

2009

A Model for Using Managed Services in Designing and Supporting a Wireless Local Area Network for the Navy Marine Corps Intranet

Joseph L. Roth

Nova Southeastern University, joe@powerfrog.com

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd



Part of the [Computer Sciences Commons](#)

Share Feedback About This Item

NSUWorks Citation

Joseph L. Roth. 2009. *A Model for Using Managed Services in Designing and Supporting a Wireless Local Area Network for the Navy Marine Corps Intranet*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (293) https://nsuworks.nova.edu/gscis_etd/293.

This Dissertation is brought to you by the College of Computing and Engineering at NSUWorks. It has been accepted for inclusion in CCE Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

A Model for Using Managed Services in Designing and Supporting a
Wireless Local Area Network for the Navy Marine Corps Intranet

by

Joseph L. Roth

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

Graduate School of Computer and Information Sciences
Nova Southeastern University

2009

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

_____ John Scigliano, Ed.D. Chairperson of Dissertation Committee	_____ Date
-------------------------------------------------------------------------	---------------

_____ Easwar Nyshadham, Ph.D. Dissertation Committee Member	_____ Date
-------------------------------------------------------------------	---------------

_____ Peixiang Liu, Ph.D. Dissertation Committee Member	_____ Date
---------------------------------------------------------------	---------------

Approved:

_____ Amon Seagull, Ph.D. Dean	_____ Date
--------------------------------------	---------------

Graduate School of Computer and Information Sciences
Nova Southeastern University
2009

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

A Model for Using Managed Services in Designing and Supporting a
Wireless Local Area Network for the Navy Marine Corps Intranet

by

Joseph L. Roth

October 2009

The purpose and content of this work are to explore the proper strategy on how to deploy multi-service mobile net centric warfare, or FORCEnet, the Navy's concept for Net Centric Warfare. In this research, the author examined where the Navy Marine Corps Intranet (NMCI) fits into this vision and how it is mobile and multi-service compatible. It also explored how low-cost commercial approaches such as IEEE 802.11 wireless local area network technologies can be implemented as a joint notion of Net Centric Warfare in terms of a Service Oriented Architecture (SOA). The problem investigated in this study was to evaluate what cost savings and/or efficiencies were achieved by organizing and transitioning from a traditional network operation center to a managed services operation in the development of a wireless local area network (LAN) in a military setting. The military needs a road map on how to deploy wireless networks in a secure, supportable, and usable fashion that is in concert with the core mission of the military business requirements, i.e., a service oriented architecture. The research took place at several naval bases in San Diego. The methodology included the "case study," as described by Robert Yin (2003), and the systems development life cycle (SDLC). The expectation of the researcher in this study is the development of a managed services operation in the creation of a wireless LAN on a military base.

Acknowledgments

I would like to thank Dr. John Scigliano, Dr. Easwar Nyshadham, and Dr. Peixiang Liu for their guidance, patience, and high standards that allowed me to learn. I would also like to thank Steve Frisbie and Ron Broersma for their system engineering assistance and technical mentorship, Chris Collins for his assistance with end-user wireless procedures and policy guidance, Keith Kaufman and Mary Wadsworth for their JTRS project funding, and Lynette Smith, whose editing help allowed me to be 100% APA compliant.

Table of Contents

Abstract	iii
Acknowledgement	iv
List of Tables	vii
List of Figures	viii

Chapters

1. Introduction 1

1.1	Problem Statement and Goal	3
1.1.1	Problem Statement	3
1.1.2	Goal	3
1.2	Relevance and Significance	5
1.3	Barriers and Issues	9
1.4	Background of Case Studies	11
1.4.1	JTRS	11
1.4.2	NMCI and Managed Services	12
1.4.3	Technical Background	18
1.5	Players and Key Organizations	20
1.6	Research Questions Investigated	21
1.7	Summary	22

2. Review of the Literature 24

2.1	Introduction	24
2.2	Theory and Research Literature Specific to the Topic	25
2.3	Contribution This Study Will Make to the Field	41
2.4	Summary of What Is Known and Unknown About the Topic	42

3. Methodology 44

3.1	Introduction	44
3.2	Research Methods Employed	46
3.3	Specific Procedures Employed	57
3.4	Resource Requirements	57
3.5	Summary	61

4. Results 62

4.1	Findings	62
4.2	Technical Issues	69
4.3	Integration with NMCI	71
4.4	Summary of Results	73

5. Conclusions, Implications, Recommendations, and Summary 79

- 5.1 Conclusions 79
- 5.2 Implications 80
- 5.3 Managing the Political Landscape 81
- 5.4 Contracting Challenges and Procurement Strategies 85
- 5.5 Recommendations 90
- 5.6 Summary 93

Appendixes

- A. Interservice Support Agreement 99
- B. Purchase Order 105
- C. Wireless Floor Plan/Access Point Placement 109
- D. User Agreement 119
- E. Support Contractor Statement of Work (SOW) 122
- F. Customer Service Survey 125
- G. Wireless Configuration Instructions 127

Reference List 155

List of Tables

Tables

1. Advantages and Disadvantages of Contracted Managed Services 15
2. Sailor/Marine System Location Matrix 37
3. Technical Task List 60

List of Figures

Figures

1. Wireless Pier Connectivity System (WPCS) 9
2. NMCI Service Level Agreement Briefing by Captain Chris Christopher, 29 March 2001, to Joint Logistics Council 13
3. Managed Services Continuum 27
4. GIG—Holistic View 27
5. Naval Networking Environment 2010–2016 Transformation 38
6. Advantages of SOA Over Client Server Architectures 39
7. Lieutenant General Sorenson’s Transformation Model 40
8. Architectural Development 44
9. DOD Architectural Framework 45
10. SUS Trinity Model 49
11. JTRS Wireless Concept Diagram 52
12. Fleet Anti-Submarine Warfare (ASW) Naval Base Map 53
13. Wainhouse Research Service Delivery and Strategy Models 55
14. 802.11a Point-to-Point Connection, Bird’s Eye View 64
15. 802.11a Point-to-Point Connection, Ground View 64
16. JTRS Buildings with 802.11b/g Wireless Coverage, Bird’s Eye View 65
17. JTRS Buildings with 802.11b/g Wireless Coverage, Ground View 66
18. JTRS Wireless Network “SPAWAR” and “jtrs-guest” 68
19. Edimax Wireless NMCI Connection Device 73

List of Figures (continued)

Figures

- G-1. Microsoft Wireless Configuration SSID Selection Tool 130
- G-2. Microsoft Wireless Configuration Tool Advanced Settings General Tab 131
- G-3. Microsoft Wireless Configuration Tool Advanced Settings Wireless Networks Tab 132
- G-4. Microsoft Wireless Configuration Tool Advanced Settings Association 133
- G-5. Microsoft Wireless Configuration Tool Advanced Settings Association 134
- G-6. Microsoft Wireless Configuration Tool Association Tab Data Encryption Menu 135
- G-7. Microsoft Wireless Configuration Tool Association Tab Data Encryption AES setting 136
- G-8. Microsoft Wireless Configuration Tool Authentication Tab 137
- G-9. Microsoft Wireless Configuration Tool Smart Card Screen 138
- G-10. Microsoft Wireless Configuration SSID Selection Tool 139
- G-11. Microsoft Wireless Configuration SSID Selection Tool 140
- G-12. Microsoft Wireless Configuration SSCSD Connection Screen 140
- G-13. Pin Entry Screen 141
- G-14. Microsoft Wireless Configuration SSID Selection Tool SSCD Authentication Feedback screen 141
- G-15. Microsoft Wireless Configuration SSID Selection Tool Connection feedback Screen 142
- G-16. Microsoft Network Connection Screen 143
- G-17. Microsoft Wireless Configuration SSID Selection Tool “JTRS-Guest” screen 144
- G-18. Network Key Entry Screen 144

List of Figures (continued)

Figures

- G-19. Microsoft Wireless Configuration SSID Selection Tool “JTRS-Guest”
Connection Screen 145
- G-20. Aruba Authentication Screen 146
- G-21. Microsoft Wireless Configuration SSID Selection Tool 147
- G-22. Xerox Driver Run Screen 148
- G-23. Xerox Initial Driver Configuration Screen 149
- G-24. Printer Wizard 150
- G-25. Local Printer Configuration Screen 150
- G-26. Printer Port Configuration Screen 151
- G-27. Printer IP Configuration Screen 152
- G-28. Xerox Driver Configuration Finish Screen 153
- G-29. Printer Selection Screen 154

Chapter 1

Introduction

With the advancement of technology and the economic constraints placed on the Department of Defense (DOD), there is a revolutionary shift to centralize from platform-centric warfare to Net Centric Warfare (Mullen, 2006). Historically, the military uses the platform as the focus of its military doctrine. The platform in this sense is an aircraft, ship, tank, or any other war-fighting apparatus. This focus is called platform-centric warfare. In the past, command and control systems, combat systems, and navigation systems have been tailored and centered on the type of platform. The concept of Net Centric Warfare focuses less on the weapon system or platform, whether it is an airplane, submarine, or surface combatant, and more on how to command and control assets in concert, combining weapon platform assets in network terms.

The U.S. Navy is following suit to include other services and nations: Army, Air Force, and coalition partners (Mullen, 2006). The focus of this work is to explore the proper strategy on how to deploy multi-service mobile Net Centric Warfare, or FORCEnet, the Navy's concept for Net Centric Warfare. In this research, the author examined where the Navy Marine Corps Intranet (NMCI) fits into this vision and whether it is mobile and multi-service compatible. It explored how low-cost commercial approaches, such as IEEE 802.11 wireless local area network technologies, can be

implemented as a joint notion of Net Centric Warfare in terms of a Service Oriented Architecture (SOA).

The goal of FORCEnet and Net Centric Warfare is much more than a technology enhancement. It is a strategy that provides technologies and processes that allow decision makers to make decisions faster. This is realized by connecting information sensors and data nodes to the FORCEnet network at high speeds. One of the physical realizations of FORCEnet is the Navy Marine Corps Intranet (NMCI). The NMCI project office manages a \$9.3 billion contract from Electronic Data Service (EDS) that was awarded in the fall of 2000 “to provide information superiority and to foster innovation via interoperability and shared services” (“DOD Needs,” 2006). As of 2004, NMCI is the world’s largest private network, having over 360,000 desktops in over 300 locations, second in size only to the Internet itself (Dalaklis, 2004). A recent Government Accounting Office (GAO) report claimed that as of June 2006 NMCI had grown further and deployed to 550 locations. The Navy currently employs 350,000 active duty sailors, 130,000 reserves, and 175,000 civilians. The Navy’s annual operating budget is \$120 billion (“DOD Needs,” 2006). The purpose of a managed service provider is to provide technology services that make an organization more efficient and effective and to help align their IT infrastructure with the organization’s business strategic goals (Macioce, 2007). The strategic goal of NMCI is information superiority and the fostering of innovation by having everyone in the Navy and Marine Corps—sailor, marine, reservist, and civilian—on NMCI (“DOD Needs,” 2006).

1.1 Problem Statement and Goal

1.1.1 Problem Statement

The problem investigated in this study was to evaluate what cost savings and/or efficiencies are achieved by organizing and transitioning from a traditional network operation center to a managed services operation in the development of a wireless local area network (LAN) in a military setting. At the end of the 19th century, large corporations were making their own electricity and allocating a large portion of their budgets to electricity-creating machines. Suddenly, there was a shift where companies gave up running their individual electrical plants and turned to being utility providers. This same behavioral shift from a traditional network operation center to a managed services operation is now happening in the wireless information technology realm (Richter, 2007).

1.1.2 Goal

The goal of the researcher in this study was to develop a managed services operation in the creation of a wireless LAN on a military base. In the process of achieving this goal, specific organizational, managerial and technical issues were identified and related to research literature. The focused environment was the Joint Tactical Radio System (JTRS) Program Executive Office (PEO) located at the Anti-Submarine Warfare (ASW) Naval Base in San Diego, California. Specifically, the five buildings that house the Joint Program Executive Office of the JTRS program are to be included in the wireless network. A wireless point-to-point link from a nearby submarine base acted as the Internet Service Provider (ISP) gateway. The result will serve as a lesson learned for NMCI and perhaps as an example on how to deploy wireless on a large

joint scale. Key aspects of this research includes Software as a Service (SaaS), Service Oriented Architecture (SOA), wireless security, and commercial best practices.

This policy of banning wireless networks in the DOD comes indirectly from the 802.11 security concerns documented by Bill Arbaugh and Jessie Walker from 2000 to 2004, specifically with Wired Equivalent Privacy (WEP) encryption, as well as problems with 802.1X wired/wireless extensible authentication protocol (Walker, 2000; Arbaugh, 2001; Arbaugh, 2003a; Arbaugh, 2003b; Arbaugh, 2004). These efforts heavily influenced the IEEE 802.11 security committee and Wi-Fi Alliance interoperability group, producing discernable upgrades to the 802.11 encryption, authentication, and interoperability capability and thus causing the development and eventual ratification of the 802.11i and WPA-2 standards (Institute of Electrical and Electronics Engineers, Inc., 2004). These improvements were also mirrored with the Department of Commerce Federal Information Processing Standard FIPS 140-2 (*Federal Information*, 2001) regarding wireless encryption, essentially using the same technology described in the 802.11i standard, the Advanced Encryption Standard (AES). In 2006, the moratorium on 802.11 and Bluetooth networks was lifted (*Use of Commercial Wireless*, 2006), due to the positive endorsement from academia, industry, and the Department of Commerce. “By fixing the security flaws in WEP, WPA and 802.11i provide not only strong information security for individual stations, but also authentication and access control in the entire network” (Yang, Ricciato, Songwu, & Xhang, 2006, p. 446).

Professor William Arbaugh, a critic of 802.11 specifications, has limited his criticism of WPA-2 to three areas: denial of service, sessions stealing when encryption is not used, and the trust relationship between the Access Point and the Authentication

Server (Arbaugh, 2006). DOD policy requires that all wireless traffic be encrypted and use mutual authentication (*Use of Commercial Wireless*, 2006). This means that the second and third concerns are no longer valid if the implementer follows DOD policy. As for a denial of service, any radio frequency device that publishes its frequency range—in this case, 2.4–2.5 GHz—is susceptible to jamming. This is the bargain the DOD gets for using low-cost, commercially available wireless devices in an unlicensed spectrum. DOD policy mitigates this sole concern by requiring that an intrusion detection system be deployed (*Use of Commercial Wireless*, 2006) that can detect jamming and other wireless denial-of-service attempts. If the DOD wanted to be more secure, it could use licensed spectrum with unpublished/variable frequency ranges. This would drive up the cost, because it could no longer use 802.11 equipment and would require expensive, government-controlled specified hardware, manpower-intensive spectrum management, and active configuration control. Even with all 802.11 security concerns removed/mitigated and clear authorization policy published, NMCI has not announced any plans to deploy 802.11 networks, despite the strong demand and use within commercial industry.

1.2 Relevance and Significance

The military often uses commercial terms and re-labels them for its own purposes. The term *Net Centric Warfare* describes the shift from the platform-centric (aircraft, ships, tanks, etc.) mode of thought and war fighting into a network centric method (information-based command and control method to war fighting). This concept is actually a managed services evolution in a military setting using military language. In the commercial realm, the same transition has already taken place where, prior to managed services, organizations were device centric, focusing on routers, hubs, email, firewalls,

etc. With managed services, the organization becomes more focused on the core mission in a business centric services fashion (Marks, 2006).

Recently changed DOD wireless policy now authorizes 802.11 networks throughout the DOD (*Use of Commercial Wireless*, 2006). The demand for 802.11 networks is growing.

A recent successful test of 802.11 pier-side systems at the Mayport Naval Station, Fla., indicates that the Navy should deploy more wireless systems faster, said Dave Wennergren, chief information officer at the Department of the Navy, at West 2006. Marine Col. Robert Baker, technical director of the Navy Marine Corps Intranet, said the program is working to equip units with wireless systems based on next-generation 802.11i technology. Baker said Wi-Fi-based extensions of NMCI make sense and save money in small offices, such as recruiting stations. ("The Wi-Fi Navy?" 2006)

As of May 2008, no NMCI 802.11 networks have been deployed, and no managed services for 802.11 have been developed. The need for managed services in the Information Technology realm is one of the primary motivators for the Navy to go with NMCI. The Navy claims it has received great benefit from NMCI managed services in terms of cost reduction, higher security levels, and improved efficiencies. This is documented in the recent Government Accounting Office review of the NMCI program.

Navy also cited significant benefits that were to accrue from NMCI, including (1) an uninterrupted flow of information; (2) improvements to interoperability, security, information assurance, knowledge sharing, productivity, and operational performance; and (3) reduced costs. ("DOD Needs," p. 19)

The Navy further claims NMCI can improve customer approval by expanding its services into the wireless domain.

In particular, they point to such new services as broadband remote access for all laptop users, antispam services for all e-mail accounts, and antispyware services for all accounts as having improved customer satisfaction. Further, they said that the planned addition of wireless broadband access will increase customer satisfaction. ("DOD Needs," p. 53)

Until recently, the perceived security concerns made the deployment of wireless networks on a large scale a practical impossibility.

Outside of the recent GAO report, what has been written about NMCI consists of several masters theses from the Naval Postgraduate School (Graves, 2005; Dalaklis, 2004; Rozier, 2002; Fahrenthold, 2002). These works focused on ensuring and measuring performance, account management, and security. None of them addressed the possibility of the implementation of 802.11 networks within NMCI.

In 2004, all new DOD 802.11 wireless networks, both at shore and at sea, were put on hold due to security concerns. Net Warfare Command (NETWARCOM) and Fleet Forces Command (COMFLTFORCOM), which represent the policy and operational leadership of all Navy networks, declared a cessation of new 802.11 networks in the form of two navy radio messages. In 2006, the cessation was lifted with the release of an updated DOD wireless policy (*Use of Commercial Wireless*, 2006). Since that time, there has been no apparent movement within NMCI to deploy any 802.11 networks. It is suspected that this is due to the problem with NMCI's not meeting its primary mission in its wired networks.

The Navy has yet to meet the program's two strategic goals—to provide information superiority and to foster innovation. ...The Navy's mapping shows that NMCI has met only 3 of 20 performance targets (15 percent). This means that the mission-critical information superiority and operational innovation outcomes used to justify NMCI have yet to be attained. ("DOD Needs," 2006, p. 8)

The customer base is also less than satisfied.

Navy's definition of a satisfied user has remained consistently below the target. This means that after investing about 6 years and \$3.7 billion, NMCI has yet to meet expectations, and whether it will is still unclear. ("DOD Needs," 2006, p. 1)

Yet the demand for 802.11 in the commercial sector is heavy. Many major cities in the United States have deployed or plan to deploy citywide wi-fi networks, including Philadelphia, San Francisco, Los Angeles, New Orleans, New York, Washington, D.C., and others. (Bertino & Ruth, 2006). Prior to the 2004 DOD ban, there were temporary 802.11 test beds on several Navy ships. These included three aircraft carriers: USS George Washington, USS Kennedy, and USS Nimitz. Smaller ships also installed 802.11 networks: one Cruiser, USS Princeton; four Destroyers, USS The Sullivans, USS McFaul, USS Howard, and USS Mason; and four Submarines, USS Memphis, USS Norfolk, USS Alaska, and USS Alabama (Piarulli, 2004).

Additionally, a pilot pier services program was started with several ships in Pensacola, Florida, when they were removed from their homeport of Pascagoula, Mississippi, due to Hurricane Katrina (The Department of the Navy, 2008). Historically, when a ship docks it is connected to many cables so it will be connected to all the pier network shore services. This is a labor-intensive process, and the number of ships that can be connected is limited to the pier slots available. When the Wireless Pier Connectivity Systems (WPCS) were employed, the labor and time response effort was discernibly reduced, and the number of ships that could be connected was increased (The Department of the Navy, 2008). Figure 1 shows both traditional wired pier service on the left and the wireless piers on the right.

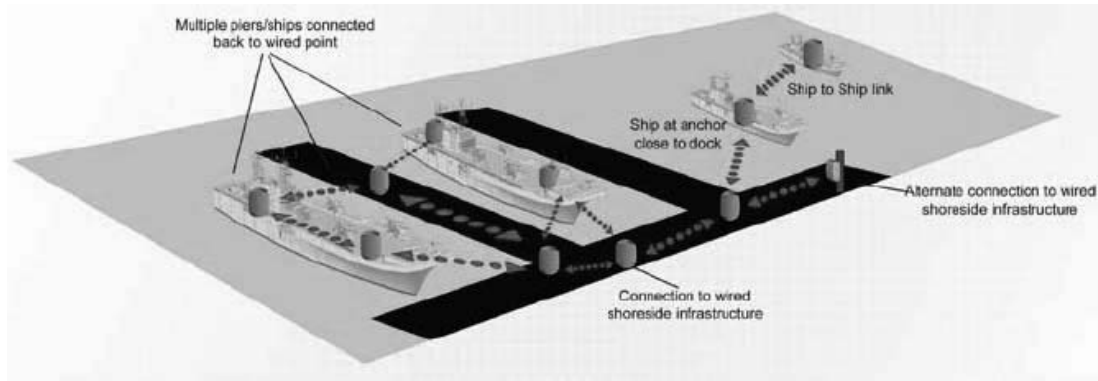


Figure 1. Wireless Pier Connectivity System (WPCS). (The Department of the Navy, 2008)

1.3 Barriers and Issues

Both the JTRS and NMCI programs were riddled with problems in the beginning. The Government Accounting Office has scrutinized both programs. The causes of these problems may be attributed to internal inefficiencies such as organizational conflict. Comprehending and defining these issues can be difficult, as can properly defining the metrics. Publicly admitting fault outside of what is in GAO reports may be one of the politically induced barriers where insiders may not be forthright with criticism for fear of disclosure. This does not mean that the NMCI culture is repressive, or that it actively punishes those who are critical. Nevertheless, whistle blowing in general has few rewards and has been clearly documented in the scholarly literature.

“It almost always turns out badly for the whistleblower,” says James Fisher, director of the Emerson Center for Business Ethics at Saint Louis University. “Often they regret it. They lose their jobs, they have family problems, or they’re shunted off to the side.” The most common reactions of those who discover dubious employer practices are to either leave or look the other way. (McCafferty, 2002)

The core requirements of each program are extremely complex and difficult to measure. Existing measures of success may be inflated, and measures of failures may be deflated.

This may be traced to the desire by senior naval leadership for the program to be perceived as a success. It is also important to note that competition does not exist in the public sector. Due to the lack of competition from simple economic forces, bad programs do not go out of business like bad commercial ventures would. Often, governmental programs have an incremental nature about them where programs are reborn out of the ashes of the failures of the preceding incarnation (Rauch, 1996). This is the case with JTRS and NMCI, that it either has reorganized or is being pressured to change in the form of negative Government Accounting Office reports (“Restructuring JTRS,” 2006; “Briefing to the House,” 2003; “Challenges Associated,” 1999; “Defense Information,” 1998).

