

Wireless LAN Technologies: A Model for Planning, Designing, and
Implementing a WLAN Solution in a Global Manufacturing Enterprise

by

Ronald G. Wolak

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy

Graduate School of Computer and Information Sciences
Nova Southeastern University

2003

We hereby certify that this dissertation, submitted by Ronald G. Wolak, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Marlyn Littman, Ph.D.
Chairperson of Dissertation Committee

Date

Sumitra Mukherjee, Ph.D.
Dissertation Committee Member

Date

Junping Sun, Ph.D.
Dissertation Committee Member

Date

Approved:

Edward Lieblein, Ph.D.
Dean, Graduate School of Computer and Information Sciences

Date

Graduate School of Computer and Information Sciences
Nova Southeastern University

2003

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Wireless LAN Technologies: A Model for Planning, Designing, and
Implementing a WLAN Solution in a Global Manufacturing Enterprise

by
Ronald G. Wolak

April 2003

The dissertation that follows is submitted to partially fulfill the requirements for the degree of Doctor of Philosophy. Wireless Local Area Networks (WLANs) have the potential to improve the flexibility, productivity, and work environment of employees in an enterprise. WLAN technologies offer the benefits of mobility, reduced installation time, and decreased cost. However, major issues related to security, speed, interoperability, equipment selection, ease of use, reliability, signal interference, and installation must be resolved by companies moving forward with WLAN solutions. The research addressed a problem confronting many large manufacturing companies in the present-day environment. The problem was how to effectively plan, design, and implement WLAN technologies. The goal of the research was to provide large manufacturing enterprises a model for deploying secure WLAN technologies in offices, manufacturing facilities, and employee residences. The model was developed from a case study of WLAN projects implemented at American Axle and Manufacturing (AAM). Four WLAN initiatives were the subject of the case study: Wireless Connectivity in Executive Conference Rooms, Wireless Connectivity on the Plant-Floor, AAMatHome, and Enhanced Wireless LAN Security. Throughout the investigation, an emphasis was placed on the reliability, replicability, validity, and transferability of research results.

Acknowledgements

The support, guidance, and encouragement of many individuals were critical to the completion of this dissertation. First, deepest appreciation goes to my advisor, Dr. Marlyn Littman. Her advice and support throughout my studies at Nova Southeastern along with her enthusiasm, patience, and constructive review during the dissertation process were key to my success. Her efforts are greatly appreciated and will not be forgotten.

Special thanks to the members of my committee, Dr. Sumitra Mukherjee and Dr. Junping Sun. Their scholarly review and recommendations improved the significance and quality of the project.

Special appreciation is extended Richard E. Dauch, CEO of American Axle and Manufacturing (AAM). Following his lead, AAM made employee education a high priority. Throughout the five-year doctoral process, AAM provided the time and resources required to successfully complete the doctoral program.

I would also like to thank those in the AAM IT Department for their support during the completion of the dissertation process and the execution of four WLAN initiatives at AAM. Special thanks go to Kuo-Pu Han for his support and dedication.

Finally, and most importantly, I would not have been successful without the support and encouragement of my most wonderful wife, Geeg. Her assistance in offloading a whole host of personal and household responsibilities from my shoulders began during the undergraduate program at Charter Oak State College and continued throughout the MBA program at Baker College and the doctoral program at Nova Southeastern. She is the best “study pal” anyone could ask for. I love her more than anyone or anything on heaven or earth.

Table of Contents

Abstract iii

List of Figures viii

Chapters

1. Introduction 1

Problem Statement and Goal 2
Relevance and Significance 6
Barriers and Issues 9
Research Questions 10
Limitations and Delimitations 11
Definition of Terms 12
Summary 33

2. Review of Literature 35

Historical Overview 35
Wireless LAN Technologies 37
 Ultra High Frequency (UHF) Narrowband 37
 Spread Spectrum 38
 Direct Sequence Spread Spectrum (DSSS) 39
 Frequency Hopping Spread Spectrum (FHSS) 39
 Orthogonal Frequency Division Multiplexing (OFDM) 40
 Spread Spectrum Interference 40
 Ultrawideband (UWB) 41
 Infrared 42
Wireless LAN Standards and Wireless Standards Associations 43
 IEEE 802.11 43
 IEEE 802.11b 44
 IEEE 802.11a 46
 IEEE 802.11g 47
 IEEE 802.1x 48
 IEEE 802.11i 49
 European Telecommunications Standards Institute (ETSI) 49
 High Performance Radio Local Area Network-Type 1 (HiperLAN-1) 49
 High Performance Radio Local Area Network-Type 2 (HiperLAN-2) 50
 HiperACCESS and HiperLINK 50
 Japan Ministry of Post and Telecom (MPT) Multimedia Mobile Access
 Communication (MMAC) Committee 51
 HomeRF Working Group 52
 HomeRF 1.0 53

HomeRF 2.0	53
Infrared Data Association (IrDA)	54
Wireless LAN Security	55
IEEE 802.11 Security Vulnerabilities	56
Wireless LAN Security Enhancements	60
Wireless LAN Health and Safety Considerations	63
Wireless LAN Initiatives in the Corporate Arena	64
General Motors	65
Intel	65
Office Depot	66
Corrugated Supplies Company	66
Wireless LAN Vendor Offerings	67
Wireless LAN Service Providers	68
Wireless LAN Strategy	70
Summary of Knowns and Unknowns	72
Contribution to the Field	73
Summary	74
3. Methodology	75
Research Method Employed	75
Case Study	76
Modern Systems Development Life Cycle (MSDLC)	78
Audience	80
Specific Procedures Employed	80
AAM Wireless LAN Initiatives	80
Wireless Connectivity in Executive Conference Rooms	81
Wireless Connectivity on the Plant-Floor	84
AAMatHome (AAM at Home)	88
Enhanced Wireless LAN Security	91
Case Study	93
Design	94
Data Gathering	96
Evidence Analysis	97
Formats for Presenting Results	97
Outcome	98
Resources Used	98
Reliability and Validity	99
Summary	100
4. Results	101
Empirical Data Sources	101
Data Analysis	103
Case Study Narrative - AAM Wireless LAN Initiatives	106
Wireless Connectivity in Executive Conference Rooms	106
Systems Planning Phase	107
Systems Analysis Phase	109

Systems Design Phase	110
Systems Implementation Phase	117
Systems Support Phase	120
Wireless Connectivity on the Plant-Floor	121
Systems Planning Phase	121
Systems Analysis Phase	123
Systems Design Phase	125
Systems Implementation Phase	134
Systems Support Phase	136
AAMatHome	136
Systems Planning Phase	137
Systems Analysis Phase	138
Systems Design Phase	140
Systems Implementation Phase	146
Systems Support Phase	150
Enhanced Wireless LAN Security	154
Systems Planning Phase	154
Systems Analysis Phase	156
Systems Design Phase	156
Systems Implementation Phase	162
Systems Support Phase	163
Summary	164
Findings	166
Research Questions	166
Case Study Propositions	168
Model	169
Systems Planning Phase	170
Systems Analysis Phase	171
Systems Design Phase	173
Systems Implementation Phase	175
Systems Support Phase	176
Summary of Results	177
5. Conclusions, Implications, Recommendations, and Summary	179
Conclusions	179
Implications	180
Recommendations for Further Research	181
Summary	182
Appendixes	
A. Dissertation Topic Approval Letter from AAM	186
B. AAM WLAN Initiatives Journal Database - Microsoft Excel Listing	187
C. Microsoft Project Gantt Chart of the AAM WLAN Initiatives Schedule	197
Reference List	203

