security policy must strike a balance between functionality and security.

- *Consistent* — It is important to maintain consistency with the policy. Policy should not change often or it will add confusion to personnel.
- *Enforceable* — Policy must have the full support of all management levels. If consequences are not applied equally when personnel are found in noncompliance the policy is effectively irrelevant.
- *Visible* —Users must be aware of the policy and understand it for it to be effective.
- *Flexible* — The policy should permit adaptation to the ever-changing world of technology and people.
- *Reviewed* – The policy must be maintained by reviewing it on a recurring basis in order to prevent the information from becoming obsolete. [19]

1. Considerations for Wireless Policy

The wireless policy will be developed similar to any IT security policy. For instance, definition of the security goals and objectives as well as the identification of authority and their responsibilities, is foremost to a wireless security policy. Effective wireless security policy within an organization will encompass procedural controls in addition to technological restraints. In perspective, there are affects from wireless technology that require special consideration during the wireless security policy development. For the sake of brevity, the following sections describe fundamental policy considerations that are applicable to wireless networks:

Risk Assessment

Risk assessments are imperative to the development of a well-planned wireless security policy. The vulnerabilities and threats applicable to wireless technology should be identified and investigated for the possible damage an associated attack(s) would cause to the organization. Additionally, each threat and vulnerability should have mitigation strategies developed and evaluated. Risk mitigation information acquired during this period will contribute to the design segment of the wireless implementation.

Ad Hoc versus Infrastructure

It is more difficult to regulate security within an *ad hoc* network. For this reason, an organization may consider using the wireless security policy to deny use of all *ad hoc* configurations within a wireless network. If the organization chooses to allow *ad hoc* as a benefit to its employees it would behoove them to place boundaries on the *ad hoc* standard and implementation through strict policy. [20]

Information Classification

It may be important for an organization to analyze the information it processes and establish categories for information management. Introduction of wireless technology may require the organization to evaluate additional policy requirements on certain categories of its data. Keep in mind that in a wireless environment, the risks will most likely always outweigh any benefit of allowing sensitive organizational data onto wireless segments. For instance, in order to protect from compromising sensitive data it may require policy of no sensitive data on wireless segments.

Network Segregation

A common technique for a wireless design within an organization is separate and distinct wireless and wired networks. Wireless segments must connect to a wired network at some point to allow Internet or Intranet communications. In order to successfully maintain separation, the connection of these networks should be separated by a gateway so that wireless communications only traverse wired network when absolutely necessary, Figure V-1 Example of a Segregated Wireless Network. In addition, the organization may even decide to develop policy to require a network firewall between the wired and wireless portions of the LAN as an added safeguard. For instance, if a security breach of sensitive network data is not acceptable by an organization, policy requiring separateness may be practical. [21]

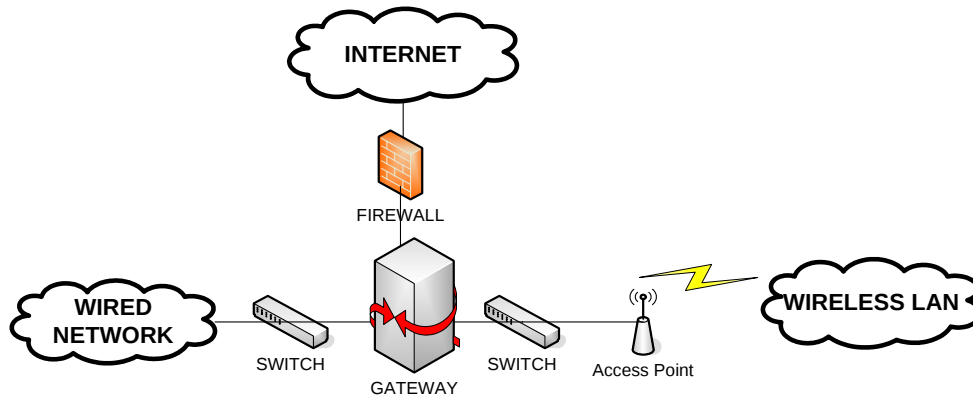


Figure V-1 Example of a Segregated Wireless Network [21]

Wireless Access Point Security

Depending on the organizational environment and the sensitivity of data on the network, an organization may specify certain requirements for AP deployment and utilization within the wireless policy. APs create risks altogether different from normal networks. The organization must evaluate the necessity for policy to dictate certain aspects of wireless AP deployment. Organizational concerns can be mitigated by integrating specific AP topics into policy.

For instance, most APs can be reset to the insecure default mode with physical access to the hardware. With policy, the organization can dictate that APs only be located in physically secure spaces where only authorized system administrators have access for maintenance and configuration. Another concern of APs may be the SSID broadcast mode. It may be pertinent to the organization to dictate within the policy that all APs have broadcast mode turned off as standard configuration. Finally, the wireless security policy may also establish that no personal wireless APs can be operated within the organization's LAN.

Wireless Client

Another category that may require clarification within the wireless security policy is wireless client equipment and ownership. For instance, the organization may already allow personal laptops on the organization network. In this case, the organization should consider a wireless security policy dictating user registration requirements for personal hardware, as well as stringent requirements for acceptable operating system and

application software in addition to requirements for host security mechanisms such as virus and personal firewall software. On the other hand, the organization may desire to disallow all personal equipment on the wireless network. In this is the case, the organization would supply all of wireless equipment and there may be additional security policy specifying that the IT department maintain plant account records for wireless equipment.

Authentication

A wireless environment presents additional authentication concerns that can be addressed in the wireless security policy. Since the ability to spoof an AP is an elevated possibility in the wireless environment, it is important to exercise safeguards not necessary within a comparable wired network. For instance, through security policy the organization can require mutual or two-way authentication between host stations and APs without dictating any specific design. Thus, this policy requirement would compel the designers to employ a solution more robust than standard WEP.