Finally, the theoretical concepts of SOA and SaaS have various meanings and are difficult to quantify with precise metrics. Numerous articles and texts have attempted to define Web services and have agreed that there is a variation in the definition of service with subjective interpretations (Allen, 2006; Jones, 2005; Newcomer & Lomow, 2005). One of the major challenges of this research will be to describe the service aspects of the wireless model, as well as to clearly define the metrics.

Cost, schedule, and performance are the key metrics of any well-managed project (Meredith & Mantel, 2006). The most common manner for measuring performance is through earned value metrics. Earned value compares cost, performance, and schedule through several tracking variables. The five key tracking variables of earned value are BCWP, budgeted cost of work performed; ACWP, actual cost of work performed; BCWS, budgeted cost of work scheduled; STWP, scheduled time for work performed; and ATWP, actual time of work performed (Meredith & Mantel, 2006). These metrics

allow a manager to know where a project stands in terms of budgets (costs), calendar (schedule) and performance. When one combines an academic work with an operational project, artificialities can occur where the operational project leadership may develop different goals than the academic research goals. These differences could potentially degrade the researcher's ability to perform his or her job. There may be differences in terms of the allocation of cost, schedule and performance. This budget and time scale may or may not be in synch with the academic research calendar or the academic-desired budget or performance. Normally, funding, permission, and leadership buy-in are challenges to actually deploying a large-scale managed service network. This is not the case in this instance, however. The JTRS leadership has allocated \$200,000 to allow this wireless network to be built. The JTRS leadership has also expressed that the project needs to be operational by the first quarter of 2009.

1.4 Background of Case Studies

1.4.1 JTRS

The Joint Tactical Radio System (JTRS, pronounced "jitters") is the future of military radios through software-defined design within the Department of Defense (DOD). Since 1967, the DOD has been trying to establish a department-wide architecture and to date has been unsuccessful ("Defense Information," 1998). Documented cases in the Vietnam, Granada, and Persian Gulf wars have shown serious problems of communication interoperability. In 1997, the JTRS program office was created to address these concerns. It has reorganized several times. This fact is well documented in the GAO reports from 1999 ("Challenges Associated"), 2003 ("Briefing to the House"), and 2006 ("Restructuring JTRS").

The JTRS office is staffed by military officers and civilians from all the services: Navy, Marine Corps, Air Force, and Army. Their offices are housed on a Navy base, Fleet Anti-Submarine Warfare. Their primary administrative access to unclassified Internet access is through the NMCI network. NMCI is ill suited to support Army/Air Force personnel or transient visitors from academia and commercial industry. This is documented in a recent GAO report: "... did not meet the critical joint applications interoperability target, and it could not determine whether it met the operational testing target because of insufficient data" ("DOD Needs," 2006, p. 22). *Joint* is the term in the DOD describing multi-service events; the need for wireless network access will be properly solved if implemented in a secure, usable, and supportable fashion. Wireless users will have access to the Internet and therefore will be able to connect to NMCI through a Virtual Private Network (VPN) if required to do so.

The ASW base commander owns all buildings on the base. JTRS is a tenant command that requires work spaces. The five buildings that house JTRS personnel are part of the negotiation that occurred between the base commander and the JTRS leadership. The base commander had offered up these buildings and floors to house JTRS employees. They were historically barracks that are in the process of being converted to office spaces.

1.4.2 NMCI and Managed Services

The mission of NMCI is to replace the thousands of Navy unclassified and classified networks (secret and below) with one centrally managed and configured network. This includes all servers, applications, clients, cell phones, security, videoconferencing, and the entire IT infrastructure ("DOD Needs," 2006). Figure 2

shows the NMCI functionality breakdown by Service Level Agreement (SLA). The NMCI contract provides financial incentives to Electronic Data Systems (EDS) Corporation, the prime NMCI vendor, by meeting SLAs. The purpose of the consolidation is to gain savings by reducing the number of support help-desk sites, as well as standardizing business processes, hardware, and software. EDS is challenged with managing workload, tracking costs, improving security, reducing unneeded manpower, and ensuring standardization. The Program Executive Officer for the Enterprise Information System (PEO-EIS) and the NMCI Program Office are in charge of all aspects of the contract performance and have acquisition authority for modifications. The service areas were developed in conjunction with EDS Corporation as well as with

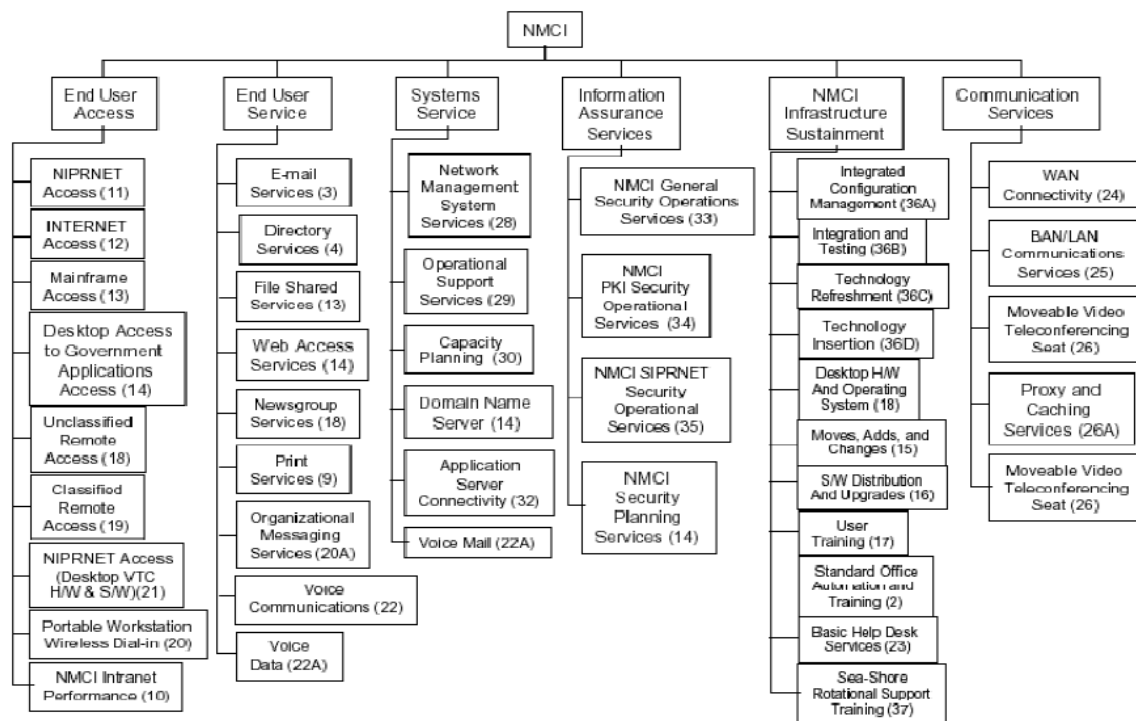


Figure 2. NMCI Service Level Agreement briefing by Captain Chris Christopher, 29 March 2001, to Joint Logistics Council.

input from Navy and Marine Corps units in the form of the Navy Information Executive Council. PEO-EIS and the NMCI program office are chartered with ensuring that SLAs are maintained and kept up-to-date. NMCI's goal is to take control of all legacy networks, convert them over to NMCI, and thwart the growth of further non-NMCI networks within the Department of the Navy.

The purpose of managed services is to allow an organization (public or private) to focus on its core business and to treat its IT functionality requirements as a service to be contracted out, like water or electricity (Marks, 2006). There are potential cost savings and capability enhancements due to the advantages of the economies of scale and infusing "best practices" via subcontracting. A small organization, such as a real estate agency, brokerage firm, or public elementary school, will not normally have the expertise to run a network, Web server, e-commerce, network security, etc. The choice of a small organization is that it is willing to accept a security risk to its data by having a third-party company manage its data instead of having to pay the higher costs of training/developing its own capability. Larger companies also have diverse requirements; for instance, an accounting department will be security focused, and a research and development department will require greater end-user autonomy to have access to greater application-wide configurations. Off-site contact staff may not be able to respond to R&D demands in a timely fashion. Large companies have the resources to grow their own staff capability but may be hampered by the hiring/firing/screening capability because of the bureaucratic characteristics of large organizations that are especially characteristic of public institutions. Table 1 contains summaries of the advantages and disadvantages of contracted managed services.

Table 1. Advantages and Disadvantages of Contracted Managed Services

Size/Type of Company	Contracted Managed Services	In House Services
Small/mid-size company	Large variety of services/technical competencies available that can be cherry picked to meet the needs of the company. Perceived as less secure because companies are trusting third parties with their data/network. Usually not on site and therefore perceived as less responsive.	More responsive because employee is on site. Hiring the right person may be challenging because technical criteria are not necessarily known for a company because it is out of their local expertise. Additional costs of maintaining/training technical IT personnel competency is a prevalent challenge in this scenario.
Large/government organization	Contract terms have to be carefully crafted to meet the needs of all members of the organization. This can be challenging if the organization has diverse departments with diverse requirements, often undocumented. Large variety of services/technical competencies available that can be cherry picked to meet the needs of the company. Perceived as less secure because companies are trusting third parties with their data/network. Usually not on site and therefore perceived as less responsive.	More responsive because employee is on site. Larger organizations tend to have the funds to provide larger, better-trained in-house staffs. Hiring/firing/screening processes within government agencies may be slow or ineffective due to multi-tiered bureaucratic organizational structures.
<i>Sources: McCafferty, 2006; Simpson, 2007; "The Evolution," 2006; Swanton, 2006.</i>		

The administration of the Navy Marine Corps Intranet has decided to use managed services. It is difficult to ascertain the thought process as to why, precisely, Navy leadership decided to contract out the solution versus invest in building an internal in-house capability. One factor may be that the typical military person transfers every two years from one location to another. This is true for both the typical worker (enlisted) and management (officer). This makes it difficult for local institutional knowledge and

lessons learned to be retained. Information Technology military personnel are required to be knowledgeable on military matters and have military duties that are not directly related to the Information Technology field or workload. Some examples are small arms training, warfare qualifications, physical fitness training, and administrative requirements such as evaluations and general military training (naval history, sexual harassment awareness training, etc.).

Naval culture prefers that military personnel be generalists and not specialists, and the military is often unwilling to invest in specialized training such as fiber optics, network management, 802.11 deployment, network security, and industry certifications from Cisco, Microsoft, Compia, etc. The IT field requires current technical competency that military personnel may not be able to provide, because they are not properly trained; and, by the time they get enough experience during a given tour to perform the job well, they may often be required to transfer within a few months. This reality has produce a problematic IT service that is compensated by using commercial contractors that do not have distracting military duties and can be trained by their respective companies prior to being employed by the military. The risk of trusting external third-party civilians with military data was perhaps mitigated by the fact that the military IT personnel could not maintain high enough technical competency to ensure reliable/secure data, compared to the civilian counterparts, in a cost-efficient manner.

Finally, IT prior to NMCI was budgeted at the local level, and IT expenditures were often charged as a general or administrative expenditure. Prior to NMCI, the Navy did not know what it was paying as a whole for IT, due to the inconsistent budgeting methods, and therefore from the macro level it could not plan for proper equipment life-

cycle replacement. Wealthy commands had new equipment, better security policies, and better-trained personnel. Poorer commands had the opposite. NMCI was a macro system, and it provided a total price tag that allowed the Navy to see, for the first time, what it costs to provide IT to the Navy as a whole. This is because everything is charged and tracked from a centralized point. The NMCI program is over six years old and has spent \$3.7 billion; now the program has been extended three years, totaling \$9.3 billion for the ten-year program (“DOD Needs,” 2006). The end product has received less than rave reviews:

The Navy’s three groups of NMCI customers—end users, organizational commanders, and network operators—vary in the extent to which they are satisfied with the program, but collectively these customers are generally not satisfied. (“DOD Needs,” 2006, p. 45)

The Navy’s performance or costs for IT were unknown prior to NMCI, but it is fair to say it was in a state where the Navy leadership was willing to pay out an initial \$3 billion every three years to ensure its success over the status quo. The focus is not whether the pre-NMCI was more or less cost effective than NMCI, but that it is now required to adopt the following GAO recommendations:

1. Evaluating and appropriately adjusting the original plan for measuring achievement of strategic program goals and provides for performance management implementation in a manner that treats such measurement as a program priority;
2. Expanding its range of activities to measure and understand service level agreement performance to provide increased visibility into performance relative to each agreement;
3. Sharing the NMCI performance results with DOD, Office of Management and Budget, and congressional decision makers as part of the program’s annual budget submissions;
4. Reexamining the focus, scope, and transparency of its customer satisfaction activities to ensure that areas of dissatisfaction described in this report are regularly disclosed to the aforementioned decision makers and that customer

satisfaction improvement efforts are effectively planned and managed. (“DOD Needs,” 2006, p. 55)

1.4.3 Technical Background

The present researcher will also investigate the relationships between the budget cycle, organizational structures, culture, laws/regulations, customer reaction, and technological limitations. The network will be an IEEE 802.11g wireless network. Specifically, 802.11g networks run at the unlicensed 2.4–2.5 GHz Industrial Scientific and Medical (ISM) frequency band at a data rate of 54 mbps. The 802.11g specification was developed by the Institute of Electronics and Electrical Engineers (IEEE) as the fourth amendment to the 802.11 specification under the name, Task Group G, “Further Higher Data Rate Extension in the 2.4 GHz Band” (Institute of Electrical and Electronics Engineers, Inc., 2003, p. 12). It is compatible with the original 802.11 and 802.11b specifications that represent the majority of wireless LAN users today. Almost 90% of all laptops today have 802.11 b/g capability (Cheng, 2006). Although designed for ranges less than ten meters, 802.11 b/g networks are robust, with successful testing completed for long point-to-point distance links up to 37 kilometers (Chebrolu, Bhaskaran, & Sayandeep, 2006). The 5 GHz variant, 802.11a, was considered but was eliminated because of its low market acceptance and lack of backwards compatibility with 802.11, 802.11b and 802.11g networks. There is a follow-on specification, 802.11n, with reported data rates up to 100 Mbps. Unfortunately, it has not yet been ratified/finalized by the IEEE, and industry has produced myriad non-interpretable products with a variety of incompatible technical standards. It is predicted that the 802.11n standard should be finalized by 2008 (Vaughan-Nichols, 2006). Although some pre-specification 802.11n

products are available, they were eliminated because of the uncertainty of the final specification.

Additionally, security extensions are now included such as 802.11i, 802.1X, and Wi-Fi Protected Access 2 (WPA-2) for all 802.11 lines (11, 11a, 11b, and 11n). 802.11i is an IEEE task group focused on security, migrating the encryption standard from Wired Equivalent Privacy (WEP) to the new Advanced Encryption Standard (AES).

IEEE 802.11 provides three cryptographic algorithms to protect data traffic: WEP, TKIP, and CCMP. WEP and TKIP are based on the RC48 algorithm, and CCMP is based on the advanced encryption standard (AES). A means is provided for STAs to select the algorithm(s) to be used for a given association (IEEE, 2004, p. 12).

On any DOD system, only the AES or CCMP mode is authorized (“DOD Needs,” 2006). On the other hand, 802.1X is an IEEE specification covering authentication for both wired and wireless networks (Institute of Electrical and Electronics Engineers, Inc., 2001). WPA-2 is a commercial certification accredited by the Wi-Fi Alliance, which tests the use, interoperability, and security of wireless products. WPA-2 certification means the product has been successfully tested using 802.11i and 802.1X in a Wi-Fi Alliance lab. The Wi-Fi Alliance, a commercial entity consisting of 300 company members, has tested over 3,400 products (Wi-Fi Alliance, 2007). The DOD also requires 802.11 networks to be Federal Information Protection Standard (FIPS) 140-2 certified, as well as WPA-2 certified (*Use of Commercial Wireless*, 2006, p. 3). FIPS 140-2 testing is similar to WPA-2 testing but is completed at a government-certified lab (*Federal Information Processing*, 2001).

While the dominant network at the ASW base is NMCI, the wireless network is a legacy research network unsupported and unregulated by NMCI. The wireless

implementation was completed at Joint Tactical Radio System (JTRS) offices. The JTRS organization is a tenant command of the ASW base. This was possible because the JTRS organization is allowed to do research and development and is multi-service and therefore out of the purview of the Navy, despite being housed on a Navy base. The wireless network will have no direct connectivity with the NMCI network, with the exception of a Virtual Private Network (VPN) that is available to anyone on the Internet with verifiable need. VPNs allow secure remote connectivity into a network, and the VPN framework is defined by the Internet Engineering Task Force (2001) under RFC 2764.

1.5 Players and Key Organizations

The key organizations on this research are Spawar System Center Pacific (SSC), JPEO JTRS, ASW Naval Base Point Loma, Spawar HQ, PEO EIS, EDS Corporation, L3 Corporation and Tel Tech Plus Corporation. The researcher of this dissertation is a member of SSC. JPEO JTRS has agreed to fund SSC for the purpose of creating a managed wireless network throughout the five JTRS buildings located on the ASW Naval Base Point Loma in San Diego. SSC provides technical personnel, engineering and logistical support to program offices such as JPEO JTRS. The key SSC players are the SSC Commanding Officer, JTRS Project lead (the researcher of this dissertation), SSC Chief Engineer, the SSC Contracting Department, SSC Simplified Acquisition Department, and the SSC Finance Department. The researcher in his capacity as the project leader of this research hired Tel Tech Plus and L3 Corporation to build and maintain the wireless managed network installation for the JPEO JTRS organization under SSC government oversight. The key JTRS players are the JPEO Commander, the JPEO Operations Department, JPEO Finance Department, and JPEO Facilities. The end

user of this wireless network consists of JTRS personnel. These personnel are military from all branches of the service, civil servants and contractors. Additionally temporary guests and visitors will also be using the network. These guests will be also be military, civil servants and contractors but will also include guest from academia and potential support vendors.

Another important player is PEO EIS. They are the program office that manages NMCI. They have awarded EDS corporation has the prime contractor to run the NMCI network. SSC Commanding officer reports to the Admiral at SPAWAR HQ. The ASW Naval Base Point Loma key players are the spectrum manager and the Public Works department. All these organizations are located in San Diego with the exception of PEO-EIS, which located in Washington DC.

1.6 Research Questions Investigated

According to Creswell (2008), case study research is a form of qualitative research where "... research questions assume two forms: a central question and associated subquestions" (p. 105). The central questions in this research relate to exploring the process of designing and implementing managed service wireless connectivity:

1. What are the challenges of implementing a managed wireless architecture?
2. What are the customer operational requirements of wireless implementation?
3. What is the value of a service-oriented architecture?

1.7 Summary

This chapter described the concepts of FORCEnet, managed services, wireless connectivity, NMCI, JTRS, and the technical background and capabilities of IEEE 802.11 wireless local area networks. A technical overview of the different flavors of 802.11 alphabet groups: 802.11a, 802.11b, 802.11g, 802.11n, etc. were defined in terms of frequencies used, data-rate capability, security use, and DOD regulation. Examples of wireless test use in the navy were also described: Wireless Pier Connectivity System, deployment of 802.11 on Navy war ships, and wireless use at the Mayport Naval Station. This chapter addressed the problem of evaluating the cost savings and efficiencies achieved by transitioning from a traditional network operations center to a managed-services operating center. It also introduced the goal of this research, which is to actually develop a managed service wireless network in a military setting, specifically, a multi-service military base in San Diego. The research barriers and issues are also discussed addressing the problems of large DOD programs. The specific examples used were JTRS and NMCI programs. Several GAO reports have been written about JTRS and NMCI programs in the context of program performance and problems engaged in achieving programmatic goals. These reports document that NMCI customers are dissatisfied. This chapter described the relevance and significance of this research and explained how the researcher will explore ways the military is grappling with the deployment of managed services in a joint environment and how to implement secure service oriented wireless technologies. Finally, the chapter describes the key organizations involved in this research: Spawar System Center Pacific (SSC), JPEO JTRS, ASW Naval Base Point

Loma, Spawar HQ, PEO EIS, EDS Corporation, L3 Corporation and Tel Tech Plus Corporation as well as formally describing the research questions to be explored. This research explores the many management, communication, technical, procurement, and financial challenges in bringing a large project to life.

Chapter 2

Review of the Literature

2.1 Introduction

The purpose of the literature review is to survey the existing knowledge on the research topic, specifically, the exploration of enterprise wireless implementations, managed services implementations, and mobile network architecture. Service Oriented Architectures (SOAs) used in the private and public sectors will be reviewed. The use of SOAs and 802.11 in the military, such as NMCI, is key. Commercial wireless use is ubiquitous. Numerous wireless requirements and a variety of technologies are available in terms of hardware, radio frequency/spectrum use, operating systems, physical form, security, and software applications. Cell phones, personal digital assistants (PDAs), Bluetooth ear buds, Blackberry email devices, cordless phones, wi-fi devices, and cellular data cards are some of the most used wireless tools in the business world today. Managers are put in a dilemma of deciding a hi-tech path. This is extremely difficult and is often done without the technological background or an understanding of the customer's business rules or the impact on security, usability, and supportability. These business rules may come in the form of laws, regulations, and operational objectives or thresholds.

Management should focus on the mission of the organization, not the specifics of a technology or its architecture. Of course, organizations want their devices to be reliable, secure, interoperable, and user friendly. Managed services are the path that allows the

organization to focus on the core business while forcing the infrastructure to be secure, reliable, and relevant. However, managed services are not the panacea for all problems. Managed services require supervision. IT responsibility and planning cannot be successfully delegated away through a service contract. All successful management systems need competent line management, clear requirements, and a strategic vision (Linthicum, 2007). Market forces and strong competition will also add to managed services technological competency. Even with its caveats, managed services are the wave of the future.

2.2 Theory and Research Literature Specific to the Topic

There is a change in strategic thinking: a change to managed services under the “IT as a utility model” (Grantham, 2005). Business-to-business (B2B) electronic commerce will be “outsourced to managed service providers” (Swanton, 2006). Cost saving is the prime driver: “... shave 27% from the cost of building IT in house ... managed security [saving] as much as 75% ...” (Padhye, 2004). This same issue exists in the private sector, the public sector, and the military sector.

The Internet Security System (ISS), one of the top security companies in the world and recently acquired by IBM, claimed that companies can save as much as 55% on security costs through outsourcing, allowing reallocation of funds to other needs. In 2006, the Insight Research Corporation claimed there would be great opportunity in the next five years for both wired and wireless networks, and that outsourcing would provide more savings as a company’s complexity increases (*Managed Services*, 2006). Outsourcing to a managed-service provider also frees companies from the human

resource headaches that are common in the IT sector, such as high attrition and hiring and training costs (Dev, 2006).

The traditional areas of managed services include monitoring hardware such as routers, switches, and firewalls, as well as generic applications (email, Web servers, etc.). The downside is that managed services providers are no longer meeting customer expectations. Heavy competition in the provider arena has forced providers to offer more business-focused services (Marks, 2006). Figure 3 shows the commercial transition from device centric services to business centric services. In the early stages of managed service, providers focus on monitoring the equipment, such as having systems automatically email/phone technicians when a router goes down, when a network becomes infected with a virus, or when a server is no longer functioning. These solutions focus on the health of the equipment and are described as a device centric system. The next stage of development of managed service maturation maintains all the functionality of hardware equipment health monitoring but also transcends the device centric capability by moving into the applications and business practices of the organization. The service provider offers on-demand deployment of customized software, monitors applications, and ties the device hardware health and application use to business performance. Figure 4 shows the military version of managed services, net centric operations.