List of Figures

Figures

1. Typical Records from the AAM Wireless LAN Initiatives Journal Database - Microsoft Excel Screen Print 104
2. Microsoft Project Gantt Chart Showing a Portion of the AAM WLAN Initiatives Schedule 105
3. Dell Hardware Test Configuration in Detroit Forge Plant Manager's Conference Room 114
4. Dell TrueMobile 1150 PCMCIA Wireless Client Adapter 115
5. Dell TrueMobile AP1000 Access Point 115
6. Agere Orinoco Range Extender Antenna 116
7. AAM Wireless Device Policy 119
8. Agere Orinoco EC Converter 126
9. Picture of the AAM Detroit Forge Komatsu Area 127
10. Agere Orinoco AP500 Access Point 127
11. AAM Detroit Forge Komatsu Area - Test WLAN Diagram 128
12. AAM Detroit Forge Plant 1 - Map of Reliable FIS WLAN Coverage 130
13. Picture Showing FIS Wireless Box - Side Mounted on Plant-Floor Electrical Panel in the Detroit Forge Plant 131
14. AAM Detroit Forge - Typical Plant-Floor FIS WLAN 132
15. AAM Detroit Forge - Die Room DNC System WLAN 133
16. AAMatHome Residential WLAN Test Configuration in ATL 143
17. Agere Orinoco USB Client Gold Wireless Adapter 144

18. Linksys BEFSR41 Cable/DSL Router 144
19. AAMatHome Service Infrastructure 147
20. AAMatHome WLAN Hardware Installation in Researcher's Residence 148
21. AAMatHome Terminal Server Desktop 149
22. AAMatHome.com Web site 151
23. Graph Showing Ping Responses with a Normal Comcast Connection 152
24. Graph Showing Ping Responses with an Abnormal Comcast Connection 152
25. Web-based Uptime Report for Researcher's Comcast Broadband Connection to the Internet 153
26. ReefEdge Connect Server CS100 158
27. ReefEdge Connect Bridge CB25 158
28. ReefEdge Evaluation - Hardware Configuration Diagram 159

Chapter 1

Introduction

Wireless Local Area Networks (WLANs) have the potential to improve the flexibility, productivity, and work environment of employees in an enterprise ("*Wireless LANs*," 2001). American Axle and Manufacturing (AAM) is typical of a large manufacturing company. Headquartered in Detroit, Michigan, AAM is a tier one supplier of automotive driveline systems (Manardo, 2001a). AAM specializes in the design, engineering, validation, and manufacture of driveline systems, chassis systems, and forged products for trucks, buses, sport utility vehicles, and passenger cars. The company is a global enterprise with 12,000 employees and 7 million square feet of manufacturing space in 17 manufacturing facilities located in the United States, Brazil, Mexico, and the United Kingdom.

AAM's Local Area Network (LAN) at corporate headquarter in Detroit, Michigan is based on air-blown multimode optical fiber (Blair, 2002). Employees at AAM locations worldwide connect to the AAM network infrastructure via wired ports interlinked to the ATM (Asynchronous Transfer Mode) fiber optic backbone. The wireline LAN technologies employed by AAM include 10 Megabits per second (Mbps) Ethernet and 100 Mbps Fast Ethernet at each desktop. These Ethernet ports are switch connected to the ATM fiber optic backbone.

Remote facilities connect to the AAM ATM backbone network via switched Frame Relay services along with Internet-based Virtual Private Network (VPN) links (Blair, 2002). AAM's in-place wireline network severely limits the accessibility and effectiveness of the AAM network. For example, employees in AAM facilities are unable to access the network easily from meetings, the cafeteria, or anywhere other than their offices. In addition, the effectiveness of remote employees is limited by the slow speed of present-day dial-up modem connections.

In the following sections, the problem to be investigated and the goal to be achieved in this dissertation study are described. Also provided are an analysis of the relevance and significance of the research and a discussion of barriers and issues related to achieving the goal. Next, the research questions to be explored are briefly stated, and definitions of key terms used throughout this investigation are provided. Finally, the limitations and delimitations of the research are described and a short summary is presented.

Problem Statement and Goal

This researcher addressed a problem confronting many large manufacturing companies in the present-day environment, specifically, how to effectively plan, design, and implement WLAN technologies (Dulaney, 2002; Geier, 1999; Rogak, 2001; Sbihli, 2002). WLAN technologies offer the benefits of mobility, reduced installation time, and decreased cost. However, major issues related to security, speed, interoperability, equipment selection, ease of use, reliability, signal interference, and installation must be resolved by companies moving forward with WLAN solutions (Geier, 2001).

Rapidly emerging WLAN standards are making it difficult for business organizations to choose the right technology when deploying WLAN solutions (Railsback, 2001). This is further complicated for manufacturing enterprises such as AAM where networks in plant-floor environments are combined with configurations in office and residential settings. WLAN technologies must by design interface with all areas of AAM's network infrastructure, thereby making interoperability a necessity.

AAM's in-place wireline technologies are of limited effectiveness in connecting employees while at work and at home to the AAM network (Blair, 2002). The company's wireline infrastructure does not allow employees on the move to leverage the time they spend at meetings, in the cafeteria, and other locations to catch up on e-mail, retrieve information, or perform other work-related activities ("*Wireless LANs*," 2001).

By contrast, the way Microsoft employees interact at work is dramatically affected by the company's installation of Institute for Electrical and Electronic Engineers (IEEE) 802.11b WLANs (Orenstein, 2001a). Microsoft employees no longer attend virtual meetings via desktop videoconferences at the workplace. Instead, they go to a real meeting place and bring their offices with them by wirelessly connecting their laptops to corporate Information Technology (IT) resources.

Large manufacturing enterprises must also consider the cost and time required to install and operate wireline networks in office and production facilities (Blackwell, 2001). For example, the Total Cost of Ownership (TCO) for a WLAN in the typical small office is 15% lower than the TCO for a wired LAN. The spread between wired and wireless LAN TCO is likely to be greater for LANs installed in large manufacturing facilities. These plant-floor LANs are common in AAM's facilities and are comprised of

thousands of feet of cable (Blair, 2002). This cabling connects a variety of industrial automation controllers together and facilitates System Control and Data Acquisition (SCADA) along with control program uploads and downloads. Wireless LAN technologies would seem to be more appropriate than a wireline installation in this environment since plant-floor LAN cabling is frequently removed or relocated in reaction to changing manufacturing process requirements.

The limitations of the AAM wireline network also affect networking activities in AAM employee residences (Blair, 2002). Remote users connect to the AAM network using dial-up connections with a maximum data rate of 56 Kilobits per second (Kbps) downstream and 33.6 Kbps upstream. This remote access solution does not provide telecommuters and other less frequent work-at-home users the benefits of untethered high-speed access to corporate applications from Small Office/Home Office (SOHO) venues.