Encryption

Confidentiality is one of the three key factors in network security. In order to provide confidentiality within a wireless network it is crucial to deploy encryption. The wireless security policy should be the guideline to ensure confidential wireless communications. The policy should address the minimum requirements for encryption on the wireless network.

The organization must determine the factors to be included within policy for encryption topics such as strength, method, implementation, management, and frequency of use. [21] For instance, the organization may designate an encryption management requirement that different keys be utilized for authentication and encryption. Another point to consider is the utilization of encryption that employs derived keys instead of master keys for the encryption process. This will help to limit the availability of the master key to attack. [22] The specified level of each encryption factor in the wireless security policy should be chosen based on corporation threat factors and sensitivity of network data.

Availability

Although not required, the wireless security policy can delineate AP propagation and availability testing. Testing propagation characteristics prior to implementation minimizes deployment issues such as radio frequency (RF) interference by addressing problems before implementation. The security policy can include requirements for pre-deployment testing as well as periodic maintenance testing after implementation.

“The policy should force the execution of wireless availability tests, indicate the specific testing tools, provide a reasonable frequency for which the tests are to be conducted, and define a time-frame for test completion. While wireless networks will undoubtedly encounter interference from time to time, defining availability tests and tools in the policy and the subsequent execution of these tests will help reduce signal loss and improve availability.” [21]

Education

The wireless security policy can be used to dictate policy for educating users, administrators, and managers regarding wireless security issues. For instance, an organization can use wireless security policy to require IT personnel receive yearly off-site training on wireless security issues. If the personnel are taught how to secure their systems and informed of the latest threats to wireless technology, the benefits are two-fold, individuals will more likely appreciate security issues and they will be more apt to take the steps necessary to limit activities that put the network at risk. [23]

Enforcement

In order to enforce the security policy over time, it is important to describe maintenance requirements. The wireless security policy can dictate to the IT security staff exactly what should be monitored for noncompliance, how often monitoring should take place, what should be accomplished when noncompliance is discovered, and what should be documented, including routine tests where no discrepancies are noted. For instance, it is important to test for wireless APs that are operational on the network, but not specifically authorized.

In addition, during the initial implementation of a wireless policy in an environment where a certain number of wireless devices already exist, the organization may provide a grace period for all users to comply with the new policy. The extent of the

allotted time to comply with the policy is determined by the organization but it is suggested this period not be more than 90 days. This situation is unlikely for the FAA given the moratorium on wireless. [23]

Summary

Within a wireless network environment it is paramount that organizations develop and implement security policies specific to wireless technology in order to ensure optimum security. A well-planned wireless security policy is an important step in a methodical implementation of wireless networking.

C. DEPARTMENT OF TRANSPORTATION WIRELESS STANDARD OVERVIEW

The focus of this section is to describe the draft version of The DOT *PDA/Wireless Security Implementation Standard* dated November 2003. The first section of the DOT standard identifies some of the common forms of wireless attacks. The second section defines some of the general security controls. The next three sections outline the access point, PDA, and blackberry device security settings. The final section introduces some of the wireless security products on the market.

The Department considers wireless technologies a high risk. The DOT standard requires that all IT technologies be validated through the NIST SP800-37 Certification and Accreditation program. [24] The DOT recommends that all new wireless network implementations should be Wireless Protected Access (WPA) or 802.11i compliant. The DOT also recommends that the following mechanisms should be added if they are not currently being used:

- A RADIUS Server for 802.1X support for access control and authentication
- Client 802.1X software for access control and authentication
- EAP-TLS for authentication
- PKI (Public Key Infrastructure)

FAA

The FAA is required to align its wireless policy with that of the Department of Transportation. Consistency with the DOT Security Policy is recommended since it adheres to commercial practices and it is not overly restrictive.

D. DOD DIRECTIVE 8100.2 WIRELESS USE

In April 2004, the DoD released a policy (DoD Directive 8100.2 Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)), signed by Deputy Secretary of Defense Paul Wolfowitz. This is a high level wireless directive that establishes policy and responsibilities to ensure information confidentiality, authentication, availability, integrity, and non-repudiation of communications carried by wireless technology within the DoD Global Information Grid (GIG).

The policy lays out the responsibilities for a number of different defense agencies. It requires end-to-end use of data encryption on wireless systems to include cell phones, wireless laptop computers, personal digital assistants and a variety of other devices. It requires that the encryption technologies used for wireless communication comply with the Federal Information Processing Standard (FIPS) 140-2 security level 1 or level 2 cryptographic validation program based on the sensitivity of the data.

FIPS 140-2 defines the security requirements for all software and hardware products implementing cryptography. Within FIPS 140-2, there are 4 different security levels. Security Level 1 provides the lowest level of security. Security Level 2 provides physical security of Level 1 with tamper evident coatings or seals. The next two levels improve and enhance physical protection. [25]

The DoD policy requires strong Identification and Authentication measures at the device and network level for accessing DoD databases in accordance with DoD Instruction 8500.2: Information Assurance Implementation. [26] The DoD prohibits the storing of classified data unless approved by the Designated Approving Authority (DAA). Classified data must be encrypted by NSA approved encryption e.g., AES. Other provisions of the directive prohibit the downloading of mobile code from non-DoD

sources, and require the installation of anti-virus software on wireless-capable workstations and portable devices.

Department officials also were directed to establish a knowledge management process enabling users to share information on vulnerabilities, best practices and alternative mitigating techniques. The DoD requires all wireless devices to be in compliance with DoD Instruction 8500.2 Information Assurance Implementation. The DoD requires compliance to this directive from all services within 180 days.