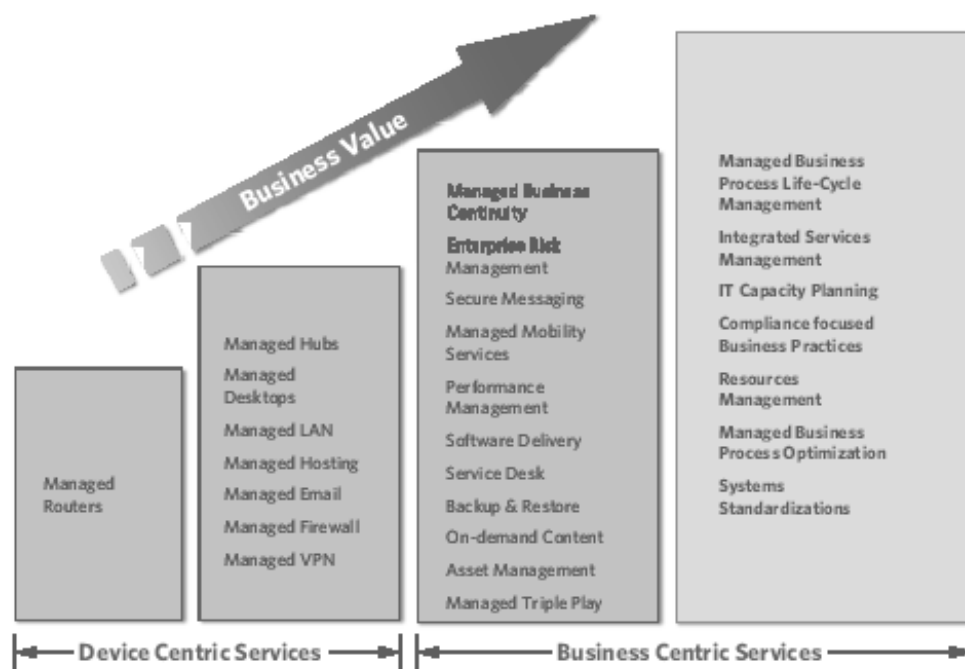


Figure 3. Managed services continuum. (Marks, 2006)

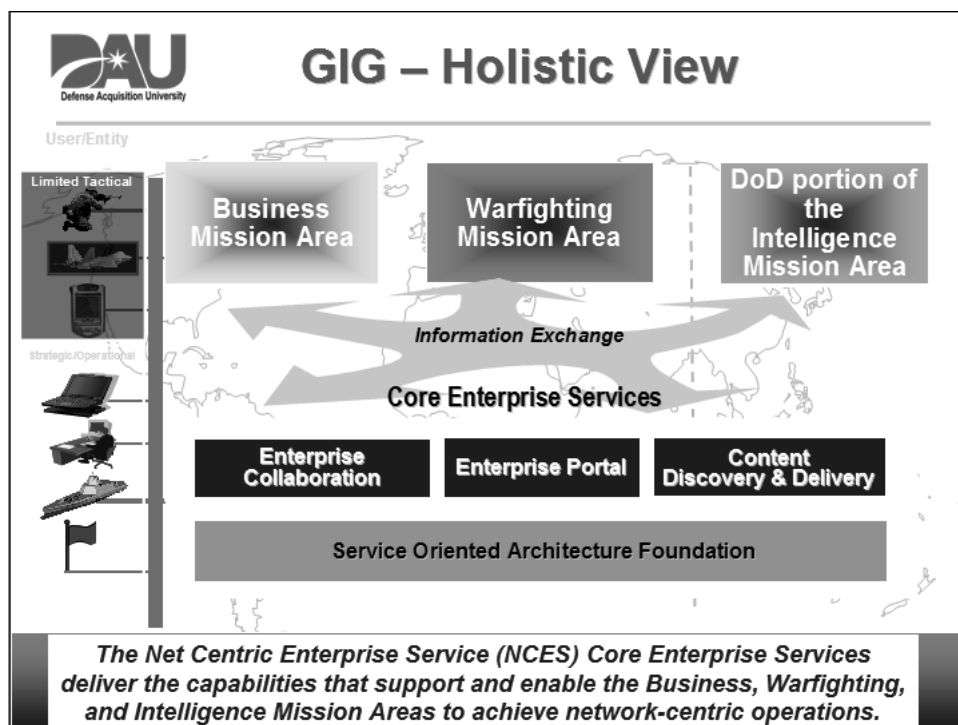


Figure 4. GIG—holistic view. (Defense Acquisition University, 2007)

The Net Centric Enterprise Services (NCES) has three product lines: Collaboration, Content Discovery/Delivery, and User Portal Access. The foundation of these product lines is the enterprise Service Oriented Architecture (SOA). These three product lines support the Department of Defense in the areas of business, war fighting, and intelligence (Net Centric Enterprise Services, 2008). The difference between commercial managed services and net centric managed services is that the business of the military is not solely profit driven, because it must broaden the business balance between the financial aspects of decisions with the war fighting and intelligence aspects. This is the nature of the Global Information Grid (GIG). The research problem of deploying a wireless managed service operation is consistent with the DOD's macro plan for the GIG's managed services operations.

The demands for mobile connectivity, ad-hoc connectivity, and guest connectivity remain met. Wired solutions are prohibitive due to technological or costs barriers. NMCI currently does not have the capability to provide guest connectivity to a temporary visitor from another service, academia, or industry; nor does it normally dedicate spare ports for traveling NMCI users to plug into for wired connectivity. This problem creates a productivity barrier. Jim Geier, a noted author on wireless local area network technology, claimed:

Microsoft obtains a \$6.1M per year return on a \$9M investment in the wireless LAN, which has led to a return in just over one year. Microsoft found that the convenience and flexibility of having wireless access to email was the primary contributor to the gains in productivity. (Geier, 2005, p. 1)

Geier also claimed, "...Companies can save at least \$200 per connection by eliminating the cable, wall outlet, and associated installation labor" by augmenting wireless access points instead of additional wired outlets (Geier, 2005, p. 1). The NOP Research group

also found increased employee productivity and cost savings achieved by end users from 300 U.S.-based organizations that deployed 802.11 wireless networks on an enterprise scale. Their results showed that wireless LANs allowed end users to stay connected to their home company network 1.75 hours more per day, amounting to a time savings of 70 minutes for the average user and a productivity increase of as much as 22% (NOP Research, 2001). Sage Research (2001), a venture capitalist research firm, interviewed numerous companies that had over 1,000 employees and had used 802.11 wireless technologies for over a month. In these interviews, they found that civilian companies embracing and implementing 802.11 wireless technologies on an enterprise basis gave an overwhelmingly positive response. The main conclusion characteristics were (a) self-reliance in being able to get the information desired, when it is wanted, (b) instant gratification of being able to solve a problem on the spot, (c) sense of empowerment by eliminating common process bottlenecks, and (d) satisfaction of impressing customers with speedy, accurate responses to their requests.

Technical/business pundit and editor in chief of *Wired Magazine*, Chris Anderson, wrote several articles and a recent best seller entitled *The Long Tail: Why the Future of Business is Selling Less of More*. In his works, he described the success of mass online retailers like Amazon and Netflix, due to their ability to focus on thousands of niche markets with low individual demand but which, when combined, represent the majority of growth and revenue, hence the name “the long tail.” Traditional companies find it hard to compete with the vast inventories of these companies. This “long tail” phenomenon is heavily dependent on the successful deployment of Service Oriented Architecture (SOA), allowing an organization to provide for a large depth and breadth of customer

requirements. In a recent article, *Information Week* claimed that state Chief Information Officers (CIOs) top their wish list with wireless and SOA as “a way to break through the bureaucracy that separates governments and their citizens” (McCafferty, 2006). A recent case study on SOA and NMCI claimed, “... There’s no more complex IT environment than the US Department of Defense” (Schmelzer, 2004, p. 2), and recommended seven ways the Navy’s legacy systems could be improved:

1. Utilize Terminal Services as a way to provide access to legacy systems.
2. Transform existing code into new formats using code transformation technology.
3. Rewrite application functionality into ERP systems.
4. Remotely host existing applications.
5. Apply gateway-type or data centric tools.
6. Use specific data, OS, platform, code, database, logic, business rules, meta data migration, and tools and methodologies.
7. Use Service Oriented Architecture approaches to service-enable legacy systems and allow for creation of new capabilities through composition.

The case study also claimed that the DOD is the “largest spender on SOA projects,” and NMCI has the potential to set an SOA precedent/standard for the entire IT industry (Schmelzer, 2004). Technical icons, such as the co-founder of Microsoft, Paul Allen, also described SOA and Web services as the prime path for 21st century IT modernity (Allen, 2006). “Software as a service will change the way people build, sell, buy, and use software” (Chong, 2006, p. 1). The problem is clear; NMCI needs a wireless network that is supported through a managed service model.

The legacy of the term of managed services has evolved originally from Application Services Providers (ASPs) and is further being replaced by the term Software as a Service (SaaS). The goal of managed services, ASPs, or SaaS, is to mature the information system by transforming data into information, information into knowledge, and knowledge into wisdom. SaaS injects the business elements throughout the design and development process. This is the role of Service Oriented Architecture (SOA; Foster, 2005). The GIG in Figure 4 shows that the foundation is based on SOA. In the 1990s, platforms were mostly proprietary systems and were not designed to communicate with competing technologies. Then came Web services that began to provide for interoperability across a large variety of platforms. Web services allowed for the notion of business transactions to be separated from the traditional hardware technologies, allowing for an on-demand SOA. IBM, in its SOA product, WebSphere (*WebSphere Application Server*, 2006), claimed that a successful SOA needs to address the following four areas:

1. Simplify tasks.
2. Enhance security, availability and scalability.
3. Improve communication services for the purpose of increased access and reusability.
4. Improve the infrastructure for management and maintenance.

The preceding areas are often the job of the Software as a Service (SaaS) provider. SaaS is a type of managed service that focuses on software. SaaS tries to incorporate best practices into all aspects of the software. The managed-services

operation envisioned for this research for the base-wide operation incorporated the preceding steps listed by Websphere (*Websphere Application Server*, 2006).

One example of SOA implementation is through the use of extensible markup language (XML) technologies. XML separates the data-storing function from the data-presentation function. This allows the data to be transformed for use on multiple platforms and for a variety of different users. Thus, a company Web page written using XML technology can have the same content transformed to work on a computer with different operating systems and on a variety of cell phones and Blackberry devices. The display of data is restructured to fit the technical limitations of devices, such as the size of the screen or the protocols supported on the device, to include the hardware and operating system. A cell phone browser may not be able to support Flash/Adobe protocols. Many have smaller display resolutions, may have limited computing power, and may have to function in an environment that has intermittent connectivity (Prensky, 2005). This may require special licensing arrangements to unique operational requirements such as screen-scraping legacy application on small portable devices. This scenario is directly on point to the technological challenges associated with wireless deployments.

The line management/customer perspective is for the data to be easily displayed on any device used, without concern for how it is done, just as long as it is done in a reliable, inexpensive, and secure fashion (Schmelzer, 2004). SaaS has to marry the line-management generic requirement into a technological reality. SaaS also couples the business rules with the software to ensure that best practices are followed.

The role of management is to define and ensure that the SaaS provider is meeting the requirement metrics. The role of the SaaS provider is to determine the best way to

leverage existing technologies to meet the requirement (Schuller, 2007). A SaaS provider can determine whether to use a generic application that uses an industry's best practice to create an application particularly for the customer or to do something in between. A SaaS provider will examine what is currently being done by the customer and analyze if there are efficiencies to be gained by changing a business practice. Defining and understanding the responsibilities of management and the service provider will be key in this research.

The implementation of SOA has been lauded for its cost savings and cost avoidance capabilities, as well as its operational enhancements in industry (Koch, 2005) and specifically in wired architectural planning for NMCI (Marsan, 2006). Nevertheless, NMCI is lacking in application planning at the strategic level. A recent interview by *Network World* of NMCI technical director Colonel Baker confirmed this: "We just provide the infrastructure the applications ride on. Other people in the Navy are responsible for the consolidation of servers" (Marsan, 2006). Web 2.0 frameworks and Software as a Service (SaaS) planning requires centralized control for next-generation wireless collaboration applications. The complexity of SaaS requires that the architecture be orchestrated with the application, which is driven by the business needs of the organization.

One example of the managed service evolution is the Outrigger Hotels and Resorts, which owns over 51 properties in Hawaii and Asia (*ROI Case Study*, 2006). Outrigger wanted to improve its productivity by adding email, chat, and instant messaging to its call center staff without a discernable technological hardware investment. Outrigger shopped around and selected an on-demand service provided by Echopass and Sprint, because they had the lowest cost and greatest expected return on

investment (ROI). The key areas were software service fees, representing 98% of the cost, and hardware and training, representing the remaining 2%. Outrigger was able to migrate from its old hardware-based system within 60 days. The training process was seamless; teams were up and running in less than two hours. The new system allowed the team to handle incoming calls, chat, email, and instant messaging under one software system with one support vendor. This system also allowed employees to work from home and remote locations. Outrigger claims that this service allowed for 300% ROI within a two-month payback.

Another example is Fiducia, a 3,000-employee IT provider serving 850 banks (IBM, 2007). Fiducia delivers key IT financial and brokerage infrastructure services and solutions to its bank clients. As banks grow, customer service deteriorates because they often depend on records systems that are distributed across numerous branches and rely on human review of manual records. Customers may have to wait days for the correct paperwork to be found and answered. Fiducia found its business niche by providing a solution to this problem in the form of a Service Oriented Architecture (SOA). Fiducia worked with IBM and deployed a secure virtual filing cabinet, allowing bank employees to retrieve information in a real-time, secure fashion. Customer service improved, allowing Fiducia to cement its relationship with the banks, and the SOA saved them thousands of dollars each month because paper files were no longer required to be stored and therefore fewer office spaces needed to be rented.

Another example is the Sherman Independent School District (SISD), a K-12 school district with over 6,300 students and 12 campuses spread over a 12-square-mile area (*Managed Ethernet*, 2004). SISD needed to update its aging ATM network. The

district wanted consistent, reliable service to every campus. The network was used not only for educational functions but also for food preparation, point of sales, and other logistical and communication functions. The district wanted improved network performance in terms of speed, availability, reliability, security, and redundancy. It did not want the headache of managing the system, and it wanted to accomplish this within a limited budget. SISD chose Verizon as its service provider under the Transparent LAN Services (TLS) agreement. TLS allows SISD a reduction on the total cost of ownership by allowing the SISD to focus on its core mission, to educate the children of Sherman, Texas (*Managed Ethernet*, 2004).

But not all SOAs have been successful. There is dissatisfaction with NMCI from the ground up, as documented in a recent issue of the *Marine Corps Times*:

The Navy-Marine Corps Intranet, better known as NMCI, has spawned numerous nicknames over its seven-year existence, most of them far less complimentary than 'No More Contracted Infosystems,' one of the few clean enough for print. It's also become a verb—"I've been NMCIed!"—generally screamed by a Marine or sailor in frustration after a spectacular computer crash Ask the average Marine, sailor or civilian who uses NMCI for an opinion of the system and prepare to get an earful. While some report few problems, the majority have vivid recollections of waiting, waiting, waiting.... 'It would take me 20 minutes to boot up the system,' he said. "I would come in, in the morning, and turn on the computer and then have time to go have a cigarette and a cup of coffee before it would come up." (Hoffman, 2007)

Navy leadership until recently has been unwilling to publicly admit that there is a problem. In fact, in 2004 the Navy leadership was claiming, at least officially, that most users were satisfied. Nevertheless, a journalist from the *Government Computer News* reported that these results may not be valid because they were not done by an independent organization and the complete results were not released:

The NMCI program office announced the results of the fourth-quarter 2004 survey, which found that 72.2 percent of users were satisfied with the program the NMCI program office has steadfastly declined to release a complete copy of

the questionnaire, instead just issuing a release about the results. [Rear Admiral] Godwin said releasing the results would challenge the 'integrity of our data.' Many users have suggested the need for an independent organization to conduct future surveys. Some Navy officers have said that with the Navy and EDS conducting it, respondents are reluctant to give their true opinions. (Onley, 2005)

In 2008, following the groundswell of complaints and the less-than-flattering GSA report, the Navy made a strategic decision to transition a \$9.9 billion NMCI contract to a new system in September 2010. The new system is called Next Generation Enterprise Network (NGEN). Military personnel will have greater control of NGEN than they currently have with NMCI. It will also encompass ships at sea and foreign bases, neither of which NMCI currently has under its control. It is clear that the Navy will have greater control with NGEN than with NMCI, but it is unlikely that the Navy will assume the responsibility of the 4,000 Electronic Data Systems (EDS) employees with sailors and marines as replacements. Total outsourcing is what the Navy has with NMCI, whereas NGEN will be partial outsourcing:

“We are working on ... reinvigorating the IT work force and its skill set in anticipation of some changing roles,” Carey [Department of the Navy CIO] said. Yet, “there isn’t going to be a light switch turned on October 2010 and suddenly the Navy is standing there with thousands of folks ready to push aside contract workers.” (Boessenkool, 2008)

The Navy is developing an acquisition strategy for NGEN to determine the sailor/marine-to-contractor ratio for the existing NMCI activity and the added at-sea and foreign-base responsibility. The at-sea networks, which are the counterparts to NMCI shore, are called Information Technology of the 21st Century (IT-21) or Integrated Shipboard Network System (ISNS). IT-21 and ISNS are being renamed/replaced again to Consolidated Afloat Network Enterprise Services (CANES). The Marine Corps Enterprise Network (MCEN) is the counterpart to the Navy afloat IT-21/ISNS/CANES system. It is used by marines when they are forward deployed from their home base.

There are also networks with which the Navy communicates with its foreign coalition partners, such as NATO allies, Japan, Korea, and many others. The coalition network is called the Combined Enterprise Regional Information Exchange system (CENTRIX). When sailors are stationed at an overseas facility (not a ship), they will use another system called Base Level Information Infrastructure (BLII) program/Overseas Navy Enterprise Network (ONE-Net). Additionally, some shore facilities still use older systems, called legacy systems, that have not yet converted to NMCI, BLII/ONE-Net, MCEN, or IT-21/ISNS/CANES (Carey, 2008). Table 2 summarizes the different types of systems for sailors and marines and how the type and location of their duty drives the type of system they will use. Changing systems every time a sailor or marine transitions from shore duty to sea duty (deployment) and overseas duty is stressful for both the individual and the overall organization.

Table 2. Sailor/Marine System Location Matrix

Location of System	Sailor	Marine
Non-deployed shore duty in continental United States, Alaska, or Hawaii.	NMCI/NGEN	NMCI/NGEN
Overseas permanent facility (shore duty) not on a ship or forward-deployed marine base	BLII/ONE-Net	BLII/ONE-Net
Sea duty or forward deployed	IT-21/ISNS/ CANES	MCEN
Coalition Partner Communication	CENTRIX	CENTRIX
Other	Legacy	Legacy

Source: Carey, 2008

The environment of systems, specifically, NMCI/NGEN, BLII/ONE-Net, IT-21/ISNS/CANES and CENTRIX, is defined by the Navy Chief Information Officer, Robert Carey, as the Naval Networking Environment (NNE). Each of these different systems has different program managers, different funding cycles, and different strategies. Carey's vision is to begin the transition of these systems in 2010, with the goal of common enterprise vision and architecture by 2016. Figure 5 shows the 2010 transformation to a 2016 NNE with a common architecture and standards that are integrated under the Global Information Grid (Carey, 2008).

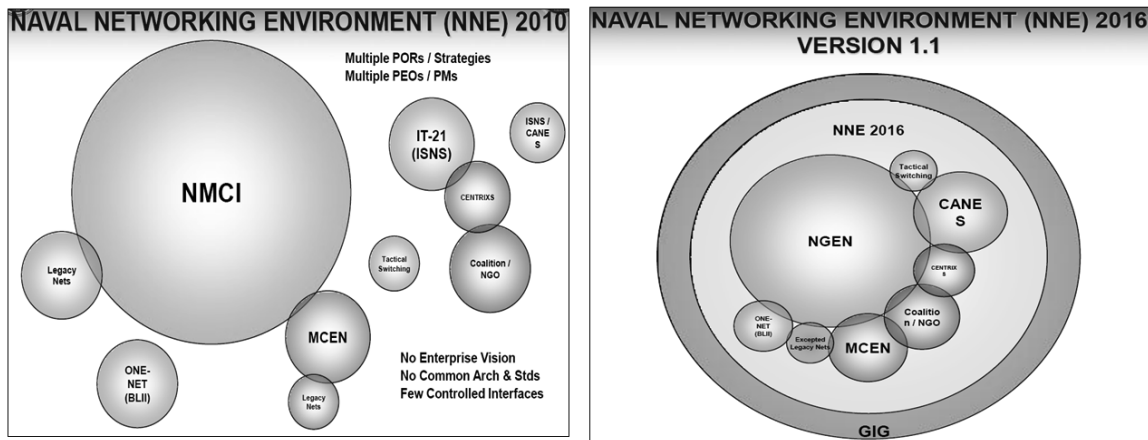


Figure 5. Naval Networking Environment 2010–2016 transformation (Carey, 2008).

Integrating diverse systems and programs in an overall managed service environment can be challenging and requires extensive resources. The current method of integration, a client server architecture, is problematic: The more systems to be integrated, the more exponentially difficult each system introduction becomes. These resources come in the form of engineering, security accreditation, and political coordination. With a Service Oriented Architecture (SOA), a loose coupling through open standards allows for ease of integration and reuse of data structure discernibly

reduces the engineering and security barrier. Organizing the system-engineering effort from a program centric environment into an operational focus reduces the political barriers (Diaz, 2008). Figure 6 shows the advantages of service oriented architecture over traditional client/server architecture.

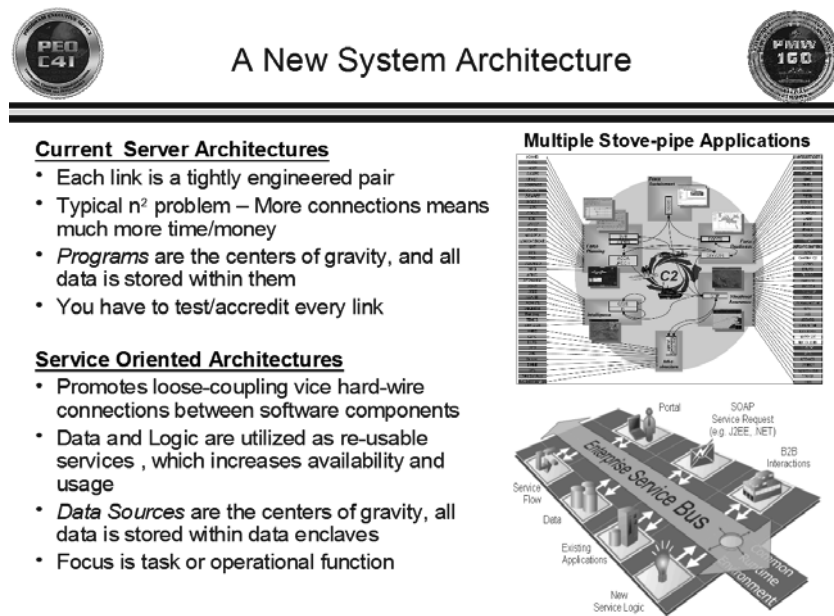


Figure 6. Advantages of SOA over client server architectures (Diaz, 2008).