Alternatives include wireline and wireless broadband residential access solutions such as cable modem, Local Multipoint Distribution System (LMDS), Multichannel Multipoint Distribution System (MMDS), Very Small Aperture Terminal (VSAT), and Digital Subscriber Line (DSL) technologies (Littman, 2002). However, LMDS and MMDS services are not available in AAM residential areas. While VSAT, Digital Subscriber Line (DSL), and cable modem services are available in AAM residential areas, these services cannot provide secure connections to AAM's in-place network infrastructure (Blair, 2002).

Companies such as Honeywell, General Motors, and Intel were quick to embrace WLAN technologies and applied a strategic rather than a tactical approach to company

deployments (Moozakis, 2001; "*Honeywell goes*," 2002; "*Wireless 802.11*," 2001).

Honeywell, for example, has a vision and strategy for corporate digitization based on a wireless infrastructure ("*Honeywell goes*," 2002). The company is aggressively deploying WLAN technologies to increase productivity and reduce costs.

In contrast, other companies including Allina Health System, Andersen Cancer Center, and Best Buy reconsidered planned wireless initiatives in light of security inadequacies, changing standards, and equipment interoperability issues (Brewin, 2001b; Lipschultz, 2001; Smith, 2002). Allina, for example, originally planned a full-scale implementation of WLAN technologies throughout company medical facilities. However, security issues forced the company to reconsider the plan. To minimize such cancellations or delays, WLAN suppliers now emphasize that the implementation of wireless technologies must be part of an overall wireless strategy ("*The wireless wave*," 2001). An enterprise wireless strategy minimizes the existence of multiple standards, devices, and applications and allows a company to leverage investments and create tangible business value (Sbihli, 2002).

The goal of this research was to provide large manufacturing enterprises with a model for deploying secure WLAN technologies in offices, manufacturing facilities, and employee residences. The approach was to develop the model from previous research literature, the Modern Systems Development Life Cycle (MSDLC) strategy defined by Whitten, Bentley, and Barlow (1994), and the results of a case study of AAM WLAN initiatives.

Relevance and Significance

WLANs are beginning to replace traditional wired LANs as the preferred approach to the “last ten feet” of enterprise network environments (Singhal, 2001, p. 1). In fact, more than 50% of small-sized and large-sized companies plan to purchase and install WLAN systems. The release of high data rate and Ethernet-equivalent WLAN technologies is primarily responsible for this trend ("*IEEE 802.11b*," 2001). Low cost, high-speed, and interoperable products provide corporate personnel the flexibility to wirelessly transfer large data files, access the Internet, support videoconferencing, and rapidly reconfigure networked sites. WLANs also increase productivity by encouraging greater collaboration among employees (Singhal, 2001).

Most WLAN systems use spread spectrum technology (Garg, 2001). This wideband Radio Frequency (RF) technique uses the entire allotted spectrum in a shared manner as opposed to dividing the allotted spectrum and employs Frequency Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS) modulation. The IEEE 802.11 family of standards employs spread spectrum solutions.

The IEEE 802.11 specification and its extensions provide the framework for broadband Fixed Wireless Access (FWA) LAN implementations (Littman, 2002). IEEE 802.11 extensions include IEEE 802.11a, IEEE 802.11b, and the recently approved first draft of IEEE 802.11g (Krazit, 2001). IEEE 802.11-compliant WLAN systems provide 1 Mbps or 2 Mbps transmission in the 2.4 GHz (Gigahertz) band using either FHSS or DSSS modulation techniques (O'Hara & Petrick, 1999). IEEE 802.11b-compliant WLAN solutions deliver data rates up to 11 Mbps. IEEE 802.11a-compliant WLAN solutions

provide data rates up to 54 Mbps in the 5 GHz band, and IEEE 802.11g-compliant WLAN solutions deliver data rates up to 54 Mbps in the 2.4 GHz band.

Bluetooth is an evolving third-generation specification that provides the framework for Wireless Personal Area Network (WPAN) implementations (Littman, 2002). Bluetooth short-range low-power solutions employ FHSS technology to eliminate signal interference, Time-Division Duplexing (TDD) for modulation, and Forward Error Correction (FEC) to limit the effects of random noise. Bluetooth WPANs are rapidly deployed and capable of data rates up to 720 Kbps in the 2.4 GHz band.

Companies deploying high rate WLAN technologies must be aware of possible interference between IEEE 802.11 WLAN and Bluetooth WPAN devices sharing the same 2.4 GHz RF spectral bands (Brewin, 2001a). IEEE 802.11b-compliant WLANs support network operations at hospitals, university campuses, retail stores, and warehouses (Wheat, Hiser, Tucker, Neely, & McCullough, 2001).

WLAN technologies offer large manufacturing companies the ability to enable wireless mobility throughout a facility ("*IEEE 802.11b*," 2001). WLANs also facilitate the addition or relocation of workstations and the connection of users in areas where the installation of a wireline network is difficult. However, as widespread deployment of WLAN technologies continues, companies must ensure that wireless networks integrate with wireline networks to form a seamless infrastructure.

The model for the deployment of WLAN solutions based on outcomes from this inquiry facilitates the WLAN implementation process in large manufacturing companies. This research contributed to the body of knowledge and improved professional practice by employing a MSDLC approach (Whitten, Bentley, & Barlow, 1994). The MSDLC

approach contributed to the development of a WLAN model that facilitates the development, design, and implementation of enterprise wireless initiatives. As indicated, this model was based on previous research literature and real life lessons drawn from a case study of AAM WLAN projects (Yin, 1994).

In terms of the MSDLC, Phase 1 or the Systems Planning Phase identified and prioritized wireless technologies and applications that provided the greatest return on investment to a large manufacturing company such as AAM (Whitten et al., 1994). Activities performed in Phase 1 included specifying the business mission, defining an information architecture, and evaluating business areas. Phase 2 or the Systems Analysis Phase studied current company networks and defined user requirements and priorities for the WLAN. Phase 2 consisted of three basic activities: surveying project feasibility, analyzing current infrastructures, and defining and prioritizing user requirements.

Phase 3 or the Systems Design Phase of the process included the evaluation of different wireless systems and the specification of a detailed WLAN solution (Whitten et al., 1994). The criteria for evaluating WLAN effectiveness in terms of business requirements included performance, manageability, and cost (Molta & Laxminarayanan, 2002). In addition, factors such as interoperability, reliability, scalability, ease of deployment, ability to upgrade, industry compliance, power consumption, and VPN compatibility were considered (Molta, 2001). Security issues were addressed through the assessment of both industry standard and proprietary wireless security solutions.

The Systems Design Phase or Phase 3 was followed by Phase 4, the Systems Implementation Phase, which involved the construction of the wireless network and the delivery of a working system into day-to-day operation (Whitten et al., 1994). The final

stage of this MSDLC process was Phase 5 or the Systems Support Phase. Phase 5 involved ongoing support and included program maintenance and system improvement.