This Page Intentionally Blank

VI. RECOMMENDED WIRELESS ROLLOUT PLAN FOR FAA

A. INTRODUCTION

Network security is a vital requirement today. In order to maintain security while implementing wireless technology it is necessary to approach the implementation systematically. It is important to prepare an implementation plan that will methodically address major concerns associated with the technology while maintaining security during the course of action. Major concepts instrumental in the rollout of wireless technology include policy, planning, and requirements.

Policy in the case of wireless implementation holds two major purposes. First, the organization's security policy provides the primary guide to developing the internal implementation plan. When dictated from senior management, security policy delineates goals and restrictions of the technology implementation guiding decisions throughout the wireless implementation. Second, security policy developed to define the internal uses of a new technology will assist management with a documented record of constraints for its employees. While the organization's existing security policy will be a guide throughout the implementation process, the internal security policy will be a vital security tool within the organization.

Planning is a vital part of any implementation. The implementation plan must define the individual actions required to accomplish the wireless implementation. The intent of a plan is to portray the intended path for management and for employees of an organization. The plan adds organization to the process.

Requirements are necessary to define the boundaries of the implementation. It is important to develop requirements in order to shift from planning into actual implementation. Without defined requirements, there would be no means to determine if the plans are sufficient to accomplish the implementation.

It is also important to understand that planning, policy, and requirements are not mutually exclusive entities within an implementation plan. While the plan will be the overarching product driving the implementation process, it is important to consider that it is interwoven with policy and requirements. The internal policy development will

ultimately drive the requirements. The requirements will be used to document organization specific needs for the implementation. The plan must initially be outlined in order to recognize a process for wireless implementation but, both policy and requirements may drive changes to the timeline of the initial plan during the implementation process.

Finally, it is important that research play a role in the development of the wireless implementation plan for the FAA. For instance, National Institute of Standards and Technology (NIST), Technology Division U.S. Department of Commerce, offers an extremely helpful tool, Wireless Network Security 802.11, Bluetooth and Handheld Devices, Special Publications 800-48 [27]. Although it was completed prior to the release of 802.11i it describes general information on wireless technology that will be a helpful tool throughout the planning and implementation process.

B. POLICY

The previous chapter expresses the importance of security policy within an organization. For all organizations it is vital to develop a policy coupled to the goals and objectives of their mission. It is strongly recommended that senior management within FAA provide for the development of a thorough security policy in conjunction with the implementation plan of wireless components.

C. DEFINE A GENERAL PLAN OF ACTION WITH MILESTONES

One of the major recommendations to the FAA is to institute a phased installation plan of the wireless network. For instance, within a large enterprise such as the FAA the initial phase may be a prototype implementation that includes only one department, the second phase may include an entire geographic location within the organization, and the third phase may be the enterprise wide implementation. Each phase might be contingent upon the successful completion of the previous phase.

Development of a plan of action and milestones (POA&M) for each phase of implementation will assist the FAA by offering a managed approach to the process. It is important that the POA&M include all the items affecting a wireless implementation. For instance, existing network security policy should be modified to include wireless technology prior to the implementation. It is important to have policy modification

included within the POA&M. It is suggested that the FAA include, but not be limited to, defined stages such as policy development, wireless requirements development, wireless design development, hardware testing and infrastructure implementation. Include the timeframe expected for completion of each stage when applicable. It is also necessary to be as specific as possible with the steps required within each phase, but not be overly detailed.

During creation of the POA&M it is important to investigate relationships between the stages in order to delineate precedence and prerequisites. For instance, it is important to test preferred hardware for proper configuration on a test network prior to installation within the active network. In addition, training IT system administrators must be complete before final installation. Both of these can be completed in parallel within the hardware testing stage on the POA&M, but should be listed as separate requirements. Together, both steps can be considered a prerequisite to installation of the hardware within the infrastructure implementation stage. Also, note that the testing of hardware for proper configuration can be started before the wireless policy has been officially approved, but training the IT system administrators would not be prudent until the hardware and software suite selection has been approved by senior management.

It is important that while the wireless policy is being defined that it maintains consistency with DoT and FAA security policy for the general employee. The level of authority and responsibility of the general employee must be defined as well. For example, if the general employee will be allowed personal laptops on the wireless network, then the rules for laptops must be documented clearly within the security policy. Such rules might require that each personal laptop be single boot with Windows 2000 and later, Linux Red Hat 9 and later, etc, and all personal equipment must be brought into the IT department and MAC addresses and serial numbers recorded before the personal laptop will be allowed to use the FAA network. Another option would be that wireless users will be chosen by the FAA, and government equipment will be the only equipment (access point and PCMCIA or PCI cards for wireless) accepted on the FAA wireless LAN.

D. DETERMINE THE REQUIREMENTS

Once a general POA&M has been defined for an implementation requirements can be established. The requirements will be used to guide design decisions and hardware selection. An employee survey may be the most practical way to explore overall options for each phase. A well developed survey could determine employee interest and partial physical requirements for a specific implementation. For instance, a survey within a specific department for the prototype phase would reveal a fairly accurate number of personnel within the department wanting or needing to utilize wireless technology.

An important requirement is to designate the physical location that requires coverage in each specific phase of wireless implementation. It is also important at this point to begin putting boundaries on the requirements. For instance, in order to cover an entire department during the first phase of implementation, the designated buildings must be completely wireless capable. In addition, since it is a desire to minimize outside exposure the intent might be to keep the wireless AP propagation to within 100 feet of the building. These requirements will be useful when calculating the physical equipment requirements.

In addition, it is important to begin calculating the number of users expected and the predicted throughput for the first phase of implementation defined. Scalability will be a later consideration, but look now at how many employees will be included within the first actual infrastructure implementation. This gives a general design target.