A recent brief given by the Army's Chief Information Officer Lieutenant General Sorenson lauded the implementation of a service-oriented enterprise. Like the Navy/Marine Corps sailor/marine, Army soldier status changes. Soldiers may be at home in garrison, they may be training, or they may be deployed. These changes mean the network is changing for these soldiers. Their email changes, their network storage changes, their phone numbers change, and their software tool sets change. The ideal end state is for these items to remain the same, regardless if the soldiers are at home in garrison, training, or deployed. This means one email address, one phone number, one seamless network, one software tool set, and one network storage area (Sorenson, 2008). Right now, such soldiers have at least three emails.

The Army is far from one email, one phone number, one network, and so on, and requires significant transformation. There needs to be a Collaboration Strategy, a Semantic Strategy, a Net Centric Data Strategy, and a Shared Situational Analysis, (Sorenson, 2008). The Collaboration Strategy allows for stakeholders to synchronize the data into a common developed roadmap. The Semantic Strategy ensures that everyone understands the definition of terms in a consistent fashion. The Net Centric Data Strategy requires clear data czars for governance and decision making: Authoritative data models and centers of data excellence have to be identified, and communities of interest have to be maintained, integrated, and harmonized. Shared Situational Analysis is a support discipline that allows governing service-oriented enterprise (SOE) transformation (Sorenson, 2008). Figure 7 shows all the elements of how to enable transformation through a capability-driven architecture.

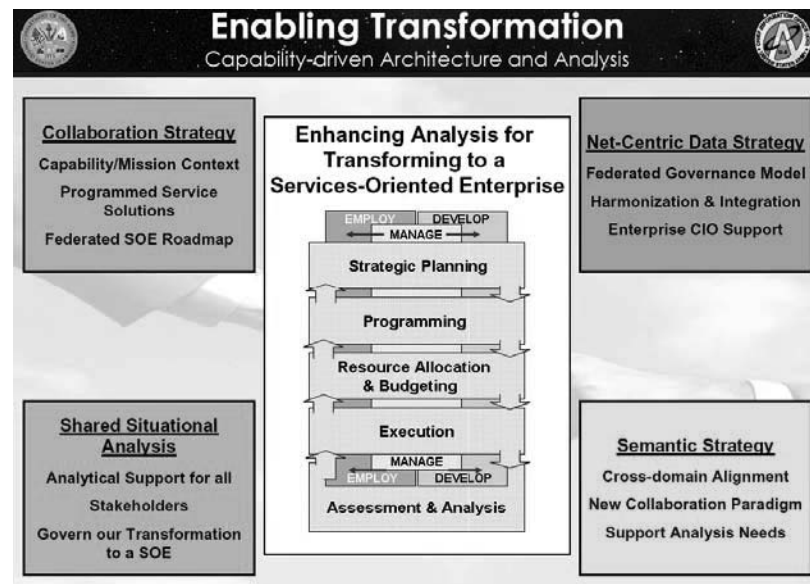


Figure 7. Lieutenant General Sorenson's transformation model. (Sorenson, 2008)

Architectures are highly relevant to the Department of Defense and its running of the Global Information Grid (GIG). The *Defense Acquisition Guidebook* (2004), or *DAG*, defined the GIG as a “globally interconnected, end-to-end set of capabilities, processes, and personnel for collecting, processing, storing, disseminating, and managing information,” essentially the entire military IT infrastructure. The DOD further dissects the GIG into core initiatives. The six core initiatives of the GIG are (a) GIG Bandwidth Expansion (GIG-BE), (b) Transformation Satellite (TSAT), (c) Joint Tactical Radio System (JTRS), (d) Network Centric Enterprise Services (NCES), and (e) Global Information Assurance Portfolio (GIAP) (Onley, 2004).

NCES is of particular relevance to this research. There are nine functional GIG NCES core services: storage, messaging, enterprise service management, discovery, mediation, information assurance, application hosting, user assistance, and collaboration (Bueno, 2004). The Defense Information Service Agency (DISA) is the organization chartered to manage the GIG within the DOD. DISA sees managed services as the future. DISA’s CIO has ordered that its acquisition workforce be trained in purchasing software based on usage, not on licenses, that is, in accord with the managed-services mode of thinking (Miller, 2007a; Miller, 2007b).

2.3 Contribution This Study Will Make to the Field

Reliable wireless service oriented architecture is in high demand. The military needs a road map on how to deploy wireless networks in a secure, supportable, and usable fashion that is in concert with the core mission of the military business requirements, i.e., a service oriented architecture. This strategic vision is clear (Mullen, 2006; The Department of the Navy, 2008), but the “how,” or actual tactical

implementation, is not. This study will explore the “how” by documenting a fairly large installation in a multi-service setting. It will also document the users’ experience with NMCI and their satisfaction level. The perceptions of an existing service oriented system can greatly influence the acceptance of future implementations such as NGEN, which can benefit both the Army and the Navy.

2.4 Summary of What Is Known and Unknown About the Topic

Several case studies dealing with Service Oriented Architectures (SOAs) were reviewed, with various levels of success. Small examples, such as Outrigger Hotels and Resorts, Fiducia, and the Sherman Hill Independent School District, lauded the benefits of SOA in terms of financial and productivity advantages. NMCI, the largest network in the world, on the other hand, has been perceived as less than successful. The primary SOA challenge the military faces is how to fundamentally integrate the multitude of systems into an orchestrated, functioning enterprise. Soldiers, sailors, marines, and others all have different emails and network services, depending on their status of being at home base, deployed, or in training. An SOA enterprise must allow for transparent network service support to war fighters, regardless of their physical location and tasking. Military SOAs have yet to deliver on this requirement. Successful wireless mobility may be part of the solution.

The commercial market has successfully deployed 802.11 SOAs on an individual basis in a variety of settings. SOAs are difficult to implement but are being deployed, based primarily on financial advantages such as cost savings and return on investment. These monetary gains are more attractive to commercial organizations because dollars are their life blood, whereas the public sector is not as drastically manipulated by

financial advantage. It is also interesting to point out that financial motivation abuses such as the Enron scandal led to Sarbanes-Oxley legislation, which requires greater financial accountability through the implementation of SOA reporting. Finance is both the carrot (improved revenue) and the stick (Sarbanes-Oxley [SOX] fines/prison time for lack of compliance) to implement these new technologies (“The case for SOA,” 2008). The DOD is not subject to SOX, but it still has a negative motivator: the threat of terrorism. Security is a mixed blessing for the DOD. It is a motivator to quickly address the realities of terrorism, but it also induces reluctance for technology improvements for fear of the potential vulnerabilities induced by a technology upgrade.

The DOD prefers an incremental improvement path to reduce risk. Thus, 802.11 and SOA in their various forms have been around for over 10 years. There is enough momentum, through the deployment precedents set in the commercial world and DOD pilot programs, for this research to be ripe for significant impact.

Chapter 3

Methodology

3.1. Introduction

The challenge of maturing an information system is to coordinate the operational system and technical requirements of the project. This requires the following actions: determine the intended purpose of the project, determine the scope, and focus on the characteristics of performance, schedule, and cost. The final step is to build it, and use the Department of Defense Architecture Framework commonly called DODAF (Defense Acquisition University, 2007); this process is shown in Figure 8. These steps were used

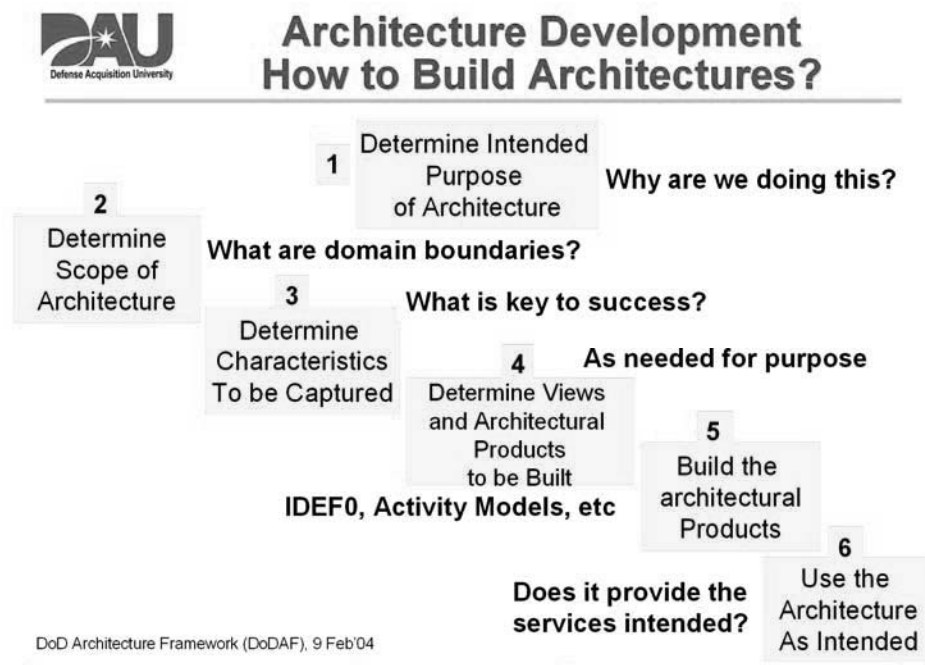


Figure 8. Architectural development. (Defense Acquisition University, 2007)

in this research for the base-wide wireless LAN and fulfillment of the goal of building a managed service operation. DODAF is the required enterprise architecture required by congressional law, specifically, the Clinger-Cohen Act. DODAF is suited for complex systems. The methodology used to develop the architecture in this research was the DODAF shown in Figure 9. The DODAF is the way the military designs/deploys systems that include managed services. The three views—operational, technical, and system—were developed in the base wireless LAN. The three different views allow for a variety of customers to understand and collaborate on the architecture. The operational view allows the end user to understand the system. The operational view will describe the key elements in terms of the end customer experience. An example of this in the setting of base wireless network is describing how the end user connects to the network and gets

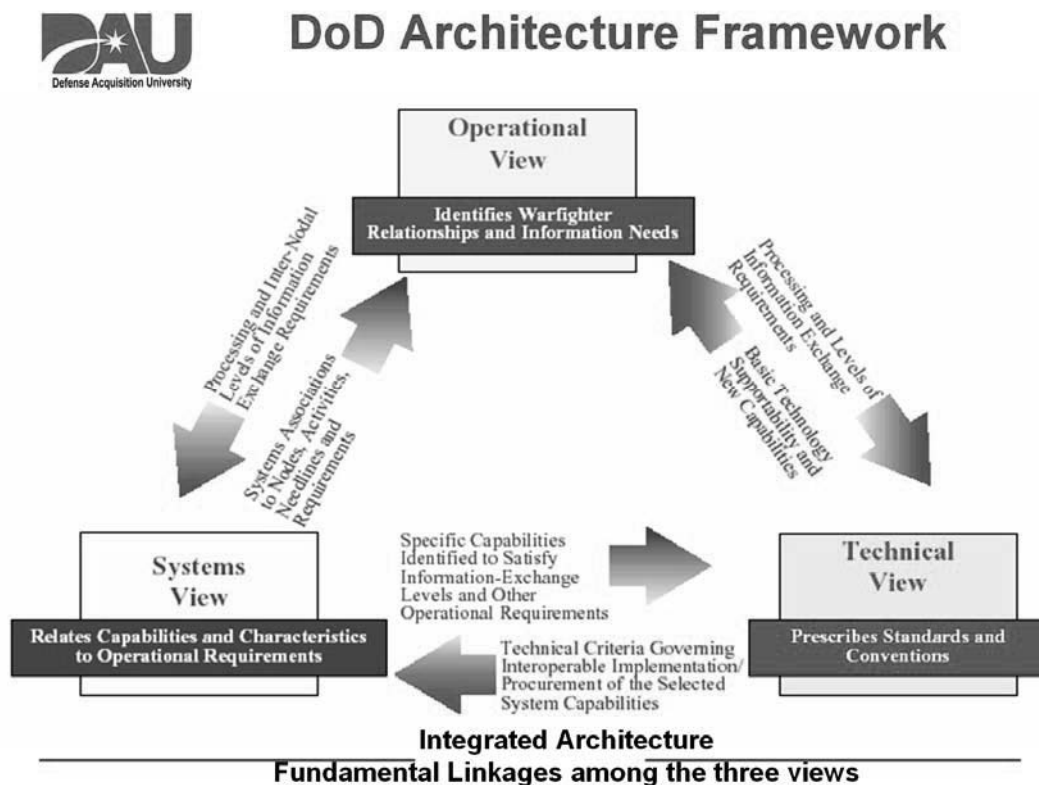


Figure 9. DOD architectural framework. (Defense Acquisition University, 2007)

access to services and applications such as email, file transfer, and Web services. The technical view describes the architecture in terms of standards and protocols. The wireless network example would show the architecture in the form of a network diagram showcasing the technologies deployed for each link and the nodes that are associated with it. The system view relates the DOD requirements documents to the actual capabilities. The final dissertation will contain all three views of the managed wireless deployment: operational, system, and technical.

3.2 Research Methods Employed

The approach includes the “case study,” as described by Robert Yin (2003), and the systems development life cycle (SDLC). The SDLC uses the system development process, which is defined as “... a set of activities, methods, best practices, deliverables, and automated tools that stakeholders use to develop and maintain information systems and software” (Whitten & Bentley, 2005, p. 30).

The first phase is to develop an overall plan/strategy for this study. The second phase is to define the requirements, design the data collection process, and write the case report. The third phase is to draw conclusions, modify the original plan/strategy based on the data, develop implications and conclusions, and then write a final report. In this case, JTRS leadership requirements have been documented through an informal interview:

1. Identify five buildings—Buildings 50 (2nd and 3rd floors), 7 (1st and 2nd floors), 17 (4th floor), 17a (3rd and 4th floors), and 17b (1st through 4th floors).
2. Use the minimum 7.5 Mbps Internet service provider data rate.

3. Meet all Department of Defense/Department of the Navy wired and wireless security requirements.
4. Have the project accredited by a designated approving authority. (*Note: Funding approval was granted on June 2008.*)
5. Build a wired infrastructure in and between buildings.
6. Use Common Access Card (CAC) Authentication. (A CAC is a DOD identification card.)
7. Determine appropriate staffing.
8. Plan for 100 simultaneous users and 200 total users.
9. Identify a centralized managed service provider to control all hardware and software.
10. Map business processes into the managed services system.
11. Estimate 50 access points to cover the five buildings.

The requirement process was completed using the Bentley Whitman method which consists of 4 activities: problem discovery/analysis, requirement discovery, document/analyzing requirements, and requirements management. The problem discovery was described in the Chapter 1 in the form of research questions. They are repeated here to maintain the focus of this research:

1. What are the challenges of implementing a managed wireless architecture?
2. What are the customer operational requirements of wireless implementation?
3. What is the value of a service-oriented architecture?

The first 3 activities in the Bentley Whitman method have already been completed. The fourth activity, requirements management, will continue to be used throughout the life cycle of the project. This is because, as the project changes, the

requirements will change; and that process needs to be managed. The Bentley Whitman method warns of potential problems such as requirements that are missing, conflicting, unfeasible, overlapping, or ambiguous. Every effort was made to avoid these pitfalls by doing site surveys, conducting interviews, and including all the stakeholders from the beginning for all the key decisions, such as technical equipment placement, contract award, and personnel hiring.

James Wetherbe, a respected information system educator, published a famous framework for identifying and avoiding information systems problems. This framework is called the PIECES framework, where PIECES is an acronym standing for Performance, Information, Economics, Control, Efficiency, and Service. Performance is first in the acronym because it is the reason the system exists so it can perform for its users and customers. Performance can use quantitative metrics such as data rate, throughput, system up time, or response time. Performance can be measured using qualitative metrics such as customer satisfaction.

Information, the second letter of the framework, analyzes the problems as a system consisting of inputs, outputs, and stored data. Use cases will be created to document and understand how the system will be used by its customers and maintainers. Economics means funding. This is important because funding is the lifeblood of any project. There are two primary aspects of economics: (a) the initial capital infrastructure costs/start-up costs and (b) the maintenance costs. Control means effective management and security. Balancing security regulation with customer service is as much an art as a science. Efficiency is to maximize the potential of the people and equipment in the

process by avoiding waste. Finally, Service is the cross check to see if the system is doing what was intended (Wetherby & Vitalari, 1994; Whitten & Bentley, 2005).

Too often, decisions are made concerning the procurement and management of IT systems without applying a balanced approach. An overzealous IT security manager might lock down a system so tightly that it is completely useless to its users. An organization that does not have a coordinated, centralized IT procurement process or strategy might purchase incompatible equipment. An organization that is too user centric may inadvertently provide security holes that could compromise sensitive data or allow the network to be degraded.

A strategic model is needed for wireless LANs. While the overall driving methodology will be the SDLC, a cross-check set of strategic tools will be used. This is called the Supportability, Usability, and Security (SUS) Trinity Model to further validate this research, and it is shown in Figure 10. The SUS Model was used as a roadmap to help the reader understand the process involved in organizing and transitioning to a managed services operation in developing a wireless Local Area Network (LAN) in a military setting.

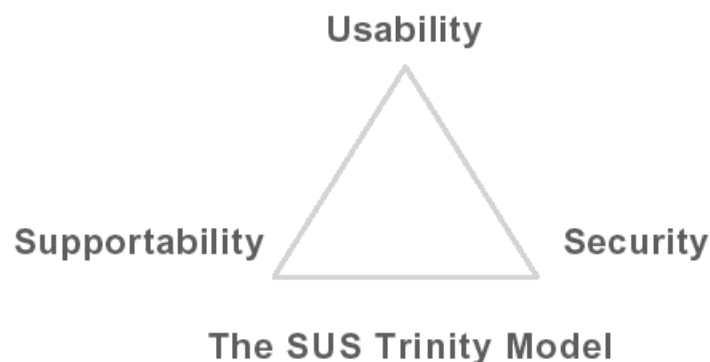


Figure 10. SUS Trinity Model. (Roth, 2002)

The Trinity Model was developed as a wireless strategic planning tool for the Naval Postgraduate School wireless campus deployment (Roth, 2002). It was developed without knowledge of the PIECES model. It looks at an information systems problem from three perspectives—supportability, usability, and security—and attempts to integrate them into a deployment plan. Supportability in a solution means that the design takes into account an organization's resources; budget, manpower, and training level must not be overlooked. The final implementation solution must take these into account. Specifically, it can be difficult to decide whether to outsource the service or whether to use existing personnel. This is where a proper risk assessment must be done. A poorly trained and shorthanded staff cannot easily support a complex system, and this factor will determine the success of the operation.

Usability means a desired end state where all users are able to seamlessly roam anywhere in the Naval base work areas and be connected to the network with a laptop or handheld device with a wired connection. Usability also means the architecture must reliably support any 802.11 wi-fi client card on any operating system. It is paramount that the end user be able to use the device effectively and efficiently. That is why usability is at the top of the pyramid.

A non-platform-specific design is in keeping with one of the fundamental principles of software engineering: low coupling and high cohesion. Low coupling means flexible response in the support of a variety of end user platforms and operating systems. High cohesion means unified support-architecture standards and limited vendor variety for ease of management and support.

The default 802.11 wireless security is not secure enough. The overarching DOD wireless policy states that in order for a wireless network to be certified at the unclassified level, an organization needs to use the FIPS 140-2 standard (“DOD Needs,” 2006). Security means to enforce existing DOD policy, incorporating private- and public-sector best practices, and orchestrate different technologies into a cohesive multilayered architecture of protection. This information also needs to be codified into a local policy and properly enforced.

The SUS Trinity Model provides the framework for better wireless networking. This is based on the campus deployment at the Naval Postgraduate School (Geier, 2003). Every decision concerning implementation should involve a review of how it can be more usable, more secure, and more supportable. During this research, the researcher further developed this model in terms of SOA, SaaS, and Web 2.0 elements. The usability area was employed as an expansion point for service-oriented modeling. SOA applications can now be verified through simulation (Tsai et al., 2007). SOA verification through simulation is different from normal methods, as it has greater focus on “reusability, collaborative behaviors, and its unique model-driven development” (Tsai et al., 2007, p. 1).

Usability should go hand-in-hand with service. Figure 11 shows the JTRS wireless LAN requirements in a notional network concept diagram. It documents the five buildings covered and their respective floors. Users are required to authenticate to the network with their Common Access Cards (CACs) through an authentication server in a secure, encrypted manner. Access points are required to provide wireless connectivity as

well as scan for potential nefarious activity by also fulfilling the role of a wireless intrusion detection system.

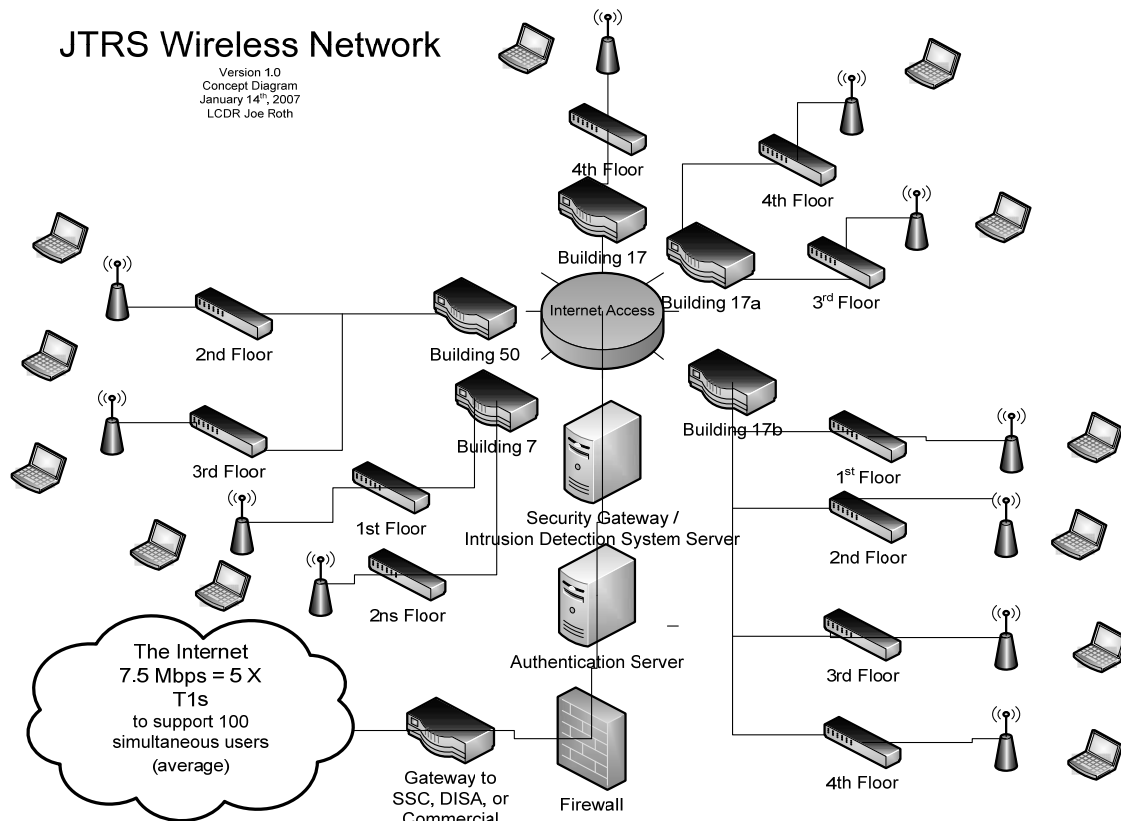


Figure 11. JTRS wireless concept diagram.