Barriers and Issues

The goal of this research was ambitious and had not already been met for a number of reasons. The complexity of planning, designing, and implementing WLAN technologies in a large manufacturing company such as AAM is a deterrent to WLAN deployment (Chen, 2002; Coffee, 2002; Crump, 2001b; Dulaney, 2002; Geier, 1999, 2001; Moozakis, 2001; MSI Editors, 2001; Rogak, 2001; Sbihli, 2002). Underlying issues at AAM included non-standard network configurations across the company's worldwide facilities, a shortage of IT Department resources, and security weaknesses inherent in the Wired Equivalent Privacy (WEP) algorithm (Blair, 2002; Fluhrer, Mantin, & Shamir, 2001). An additional challenge was the complexity of integrating new WLAN technologies with existing wireline infrastructures (Fluhrer et al., 2001). The resultant mixed-mode wireless and wired configuration should operate more efficiently than the previous single-mode implementation.

The emergence of competitive IEEE WLAN standards such as 802.11b, 802.11a, and 802.11g complicates the process of maintaining WLAN device interoperability across a large enterprise (Curl, 2001). In addition, countries in the European Union and members of the European Telecommunications Standards Institute (ETSI) promote their own WLAN standards such as High Performance Radio Local Area Network-Type 1 (HiperLAN-1) and High Performance Radio Local Area Network-Type 2 (HiperLAN-2)

(Bourin, 2001). This is an issue for AAM and other global manufacturers intending to implement a common WLAN solution across national boundaries and in all facilities.

Enterprise managers considering WLAN technologies must determine which available or emerging technology is the best fit based upon project timing, equipment compatibility, equipment availability, the existing network topology, and the available budget ("*The wireless wave*," 2001). IT managers must be careful to implement wireless applications as part of an overall wireless strategy and not just as isolated solutions.

Research Questions

One of the most important steps in conducting a case study is the definition of research questions (Yin, 1994). Often the most difficult challenge an investigator must overcome is to design research questions that will direct the study enough but not too much (Stake, 1995). This researcher strived to answer the following questions:

- What are effective procedures for planning, designing, and implementing a WLAN solution in a large manufacturing enterprise?
- What are the major benefits and limitations associated with WLAN utilization?
- What WLAN technologies and standards are currently available for deployment?
- What existing and projected WLAN technologies and standards are most appropriate for deployment?
- What mechanisms adequately secure the integrity of WLAN transmissions?
- What WLAN strategies should be employed to ensure the most effective use of wireless technology?

Limitations and Delimitations

A number of restrictions beyond the control of the researcher influenced the study. These constraints included limitations related to corporate business objectives, resource availability, and changing WLAN standards and technologies. For example, the wireless initiatives that served as the subject of the case study were selected based on appropriateness to the research and ability to return immediate value to the corporation. Resource availability including monetary and IT staff was another limiting factor. The wireless projects were funded from a predefined departmental expense budget, and staff were required to complete the projects along with their regular work activities. In addition, changing wireless standards and technologies delayed progress until the required standards-based hardware and software became available.

In addition to the aforementioned limitations, several constraints influenced the scope and focus of the study. Delimitations that restricted the wireless technologies deployed included the size of the WLAN user groups and the length of time allotted for project completion. For example, the focus of one of the projects was the use of WLAN technologies by users with new laptops configured with the Microsoft Windows 2000 operating system. In addition, the projects needed to be deployable in a 12-month period with limited resources and no negative affect on manufacturing operations.

Definition of Terms

The following are definitions of key terms used throughout this investigation:

2.5G - A term used to describe digital cellular phone technologies that are between second-generation and third-generation (Mitchell & Kay, 2001). 2.5G wireless systems provide fast data transfer, enhanced e-mail, and Internet access. For example, 2.5G deployments by AT&T Wireless and T-Mobile, based on General Packet Radio Service (GPRS) technology, provide a maximum transfer rate of 144 Kbps.

3G (Third-Generation) - A term used to describe digital cellular phone technologies designed to transmit enhanced multimedia such as voice, data, video, and remote control (Agrawal, 2002). The Universal Mobile Telecommunications System (UMTS) is a 3G system that is standardized in the European Union (Littman, 2002). Wideband-Code Division Multiple Access (Wideband-CDMA or W-CDMA) and CDMA2000, the primary 3G technologies, support both circuit-switched and packet-switched operations (Komagan, 2000). W-CDMA solutions enable transmission rates up to 2 Mbps and provide Quality of Service (QoS) assurances for multimedia applications. In addition, 3G systems facilitate advanced global roaming.

Advanced Encryption System (AES) - AES is the National Institute of Standards and Technology (NIST) standard for secret key cryptography that officially replaced the Triple DES (Data Encryption Standard) method in 2000 as the United States government standard (Smith, 2001). AES protected technologies employ the Rijndael algorithm and are able to encrypt in a single pass instead of three passes. While Triple DES technology is designed for hardware, AES technology is efficient in a range of

environments that include smart carts, programmable gate arrays, and PCs (Personal Computers).

Advanced Mobile Security Architecture (AMSA) - A proprietary security scheme developed for use with IEEE 802.11 WLANs by Agere Systems that specifies authentication and encryption services ("*Agere Systems announces*," 2002). ASMA systems use RC4 (Ron's Code 4) per-user per-session encryption with Diffie-Helman key exchange (Molta, 2001). Authentication is managed by a Remote Authentication Dial-In User Service (RADIUS) server.

ALOHANET - A University of Hawaii research project and the first packet radio network. ALOHANET connected computers at the University's seven campuses on four neighboring islands with a mainframe computer on the island of Oahu (Geier, 2001). ALOHANET operated at 9600 bps (bits per second) and was the basis of Ethernet (Abramson, 2002).

American Radio Relay League (ARRL) - An organization of approximately 163,000 radio experimenters that promotes interest in amateur radio communications and experimentation ("*About the ARRL*," 2002). The ARRL maintains a standard of conduct for radio operators and represents United States radio amateurs with the Federal Communications Commission (FCC) and other government agencies in the United States and abroad.

Asynchronous Transfer Mode (ATM) - ATM is a broadband network technology that supports voice, video, and data transmissions at rates from 1.544 Mbps to 13.21 Gbps (Gigabits per second) (Littman, 2002). ATM networks employ Classes of

Service (COS) to optimize network performance. Each COS supplies a different level of service and associated Quality of Service (QoS) guarantees.

Basic Service Set (BSS) - A set of wireless stations that are logically associated with one another (Gast, 2002). The BSS is the building block of IEEE 802.11 wireless networks.

Bluetooth - A wireless networking technology that operates globally in the 2.4 GHz license-exempt RF band (Littman, 2002). Bluetooth technology is designed for short-range, low-power transmission of voice and data between mobile and desktop devices. Bluetooth Wireless Personal Area Networks (WPANs) are freestanding and ad hoc network configurations that function without a wireline infrastructure. Bluetooth WPANs employ FHSS technology to minimize signal interference.

Canadian Radio Relay League (CRRL) - An organization of Canadian amateur radio enthusiasts that merged with the Canadian Amateur Radio Federation in 1993 to form the Radio Amateurs of Canada (RAC) ("*What is Amateur*," 2002). The RAC is the official voice of Amateur Radio in Canada.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) - A network random access control method that was created following the deployment of the Aloha radio network (ALOHANET) (Littman, 2002). ALOHANET's Aloha protocol led to the development of CSMA/CA and CSMA/CD (CSMA/Collision Detection). IEEE 802.11-compliant wireless networks employ access control mechanisms based on the principle of CSMA/CA (Geier, 1999a). CSMA/CD is a commonly used protocol in Ethernet networks.