Finally, determine logical network requirements such as the number of IP addresses required to support the specific phase. Establish the IP address and subnet mask that will represent the WLAN. This range should include the only the IP addresses assigned to the wireless clients in order to track wireless clients separately from the general network hosts.

E. THE RF SITE SURVEY

The site survey is critical to the topographical design phase. The site survey examines the physical layout of the office space and determines optimal placement and number of access points to maximize client connectivity and throughput. Therefore, it is

necessary to perform a RF site survey to fully realize the behavior of RF within a facility before deploying wireless access points.

Given the different propagation characteristics of the 802.11a and 802.11b/g this may require planning for coverage for 802.11a, then 802.11b/g and a financial comparison between the two types before one can be settled on. It will also be necessary to research RF coverage information in order to determine number of APs required that will offer appropriate propagation coverage. Since, RF propagations are different from building to building it may require actual field testing of intended equipment to determine adequate coverage within the buildings. Often it is best to use the same vendor for APs and PCMCIA and PCI cards, but this is not a requirement. Make sure to test with the same model APs and PCMCIA and PCI cards that are expected for the design. In other words, do not use a home network AP if the intent is to design to a commercial office AP. A possible software tool to assist with designing to the propagation requirements of a wireless network is the Proxim ORiNOCO Ekahau Wi-Fi Site Survey and Prediction Software from www.proxim.com.

Before conducting the actual site field test survey, obtain a copy of the building layout and conduct a walkthrough of the building to ensure the copy of the layout is current and accurate. Make sure to use the boundary requirement information gathered during the determination of requirements time frame. This is a perfect opportunity to survey for required electrical and space cooling capabilities within the AP locations. If the electrical and space cooling capacities of the existing facilities are inadequate it must be addressed and fixed before the installation stage.

Once the FAA wireless team is satisfied with the AP locations and the RF coverage, the AP installation positions should be recorded on facility diagrams. The signal readings and supported data rates should be included near the outer propagation boundary lines of each AP as a baseline for future redesign efforts. Up through this point the APs will only be operated during propagation testing. The site survey is only responsible for investigation of RF site hardware requirements. [28, 29]

Lab testing the selected equipment will be conducted at this time to assist in solving additional site survey requirements such as throughput verification which can not

be addressed on the active network until an implementation design is accepted. Overall, the site survey should answer the following points:

- Locations APs are to be connected to the wired LAN.
- Optimum placement of APs to provide the most efficient coverage and maximum throughput.
- The number of APs sufficient to support the characteristics of the building with respect to radio waves (lab testing will assist with this).
- Actual performance characteristics with respect to locations anticipated to have a large number of users (lab testing will assist with this).
- The organization's applications performance characteristics on the wireless LAN (lab testing will assist with this). [30]

F. DESIGN CONSIDERATIONS

The design stage produces a logical and consistent definition of how the wireless LAN will satisfy requirements. At this point, specific equipment is selected from the site survey and lab testing results. The actual implementation design will be formulated to include but not be limited to the site survey facility documentation and a topology map of the designed wireless network. Several considerations must also be addressed within the design documentation. These include interoperability, performance, scalability, and security as addressed here:

Risks Assessments

Thorough risk assessments are imperative to the development of a well-planned wireless implementation. A true risk assessment requires several steps. First, the vulnerabilities and threats must be identified, but that alone is not enough. It is important the organization also investigate each threat or vulnerability for what possible damage the associated attack(s) would cause to the organization. Additionally, each threat and vulnerability should have mitigation strategies developed and analyzed for cost. Each threat and vulnerability should then be compared against probability of it happening and likely mitigation costs.

A cost benefit analysis at this point will create a visible risk environment for the organization. The organization can complete a true risk assessment and make sound decisions concerning operational security for the organization based on this information.

It is prudent for an organization to prepare documentation delineating each of these steps as it will represent the methodology behind sound security practices.

Interoperability

Although interoperability of wireless infrastructure is not generally an issue with Ethernet networks, WLAN systems are often vendor proprietary and do not always operate well in a mixed vendor environment. In order to maximize interoperability with future design requirements, choose products with Wireless Ethernet Compatibility Alliance (WECA)'s Wi-Fi certification. "The Wi-Fi Alliance offers a Wi-Fi CERTIFIED* logo on products to show that they have been successfully tested as an interoperable, regardless of the vendor." [31]

Scalability

The design should allow for flexibility and growth. The FAA department size varies from region to region; the design should scale with the size of the department and the number of users.

Security

Assess the organization's information sensitivity and security requirements for the separate categories of information. Establish wireless security mechanisms based on the value of information that will transverse the wireless segments. [32] Wireless APs most often are not secure with factory default configurations and settings. Document required security configurations and settings for APs during the design stage. Table VI-1 lists the security combination of authentication and encryption methods available and a short description of the associated security strengths. This table is provided as a high level reference guide. It is suggested that the FAA determine what best meets the organization's security protection level through more extensive research means.

G. INSTALLATION AND USER REGISTRATION

Once the requirements are determined and listed, a thorough site survey has been conducted, and the security infrastructure is in place, it is time to roll out the equipment

and begin the wireless program for a given phase. The APs should be in place and operational. If personal equipment is authorized on the LAN make sure that users accessing the network have properly registered the equipment. If there is no personal equipment authorized on the network distribute the required hardware to authorized users. It is important the IT department maintain records of registered users. It is recommended that the IT department continues to monitor and conduct wireless network analysis as described in the next section in order to prevent and reduce chances of an attack.

H. SECURITY MAINTENANCE OF THE WIRELESS NETWORK

Once the wireless network is operational it is vitally important that the IT security administrators routinely test for general user compliance. This step is by no means a trivial matter. A major indication of noncompliance is unauthorized users on the network.