Figure 12 shows the map of the ASW base where the JTRS buildings are located. The ASW base obtained its external network Internet access from a nearby submarine base located 2.5 kilometers (km) southeast of the ASW base. After the funding for the project was secured and the requirements clearly defined, the researcher let out a contract to bid through the federal government contracting process. Each applicant must be able to complete all aspects of the project: hardware, software, installation, and technical support. The equipment must be compatible with existing

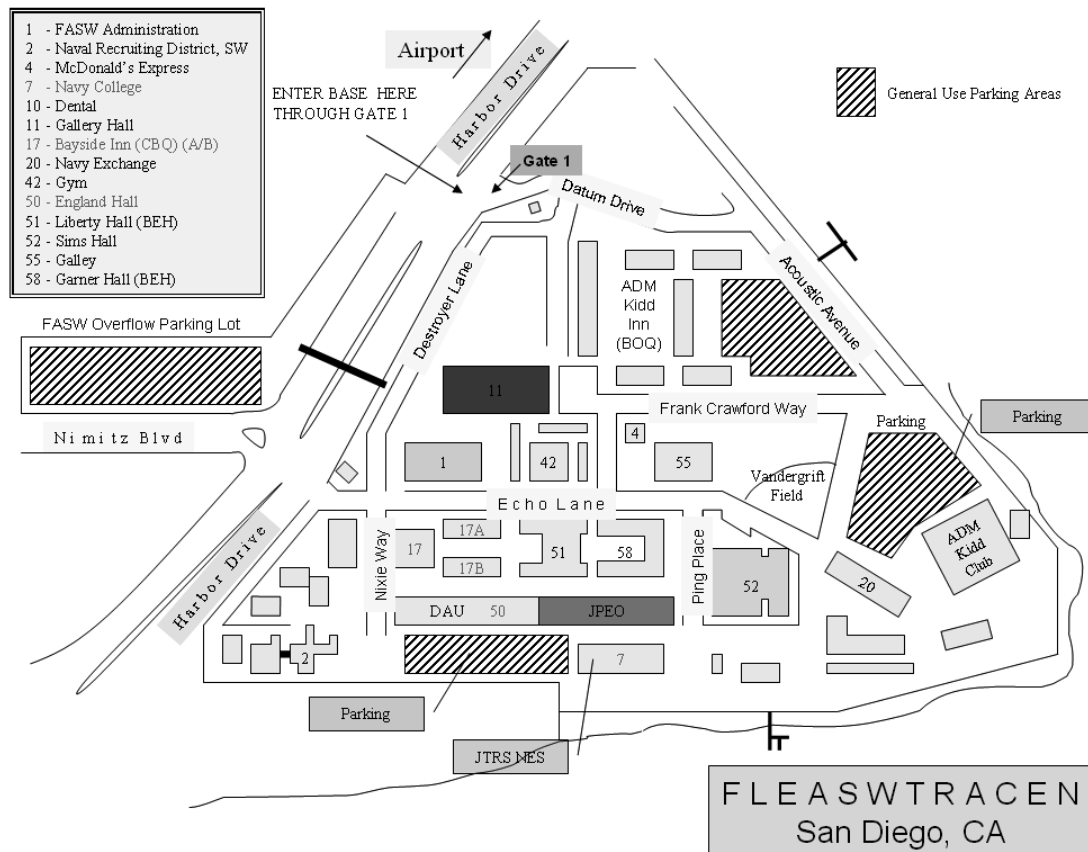


Figure 12. Fleet Anti-Submarine Warfare (ASW) naval base map.

infrastructure and meet all Federal and Navy security requirements. Normally the process consists of obtaining three quotes and submitting those quotes to a contracting officer for contract award. A copy of the final contract purchase order is included as an appendix for proof of delivery and for repeatability, if desired by others.

Just as important as examining the technological challenges is determining the human element, such as staffing. Exploring a methodology to determine whether to complete the job with in-house talent or to outsource the job is often a significant challenge for CIOs.

Wainhouse Research, a top IT research firm, analyzed the impact of service delivery. The firm discovered there are essentially four options for organizations to

implement IT services. The first option is a complete in-house solution in terms of equipment and manpower. Wainhouse calls this the Customer Premise Equipment (CPE) option. The second option is the Application Service Provider (ASP). This is the complete outsource option, wherein the organization pays only for usage on a time metric per minute, per hour, or per connection. This option requires no in-house capital cost or expertise. The third option is the Remote Managed Service Provider (RMSP). This hybrid solution requires the customer to make the capital investment in the hardware infrastructure, but to outsource the manpower from a remote location. The fourth option is the Dedicated Managed Service Provider (DMSP). This option is similar to the RMSP, as it requires the customer to buy the infrastructure as capital investment but provides on-site manpower support. The on-site support is not limited to managing a single type of equipment, but instead is involved in all aspects of the IT organization, as well as strategic planning and integrating business processes (Davis & Greenberg, 2004).

Wainhouse Research chose the metrics of cost/ROI and utilization as the key variables that should influence decision making in choosing one of the four options: CPE, ASP, RMSP, or DMSP. Wainhouse found option one, CPE, to have predictable high ROI, because the capital costs are incurred up front in building the infrastructure, and the maintenance of equipment is predictable. This is reflected as a flat line for CPE in Figure 13. The second option, ASP, has the lowest initial cost because the organization is paying only for usage and makes no capital infrastructure investment.

ASP may be the only solution for organizations that have no capital funds. Because costs increase as utilization increases, there is financial disincentive to use the service; and members of an organization that could benefit from using the service may

not be able to use the service due to financial constraints, even though it is physically available. This option is reflected in Figure 13 as ASP on the left and CASP on the right. This figure reflects this option compared to the other three options as the low-cost and low-utilization leader.

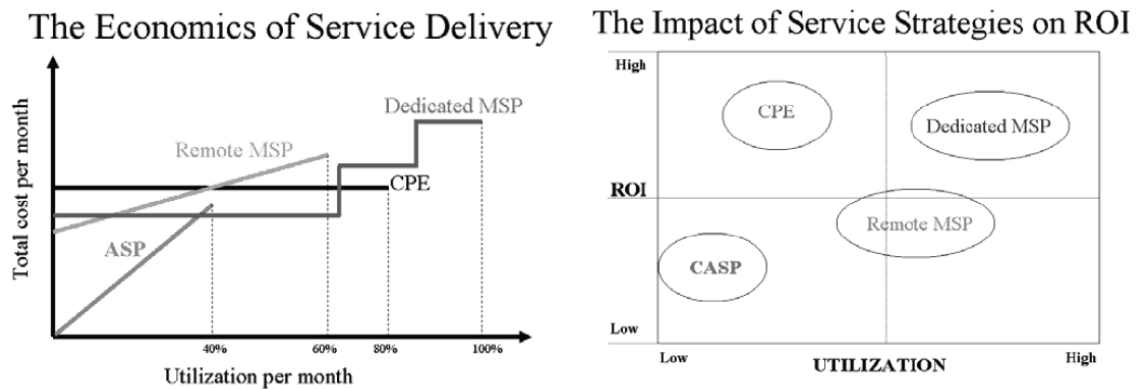


Figure 13. Wainhouse Research service delivery and strategy models. (Davis & Greenberg, 2004)

RMSP is reflected in the lower portion of the Figure 13 utilization grid as the moderate-cost, moderate-utilization leader. RMSP has predictable costs because the infrastructure is paid for and the manpower is off site, and it is not as burdensome a cost as if it were paid for in house, like the CPE or DMSP options. It is ideal for an organization that does not wish to change or grow its IT capability.

The DMSP option is described as “... a strategy that can provide the best of the two worlds—security, expertise, and reliability, with minimum total cost of ownership—and strategy that can drive wide-scale adoption in the enterprise” (Davis & Greenberg, 2004, p. 4). Wainhouse Research claims that DMSP can outperform the other options in terms of utilization, because the onsite expertise not only operates the equipment but contributes, plans, integrates, and helps lead the organization on a strategic level.

Wainhouse Research describes deciding between the four options as the “Managed Services Conundrum.” The firm developed a list of questions to assist in choosing the best provider between CPE, ASP, RMSP, and DMSP:

1. Can you supplement remote management with on-site experts?
2. Can you work with my audio/visual team to integrate with collaboration applications?
3. Can you deliver and support endpoint devices as well as bridges and servers?
4. How do you handle break/fix and normal device maintenance implementations?
5. Can you deliver 24 x 7 support?
6. What service level agreements can you provide?
7. Can you work with my network team to develop a short term and long term strategy for network migration while supporting audio, video, and Web conferencing services?
8. Can you help with billing and reporting issues?
9. How can you assist with our long term integration strategy for rich media tools?
10. What R&D does your company do and how does that R&D help me?
11. Can your team customize software according to our needs?
12. What programs have you implemented that will help my company drive utilization inside my enterprise?
13. What tools do you offer to help my transition to IP, integrate audio, video, and Web conferencing, and manage resources and usage?
14. What experience do you have in providing MSP services? Can you provide existing customer case studies that show your MSP offering can be customized to differing customer needs?
15. How do you find, train, and maintain experienced personnel? (Davis & Greenberg, 2004, p. 8)

The Wainhouse options and questions are useful in determining the level of support and strategy to be used in this research and in complementing the SUS model described earlier this in chapter.

3.3 Specific Procedures Employed

Data for case study research are provided in six different forms: documents, archival records, interviews, direct observation, participant observation, and physical artifacts (Yin, 2003). The primary method of evidence collection for the author was through documents, interviews, and direct observation. These three methods were used in both cases, and the data was triangulated to ensure that the data and conclusions derived from the data are valid. There are no physical artifacts in these cases, and access/existence makes the choice of archival records impractical, if they exist at all. Access to the JTRS/NMCI program offices, staff, and researchers is key to the success of this project. Participant observation exists to the extent that the researcher works in support of the JTRS program. The researcher currently works at SPAWAR System Command in San Diego, California, as the lead JTRS action officer in support of the Network Enterprise Domain (NED). He has been specifically tasked to implement the wireless network for the ASW base. The NMCI program officer is also co-located in San Diego and is accessible to the researcher. Further, the researcher is a current user of the NMCI network and has been one for the past five years.

3.4 Resource Requirements

The System Development Life Cycle (SDLC) of this undertaking consists of seven steps: feasibility study, analysis, design, development, testing, implementation, and maintenance. The SDLC is a popular methodology used to develop information systems.

The feasibility, analysis, and design steps are be done primarily by the researcher alone, in consultation with the JTRS customers and the existing IT support staff. The normal funding process is for a proposal to be given to a fund holder in the form of an informal brief used as a proposal estimate. It is called a Rough Order of Magnitude, or ROM. The ROM is essentially the feasibility portion of the SDLC. If the ROM is funded, i.e., if the sponsor approves the ROM, then the project is feasible. A ROM is also known by other names, such a project scope or a feasibility study. Whitten and Bentley (2005) define a project scope as a plan that consists of five elements:

1. Identify the problems and opportunities.
2. Negotiate baseline scope.
3. Assess base project worthiness.
4. Develop schedule and budget.
5. Communicate the plan. (p. 167)

The ROM used in this project is inserted as an appendix. The ROM was briefed to JTRS leadership in March 2008 and was funded in July 2008, and an initial contract has been awarded as of January 2009. The technical aspects of the project are listed in Table 3. This table was jointly developed with the JTRS leadership (S. Frisbie & R. Broersma, personal communication, January 2007).

The Defense Acquisition University is collocated with the JTRS offices in building 50, shown previously in Figure 12. There is potential for cost infrastructure savings by introducing a partnership between JTRS and DAU offices, which is why the partnership between JTRS and DAU is listed in Table 3. The floor plans with the access-point placements are included in the appendix of this report. The Internet provider

decision is key because it must support both government and non government users. A determination by JTRS leadership was made in consultation with the researcher that non government users and visitors are not allowed access to a government network causing the requirement for both a government network for government workers and a commercial network for non government workers and visiting government workers.

Table 3. Technical Task List

Task Name	Duration	Status
Explore possible partnership with Defense Acquisition University and Naval Base Point Loma	16 days	Complete
Determine government Internet provider	33 days	Complete
Determine commercial ISP (MCI or other)	16 days	Complete
Determine cost from potential provider(s)	13 days	Complete
Get JPEO and security approval for ISP choice	6 days	Complete
Get Funding from JPEO and Contract ISP	16 days	Complete
Get maps of all buildings	6 days	Complete
Talk to Facilities Manager	6 days	Complete
Design inter-building non wireless network	17 days	Complete
Determine hardware installation requirements	17 days	Complete
Determine overall bandwidth requirements	17 days	Complete
Obtain route accreditation	58 days	Complete
Complete SSAA paperwork	58 days	Complete
Establish initial authority to operate (IATO)	58 days	Complete
Conduct general DOD/NAVY Policy review	13 days	Complete
Conduct site survey	36 days	Complete
Determine interferences with cordless phones, microwaves, etc.	20 days	Complete
Determine AP placement	20 days	Complete
Rough the network architecture	36 days	Complete
Determine vendor	34 days	Complete
Research access-point capabilities	1 day	Complete
Research intrusion-detection system	1 day	Complete
Purchase small buy for high-priority spaces	22 days	Complete
Write local policy/confer with JPEO	22 days	Complete
Define responsibilities	21 days	Complete
Provide total cost estimate to JPEO	11 days	Complete
Obtain funding from JPEO	69 days	Complete
Contract AP vendor and installer	23 days	Complete
Hire/Assign IT Support Staff	11 days	Complete
Conduct post-installation site survey	10 days	Complete
Conduct testing	10 days	Complete
Provide user training	1 day	Complete

3.5 Summary

This chapter described the research methods, specific procedures, and resource requirements to be employed during the research. The methodology included the “case study,” as described by Robert Yin (2003), and the systems development life cycle (SDLC). This chapter also described the architectural development process and the DOD architectural framework (DODAF). The requirement process was also explored. The Bentley Whitman methods of SDLC and problem identification were defined in detail. The Bentley Whitman method warns of potential problems in the form of missing, conflicting, unfeasible, overlapping, and ambiguous requirements.

Another framework, James Wetherbe’s PIECES model, was examined as a framework for problem identification. Chapter 3 also described the wireless Supportability, Usability and Security (SUS) model as a strategic wireless deployment framework. Wainhouse Research staffing methods were described in the form of four options: Customer Premise Equipment (CPE), Application Service Provider (ASP), Remote Managed Service Provider (RMSP), and Dedicated Managed Service Provider (DMSP).

The expectation of the researcher in this study was to develop a managed services operation in the creation of a wireless LAN using both SUS model and Wainhouse staffing methodology. The Wainhouse options, along with a questionnaire, are useful in determining the level of manpower support required for a deployment, as well as the form of that manpower, that is, whether it should in-house talent, contractor support, or a combination of the two. The chapter also provides a plan of action and milestones, Rough order of Magnitude/ Statement of Work process, and an initial schedule for dissertation completion.

Chapter 4

Results

4.1 Findings

The goal of the researcher in this study was to develop a managed services operation in the creation of a wireless LAN on a military base. The following actions were taken to meet this goal using the Supportability, Usability, and Security (SUS) wireless deployment framework strategy model.

First, a support agreement was signed between JPEO JTRS leadership and the researcher's office at Spawar System Center Pacific (SSC) San Diego. A copy of this agreement is provided in Appendix A. Wainhouse manpower methodology, described in the previous chapter, satisfied the supportability portion of the SUS model to determine the kind of personnel support structure to be used. Discussions of the four Wainhouse manpower options were evaluated with JTRS leadership: Customer Premise Equipment (CPE), Application Service Provider (ASP), Remote Managed Service Provider (RMSP), and Dedicated Management Service Provider (DMSP). Due to previous dissatisfaction with NMCI, which uses the RMSP approach, it was agreed that the JTRS organization required greater control of the operation. The organization wanted to own the infrastructure and also wanted an onsite technician to support all customer service technical needs, but realized it lacked the in-house expertise to manage the infrastructure. These requirements eliminated the CPE option, because it lacked in-house expertise. It

also eliminated the ASP option because it wanted to own the infrastructure and wanted on-site support. The JTRS leadership therefore chose the DMSP option. The support agreement, which allows for 200 wireless users, shows a recurring cost of \$133,200 per year. This option requires the customer to buy the infrastructure as a capital investment.

Second, an initial equipment breakdown was created, showing a total cost of \$194,272; this breakdown is provided in Appendix B. Among four buildings, 60 of the 802.11g Aruba access points were installed. The exact location of each access point is provided in Appendix C. The tool used for access-point placement was the Aruba Visual RF mapping package. The goal was to have 100% radio frequency coverage throughout all JTRS buildings with the fewest number of access points. The power levels and geographic coverage areas for all 60 access points were verified using a portable Apple iPhone 802.11 scanner called Stumbler Plus. Additionally, fiber-optic cable was run to connect the five buildings together, and Cat 5 Ethernet cable was run to each of the 60 access points to provide connectivity and power.

Third, two unclassified networks were provided to JPEO JTRS from the SSC San Diego via an 802.11a 54 Mbps wireless link. This link uses directional antennas from the SSC Network Operating Center, which is located 2.5 kilometers southwest of the JTRS ASW base. The first network is used for guests and contractors and connects to the Internet through a commercial connection. The second network connects to the Internet through the military NIPRNET infrastructure. Figures 14 and 15 show the 2.5-kilometer point-to-point connection; Figure 14 shows the connection from a bird's-eye perspective, and Figure 15 shows the same connection from the top of the network operating center



Figure 14. 802.11a point-to-point wireless Radio Frequency (RF) connection, bird's eye view.

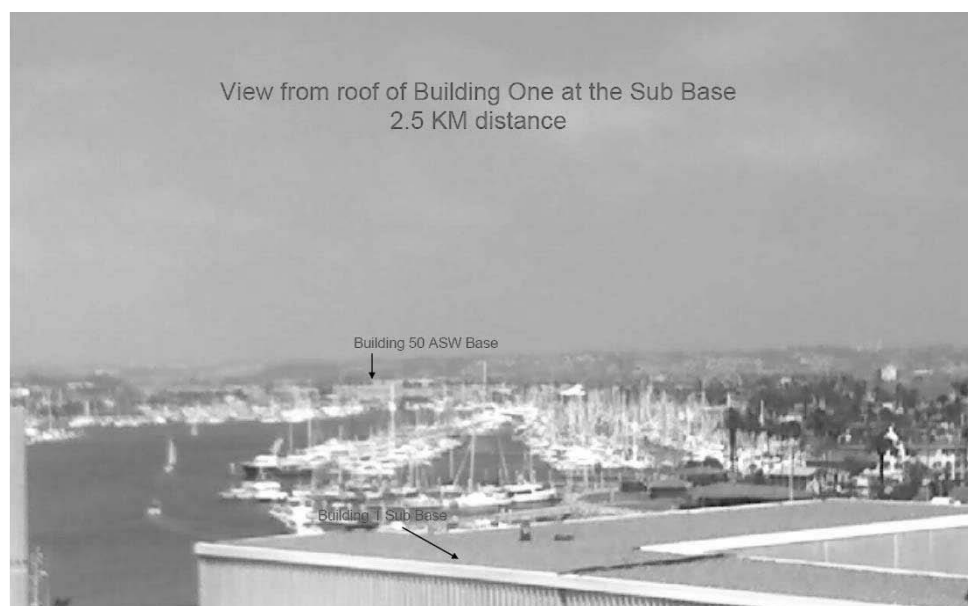


Figure 15. 802.11a point-to-point connection, ground view.

building at the submarine base. Figures 16 and 17 show the five buildings with 802.11 b/g wireless access points.

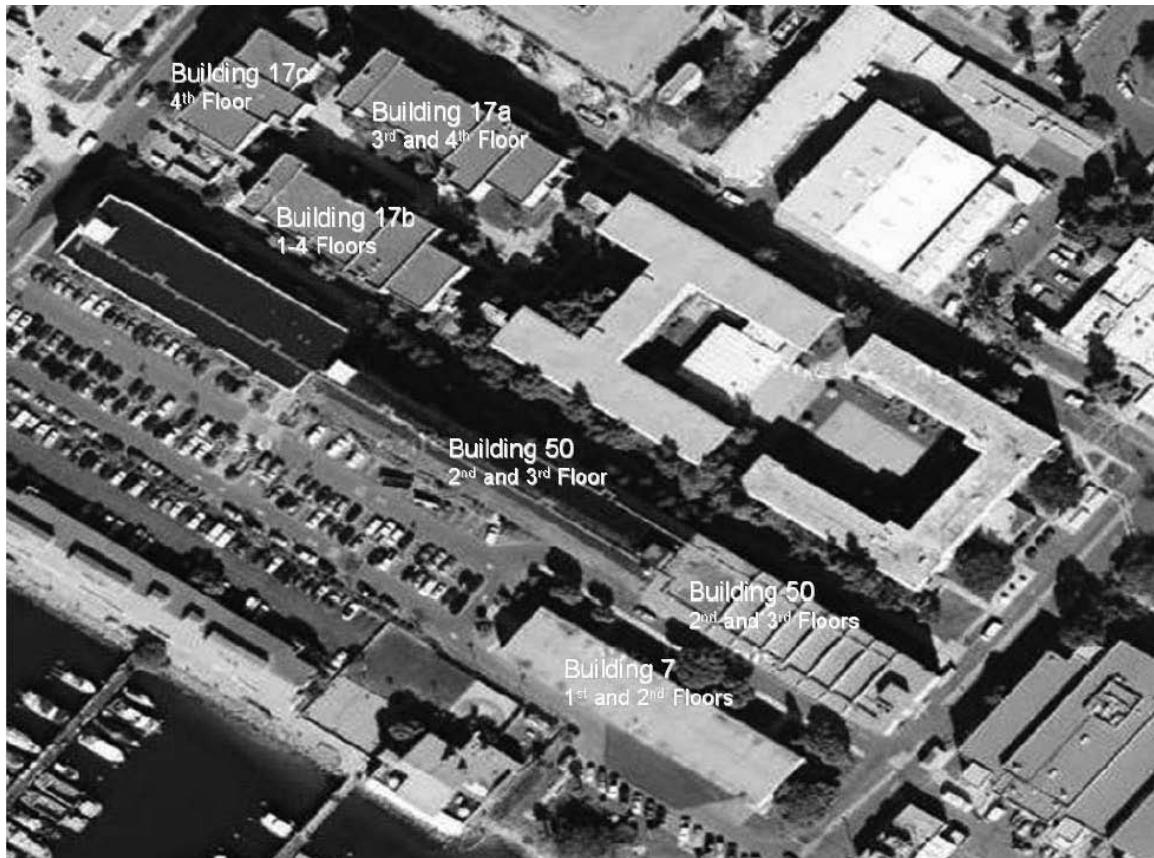


Figure 16. JTRS buildings with 802.11b/g wireless coverage, bird's eye view.