CDMA2000 - A third-generation (3G) cellular communications technology that employs the 1xRTT (ITU Radio Transmission Technologies) specification as an operating foundation (Littman, 2002). CDMA2000 circuit-mode and packet-mode transmissions are able to achieve data rates reaching 2.4 Mbps.

Computerized Numerical Control (CNC) - A term used to describe automated machine tools used in manufacturing to perform tasks such as milling, punching, turning, and drilling (Martec, 2002). CNC machines are able to produce accurately machined parts at rates greater than manually machined parts. Computer Aided Manufacturing (CAM) systems generate the CNC tool path programs used to machine the required parts.

Complimentary Code Keying (CCK) - CCK is a set of 64 eight-bit code words used to encode data for IEEE 802.11b-compliant WLANs transmitting at rates of 5.5 Mbps and 11 Mbps in the 2.4 GHz band ("*CCK*," 2002). CCK code words have unique mathematical properties that allow them to be distinguished from one another in noisy environments. CCK works in conjunction with the DSSS technology specified in the IEEE 802.11b standard.

Customer Premises Equipment (CPE) - Communications equipment that is located on the customer's premises ("*CPE*," 2002).

Cyclic Redundancy Check (CRC) - A technique used to check the accuracy of digital data transmissions (Scott, 1999). A CRC performs a mathematical calculation on a block of data and returns a number or fingerprint that represents the organization and content of that data. The number that is used to identify the data is called a checksum.

Digital Signal Processor (DSP) - A specialized microprocessor designed to manipulate analog information that has been converted to digital format ("*Digital signal*," 2002).

Digital Subscriber Line (DSL) - A high bandwidth transmission service that operates over standard copper telephone lines (Flickenger, 2002). A range of transmission rates are supported depending on the DSL variant used. Asymmetric Digital Subscriber Line (ADSL), for example, supports rates ranging from 1.544 Mbps to 8 Mbps within 18,000 feet of the telephone company central office (Littman, 2002).

Direct Sequence Spread Spectrum (DSSS) - A radio transmission technique that spreads the RF signal over a wide frequency band and continuously alters the transmission pattern by constantly changing the data pattern (Gast, 2002). DSSS multiplies the data bits by a pseudo-random bit pattern. This spreads the data over a coded stream that utilizes the full bandwidth of the channel.

Dynamic Security Link - A proprietary security mechanism developed by 3Com for use in IEEE 802.11 WLANs ("*3Com unveils*," 2002). Dynamic Security Link provides authentication and 128-bit encryption. In addition, each user is given a unique key, which is changed every session.

EAP-MD5 (Extensible Authentication Protocol - Message Digest 5) - EAP-MD5 is a challenge handshake authentication protocol that enables the authentication of remote clients of Ethernet LANs ("*EAP*," 2002).

EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) - An EAP type used in certificate-based security environments ("*EAP*," 2002). EAP-TLS

enables encryption method negotiation, mutual authentication, and secure private key exchange for wireless LANs.

EAP-TTLS (Extensible Authentication Protocol - Tunneled Transport Layer Security) - A proprietary protocol developed by Funk Software and Certicom (Funk, 2002b). EAP-TTLS is a strong authentication method that operates in conjunction with the IEEE 802.1x security protocol. In addition to enhancing WLAN security, EAP-TTLS reduces WLAN management tasks.

Enterprise Resource Planning (ERP) - An all-in-one integrated information system that is utilized by the manufacturing industry (Freedman, 2002). ERP systems typically include software modules for shipping, receiving, manufacturing, order entry, accounts receivable and payable, general ledger, purchasing, and human resources. ERP application companies include SAP, Oracle, PeopleSoft, Oracle, Baan, and J.D. Edwards.

Ethernet - A local area network medium access method that operates at 10 Mbps, 100 Mbps (Fast Ethernet), 1 Gbps (Gigabit Ethernet), and 10 Gbps (10 Gigabit Ethernet) (Littman, 2002). Ethernet is the technology of choice for LAN implementations in schools, hospitals, government agencies, libraries, and corporations.

European Telecommunications Standards Institute (ETSI) - ETSI is a multinational body of 912 members from 54 countries with regulation and standardization authority over much of Europe ("*ETSI*," 2002). ETSI represents administrations, network operators, manufacturers, service providers, and research bodies. The Institute develops a wide range of telecommunications, broadcasting, and information technology standards and technical documentation. Examples include the

Global System for Mobile Communications (GSM), HiperLAN-1 and HiperLAN-2 standards.

Extended Service Set (ESS) - A set of two or more wireless Access Points (APs) and associated wireless devices in the same network subnet (Gast, 2002). When all stations are configured to recognize each other, link layer roaming is possible.

Extended Service Set Identifier (ESSID) - The name that identifies an IEEE 802.11 wireless network ("*WiFi Alliance*," 2002). Also called Service Set Identifier (SSID), Network Name, Preferred Network, or Wireless LAN Service Area, the ESSID differentiates one WLAN from another. The ESSID is a 32-character unique identifier attached to packet headers transmitted over an IEEE 802.11-compliant WLAN. All APs and devices attempting to connect to a specific WLAN must use the same ESSID.

Extensible Authentication Protocol (EAP) - An extension of Point-to-Point Protocol (PPP), EAP enables a number of authentication protocols and is not tightly bound to the security method (Blunk & Vollbrecht, 1998). PPP enables the transport of multi-protocol packets over point-to-point links. PPP is extended by EAP, which provides negotiation of an authentication protocol for authenticating peers before allowing network layer protocols to transmit over a data link.

Frequency Hopping Spread Spectrum (FHSS) - A radio transmission technique where the data signal is modulated with a narrowband carrier signal that hops in a random but predictable sequence from frequency to frequency as a function of time over a band of frequencies ("*FHSS*," 2002). Two types of spread spectrum systems are most frequently used: FHSS and DSSS (Perez-Jimenez, Riera, & Lopez-Hernandez, 2001).

The unauthorized monitoring of FHSS transmissions is extremely difficult because a fixed frequency is not used.

Gantt Chart - A floating horizontal bar chart developed as a production control tool in 1917 by Henry L. Gantt ("*Gantt chart*," 2002). Gantt charts show the progress of a project in relation to time. The horizontal axis of a Gantt chart represents the total time span of a project and a vertical axis represents the tasks that make up a project.

General Packet Radio Service (GPRS) - GPRS is an advanced second-generation cellular telephone solution capable of data rates up to 171.2 Kbps (Littman, 2002). GPRS networks are packet-switched and operate in conjunction with GPRS circuit-switched networks.

Global System for Mobile Communications (GSM) - A second-generation digital cellular phone solution popular throughout the European Union, South America, Asia, Australia, New Zealand, Africa, and the Middle East (Littman, 2002). GSM uses Time-Division Multiple Access (TDMA) and Frequency-Division Multiple Access (FDMA) technologies for base station carrier frequency assignment.