In a wireless network it is important to test for unauthorized users from within the network as well as the propagation of unauthorized APs within the designated FAA footprint area. Testing of the internal network for unauthorized users is best controlled through routine collection of network traffic logs and log examination by security administrators. Testing for propagation of unauthorized APs requires security administrators to routinely scan for “hot spots” with propagation testing software. Another propagation test includes the routine monitoring of the broadcasted messages to verify the traffic is of expected nature. [23] For instance, it is important when a wireless LAN is invoking 802.1X that there be no “in the clear” traffic. This would be an indication of a malfunctioning AP, or unauthorized AP.

Table VI-2 provides a list of monitoring tools and vendors that may prove helpful for researching products for the FAA. The inclusion of this information here does not imply product or vendor endorsement by the author or the Naval Postgraduate School.

Authentication Method	Encryption Method	EAP Needed?	RADIUS Needed?
Shared-key	Static WEP	No	No
	Remarks: Data security is not a primary concern. Selected for ease of implementation over data security and authentication complexity. Also good for guest networks and low security network		
MAC Address Filtering	Optional	Optional	Optional
	Remarks: MAC filtering is a separate authentication scheme that can be applied to any of the security combination already mentioned. It adds a layer of security but also adds maintenance complexity.		
802.1X	WEP	Yes	Yes
	Remarks: Strong user authentication against a RADIUS server and unique encryption keys are generated randomly for each user per session. Require more overhead to setup, but offers good security. Most client software and wireless network cards will support this method. Complexity of rollout depends on EAP type selected		
Pre-Shared Key	WPA	No	No
	Remarks: Strong data encryption is provided through WPA using TKIP or AES. Generally used in smaller wireless deployments where authentication simplicity is desired over deployment of RADIUS server and 802.1X clients.		
802.1X	WPA	Yes	Yes
	Remarks: Very strong security solution using a RADIUS server to authenticate each user and WPA with TKIP or AES to encrypt the data. Client wireless network cards must support WPA and 802.1X clients and 802.1X compliant RADIUS server must be deployed. Good for enterprise wireless LANs that require strong authentication of wireless users and strong data encryption. Complexity of rollout depends on EAP type selected.		

Table VI-1 Security Protocols [33]

I. CONCLUSION

It is important to understand that a wireless implementation is a major modification to any network. Although wireless hardware can easily be selected and installed within any network, wireless technology generally introduces greater security

risks. Therefore, a clear, well planned rollout process is required to introduce wireless technology in a controlled, systematic manner in order to mitigate these security risks.

<u>Network Discovery Tools</u>	
Boingo Hot Spot Finder (PC, PDA)	www.boingo.com
BSD AirTools (BSD)	www.dachdb0den.com/projects/bsd-airtools.html
Kismet (several OS)	www.kismetwireless.net
MacStumbler (Mac OS X)	www.macstumbler.com
NetStumbler (PC) MiniStumbler (PDA)	www.netstumbler.com
WaveStumbler (Linux)	www.cqure.net
<u>WLAN Analyzers</u>	
AirMagnet	www.airmagnet.com
AirScanner Mobile Sniffer (freeware)	www.airscanner.com
Ethereal	www.ethereal.com
Fluke Networks WaveRunner	www.flukenetworks.com
Network Instruments Network Observer	www.networkinstruments.com
Network Associates Sniffer Wireless	www.sniffer.com
WildPackets AiroPeek NX	www.wildpackets.com

Table VI-2 WLAN Monitoring Tools

It is most important that leadership maintain overall accountability for the implementation process and put forward the required resources associated with the development of a wireless implementation plan. The steps offered here are generic in nature due to the complexity of a large organization's requirements. It is important that the organization designate internal personnel to guide the implementation process in an approach relevant to specific executive requirements.

In addition to the resource allocation from senior management, it is suggested that an internal team of employees be selected and empowered by senior management to make use of these steps for the development and execution of the organization's wireless implementation plan. An internal team of personnel skilled in IT security, the organization's network, and internal managerial practices will be best able to develop a pertinent wireless implementation plan. The development of a written implementation POA&M can suffice as a logical and comprehensive methodology for each phase of implementation for wireless technology within the establishment.

Wireless technology offers a level of freedom to users that greatly increases flexibility over normal networks, yet it requires greater implementation planning and increased network examination after installation. By following the methodology offered here a large organization can develop an implementation plan that directly supports user requests for wireless connectivity while maintaining an elevated level of network security throughout the implementation process.

This Page Intentionally Blank

APPENDIX 1. AN EXAMPLE DESIGN FOR A SECURE WIRELESS LAN

The purpose of this appendix is to provide an exemplar design for a secure wireless local area network (WLAN). The design will address the WLAN topology, select the appropriate 802.11 standards and define a strong security method. For this example, we will assume there is a requirement to support two APs and ten mobile devices with considerable throughput.

The WLAN Topology

The WLAN topology should be simple and flexible to allow for future growth. For illustration, Figure 1-1 shows a generic wireless topology consisting of a client, an AP, a switch, a gateway, a firewall, a router, and authentication servers. The gateway provides an initial line of protection to the internal wired network by separating the wireless network from the wired network. The servers are responsible for the authentication process through the utilization of certificates. The switch prevents access to the internal wired network by wireless clients until the authentication is successful. We will build further on this topology for our exemplar design.