Fourth, several meetings were held with the base frequency manager to ensure that the 802.11 devices were in fact designed to use only unlicensed spectrum and did not require FCC or higher DOD approval to operate. There was concern that any new radio introduced on a base could potentially cause interference with existing systems or, worse, that the power levels/gain might be high enough to be a radiation hazard to personnel. After providing appropriate documentation to show that power levels were only 0.1 watt and that the frequency used did not require licensing, permission was granted by the base



Figure 17. JTRS buildings with 802.11b/g wireless coverage, ground view.

frequency manager. An additional meeting took place with the public works department, and direction was given that the antennas and outside equipment needed to be (a) painted white to match the building color and (b) properly secured in case of high wind so the directional antennas would not become flying missiles that could injure personnel or property. The equipment was painted, properly secured, and inspected by the public works department.

To satisfy the usability portion of the SUS model, the network has to meet the core needs of the customer. These needs were recorded as requirements in Chapter 3, and all requirements were met. The highlights of these usability requirements are (a) 100% wireless coverage of all JTRS spaces, and (b) two wireless networks, one for guests/contractors and one for government personnel, both military and civilian. Figure 18 shows the wireless networks: the guest network that uses a commercial connection to the Internet, called “jtrs-guest”; and the workhorse wireless network, called “SPAWAR,” which connects via a secure government network to the Internet.

A user agreement was developed with the JTRS administration, and a copy is provided in Appendix D. Each user is required to sign this agreement prior to being allowed access to the network. Additionally, a Statement of Work (SOW) was jointly developed with the JTRS administration, describing the duties and responsibilities of the onsite contractor support, and a copy is provided in Appendix E. The SOW was used as the skeleton for a task order for supplemental work under an existing agreement with L3, a defense contractor.

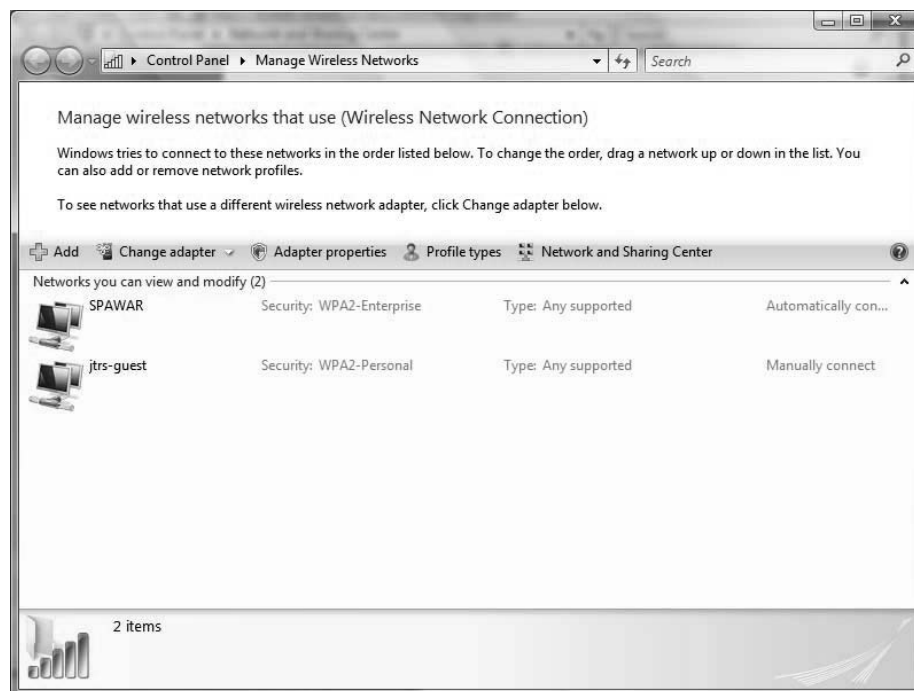


Figure 18. JTRS wireless network “SPAWAR” and “jtrs-guest.”

The SOW and Interservice Support Agreement (ISA) provide clarity for all parties to ensure proper supportability in terms of customer satisfaction, cost, and security requirements. After the wireless network was operational for six months, Keith Kaufman, JPEO JTRS operations representative for the wireless network, completed a customer survey. The completed survey is provided in Appendix F. He gave the maximum grade of “Extremely Satisfied” in the areas of “Quality of products and/or services,” “Time and schedule performance,” “Budget and financial performance,” and “Overall Performance.”

User configuration instructions were developed by the SSC network team. These instructions show prospective users how to connect to the wireless network and print for both the government and commercial networks. The configuration instructions are provided in Appendix G.

4.2 Technical Issues

After informal interviews with support staff, the most common connectivity problems were attributed specifically to the following:

1. Users' entering the wrong ID and/or password (commercial network) or CAC pin (government network).
2. Users' checking email without properly authenticating to the system (commercial and government networks).
3. Wireless network driver and/or network hardware does not support WPA2 (commercial and government networks).
4. Users' preference to use the commercial network over the government network, because commercial setup can be done in less than five minutes, whereas government configuration can take up to 90 minutes because of the need to update all service packs, such as Windows Service Pack III.
5. Printer-setup configuration continues to be an issue because users would rather have a system administrator do the configuration than to configure it themselves.
6. The wide variety of user end equipment is a system administrator challenge. Configuration is made difficult for support personnel, due to numerous operating systems, such as the Apple iPhone, Windows 2000, Windows XP, Windows Vista, Redhat Linux, Apple Mac OS X, and Nintendo DS.
7. Often wireless network card manufactures provide proprietary wireless configuration client software that overrides the built-in operating-system wireless client. These proprietary clients can be difficult to configure, may

experience reduced functionality, may conflict with the operating system clients, and/or may require additional training to operate.

8. Contractors from the following companies—SAIC, L3, Booz Allen Hamilton, CSC, IT Mentor, CSC, EMN Defense, and SRA—all have personnel working on site. Each company provides laptops with different hardware, different software, and different levels of access. Additionally, military personnel and civil servants from all branches of the military are represented on site; some use NMCI equipment, and some bring their own equipment from their respective service. Additionally, visitors from these groups (military, contractor, and civil servant), as well as guests from industry and academia, all want access to the wireless network. The plethora and diversity of the user base requires on-site system administrator support.

The JTRS commercial and governmental wireless networks have been operational for over six months. The network has consistently run in a flawless fashion. The potential negative impacts of signal multipath from the RF physical properties, such as reflection, refraction, diffraction, scattering, or absorption, were mitigated because each radio has two antennas, allowing for diversity, which minimizes the impact of multipath. The only interruption of service was when a crane temporarily blocked the 2.5 km line-of-sight 802.11a link. The crane interrupted the link for only a few hours during some minor building construction. The crane was located approximately one mile from the ASW base, in the line of sight between the sub base and the ASW base. The outdoor antennas have a radome, so they are protected from the elements such as rain and fog. The antennas also have lightning arresters in case of a lightning strike.

4.3 Integration with NMCI

There was concern from many end users that a large investment in NMCI hardware was significant and this investment would have been wasted if a policy or technical solution was not made to allow connectivity of the NMCI laptops to the non NMCI wireless JTRS networks, either commercial or government. Current NMCI laptops and desktops do not have 802.11 network cards installed, and this researcher does not have administrative rights on NMCI machines to install the required software drivers and wireless cards in order to connect these machines to either the wireless 802.11 Research, Development, Testing, and Evaluation (RDT&E), or the wireless 802.11 commercial network.

The policy and configuration of NMCI machines do allow external connection via the wired non-wireless 802.3 Ethernet port. The remote system is called the Broadband Unclassified Remote Access Solution (BURAS). This port is open so that, when NMCI users are traveling, they can get network connectivity through a hotel wired port and use the VPN software to securely connect to the NMCI network (Navy/Marine Corps Intranet Public Affairs, 2005). A portable bridge appliance device that has both an Ethernet and 802.11 would allow connectivity to an NMCI laptop without any configuration to the NMCI laptop, as long as the device supports WPA-2 in client configuration. An Edimax 7206-APG wireless LAN device was purchased for \$30 from newegg.com. According to the Edimax online manual, “EW-7206APg is a bridge between the wired Ethernet and the IEEE 802.11g/b wireless network. EW-7206APg lets your wireless client stations access both the wired and the wireless network nodes” (Edimax, 2009, p. 10). This device is unique in that its firmware allows it to be treated as if it were a client station, i.e., a laptop. Most wireless access points or firmware does not have this capability. This device

was tested and successfully connected several NMCI laptops to the commercial wireless network with zero configuration to the NMCI machines.

NMCI users were able to successfully VPN back to the NMCI network through the commercial wireless network. The Edimax device had to be preconfigured with the WPA-2 SSID and infrastructure pre-shared key. Users are required to use a userid and password, which are entered via a Web browser on a connected laptop via its wired Ethernet port. The Edimax device would successfully connect only to the commercial wireless system and not to the government wireless network, because the government network requires the Edimax device to have a CAC reader for authentication.

Theoretically, the hardware and firmware of the device could be altered to allow connectivity to the government wireless network. To support this capability, the device would require the soldering of an additional USB port to the unit and modifying the operating system of the device, a task beyond the scope of this research. An Edimax device, shown in Figure 19, was put in a conference room to allow NMCI users zero configuration connectivity. The device does require power via 110V AC adapter. This makes it awkward to use it in a mobile fashion, because a laptop user would need to find two 110 plugs: one for the laptop and one for the Edimax device.

The Edimax solution also works with non NMCI laptops that do not have a wireless card installed, with users who do not possess the technical ability to configure a wireless card, or in situations where users do not have system access to activate the wireless card in their machine. Additionally, a formal request has been submitted to the NMCI leadership requesting the ability to have administrator access and the ability to install PCMCIA wireless cards on NMCI machines. If this request is approved, then the



Figure 19. Edimax Wireless NMCI connection device.

NMCI users would be able to easily access JTRS commercial and government wireless networks without being tethered to the EDIMAX device.

4.4 Summary of Results

The problem investigated in this study was to evaluate the efficiencies achieved by organizing and transitioning from a traditional network operation center to a managed services operation in the development of a wireless local area network (LAN) in a military setting, by asking the following research questions:

1. What are the challenges of implementing a managed wireless architecture?
2. What are the customer operational requirements of wireless implementation?
3. What is the value of a service-oriented architecture?

The greatest challenge is to have a clear strategy on defining customer requirements and transforming those requirements into technical/contractual actions while maintaining customer confidence that the project will be accomplished on time, on

budget, and in conformance with customer performance expectations. These technical and contractual actions need to be jointly developed with the customer in the form of physical deliverables mapping operational requirements. These deliverables have been previously described and are shown in appendixes A through G, encompassing the support agreement, equipment lists, wireless coverage floor plans, and more. Customers also must have the appropriate financial resources to fund the operation. These deliverables cement the operational expectations and marry them with a clear cost. DOD customers want their networks to be supportable, usable, and secure. Unfortunately, they do not always have the technological background or willingness to invest in their own personnel's technical competence to transform high-level operational requirements into a technical realization.

This is where the Wainhouse manpower options are helpful in providing a methodology to determine whether to outsource the manpower and infrastructure. The shortfalls for NMCI can be attributed to the fact that the wrong Wainhouse manpower option was chosen. The Navy and NMCI jointly chose to outsource the infrastructure and the manpower support as well as have the support infrastructure completely off site. They chose the Application Service Provider (ASP) option when they should have chosen the Dedicated Management Service Provider (DMSP) option. The transition to Next Generation Enterprise Network (NGEN) from NMCI is focused on reclaiming control by buying back the network from NMCI and having onsite support in the form of contractors and government personnel. Hopefully, when the Naval Networking Environment (NNE) is launched in 2016, the DMSP option will be the norm to correct the many problems associated with NMCI. The difficulty will not only be to replace NMCI but to align with

all the shipboard, overseas, and Marine Corps networks. The value in having a dedicated technician whom users know by name cannot be underestimated. The ASP option, where support is remote, does not allow for the personal service relationship to develop. Users frequently complained about having to start over with the background of a problem each and every time they called. NMCI technicians refuse to give out their full names or provide a direct phone number to get the same technician. They only give a tracking number, which often is useless. The DMSP option allows for greater accountability, because the users know the on-site technician personally.

Interestingly, after six months of operations, a request was submitted by the Operations Department to reduce the number of NMCI desktops that were used by contractors, and instead have contractors provide their own company laptops, with the contractors getting their Internet connectivity through the guest contractor wireless network. Many of the contractors already had company-provided laptops and were taking advantage of the JTRS commercial guest wireless network. While the plan for both the government and commercial wireless networks was designed as an augmentation to the wired NMCI network, it is not surprising that Operations Departments viewed having the wireless network as a potential replacement due to clear cost savings of not having to provide a desktop to many contractors. Some disadvantages exist in using the wireless network as a replacement for a wired NMCI:

1. Contractor laptops would need to install a CAC reader and CAC middleware software *Active Identity* to connect to government sites requiring two-factor authentication such as NMCI email, numerous government Web portals, resource management sites, and military requirement/planning sites.

2. Contractor laptops could use only the Web based email called Outlook Web Access (OWA), and not enjoy the full functionality of Outlook email. Some dissatisfaction has been expressed regarding the use of OWA because of the difficulty in managing, copying, and reading emails. NMCI policy locks out a user from sending email when that user's inbox exceeds 50 megabytes of storage. OWA does not allow the moving of emails to a local storage file, a capability available in the full Outlook application on the wired NMCI machines. OWA users cannot send emails once the 50-megabyte storage threshold is reached. They are faced with deleting emails or waiting until they can get access to an NMCI wired machine to move their emails to a local storage drive.

OWA is normally used as a temporary method to read email while traveling and using a loaner/temporary government computer. NMCI email storage policy is highly unpopular, considering that such free email services as Google's G-mail, and Microsoft's Hotmail each provide over a gigabyte of free email storage. Contractors that are heavy email users will be frustrated using OWA and will revert to using their company-provided email services for the bulk of their email communications.

3. Using alternative emails to NMCI will make it difficult to locate contractor's emails if they use their company emails, because only NMCI emails are published in the NMCI global email directory.
4. JTRS leadership may not want sensitive information on non-government emails such as contractor emails.

5. Reading digitally signed and/or encrypted email on a commercial machine is very difficult and is not supported in OWA.

Non-NMCI government laptops using the government wireless network could use a Citrix session to use the full Outlook application and other NMCI virtual Metaframe applications. Some Citrix users have complained that they cannot access their email in the mornings from 7:00 to 8:00 a.m. because the Citrix server connections are saturated at peak morning hours.

One could make the argument that Electronic Data Systems (EDS) has created technical policies that maximize the deployment of wired NMCI desktops (maximizes revenue for their company) and at the same time, their policies prevent competition in the form of OWA and Citrix. One potential alternative is to use the Army's free Web-based and client email at Army Knowledge Online (AKO). AKO allows for a 100 megabytes of storage at no cost, and it can be connected using the Web or from traditional email POP3 or IMAP clients such as Outlook.

Additionally, potential interference issues were mitigated because a thorough site survey was completed involving the Public Works Department and the base network infrastructure engineer. Having blueprints of all the buildings made the survey easy, as did having easy access to roofs and server rooms. Several areas of potential concern were cordless phones, microwave ovens, and other 802.11 networks, because they all transmit in the same 2.4–2.5 Gigahertz frequency range as 802.11 networks. A nearby barracks with young sailors showed several wireless signals. It was assumed that these were the laptops used by the young sailors.

In addition, a recreation center near the JTRS office offered free wireless. That access point was also visible during the site survey and was picked up by the Aruba system after installation. Aruba, the access point vendor selected, was chosen not only because of its FIPS 140 security certification, but also for its ability to channel-hop when it detects noise or other wireless network using the same channel. The decision to go with one vendor for the access point was the correct one. Having a multiple-vendor access point on a single network would mean management chaos, because network engineers would not have the ability to effectively determine which access points were running or what their current security posture was, and they would have to apply different security firmware patches, depending on the vendor. Other RF issues, such as multipath, near/far access point interference, or generic noise interference issues, were not observed. This was verified by doing several throughput speed tests at BroadbandReports.com. The website performs bandwidth upload and download tests. This test was run through several parts of the JTRS building with no discernable difference in results.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

5.1 Conclusion

The purpose and content of this work was to explore the proper strategy on how to deploy multi-service mobile net centric warfare. This was accomplished by achieving the research goal of developing a managed services wireless LAN enterprise on a military base. This research examined the failings of Navy Marine Corps Intranet (NMCI) resulting from the wrong manpower strategy's having been implemented. This research also showed how low-cost commercial approaches such as IEEE 802.11 wireless local area network technologies could be implemented as a joint notion of Net Centric Warfare in terms of a Service Oriented Architecture (SOA). A successful IEEE 802.11 wireless network was designed, funded, contracted, and installed that supports both government and guest connectivity using the SUS strategy model. An effective manpower service strategy was chosen using the Wainhouse Dedicated Managed Service Provider (DMSP) option.

The JTRS leadership also approved a support agreement and statement of work that defined support requirements in clear terms. A user agreement and configuration instructions were also developed to ensure that users understand (a) how to properly connect to the network and (b) how to use the network responsibly. The entire installation meets all DOD wireless security requirements. In short, a complete turnkey wireless

managed service operation was successfully deployed throughout the JTRS five-building enterprise in terms of supportability, usability, and security. All this was done on time, on budget, and in conformance with 100% of the customer requirements. The goal of the researcher in this study was to develop a managed services operation in the creation of a wireless LAN on a military base. In the process of achieving this goal, specific organizational, managerial and technical issues were identified and related to research literature. The goal was successfully accomplished. The problem investigated in this study was to evaluate what cost savings and/or efficiencies are achieved by organizing and transitioning from a traditional network operation center to a managed services operation in the development of a wireless local area network (LAN) in a military setting. The problem was successfully investigated.

5.2 Implications

This research can be used as a model for both future managed service generic network operations and wireless IEEE 802.11 deployments throughout the DOD. The research shows the importance of strategic models such as the SUS wireless model and operational manpower tactics such as the Wainhouse staffing methodology. It also shows the current security requirements for an IEEE 802.11 network. Additionally, the project management execution aspects of the research used the System Development Life Cycle methodologies. The research also provided vetted examples of a managed service wireless support agreement, support contract statement of work, equipment lists, wireless configuration instructions, and overall cost estimates and expectations. It is hoped that this research will aid in avoiding a repetition of the mistakes of NMCI and help to assure that future wireless deployment is done in a secure, usable, and supportable fashion.

The DOD prefers an incremental improvement path to reduce risk. Thus, 802.11 and SOA in their various forms have been around for over 10 years. There is enough momentum, through the deployment precedents set in the commercial world and DOD pilot programs, for this research to be ripe for significant impact. Reliable wireless service oriented architecture is in high demand. The military needs a road map on how to deploy wireless networks in a secure, supportable, and usable fashion that is in concert with the core mission of the military business requirements, i.e., a service oriented architecture.

5.3 Managing the political landscape

In dealing with the SSC organization (the technical provider of the wireless network) and JTRS (the customer), it is important to note some unique differences in the corporate culture between these groups and their impact on the process of technically fielding and funding the project. The first conceptual proposal was submitted to the JTRS leadership in early 2007. JTRS leadership agreed to fund \$200,000 for the equipment installation and the contract process was begun. Just before the contract was awarded, the funding was not transferred to SSC. No one in the JTRS Operations Department knew the reason for the funding problem.

After further research and active contact with the JTRS Finance Department, SSC was informed the project would not be funded. No explanation was given for the last-minute bad news. Six months later, inquiries were made at different points within the JTRS organization, and it was confirmed that the reason for denial was that JTRS cost overruns in other areas prevented the wireless network from being funded. In 2008, the same 2007 proposal was re-briefed and was again accepted, but this time the funding was

transferred to SSC. Often a project is technically sound and the customer wants the project fielded, but is prevented from funding the project and is embarrassed or is not allowed to explain the reason for the denial of the project. Without an explanation, project petitioners are left uncertain as to the reason for the denial and are left to speculate that the project may have been poorly presented or lacked the technical and/or political support needed for success. The success in this case was having the persistence to resubmit the proposal with the hope of approval or at least a clear explanation as to why the project was rejected. Fortunately, the project was approved the second time, a year later. While the exact reason for acceptance will never be known, it is most likely because funds had become available. A secondary factor may be that the organization felt guilty by reneging on its promise to fund the project the previous year, and/or the leadership was impressed by the petitioner's persistence to re-brief the project.

Another potential factor was that the researcher had a better understanding of the JTRS organizational hierarchy and that the assumption should not necessarily have been made that the JTRS Senior Executives leadership, the JTRS Operations Department, and the JTRS Finance Department were eager champions. In fact, early discussions with the Operations Department gave the researcher the impression that the wireless network would mean more work and liability for the Operations Department, not a goal they desired. The Finance Department treated the wireless project without approval or disapproval. To them it was simply one of a thousand different financial records that required administrative and financial accountability tracking. The Executive Leadership wanted it done, so the Operations and Finance departments were at least superficially supportive. There was also the potential threat of another project's gaining enough

political support to remove the funding from the wireless project for their needs. The potential project competitor could come from the Operations Department, the Financial Department, SSC, or anywhere else. Having a better understanding of the political landscape, the researcher needed a plan to deal with these threats. *The problem amounted to a need to understand who the customers were and how to maintain their confidence throughout the lifecycle of the project.*

The tactical goal was to improve the perception of the wireless project with both the Operations and Finance departments. The first step was to frequently interact with the customer, but not to the level of annoyance. Emails and phone calls were positively received, but in-person short briefings seemed to have better impact. Since both the researcher and the customer are government employees, the customer did not believe financial profit was the motivation for the meeting. In government led organizations, often contractors do not have the same level of trust as military or civil servants. Contractors are often perceived as profit-driven entities, so the truthfulness and the motivation of their actions are often suspect or viewed as biased/tainted. Outside contractors (i.e., non-JTRS contractors) are doubly suspected, and often this mistrust can be wrongly attributed to non-JTRS military and civil servants. SSC military and civil servants were often assigned to support the JTRS program in either a temporary or permanent role. SSC has the status of trusted agent: better than a contractor, but not on the same footing as a JTRS military or civil servant regular.

The researcher's status of being military and not a for-profit entity was reinforced with all customers, as well as the notion that the researcher's motivation was to improve his reputation by making the project a success. Statements such as "I am one of you" and

“I am on team JTRS” were frequently used to contradict any perceived outsider xenophobic sentiment. The lesson learned from the year-long funding delay was that the customer may include several groups of an organization, not just the top leadership. The customer may also include different groups at different phases of project’s lifecycle. In this case, during the proposal phase the researcher did not understand that the customer was not only the executive leadership, but also the Finance and Operations departments. Had the researcher established positive rapport with the Finance Department earlier, then the wireless project may have been funded the prior year.