High Performance Radio Local Area Network (HiperLAN) - A wireless standard developed and endorsed by the ETSI (Littman, 2002). HiperLAN-Type 1 (HiperLAN-1) supports wireless operations and communications services in infrastructure-based and ad hoc configurations. HiperLAN-1-compliant systems operate in the 5 GHz frequency band and support data rates up to 20 Mbps ("*ETSI HIPERLAN/1*," 2002).

HiperACCESS - A wireless standard defined by the ETSI ("*ETSI approves*," 2002). HiperACCESS-compliant systems support fixed wireless point-to-point communications with data rates up to 100 Mbps.

HiperLAN-2 (HiperLAN-Type 2) - A radio LAN (RLAN) specification, developed by the ETSI, that supports wireless operations and communications services in infrastructure-based and ad hoc configurations (Littman, 2002). HiperLAN-2-compliant systems operate in the 5 GHz frequency band and support data rates up to 54 Mbps ("*ETSI HIPERLAN/2*," 2002).

HiperLINK - A wireless standard defined by the ETSI (Prasad & Prasad, 2001a). HiperLINK-compliant solutions provide interconnections between HiperLAN and HiperACCESS compliant systems. HiperLINK-compliant systems support data rates up to 155 Mbps.

HomeRF - A home wireless networking standard created by the HomeRF Working Group ("*HomeRF*," 2001). HomeRF specifies FHSS technology and the Shared Wireless Access Protocol (SWAP) to enable an open standard for short-range transmission of digital voice and data. HomeRF and Wi-Fi (Wireless Fidelity) solutions are competitors in the marketplace.

Hot Spot - A geographic area covered by a wireless Access Point (AP) that allows users to connect to the Internet ("*Hot spot*," 2002). Hot spots are typically located in airports, train stations, hotels, and convention centers.

IEEE 802.11 - A specification by the IEEE that defines WLAN operations at Layer 1 and Layer 2 of the OSI (Open Systems Interconnection) Reference Model (Littman, 2002). The IEEE 802.11 standard specifies an open architecture and

interoperability between WLAN equipment in multivendor environments. The initial IEEE 802.11 standard specified a 2.4GHz operating frequency with data rates of 1 Mbps and 2 Mbps (Geier, 2002a). When deploying a wireless LAN using the initial specification, either FHSS or DSSS can be selected.

IEEE 802.11a - An extension of the IEEE 802.11 specification (Geier, 2001). IEEE 802.11a-compliant WLAN solutions employ Orthogonal Frequency Division Multiplexing (OFDM) technology and support data rates up to 54 Mbps in the 5 GHz frequency band.

IEEE 802.11b - An extension of the IEEE 802.11 specification (Geier, 2001). IEEE 802.11b-compliant WLAN solutions employ DSSS technology and support data rates up to 11 Mbps in the 2.4 GHz frequency band (Geier, 2001). Most present-day WLAN installations comply with IEEE 802.11b, which is also the basis for Wi-Fi certification from the Wi-Fi Alliance (Geier, 2002a).

IEEE 802.11g - An evolving extension of the IEEE 802.11 specification ("*Wireless LAN glossary*," 2002). IEEE 802.11g-compliant WLAN solutions employ OFDM technology and support data rates up to 54 Mbps in the 2.4 GHz frequency band. The IEEE 802.11g Extension will implement all mandatory elements of the IEEE 802.11b Extension and allow IEEE 802.11b clients to associate with IEEE 802.11g-compliant APs (Geier, 2002a).

IEEE 802.11i - An evolving security extension of the IEEE 802.11 standard that specifies encryption that is stronger than WEP (Vaughan-Nichols, 2002). IEEE 802.11i replaces WEP's RC4 encryption algorithm with Temporal Key Integrity Protocol (TKIP) and AES.

IEEE 802.1x - A security protocol defined by the IEEE 802.11 specification ("*802.11 security*," 2002). Combined with an authentication protocol such as EAP-TLS or EAP-TTLS, IEEE 802.1x-compliant WLANs provide port-based access control and mutual authentication between clients and APs via an authentication server. IEEE802.1x-enabled WLANs also provide a method for distributing encryption keys dynamically to WLAN devices.

Independent Basic Service Set (IBSS) - A set of wireless devices operating without an AP (Gast, 2002). Devices in an IBSS network operate in ad hoc or peer-to-peer mode.

Industrial, Scientific, and Medical (ISM) Bands - Bands of frequencies originally reserved internationally for non-commercial use of RF electromagnetic fields for industrial, scientific, and medical purposes ("*ISM band*," 2002). The ISM bands are defined by the International Telecommunications Union-Telecommunications Standards Section (ITU-T). IEEE 802.11-compliant WLANs operate in ISM bands.

Infrared (IR) - Invisible light waves with wavelengths between .75 and 1,000 microns (Geier, 1999b). Direct infrared platforms support point-to-point connections and are dependent on direct line of sight for transporting data (Littman, 2002). Diffuse infrared platforms support multipoint-to-multipoint connections and are not dependent on a direct line of sight for information transport.

Initialization Vector (IV) - A term used to describe the exposed key in a cryptographic header (Gast, 2002). The IEEE 802.11b WEP initialization vector is 24 bits in length.

Institute of Electrical and Electronics Engineers (IEEE) - The IEEE is an organization of more than 377,000 engineers, scientists, and students in 150 countries ("*About the IEEE*," 2002). The IEEE is engaged in setting standards for computers and communications and produces 30% of the world's published literature in electrical engineering, computers, and control technology.

Infrared Data Association (IrDA) - IrDA is an international organization that creates and supports low cost, interoperable infrared data interconnection standards ("*The Infrared*," 2002). IrDA's membership is composed of hardware, systems, software, and communications manufacturers.

Infrared Link Access Protocol (IrLAP) - IrLAP is an IrDA protocol that enables the establishment of a logical relationship and the transmission of data between two IrDA-compliant machines (Rodbell, 2002).

Infrared Physical Medium Dependent (PMD) - The PMD sub-layer of the Physical Layer enables the actual transmission and reception of data between two IR stations ("*Reducing total cost*," 2002). The PMD service interfaces with the air and modulates and demodulates frame transmissions.

Infrared Physical Layer Convergence Procedure (PCLP) - The PCLP layer delivers incoming frames from the infrared medium to the Medium Access Control (MAC) layer ("*Physical*," 2002). The PLCP layer communicates with the MAC layer through the Physical Layer Service Access Point (PLSAP).

IP Security Protocol (IPSec) - A group of protocols developed by the Internet Engineering Task Force (IETF) to secure packet exchange at the IP layer ("*IPSec*," 2002). IPSec enables secure transmissions via Virtual Private Networks (VPNs).

IrDA Link Management Protocol (IrLMP) - The IrLMP is a protocol for IrDA-compliant devices that enables walk-up, ad hoc connection between devices (Seaborne, Williams, & Novak, 1996). The protocol supports the operation of concurrent and independent multiple software applications.

IrDA Serial IR (IrDA-SIR) - IrDA-SIR is the physical layer that enables half-duplex IR connections with data rates up to 115.2 Kbps (Freedman, 2002).