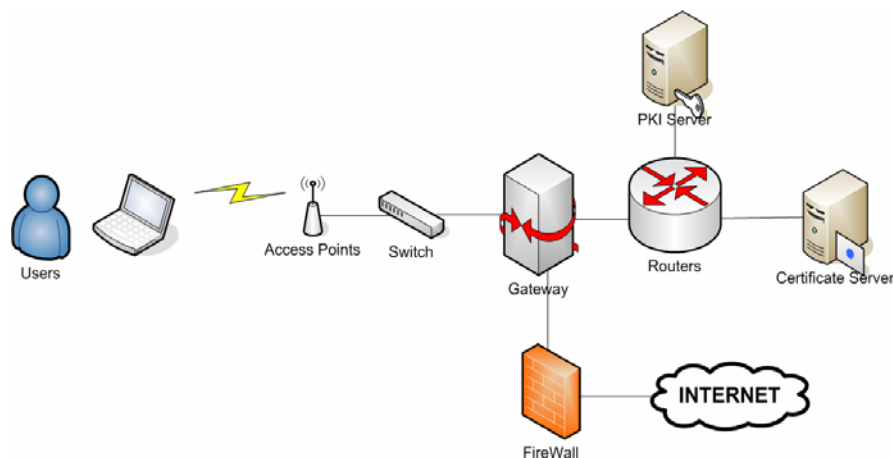


Figure 1-1 A Generic Wireless Topology

Selecting the Appropriate IEEE 802.11 Standard

There are three IEEE 802.11 standards to be considered when selecting wireless broadcast devices: IEEE 802.11b, IEEE 802.1a, and IEEE 802.11g. Table 1-1 briefly outlines

the IEEE 802.11 b/a/g maximum throughput and number of channels available from each standard to assist in the selection of the best IEEE 802.11 standard for the design.

IEEE Standard	Frequency	Maximum Throughput	Non-over lapping channels
802.11b	2.4GHz	11Mbps	3
802.11a	5GHz	54Mbps	12
802.11g	2.4GHz	54Mbps	3

Table 1-1 IEEE 802.11 Standard Comparisons [7]

It is important to also consider the range of devices when selecting a standard. Although IEEE 802.11a provides a high throughput of 54Mbps at 5GHz it is not necessarily the best choice in all situations. In order to realize the maximum throughput for the 802.11a (54 Mbps) the AP must be within 10 -15 meters of the host station. On the other hand, the 802.11b device has a maximum low throughput range (1 Mbps) of 500 meters. If the requirement is for many users within a closed in area the 802.11a may prove more functional, but if the users cover a large footprint, and do not require large bandwidth, the 802.11b may be best. [34]

802.11g was ratified in 2003 and provides a throughput of 54Mbps at 2.4 GHz. Dissimilar to the 802.11b, the 802.11g is capable of utilizing the same OFDM waveform as the 802.11a. Side by side testing of the OFDM waveform with the 802.11a and 802.11g has shown that the 802.11g “is capable of higher data rates at longer ranges than any competing WLAN technology.” [35] The 802.11g is gaining momentum as a popular alternative to the 802.11a and 802.11b.

Additionally, if scalability is an important consideration the non-over lapping channels of 802.11a may be more appealing than throughput versus distance. Since this exemplar does not define the client wireless network cards standard, the APs for this exemplar will have dual-mode frequencies (2.4GHz and 5 GHz) capabilities to support all users.

Security Methods

Early wireless technology offered WEP as the only means of wireless security. Yet, over time WEP has proven principally insecure. Within the past few years introduction of the WPA 2002 standard has significantly increased the WEP security. WPA, commercially available

today, is compatible with 802.11a, b, and g and is actually is a subset of 802.11i. WPA is a specification of standards-based, interoperable security enhancements that increases the level of data protection (encryption) and access control (authentication) for existing wireless LAN systems. WPA includes 802.1X Authentication which is an essential element of network security in a wireless capable network. Figure 1-2 shows the basic setup of an 802.1X network.

Future systems based on IEEE 802.11i will provide the most secure wireless design to date. The WPA standard of 2002 enhances the mechanisms of existing WEP by changing to temporary key integrity protocol (TKIP) but maintains the underlying security algorithm, RC4, established with WEP. On the other hand, 802.11i modifies both the underlying security algorithm to EAS and the security protocol to counter mode cipher-block-chaining message authentication code protocol (CCMP), thus requiring complete redesign of wireless equipment. Although the IEEE 802.11i CCMP will improve security in the future, it is not available on the market today.

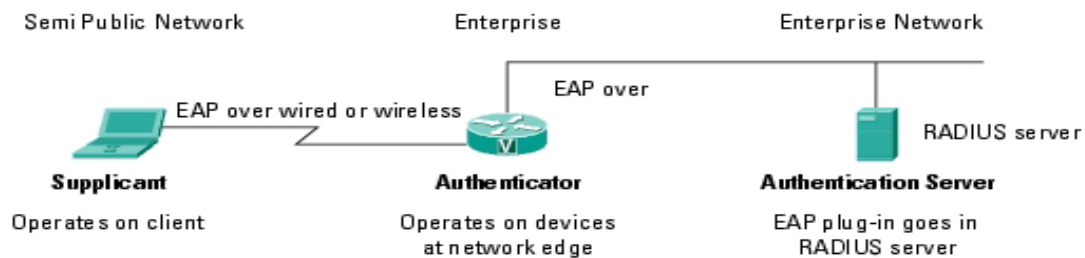


Figure 1-2 IEEE 802.1X Technology [36]

Security Selections

802.1X uses the Extensible Authentication Protocol (EAP) and a RADIUS Server for network access control, see Figure 1-2 IEEE 802.1X Technology. EAP-TLS is selected for use as it offers a robust solution for security. In order to use 802.1X and EAP-TLS, the following components are required [37]:

- Client wireless cards compatible with 802.1X (for authentication)
- Client access software capable of EAP-TLS (for encryption)

- Wireless AP compatible with 802.1X and EAP-TLS (for authentication and encryption)
- RADIUS compatible with EAP-TLS (for encryption)
- Public key Infrastructure (PKI) (for authentication and encryption)

Most add on wireless cards support 802.1X and can be used in the context of the Windows XP operating system. Some laptop vendors even have integrated wireless support for 802.1X and EAP-TLS. For client access software, again the Windows XP operating system supports EAP-TLS. Only industrial-grade APs support 802.1X and EAP-TLS. Those APs cost more than the small office and home office grade systems but they offer superior features including Dynamic WEP, better quality antennas, and dual-band 802.11a, 802.11b and 802.11g. Both the 2000 and 2003 versions of Microsoft Server have RADIUS capabilities that support EAP-TLS and Certificate Authority services in a support PKI.