The researcher was not going to make the same mistake twice. Building confidence with all three customer groups was a top priority. This was achieved by the researcher’s personally visiting each department weekly to brief them on the progress of the project. It is more difficult to cut programs with a trusted colleague than a stranger. This is basic human nature. A marketing education campaign was focused on the Finance Department to personalize the project as much as possible. Another measure to protect against financial threat was to obligate the funding as quickly as possible by putting the equipment on order via a contract. Once the contract is awarded, it becomes impossible for the JTRS office to take back the funding.

The researcher also commenced a concerted effort to minimize the fears of the Operations Department that the wireless project would only mean more work and liability. This was done by heavily involving them with the decision to hire a support contractor, allowing them input and edit on the statement of work for the support contractor as well as involving them with the Interservice Support Agreement (ISA) provided in appendences D & E. Additionally, JTRS enterprise-wide meetings were co-

chaired by the researcher and the Operations Department, allowing for enterprise education, input, and acceptance of the project. Additionally, once the contract was awarded and actual construction began, greater confidence from the customer was achieved. Once the project was operational, the JTRS organization was addicted to the wireless. This was a strong position for the researcher to be in.

The political landscape was not easy at SSC either. Since SSC, according to the ISA, is the provider of the network, then the commanding officer of SSC becomes the accountable officer for any security problems associated with the JTRS operation. Historically, 802.11 operations had been banned in the DOD. The SSC Commander required several briefings that the JTRS network was in 100% compliance with all existing Department of Defense and Department of the Navy policies and the risk to the Navy's network was minimal. The SPAWAR Admiral at headquarters was also briefed on the plan. Eventually,, the Commander signed the ISA, agreeing that the risk was acceptable for the JTRS wireless project to proceed.

5.4 Contracting Challenges and Procurement Strategies

One interesting challenge after the funding was secured from the sponsor was the process of converting dollars into equipment and services. This process, called the contracting process, is not as easy as one would expect. Because project managers in the public sector are dealing with taxpayer money, they are subject to Federal Acquisition Regulations, commonly called the FAR. Only procurement specialists designated in writing as a Contracting Officer, commonly abbreviated as *KO*, have the authority to obligate the government to purchase equipment. (The abbreviation *CO* is reserved for Commanding Officer, who is normally the senior military officer of a military

organizational unit such as a ship, squadron, or base.) Project managers must be very careful when dealing with commercial vendors/contractors who provide equipment services to the government. If a project manager tells one of these vendors to ship equipment without an approved purchase order signed by a KO, it can create a legal problem in which the project manager is often held personally liable for the unauthorized purchase. When dealing with equipment in excess of \$100,000, acting without KO approval can be expensive for a project manager and potentially detrimental to the career. The solution is simple: Do not act unless one has consulted with the KO. When one talks with vendors/contractors, it is highly advisable to send an email to them stating that the requester does not have procurement authority, and any quotes requested are for market research purposes only. The KO expects project managers to provide the KO with at least one quote from an acceptable vendor, stating exactly what equipment to purchase. The KO will often try to get additional competitors' quotes to be evaluated by the project manager/government engineering team to choose the best value for the government. KOs want the lowest price for the equipment requested but will allow the project manager to review the quote to ensure that the vendor selected meets the minimum criteria and is "best value" of all the choices. The contracting selecting process can take up to six months, depending on the cost and complexity of the quote.

The first vendor chosen to quote (For market research purposes only) was Tel Tech Plus (TTP). TTP was chosen because they have done several information technology infrastructure installs on the ASW base, they had the confidence of the SPAWAR Pacific Chief Engineer, all their employees already had passes/clearances to work on the base, and they were subcontracted by NMCI to do NMCI installation. There

was concern that NMCI would try to block this project because they would see it as a competitor. By potentially hiring their subcontractor one could navigate the political waters more easily, specifically ensuring that no IT infrastructure would be shared or interference created between the project infrastructure and the NMCI infrastructure such as telecommunication closets and wiring runs.

The slowness of this process can be frustrating to project managers. The process of getting the quote from a vendor can be laden with challenges such as the vendor's trying to "pad the bill" by adding unneeded items to a quote. When this happens project managers often keep the unneeded item on the quote due to possible procurement time constraints or unfamiliarity with the individual functionality of each line item of the quote. Technically proficient project managers will request another quote instructing the removal of the unwanted items. KOs have a limited technical background and require project managers to certify that the quote meets all the technical requirements of the project. In this case, the researcher/project manager met with the SPAWAR Pacific Chief Engineer and the vendor. The Chief Engineer and the project manager made it very clear that the project would be competitively bid, that the vendors needed to provide their best price, and that the vendors needed to provide a 100% turnkey solution. No additional funding was available, and their equipment list needed to meet 100% of the requirements listed. A few weeks later, the Chief Engineer and the Project Manager reviewed the quote, certified that it met all the technical requirements, and submitted it to the KO with the funding data from the JTRS office.

KOs are also mandated by law to set goals that 23% of all purchases need to go to small businesses with preference to women owned businesses, disadvantaged minority

owned businesses, disabled veterans, and small businesses that reside in a designated underutilized business area. This 23% small-business set-aside goal can trump a non-small business competitor's bid even if they have a lower bid. In some cases a small disadvantaged company can be designated "8(a)" by the small business administration. The 8(a) designation gives KO's the option of selecting them without getting quotes from competitors. Smart project managers and smart vendors should attempt to target small businesses, because it helps KO's meet their 23% goal and thus will shorten the procurement award time, sometimes up to 75%. In this case, TTP is a small disabled-veteran-owned business under the 23% goal guideline. Nevertheless, it was not 8(a) designated, so there had to be a public advertisement asking for other bidders. Fortunately, no additional bidders responded to the advertisement. Additionally, the researcher/project manager sent a letter of urgency requesting that the procurement be awarded within 45 days. The KO transferred the procurement to the East Coast office, which was better staffed, and the TTP was awarded the contract 30 days later, a SPAWAR procurement speed record. For the network administrator support contractor, L3 was chosen for the following reasons:

1. SPAWAR already was executing a contractor with L3 in support of JTRS work, and adding an additional task order could be done in less than 60 days. This was based on the project manager/researcher's experience of getting several other L3 task orders awarded the previous six months in that time frame.
2. The L3 area manager had previously sent several résumés of engineers who needed work. One stood out because he had a technical degree, numerous

industry certifications, 802.11 wireless experience, and five years' experience in the IT industry; further, he was a former Marine officer with a security clearance.

Forty-five days later, the L3 engineer task order was awarded and the L3 engineer began working on the task. Two weeks after that, the wireless equipment from TTP arrived. Bi-weekly meetings with the project manager, TTP install manager, L3 engineer, JTRS operations manager and the SPAWAR Chief Engineer occurred until the project was installed and operational 60 days later.

The key procurement strategy lessons learned are as follows:

1. Avoid unauthorized procurements with vendors by sending them emails that the requester does not have procurement authority and all quotes requested are for market research purposes only.
2. Attempt to choose a vendor that is a small business and/or 8(a) designated, to speed up the KO selection. A letter of urgency to the KO with an expected award date also puts pressure on the KO to conform to a reasonable response time. Often, when no award date is communicated to a KO, a KO often presumes to take up to six months or longer to award.
3. Thoroughly review the quote with a senior government engineer to ensure that the vendor meets all the intended technical requirements of the project.
4. Hire support engineers with the appropriate experience, technical degrees, and certifications.
5. Nothing builds confidence in a sponsor like getting a project done technically well, on time, and under budget.

5.5 Recommendations

The results of this research can be used as a model for both future managed service generic network operations and wireless IEEE 802.11 deployments throughout the DOD. The research shows the importance of strategic models such as the SUS wireless model and operational manpower tactics such as the Wainhouse staffing methodology. It also shows the current security requirements for an IEEE 802.11 network. This work should be distributed to senior military officers and civil servants who will be project managers for SOA and wireless projects.

New research in the areas of modeling and simulating entire network operating centers is beginning to develop and will clearly impact both managed-service and wireless deployments. Additionally, the impact of security—as well as the legal issues of accountability, responsibility, and ownership—on the virtual enterprises will be profound, since physical demarcations of equipment will become more complex. The maturation and acceptance of Net Centric Warfare in terms of technology deployment should also be monitored as new threats to the DOD emerge.

The research can also be further explored in terms of new social network applications such as Twitter, Facebook, MySpace, etc. The youth of America have learned to collaborate and communicate in new ways, and these methods should be studied for possible advantages for military use. Perhaps the low bandwidth text updates that Twitter technology uses for texting could be used for weapons system reporting or aircraft maintenance status. An aircraft could report what is wrong with it before it even lands, using a combination of 802.11 wireless technologies and low bandwidth application formats used in Twitter. Facebook applications could also be used for military

personnel to hold their entire personnel records and experiences. When a commander is putting together a team he could flip through individuals' Facebook pages and see all their assignments, evaluations, photos of the individuals, etc. This would give a greater pictorial/graphic representation of who the individual is. The commander could do this with a portable secure device, assuming the infrastructure is built to support this application.

Further research can also be performed to better map traditional warfare strategies to new wireless technologies. The traditional seminal warfare strategists taught at all the War Colleges are Clausewitz, Sun Tsu, Mahan, Jomini, and Corbett. Their writings can be put in modern terms by using their time-tested ideas in new technological ways in a mobile tactical environment. Military Strategist and Command and Control expert, Colonel John Boyd, authored the combat operations decision process: the Observe, Orient, Decide, Act (OODA) loop. He brings some interesting research topics in regards to inserting new technologies that augment the speed of combat decision making. Further research could be done that could quantitatively measure the impact of inserting wireless and service oriented technologies into the combat decision cycle. Also the physical elements of wireless deployments could be examined, such as battery life and the wearability/usability of portable devices. Further examination could be made of the impact of nature, such as extreme heat, cold, sand, humidity, snow, etc., on both the equipment, service, and personnel. Nontraditional military operations, such as humanitarian relief, could be studied to see if managed services applications are resilient enough to adapt from a military's traditional role of combat operations.

Further research could also be done in the analysis/development of government policy and legislation. Computer fraud, identity theft, and surveillance are all hot topics when any new wireless technology is inserted. Understanding the Federal, State and local laws, when designing any network, is key to a successful deployment. Corporate secrets, government secrets, and personnel information are all potential legal liabilities areas for a network architect.

Further research could be done in the pursuit of developing a clear educational path for military service oriented project manager/implementers. Subject elements from business administration programs to public administration programs, system engineering programs, software engineering programs, information technology programs, computer science programs, and contracting/system-analysis programs could be compiled and analyzed for an ideal training/educational career path for potential military SOA managers.

Further research could be done in the combined areas of ad-hoc wireless network in the context of Service Oriented Architecture (SOA). Essentially, the research could be used to design and describe a portable encapsulated wireless SOA wireless infrastructure. Questions of security and scalability could be analyzed. Possible military applications are vast, as they could be applied to short military deployments in hostile areas such as the Middle East and Southwest Asia.

Further research could be done in the areas of comparing on-public infrastructure wireless networks such as 802.11 networks to such satellite networks as Iridium and the International Maritime Satellite (INMARSAT) organization compared to such cell-phone 3G/4G networks as Long Term Evolution (LTE) and Ultra Mobile Broadband (UMB).

Further research could be done analyzing the procurement, funding, and contracting process in regard to efficient and effective ways to convince financial decision makers (fund holders) to sponsor a project and the best way to procure the right services and equipment in a timely fashion. Analysis of the Federal Acquisition Regulations (FAR), in concert with Service Oriented Architectures (SOA), could lead to discernable savings for the military and the entire IT Industry.

Further research can be done on ways to help streamline the transition from NMCI to NGEN and formalize processes and methods to avoid the mistakes made with NMCI In terms of manpower strategies, the ability to make configuration changes, and general customer service procedures.

5.5 Summary

The perceptions of an existing service-oriented wireless system can greatly influence the acceptance of future wireless implementations in programs such as NGEN, which can benefit all the military services. The goal of the researcher in this study was to develop a managed services operation in the creation of a wireless LAN on a military base. In the process of achieving this goal, specific organizational, managerial and technical issues were identified and related to research literature. The focused environment was the Joint Tactical Radio System (JTRS) Program Executive Office (PEO) located at the Anti-Submarine Warfare (ASW) Naval Base in San Diego, California.

This researcher conducted an effective literature review by exploring several successful existing SOA implementations in industry at the Internet Security System (ISS), the Outrigger resorts, Fiducia (an IT provider), and the Sherman Independent

School District. These successes were transposed against the numerous military networks such as NMCI, One Net, Centrix, IT-21, CANES, etc. NMCI failures as an SOA were outlined in a recent GAO report and numerous other sources. The technical capabilities and security concerns were also thoroughly reviewed for the 802.11 wireless specification and the key seminal literature documents currently available.

The dissertation described the research methods, specific procedures, and resource requirements to be employed during the research. The methodology includes the “case study,” as described by Robert Yin (2003), and the systems development life cycle (SDLC). The study also described the architectural development process and the DOD architectural framework (DODAF), and the requirement process was explored. The Wainhouse Research staffing method was also described in the form of four options: Customer Premise Equipment (CPE), Application Service Provider (ASP), Remote Managed Service Provider (RMSP), and Dedicated Managed Service Provider (DMSP). Additionally, the researcher defined the wireless Supportability, Usability, and Security (SUS) model as a strategic wireless deployment framework. The researcher used these tools in this study to develop a managed services operation in the creation of a wireless LAN using both the SUS model and the Wainhouse staffing methodology. The Wainhouse options, along with a questionnaire, were useful in determining the level of manpower support required for a deployment, as well as the form of that manpower—that is, whether in-house talent, contractor support, or a combination of the two represented the best alternative. The research also provides a plan of action and milestones, Rough order of Magnitude/Statement of Work. The following actions were taken to meet this

goal using the Supportability, Usability, and Security (SUS) wireless deployment framework strategy model.

1. A support agreement was signed between JPEO JTRS leadership and the researcher's office at SSC San Diego. It was agreed that the JTRS organization required greater control of the operation. The organization wanted to own the infrastructure and also wanted an onsite technician to support all customer service technical needs, but realized it lacked the in-house expertise to manage the infrastructure. These requirements (a) eliminated the CPE option because it lacked in-house expertise, and (b) eliminated the ASP option because it wanted to own the infrastructure and wanted on-site support. The JTRS leadership therefore opted for the DMSP choice. The support agreement, which allows for 200 wireless users, will be provided at a recurring cost of \$133,200 per year.
2. This option required the customer to buy the infrastructure as a capital investment at a cost of \$194,272. To cover the four buildings, 60 of the 802.11g Aruba access points were installed.
3. Two unclassified networks were provided to JPEO JTRS from the SSC San Diego via an 802.11a 54-Mbps wireless link. The first network is used for guests and contractors and connects to the Internet through a commercial connection. The second network connects to the Internet through the military NIPRNET infrastructure.

4. Several meetings with the base frequency manager were held to ensure that the 802.11 devices were in fact using unlicensed spectrum and did not require FCC or higher DOD approval to operate.
5. A Statement of Work (SOW) was jointly developed with the JTRS administration, describing the duties and responsibilities of the onsite contractor support. The SOW was used as the skeleton for a task order for supplemental work under an existing agreement with L3, a defense contractor.
6. The highlights of these usability requirements are (a) 100% wireless coverage of all JTRS spaces, and (b) two wireless networks, one for guests/contractors and one for government personnel military/civilian.
7. The SOW and Interservice Support Agreement (ISA) provided clarity for all parties to ensure proper supportability in terms of customer satisfaction, cost, and security requirements.

The JTRS commercial and governmental wireless networks have been in service for over six months. The networks have consistently run without a service interruption. The military requires a road map on how to deploy wireless networks in a secure, supportable, and usable fashion that is in concert with the core mission of the military business requirements, i.e., a Service Oriented Architecture (SOA). Reliable wireless SOA is in high demand. IT architects and creators of systems must understand this technology and at the same time clearly document what the customer wants in terms of operational requirements. This research provides several planning tools to accomplish this endeavor. The SUS model is vital for strategic high-level 802.11 wireless deployment planning, SDLC is key for project execution, and the Wainhouse manpower

options allow for a decision-making framework on whether to outsource manpower support and/or infrastructure.

After six months of operations, a request was submitted by the JTRS Operations Department to reduce the number of NMCI desktops used by contractors and to have contractors provide their own company laptops, with the contractors getting their Internet connectivity through the guest contractor wireless network. JTRS users have voted and prefer the onsite managed service compared to that of NMCI. The fact that it is half the cost of NMCI is also a significant factor. The huge capability advantage of the managed service model over NMCI is the ability to effectively deal with guests. NMCI does not have this capability, whereas the managed wireless network does, regardless if visitors are military from any branch of the service, civil servants from any branch of the service, academia, vendors, or even foreign dignitaries. This is a discernable capability advantage.

The product of these tools is also important to future wireless enterprise designers, because the deliverables in the appendixes show a vetted product. These documents and strategic tools should be the starting point for DOD managed service wireless planners, managers, architects, and researchers. This study explored the “how” by documenting a large installation in a multi-service setting. It also documented the users’ experience with NMCI and their satisfaction level. The importance of communicating a plan to sponsors, contractors, and subordinates cannot be underestimated. Understanding the organizational complexities of who is funding one’s project, understanding the complexities of how contracts are approved, and understanding how people are hired (military, civil servants, and contractors) are just as important as the technical aspects of the network design and customer technical criteria.

It is important to identify the key organizations involved in this research, such as Spawar System Center Pacific (SSC), JPEO JTRS, ASW Naval Base Point Loma, Spawar HQ, PEO EIS, EDS Corporation, L3 Corporation and Tel Tech Plus Corporation; such identification brings forth the complexity in real terms by giving concrete examples of the many management, communication, technical, procurement, and financial challenges in bringing a large project to life.

Appendix A

Inter Service Support Agreement

SUPPORT AGREEMENT			
1. AGREEMENT NUMBER (Provided by Supplier)	2. SUPERSEDED AGREEMENT NO. (If this replaces another agreement)	3. EFFECTIVE DATE (YYYYMMDD)	4. EXPIRATION DATE (May be "Indefinite")
SPAWAR-99342-001		2008/07/21	Indefinite
5. SUPPLYING ACTIVITY		6. RECEIVING ACTIVITY	
a. NAME AND ADDRESS		a. NAME AND ADDRESS	
SPAWARSSYSCEN SAN DIEGO (SSC SAN DIEGO) 53560 Hull Street San Diego, CA 92118-5001 POC: Robin Joubert (619) 553-3870 robin.joubert@navy.mil		JPEO JTRS 3300 Nixie Way Building 50 Room 339 San Diego CA 92147 POC: Mary Wadsworth Tel (619)-524-4592 mary.wadsworth@navy.mil	
b. MAJOR COMMAND		b. MAJOR COMMAND	
SPAWAR		SECDEF	
7. SUPPORT PROVIDED BY SUPPLIER			
a. SUPPORT (Specify what, when, where, and how much)		b. BASIS FOR REIMBURSEMENT	c. ESTIMATED REIMBURSEMENT
Support secure 802.11b/g wireless network with coverage through buildings 50, 7, 17a and 17b. Estimated 200 users at a rate of \$666 per user per year SPAWARSSYSCEN will provide wireless access to their RDT&E Network and their OC12 Internet pipe <ul style="list-style-type: none"> As part of the SSC-SD Network support is provided in the form of: <ul style="list-style-type: none"> Network security staff Network Scans IAVA Compliance and reporting IDS/IPS infrastructure Firewalls (Juniper Net Screen) Web Proxy Incident reporting Forensics Network security Help desk (4-6 personnel) Complete Wireless Accreditation 		Total Est Reimbursement	\$133,200
ADDITIONAL SUPPORT REQUIREMENTS ATTACHED: <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No			
8. SUPPLYING COMPONENT		9. RECEIVING COMPONENT	
a. COMPTROLLER SIGNATURE	b. DATE SIGNED	a. COMPTROLLER SIGNATURE	b. DATE SIGNED
Dave Rly			
c. APPROVING AUTHORITY		c. APPROVING AUTHORITY	
(1) TYPED NAME F. D. UNETIC, CAPT, USN		(1) TYPED NAME Dennis Bauman	
(2) ORGANIZATION	(3) TELEPHONE NUMBER	(2) ORGANIZATION	(3) TELEPHONE NUMBER
SSC San Diego	(619) 553-3000	JPEO JTRS	(619) 524-4600
(4) SIGNATURE	(5) DATE SIGNED	(4) SIGNATURE	(5) DATE SIGNED

10. TERMINATION (Complete only when agreement is terminated prior to scheduled expiration date.)			
a. APPROVING AUTHORITY SIGNATURE	b. DATE SIGNED	c. APPROVING AUTHORITY SIGNATURE	d. DATE SIGNED
DD FORM 1144, NOV 2001 PREVIOUS EDITION MAY BE USED.			
11. GENERAL PROVISIONS (Complete blank spaces and add additional general provisions as appropriate: e.g., exceptions to printed provisions, additional parties to this agreement, billing and reimbursement instructions.)			
a. The receiving components will provide the supplying component projections of requested support. (Significant changes in the receiving component's support requirements should be submitted to the supplying component in a manner that will permit timely modification of resource requirements.)			
b. It is the responsibility of the supplying component to bring any required or requested change in support to the attention of <u>SPAWARSSCOM</u> prior to changing or canceling support.			
c. The component providing reimbursable support in this agreement will submit statements of costs to: <u>SPAWARSSCOM</u>			
d. All rates expressing the unit cost of services provided in this agreement are based on current rates, which may be subject to change for uncontrollable reasons, such as legislation, DoD directives, and commercial utility rate increases. The receiver will be notified immediately of such rate changes that must be passed through to the support receivers.			
e. This agreement may be cancelled at any time by mutual consent of the parties concerned. Either party upon giving at least 180 days written notice to the other party may also cancel this agreement.			
f. In case of mobilization or other emergency, this agreement will remain in force only within supplier's capabilities.			
ADDITIONAL GENERAL PROVISIONS ATTACHED: <input type="checkbox"/> YES <input checked="" type="checkbox"/> NO			

12. SPECIFIC PROVISIONS (As appropriate: e.g., location and size of occupied facilities, unique supplier and receiver responsibilities, conditions, requirements, quality standards, and criteria for measurement/reimbursement of unique requirements.)

ADDITIONAL SPECIFIC PROVISIONS ATTACHED: ☒ YES ☐ NO

DD FORM 1144, NOV 2001

Executive Summary
2008

July

Agreement Number **SPAWAR-xxxxxxx**

Supplier SSC San Diego

Receiver JTRS

MAJCOM SPAWAR

MAJCOM SECDEF

Support Category **Title**

**Estimated
Reimbursement**

INFRASTRUCUTRE
SUPPORT Network Services

133,200

GRAND TOTAL

\$133,200

INFRASTRUCTURE SUPPORT

Includes local area network services (unclassified).