Keyguard - A proprietary encryption method developed by Symbol Technologies to provide an advanced mechanism for securing Symbol WLANs ("*MobiusGuard*," 2002). Keyguard is an enhancement of the TKIP encryption standard.

Lightweight Authentication Protocol (LEAP) - A proprietary version of the Extensible Authentication Protocol (EAP) developed by Cisco Systems to secure WLANs ("*Cisco's use*," 2002). LEAP enables user-based central authentication in addition to per-user WEP session keys.

Local Multipoint Distribution System (LMDS) - A line of sight digital wireless transmission technology that supports fixed wireless access point-to-multipoint networking solutions (Littman, 2002). LMDS business networks support downstream transfer rates ranging between 51.84 Mbps and 155.52 Mbps. The technology is designed to connect the last mile from a carrier to a large building or campus with high-bandwidth communications ("*LMDS*," 2002).

Logical Link Control (LLC) - LLC is one of two sublayers of Layer 2 of the OSI Reference Model ("*The 7 Layers*," 2002). The LLC layer controls flow control, frame synchronization, and error checking.

MAC Service Data Unit (MSDU) - A MSDU is the higher-level data such as multicast packets transferred by the MAC to another MAC on the network (Gast, 2002). The primary service of the IEEE 802.11 standard is to deliver MSDUs between LLC connections to the network (Geier, 1999a).

Medium Access Control (MAC) - The function in IEEE networks that mediates the use of network capacity and determines which stations are allowed to use the medium for transmission (Gast, 2002).

Mini PCI (Mini Peripheral Component Interconnect) - Mini PCI is a specification that defines a small form factor version of the PCI card ("*Mini PCI*," 2002). Mini PCI cards use a qualified subset of the same electrical definitions, signal protocol, and configuration definitions as the conventional PCI specification.

Modern Systems Development Life Cycle (MSDLC) - A process used by systems analysts, engineers, and programmers to build information systems (Whitten et al., 1994). The five phases of the MSDLC are Systems Planning, Systems Analysis, Systems Design, Systems Implementation, and Systems Support.

Multichannel Multipoint Distribution System (MMDS) - MMDS is a line of sight digital transmission technology that enables fixed wireless broadband transmissions and employs protocols that include TDMA, FDMA, and OFDM (Littman, 2002). In Ireland, Mexico, and the United States, MMDS implementations operate in the 2.596-2.644 and 2.686-2.689 GHz licensed frequency bands. MMDS was initially designed to provide one-way cable television service to customers in remote areas. Subsequently, the technology provided two-way data and Internet services to subscribers. MMDS channels

are 6 MHz (Megahertz) wide and operate on frequencies licensed by the Federal Communications Commission (FCC) ("*MMDS*," 2002).

Multimedia Mobile Access Communication (MMAC) - A wireless LAN standard created by the MMAC Committee of the Ministry of Post and Telecom (MPT) in Japan ("*Multimedia Mobile*," 2002). The MPT created the MMAC Committee to study next-generation broadband mobile communication systems (Prasad & Prasad, 2001a). MMAC systems are able to transmit high-quality multimedia content to mobile users at ultrahigh rates.

Narrowband - A term used to describe wireless systems that transmit in a narrow band of frequencies ("*Narrowband*," 2002). The width of this frequency band is typically between 12.5 KHz (Kilohertz) and 25 KHz (Prasad & Prasad, 2001b). Narrowband technology was initially developed by amateur radio operators.

Offset Codebook Mode (OCM) - A mode of AES operation, OCM simultaneously enables privacy and authentication services (Rogaway, 2002). In addition to being simple and efficient, OCB use a provable-security paradigm. Provable-security schemes are those whose assurance does not stem from a failure to find attacks but from proofs and associated bounds and definitions.

Orthogonal Frequency Division Multiplexing (OFDM) - A modulation technique that divides a wide frequency band into multiple narrow frequency bands (Gast, 2002). The transmitted data are inverse multiplexed across multiple subchannels. Inverse multiplexing is a technique that breaks up a high-speed transmission into several low-speed transmissions. The IEEE 802.11a and IEEE 802.11g standards are based on OFDM.

Peripheral Component Interconnect (PCI) - A local data bus standard originally developed by Intel ("*Conventional PCI*," 2002). The PCI specification provides for plug and play, high-speed data connections between a computer's peripheral devices and the Central Processing Unit (CPU).

Personal Computer Memory Card International Association (PCMCIA) - PCMCIA is an international standards body and trade organization founded in 1989 and comprised of over 200 member companies ("*About PCMCIA*," 2002). The association was established to promote standards for integrated circuit cards and interchangeability among Personal Computers (PCs). The small, credit card-sized devices developed by member companies are called PCMCIA cards.

Personal Data Assistant (PDA) - A PDA is a handheld computer that serves as a Personal Information Manager (PIM) (Freedman, 2002). Common applications that are supported on PDAs include e-mail, a calendar, an address book, a task list, and a notepad. Wirelessly enabled PDAs also facilitate access to company LANs and the Internet (Gray & Cowley, 2002).

Physical Layer (PHY) - The Physical Layer is Layer 1 of the OSI Reference Model (Freedman, 2002). Layer 1 provides services to transmit bits over the network and deals only with the electrical and mechanical characteristics of the signals and signaling methods.

Programmable Logic Controller (PLC) - A computer used in manufacturing facilities to control process applications (Freedman, 2002). PLCs are typically RISC-based (Reduced Instruction Set Computer-based) microprocessors designed to operate in real-time, industrial environments.

Protected Extensible Authentication Protocol (PEAP) - A proposed standard for IEEE 802.1x authentication ("*PEAP*," 2002). PEAP enables one-time token authentication, password change, and user database extensibility.

Quality of Service (QoS) - QoS is a term used to describe the ability to define a level of performance in data communications systems (Mitchell, 2002). The goal of QoS is to provide guarantees on ability of a network to deliver predictable results. Elements of network performance covered by QoS are availability, bandwidth, latency, and error rate.

RC4 (Ron's Code 4) - A stream cipher symmetric key algorithm defined by IEEE 802.11. RC4 uses a variable length key up to 256 bytes to initialize a 256-byte state table (Rivest, 2002). The state table is then used to generate a stream that is XORed with the plain text to be encrypted. An exclusive OR (XOR) is a Boolean logic operation that is true if only one of the inputs is true, but not both (Freedman, 2002).

Remote Authentication Dial-In User Service (RADIUS) - A network access control technology that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service ("*Remote Authentication*," 2002). RADIUS access solutions are the de facto industry standard for the authentication of dial-in users.

Small Office Home Office (SOHO) - A term used to describe a business or office that consists of 10 or fewer employees and/or computers ("*WiFi Alliance*," 2002).

System Control and Data Acquisition (SCADA) - A term used to describe a computer system that collects and analyzes real-time data ("*SCADA*," 2002). SCADA systems are employed by the manufacturing, energy, oil, and gas refining industries to control and monitor manufacturing equipment.

T-1 - A 1.544 Mbps point-to-point dedicated, digital circuit provided by the telephone companies ("*T-1 carrier*," 2002). A T-1 connection is composed of 24 individual channels. Each channel has a data transfer rate of 64 Kbps and can be configured to carry voice or data traffic.