A. Topology

Figure 1-3 illustrates a topology with WPA standards and protocols implemented to provide a secure wireless LAN. This small and flexible topology is extensible and allows for expansion as needed by a particular organization.

The exemplar topology includes 10 laptops configured with the Windows XP Operating System and ten dual band wireless network cards that will communicate with the two APs. The dual-band APs allow interoperability with the users' different standards and yet provide a continuous connection with high throughput.

Microsoft Windows XP operating system installed on the laptops supports 802.1X authentication and the wireless cards support EAP-TLS for strong mutual authentication of client and RADIUS Server and dynamic key encryption. For identification, the users must obtain a private key and a public key digital certificate that has been securely distributed to the LDAP/RADIUS server. The WLAN utilizes WPA security standard that requires mutual authentication using EAP-TLS, 802.1X and RADIUS protocols.

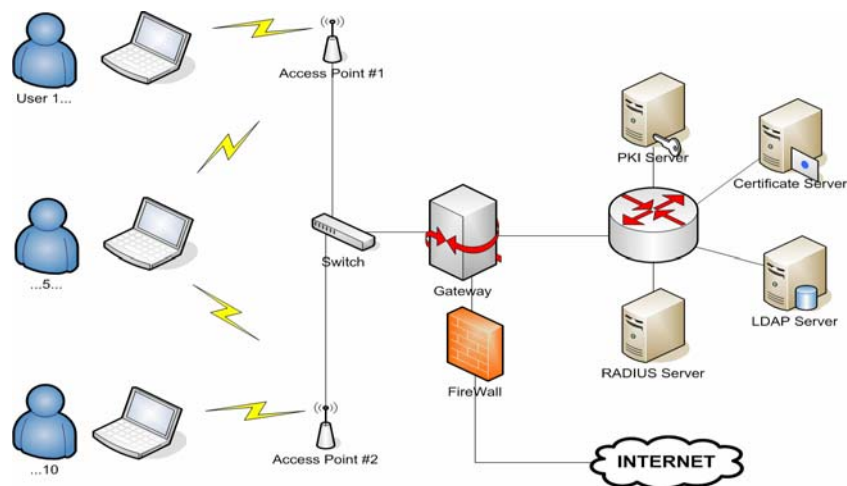


Figure 1-3 Exemplar WLAN Architecture [37]

The two APs are connected to a switch that is also connected to a gateway. The gateway protects the internal network in case the wireless side undergoes technical failure, this will allow the internal network to function and continue to support day-to-day operation. A firewall, another layer of defense, is also added to protect the internal network. Several servers are to provide PKI authentication and act as a Certificate Authority for the PKI infrastructure.

The wireless users who desire to connect to the network must provide their public key certificate to the Certificate Authority, and register their laptops with the IT department. Once their laptops are registered and the Certificate Authority server contains their certificate, they are ready to wirelessly connect to the net. Implementation of WPA is the best WLAN security until the CCMP protocol designated by 802.11i matures and the technology emerges into the market.

This Page Intentionally Blank

LIST OF REFERENCES

1. Robinson, D., "Intel Updates Wireless Kit for Centrino," Computer Reseller News, [<http://www.crn.vnunet.com/news/1147079>], November 4, 2003.
2. Greek, D., "Dell offers wireless choice," Computer Reseller News [<http://www.crn.vnunet.com/news/1139832>], March 31, 2003.
3. E-Business Strategies, Inc., "802.11b/WiFi and Bluetooth – Business and Revenue Models," Wi-Fi Technology [http://www.ebstrategy.com/mobile/revenue_models/802.11b_wifi.html], no date.
4. IEEE, "The IEEE 802® LAN/MAN Standards Committee Networking Standards For Advanced Telecommunications," Backgrounder [http://standards.ieee.org/announcements/bkgnd_802stds.html], modified: October 29, 2003.
5. Maxim Dallas Semiconductor, "An Introduction to Direct-Sequence Spread-Spectrum Communications" [<http://pdfserv.maxim-ic.com/en/an/AN1890.pdf>], February 2003.
6. Kruse, McClung, Quiroz, Weigle, University of Texas, San Antonio, IS 5203: Telecommunications [[http://faculty.business.utsa.edu/jgclark/is5203/Wi Fi presentation 2004 \(version Briefed\).ppt](http://faculty.business.utsa.edu/jgclark/is5203/WiFi%20presentation%202004%20(version%20Briefed).ppt)], October 4, 2004.
7. Cooklev, T., 2004, *Wireless Communication Standards*, Standards Information Network IEEE Press.
8. Blunk, L. and Vollbrecht, J., "PPP Extensible Authentication Protocol (EAP)," RFC 2284, March 1998.
9. Aboba, B. and Simon, D., "PPP EAP TLS Authentication Protocol," RFC2716, October 1999.
10. Thomas, T., "Wireless Security," informit.com [<http://www.informit.com/articles/article.asp?p=177383&seqNum=6>], July 16, 2004.
11. Madge Limited, "Wireless LAN Security," White Paper [http://www.madge.com/_assets/documents/guides/wlansecurity.pdf], no date.
12. LAN Access Security Interoperability Lab, "What's Wrong With WEP?" [http://www.ilabs.interop.net/LANSec/papers/14_Whats_wrong_with_WEP-LV04.pdf], no date.
13. Arbaugh, W., Shankar, N. Wan, Y.C., "Your 802.11 Wireless Network has No Clothes," Department of Computer Science University of Maryland [<http://www.cs.umd.edu/~waa/wireless.pdf>], March 30, 2001.
14. Roth, J., "Enterprise Implementations of Wireless Network Technologies at the Naval Postgraduate School and Other Military Educational Institutions," Master's Thesis Naval Postgraduate School, September 2002.