Temporal Key Integrity Protocol (TKIP) - A wireless security protocol that enables initialization, vector hashing, and message integrity checking to counteract passive snooping and determine if packets have been modified by an unauthorized user ("*Enhancing wireless*," 2002).

Terminal Node Controller (TNC) - A device that converts digital signals from a computer to signals that a ham radio is able to modulate and transmit (Geier, 2001).

Terminal Service (TS) - An option of Microsoft Windows NT 4.0 and Microsoft Windows 2000 Server operating systems that enables multiple client computers to run a server application simultaneously (Freedman, 2002). All application logic is performed in the server. Client computers only display screen changes and the user interface.

Time Division Duplexing (TDD) - A transmission method, developed by Bell Labs, that divides the entire bandwidth of the transmission medium into a sequence of timeslots (Littman, 2002). Each timeslot uses the entire frequency range for an assigned interval of time. TDM adjusts time intervals to promote efficient use of the available bandwidth.

Time Division Multiple Access (TDMA) - A technology for delivering digital wireless service ("*TDMA*," 2002). TDMA uses Time Division Multiplexing (TDM) to enable a single frequency to support multiple, simultaneous data channels. TDMA divides a radio frequency into time slots that are allocated to multiple calls.

Time Division Multiple Access/Time Division Duplexing (TDMA/TDD) - A communications technique that uses a single channel to transmit and receive data (Freedman, 2002). In addition, the technology interleaves multiple digital signals onto the same channel.

Total Cost of Ownership (TCO) - An expression that recognizes the cost of technology is often far greater than the technology's initial purchase price ("*Reducing total cost*," 2002). For example, the initial cost of a PC is only a small fraction of the total cost of using, connecting, maintaining, and disposing of the PC.

Ultra High Frequency (UHF) - A term used to describe the band of electromagnetic frequencies from 300 MHz to 3 GHz (Freedman, 2002).

Ultrawideband (UWB) - UWB is a short-range wireless technology that enables transmission and reception of very short baseband signals without a carrier (Siwiak & Huckabee, 2002). The technology reuses previously allocated RF bands by spreading RF energy thinly in a wide spectrum.

Universal Serial Bus (USB) - A hardware interface used to connect peripherals such as a mouse, scanner, and keyboard to a computer (Freedman, 2002).

Very High Frequency (VHF) - A term used to describe the electromagnetic frequencies in the range from 30 MHz to 300 MHz (Freedman, 2002).

Virtual Private Network (VPN) - A private network that is configured within a public network such as the Internet (Freedman, 2002). A VPN employs access control and encryption to ensure that only authorized users are able to access the network and that the data cannot be intercepted. VPN security mechanisms include tunneling protocols

such as Generic Routing Encapsulation (GRE) and Layer Two Tunneling Protocol (L2TP) and encryption protocols such as IPSec (Vaughan-Nichols, 2002).

Very Small Aperture Terminal (VSAT) - An earthbound device used to receive satellite data, voice, and video transmissions ("VSAT," 2002). The very small component of the acronym refers to the three to six feet diameter of the VSAT dish antenna. A VSAT system consists of two parts. The first is a transceiver that is placed outdoors in line of sight of the satellite. The second is an interface device that is placed indoors to connect the transceiver to the user's PC or network. While early VSAT systems were only able to achieve data rates of 56 Kbps, current systems, designed for SOHO venues, are capable of downlink data rates of 2 Mbps and uplink data rates of 19.2 Kbps (Littman, 2002).

WEPlus - A proprietary extension to the IEEE WEP encryption developed by Agere Systems (Baxter, 2001). WEPlus enhances WEP security by eliminating the propagation of the weak key patterns identified by Fluhrer, Mantin, and Shamir (2001).

Wideband Code Division Multiple Access (W-CDMA) - W-CDMA is a high-speed 3G mobile wireless technology that supports both circuit-switched and packet-switched operations (Littman, 2002). W-CDMA solutions enable transmission rates up to 2 Mbps and provide Quality of Service (QoS) assurances for multimedia applications.

Wideband Frequency Hopping (WBFH) - This FHSS technology operates in the 2.4 GHz frequency band (Paulo & Wolf, 2000). Unlike standard frequency hopping systems that use a 1 MHz wide channel for transmission, WBFH systems employ a 5

MHz wide channel. This wider transmission channel supports transmissions ranging from 2 Mbps to 10 Mbps.

Wi-Fi Alliance - A nonprofit international association formed in 1999 to certify the interoperability of broadband Fixed Wireless Access (FWA) Ethernet LAN products based on the IEEE 802.11 specification (Littman, 2002; "What is Wi-Fi," 2002). The organization has 193 member companies, and more than 522 WLAN products have received Wi-Fi certification ("What is Wi-Fi," 2002). Certified products feature Wi-Fi logos. The Wi-Fi Alliance was formerly known as the Wireless Ethernet Compatibility Alliance (WECA).

Wi-Fi Protected Access (WPA) - A WLAN security standard issued by the Wi-Fi Alliance (Grimm, 2002). WPA is designed to replace WEP and addresses WEP security weaknesses such as highjacking and man-in-the-middle attacks by supporting a higher level of encryption and the dynamic exchange of encryption keys.

Wired Equivalent Privacy (WEP) - An optional IEEE 802.11 wireless security protocol designed to enable frame transmission privacy similar to a wired network (Geier, 1999b). WEP-enabled systems generate secret shared encryption keys that both destination and source stations use to encrypt transmissions.

Wireless Application Protocol (WAP) - A secure standard that supports instant access to information from handheld wireless devices such as mobile phones, pagers, two-way radios, and smart phones ("WAP," 2002). WAP-enabled systems provide a complete environment for wireless applications that includes a wireless equivalent of Transmission Control Protocol/Internet Protocol (TCP/IP).

Wireless Local Area Network (WLAN) - A computer network covering a local area such as an office or a home that uses radio waves instead of wires as a carrier ("Wireless LAN," 2002). Early WLANs included industry-specific solutions and proprietary protocols that were replaced in the late 1990s by standards-based solutions such as IEEE 802.11b-compliant and HomeRF-compliant WLANs.

Work in Progress (WIP) - A term used to describe the portion of a manufacturing company's inventory that is neither raw materials nor finished goods (Wasp, 2002). A WIP consists of materials that will be integrated into sub-assemblies as part of the process of building a finished product.

Summary

The rate at which companies are deploying wireless LAN technologies has surpassed analysts' expectations (Bassuener, 2001). In fact, the WLAN market is expected to grow from 3.3 million units in 2000 to 23.6 million units in 2005. WLAN technologies provide companies with many competitive advantages when properly leveraged.

In this chapter, this investigator began by describing the problem investigated and the goal that was achieved. The focus of this research was to define procedures for enabling large manufacturing enterprises to effectively plan, design, and implement WLAN technologies. The goal of this research was to provide a model for those companies to use when deploying WLAN technologies in offices, manufacturing facilities, and employee residences. An analysis of the relevance and significance of the research along with a discussion of barriers and issues related to achieving the goal were presented. Limitations and delimitations associated with the investigation were also reviewed. Finally, research

questions related to the inquiry and definitions of key terms used throughout this inquiry were provided.