15. Naval Postgraduate School, "Adding Wireless Access to Your Area," Information Technology and Communications Services
[<http://intranet.nps.navy.mil/WirelessNetwork/>], reviewed October 20, 2004.
16. Federal Aviation Agency, "About FAA"
<http://www.faa.gov/AboutFAA/Regionalmap.cfm>, no date.
17. Federal Aviation Agency, FAA Order 1370.82 [http://www.faa.gov/aio/common/documents/HTMLfiles/1370_82.htm], June 9, 2000.
18. Federal Aviation Agency, FAA Order 1370.86, March 1, 2001.
19. Shimonski, R., "Defining a Security Policy," WindowSecurity.com
[http://www.windowsecurity.com/articles/Defining_a_Security_Policy.html], April 10, 2004.
20. "Windows XP Wireless Deployment Technology and Component Overview," Microsoft TechNet
[<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wificomp.mspx>], August 2004,.
21. Farshchi, J., "Wireless Network Policy Development (Part One)," Security Focus
[<http://www.securityfocus.com/infocus/1732>], September 18, 2003.
22. Kim, M., "ECE 575 Project: Investigation about the RC4 and the weakness of WEP," Electrical Engineering and Computer Science
[<http://islab.oregonstate.edu/koc/ece575/04Project1/Kim.pdf>], March 12, 2004.
23. Farshchi, J., "Wireless Network Policy Development (Part Two)," Security Focus
[<http://www.securityfocus.com/infocus/1735>], October 2, 2003.
24. Ross, R., Swanson, M., Stoneburner, G., Katzke, S., and Johnson, A., "Information Security: Guide for the Security Certification and Accreditation of Federal Information Systems," NIST Special Publication 800-37, May 2004.
25. National Institute of Standards and Technology, "Security Requirements for Cryptographic Modules," NIST FIPS PUB 140-2 [<http://csrc.nist.gov/cryptval>], May 25, 2001.
26. Department of Defense Instruction Number 8500.2, "Information Assurance (IA) Implementation,"
[http://www.eitoolkit.com/tools/initiation/info_assurance/03_dod_8500_2.pdf], February 6, 2003.
27. National Institute of Standards and Technology, "Wireless Network Security 802.11, Bluetooth and Handheld Devices," NIST Special Publications 800-48
[http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf], November 2002.
28. Geier, J., "RF Site Survey Steps," Wi-Fi Planet [<http://www.wi-fiplanet.com/tutorials/article.php/1116311>], May 10, 2002.

29. DISA, "Wireless Security Technical Implementation Guide, Version 1, Release 4" [<http://csrc.nist.gov/fasp/FASPDocs/STIGS/STIGs/Wireless.doc>], January 9, 2003.
30. Gast, M., *802.11 Wireless Network: The Definitive Guide*, O'Reilly, Chapter 15: Creating and Administering Wireless Networks [<http://www.oreilly.com/catalog/802dot11/chapter/ch15.html>] April 2002.
31. Intel, "Wireless LAN Deployment Considerations," Intel [<http://www.intel.com/business/bss/infrastructure/wireless/deployment/considerations.htm>], no date.
32. Geier, J., "WLAN Deployment Risks," Wi-Fi Planet [<http://www.wi-fiplanet.com/tutorials/article.php/1142791>], May 22, 2002.
33. Phifer, L., Kwan, P., "White Paper: IronShield Best Practices Deploying Wireless LANs," Foundry Networks, Inc. [[http://www.foundrynet.com/solutions/appNotes/PDFs/Deploying Wireless LANs V1-01.pdf](http://www.foundrynet.com/solutions/appNotes/PDFs/Deploying%20Wireless%20LANs%20V1-01.pdf)], September 2003.
34. Ollmann, G., "Securing Wireless Networks: Secure Configuration Advice on Wireless Network Setup," Internet Security Systems [<http://www.issadvisor.com/columns/SecuringWirelessNetworks/SecuringWirelessNetworks.htm>], no date.
35. Zyren, J., Enders, E., Edmondson, T., "802.1g Starts Answering WLAN Range Questions," CommsDesign [<http://www.commsdesign.com/showArticle.jhtml?articleID=53200017>], January 14, 2003.
36. CISCO, [http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/80211_da.jpg], no date.
37. Ou, G., "Real Products for Real WLAN Security Requirements for 802.1X and EAP," ZDNet [<http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2879236-2,00.html>], September 4, 2002.

This Page Intentionally Blank

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
8725 John J. Kingman Rd., STE 0944
Ft. Belvoir, VA 22060-6218
2. Dudley Knox Library, Code 013
Naval Postgraduate School
Monterey, CA 93943-5100
3. Research Office, Code 09
Naval Postgraduate School
Monterey, CA 93943-5138
4. Ernest Lucier
Federal Aviation Administration
800 Independence Avenue, S.W., Room 602, Washington DC 20591
5. Dr. Cynthia E. Irvine
Code CS/Ic
Department of Computer Science For
Naval Postgraduate School
Monterey, CA 93943-5118