Supplier will:

1. provide gigabit unclassified Local Area Network (LAN) (Ethernet and Internet) connectivity for all devices
2. maintain, manage, and monitor the LAN infrastructure (switches, fiber interconnects)
3. restore the network from outages during normal working hours, unless by other arrangement between the parties
4. provide connectivity to the Internet and NIPRnet via DREN and the SSCSD BAN
5. provide a security stack to protect the NADAP enclave from external (off base) connections, including firewall, web proxy, intrusion detection, and intrusion prevention components.
6. provide access to network infrastructure and network security help desk during normal working hours
7. perform regular network and device scans to detect vulnerabilities
8. provide an automated patch management capability (WSUS) for windows systems connected to the network
9. provide remote access (VPN and/or dialup) for users that subscribe to core services
10. maintain a database (LDAP) of all users and devices on the network, and provide Web access to that database
11. maintain a database of all users on the network

Receiver will:

1. adhere to all DOD, Navy, SPAWAR, and SSCSD Network Security policies and procedures
2. pay standard published rates for all devices connected to the network
3. register all devices connected to the network, and designate the systems administrator for each device.
4. register all users of the network

ADMIN SUPPORT SERVICES

Includes project and financial management services and administrative support and reporting.

SUPPLIER will:


1. provide financial accounting services to assist in managing fiscal resources provided to SUPPLIER on a cost reimbursable basis for RECEIVER support

RECEIVER will:

1. communicate any known issues to the SUPPLIER.
2. reimburse SUPPLIER for the services received.

Appendix B

Purchase Order

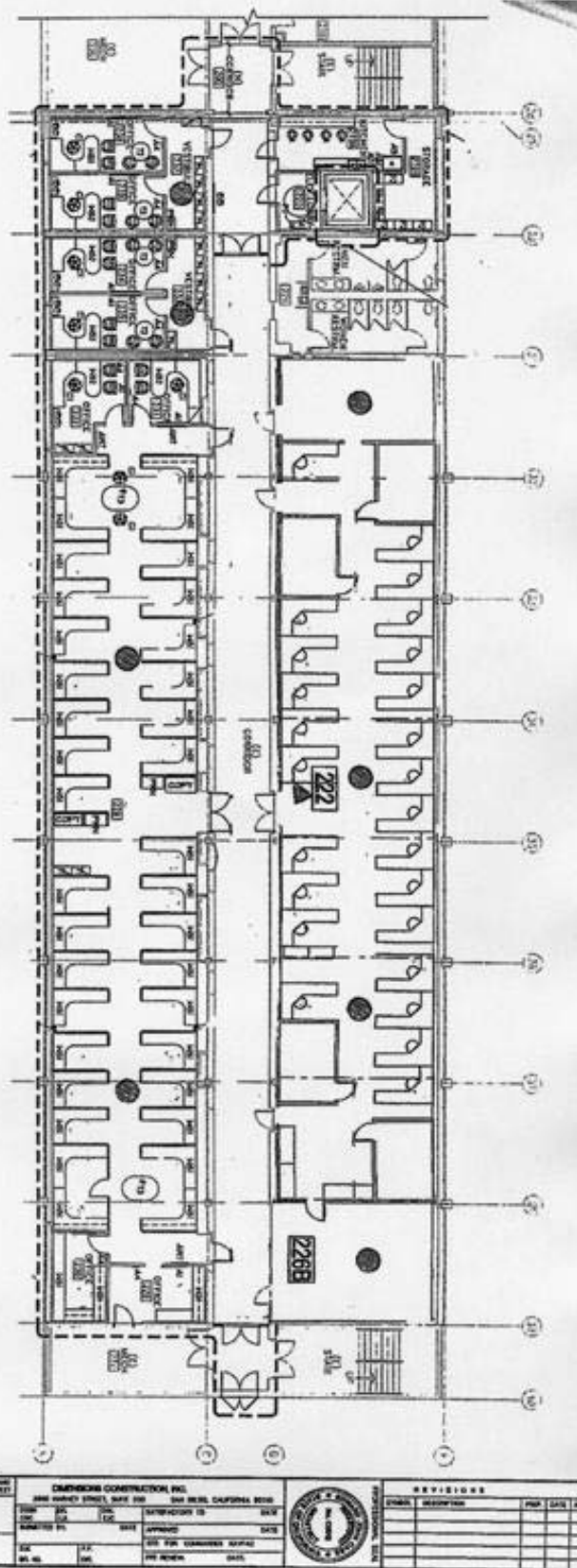
ORDER FOR SUPPLIES OR SERVICES (Contractor must submit four copies of invoice.)				Form Approved OMB No. 0704-0187		PAGE 1 OF 3	
<small>Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing 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 Department of Defense, 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 (0704-0187), Washington, DC 20503.</small>							
PLEASE DO NOT RETURN YOUR FORM TO EITHER OF THESE ADDRESSES. SEND YOUR COMPLETED FORM TO THE PROCUREMENT OFFICIAL IDENTIFIED IN ITEM 6.							
1. CONTRACT / PURCH ORDER NO. N6600108MN111		2. DELIVERY ORDER NO.		3. DATE OF ORDER (YYMMDD) 20080717		4. REQUISITION / PURCH REQUEST NO. 7000022921 8163-55208	
5. ISSUED BY * SPAWAR, SYSTEMS CENTER, SAN DIEGO N66001 * 63560 HULL STREET * SAN DIEGO, CA 92152-5001		6. CODE		7. ADMINISTERED BY (if other than 6) CODE		8. DELIVERY FOB FOB Destination	
9. CONTRACTOR NAME AND ADDRESS TEL TECH PLUS, INC. TTP-US 393 ENTERPRISE ST SAN MARCOS 1225052950000 3CP25 7605108552		10. DELIVER TO FOB POINT BY (Date) (YYMMDD) 20080801		11. BUSINESS IS SMALL		12. DISCOUNT TERMS NET 30	
		13. MAIL INVOICES TO * SSC SAN DIEGO * P.O. BOX 80818 * SAN DIEGO, CA 92138-0818					
14. SHIP TO POINT LOMA N66001 SPAWAR SYSTEMS CENTER 53560 HULL STREET, BLDG A-33 SAN DIEGO MARK SHIPMENT: 4700015714		15. PAYMENT WILL BE MADE BY * PAYMENT WILL BE MADE BY DFAS CLEVELAND * MAIL ALL INVOICES TO BLOCK 13.		16. CODE		17. MARK ALL PACKAGES AND PAPERS WITH CONTRACT OR ORDER NUMBER	
18. TYPE OF ORDER PURCHASE		This delivery order is issued on another Government agency or in accordance with and subject to terms and conditions of above numbered contract. Reference your X ACCEPTANCE. THE CONTRACTOR HEREBY ACCEPTS THE OFFER REPRESENTED BY THE NUMBERED PURCHASE ORDER AS IT MAY PREVIOUSLY HAVE BEEN OR IS NOW MODIFIED, SUBJECT TO ALL OF THE TERMS AND CONDITIONS SET FORTH, AND AGREES TO PERFORM THE SAME.					
NAME OF CONTRACTOR		SIGNATURE		TYPED NAME AND TITLE		DATE SIGNED (YYMMDD)	
<input type="checkbox"/> If this box is marked, supplier must sign Acceptance and return the following number of copies: 1							
17. ACCOUNTING AND APPROPRIATION DATA / LOCAL USE AA 97X4930 NH3P 000 77777 0 086001 2F 000000 7000022921AA							
19. ITEM NO.	20. SCHEDULE OF SUPPLIES / SERVICE	21. QUANTITY ORDERED / ACCEPTED *	22. UNIT	23. UNIT PRICE	24. AMOUNT		
	See attached page(s) for item details						
* If quantity accepted by the Government is same as quantity ordered, indicate by X. If different, enter actual quantity accepted below quantity ordered and encircle.		25. UNITED STATES OF AMERICA Robert Desmarests BY: 			26. TOTAL	\$194,272.00	
27. QUANTITY IN COLUMN 20 HAS BEEN <input type="checkbox"/> INSPECTED <input type="checkbox"/> RECEIVED <input type="checkbox"/> ACCEPTED, AND CONFORMS TO THE CONTRACT EXCEPT AS NOTED		28. CONTRACTING / ORDERING OFFICER J. SHIP NO. PARTIAL FINAL			29. D.O. VOUCHER NO.	30. INITIALS	
DATE _____ SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE _____		31. PAYMENT COMPLETE PARTIAL FINAL			32. PAID BY	33. AMOUNT VERIFIED CORRECT FOR	
34. I certify this account is correct and proper for payment.		35. DATE RECEIVED (YYMMDD)			36. CHECK NUMBER	37. BILL OF LADING NO.	
DATE _____ SIGNATURE AND TITLE OF CERTIFYING OFFICER _____		38. TOTAL CONTAINERS			39. B/R ACCOUNT NUMBER	40. B/R VOUCHER NO.	
37. RECEIVED AT	38. RECEIVED BY (print)	39. DATE RECEIVED (YYMMDD)		40. TOTAL CONTAINERS	41. B/R ACCOUNT NUMBER	42. B/R VOUCHER NO.	

ORDER FOR SUPPLIES OR SERVICES (Contractor must submit four copies of invoice.)				Form Approved OMB No. 0704-0187		PAGE 2 OF 3	
18. ITEM NO.	19. SCHEDULE OF SUPPLIES / SERVICE	20. QUANTITY ORDERED / ACCEPTED *	21. UNIT	22. UNIT PRICE	23. AMOUNT		
0001	CABLE INSTALLATION, TERMINATION, PATCH	1	LOT	\$82,989.00	\$82,989.00		
0002	OAC-ADD-F50CLT. ODESSY ACCESS CLIENT	1	EA	\$2,459.00	\$2,459.00		
0003	SVC-LTD-OAC-F-50. 12 MOS UPDATE SUPPORT	1	LOT	\$550.00	\$550.00		
0004	ARUBA 6000 CHASSIS BUNDLE&BRIDGE	1	LOT	\$67,584.00	\$67,584.00		
0005	NEXT SUPPORT/UPDATES	1	LOT	\$10,590.00	\$10,590.00		
0006	INSTALLATION/CONFIGURATION	1	LOT	\$22,400.00	\$22,400.00		
0007	XEROX 6360N PRINTERS	5	EA	\$1,400.00	\$7,000.00		
0008	FREIGHT	1	LOT	\$700.00	\$700.00		
	<p>* NOTE: THE TRANSPORTATION COST IS TO BE SHOWN ON THE SAME INVOICE AS SUPPLIES/SERVICES ARE BILLED BUT AS A SEPARATE LINE ITEM FOR EACH INDIVIDUAL SHIPMENT. TRANSPORTATION CHARGES EXCEEDING \$100.00 SHALL BE SUPPORTED BY EVIDENCE OF COST.</p> <p>* This is to support Joint Tactical Radio System Program Executive Office (JTRP) effort to field a multi-building wireless local area network at Naval Base Point Loma Anti-Submarine Warfare (ASW).</p> <p>* This purchase order includes the hardware and installation necessary to install 60 wireless access points covering three buildings as well as a point to point link back from Naval Base Point Loma ASW to SPAWAR System Center (SSC) building one. This capability increases the SSC research, development and testing network to 500 additional users significantly improving communication and research efforts across the numerous JTRP product lines. Two of the buildings that are being proposed for wireless capability will be housed with personnel that are depending upon this network as their primary means of communication, research and testing. Personnel will occupy these building by August 2008.</p> <p>* Hardware must be Aruba per Ron Broersma, Chief SSC Network Engineering, be in compliance with all Navy and SSC security requirements as well as being compatible with the existing SSC network infrastructure.</p> <p>* Purchase includes:</p> <p>* Cable installation, termination, patch cords</p> <p>* TTP cabling</p> <p>* Oac-add-F50clt, Odyssey access client/Fips G50 pack</p> <p>* Fips client/50</p> <p>* Aruba 6000 chassis bundle and bridge and AP's</p> <p>* Aruba Hardware</p> <p>* Next day support/updates</p> <p>* Installation/configuration</p> <p>* Printers, Xerox 6360N</p> <p>* Freight</p> <p>* Source:</p>						

18. ORDER FOR SUPPLIES OR SERVICES (Contractor must submit four copies of invoice.)		Form Approved OMB No. 0704-0187		PAGE 3 OF 3	
19. ITEM NO.	20. SCHEDULE OF SUPPLIES / SERVICE	21. QUANTITY ORDERED / ACCEPTED	22. UNIT	23. UNIT PRICE	24. AMOUNT
	<p>* Tel Tech Plus, Inc * 390 Enterprise Street * San Marcos, CA 92078 * Tel# 760-510-1323 * Cell# 760-1533-2110 * POC: Greg Steane * email: gsteane@tp-us.com *</p> <p>* Admin POC: Maria De Guzman, x33708 * email: maria.deguzman@navy.mil * Tech POC: LCDR Joseph Roth, x30413 * email: joseph.roth1@navy.mil *</p> <p>* PLEASE MARK ALL PACKAGES, PACKING SLIPS AND INVOICES WITH PO#N66001-08-M-N110 AND 47-15714. PLEASE PROVIDE A COPY OF PO WITH SHIPMENT. *</p> <p>* PAYMENT INSTRUCTION: INVOICE ITEMS EXACTLY AS PURCHASE ORDER IS PROVIDED. INVOICE MUST MATCH THE PURCHASE ORDER. ON THE LAST INVOICE, INDICATE, "FINAL INVOICE". * *</p>				

Appendix C

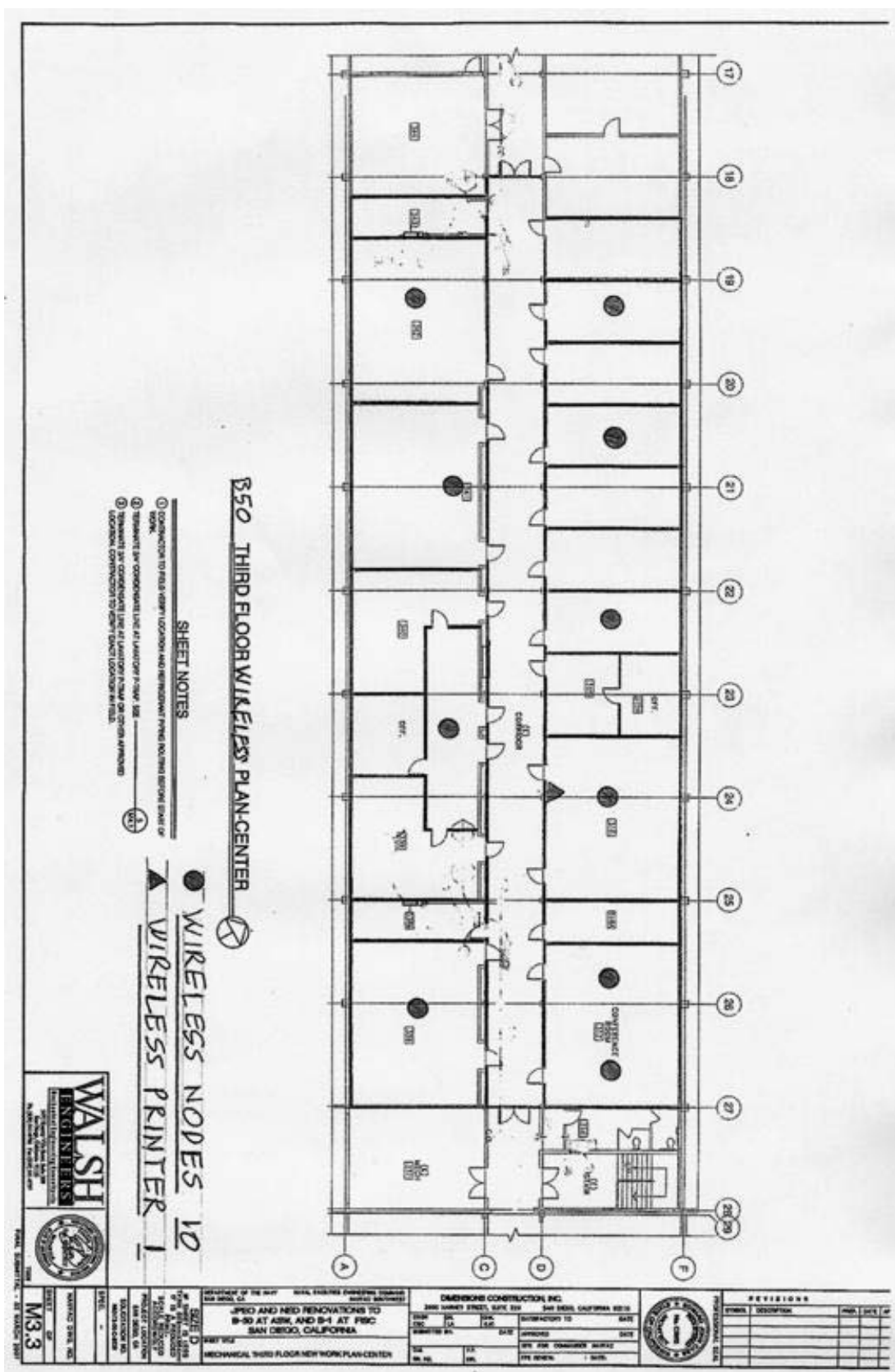
Wireless Floor Plan/Access Point Placement

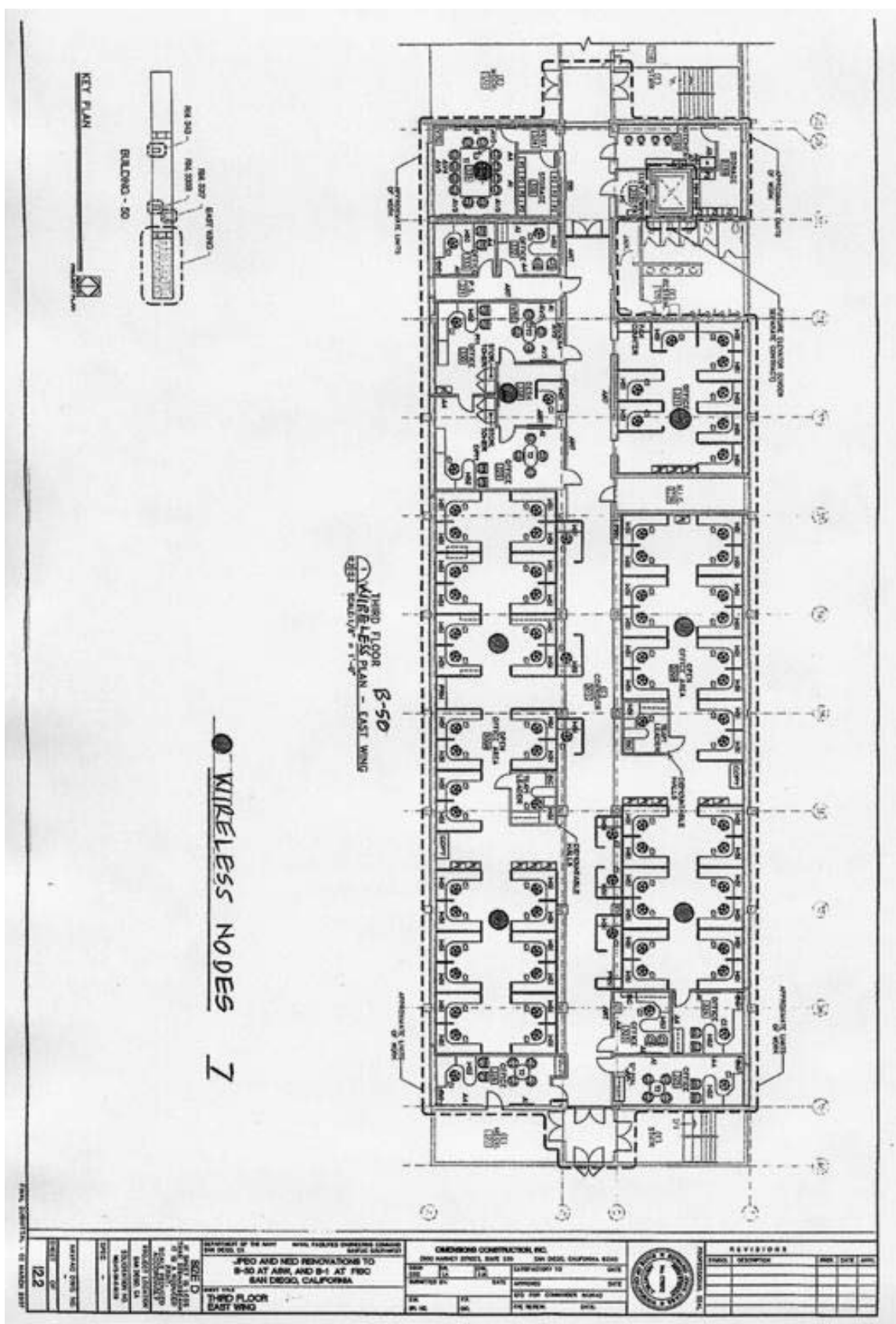


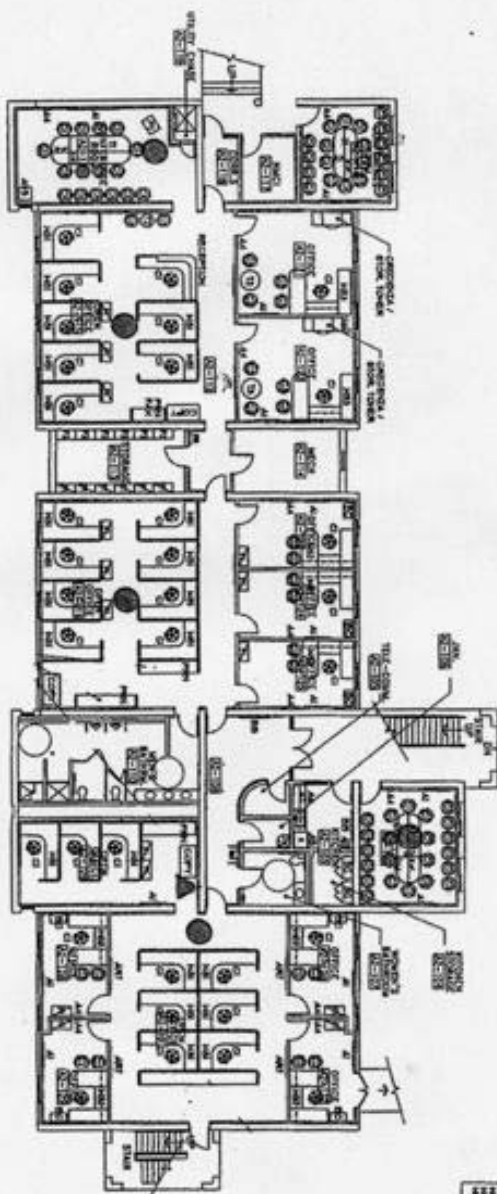
SECOND FLOOR
WIRELESS PLAN - EAST WING
SCALE: 1/8" = 1'-0"

● WIRELESS NODES B
▲ WIRELESS PRINTER I

121






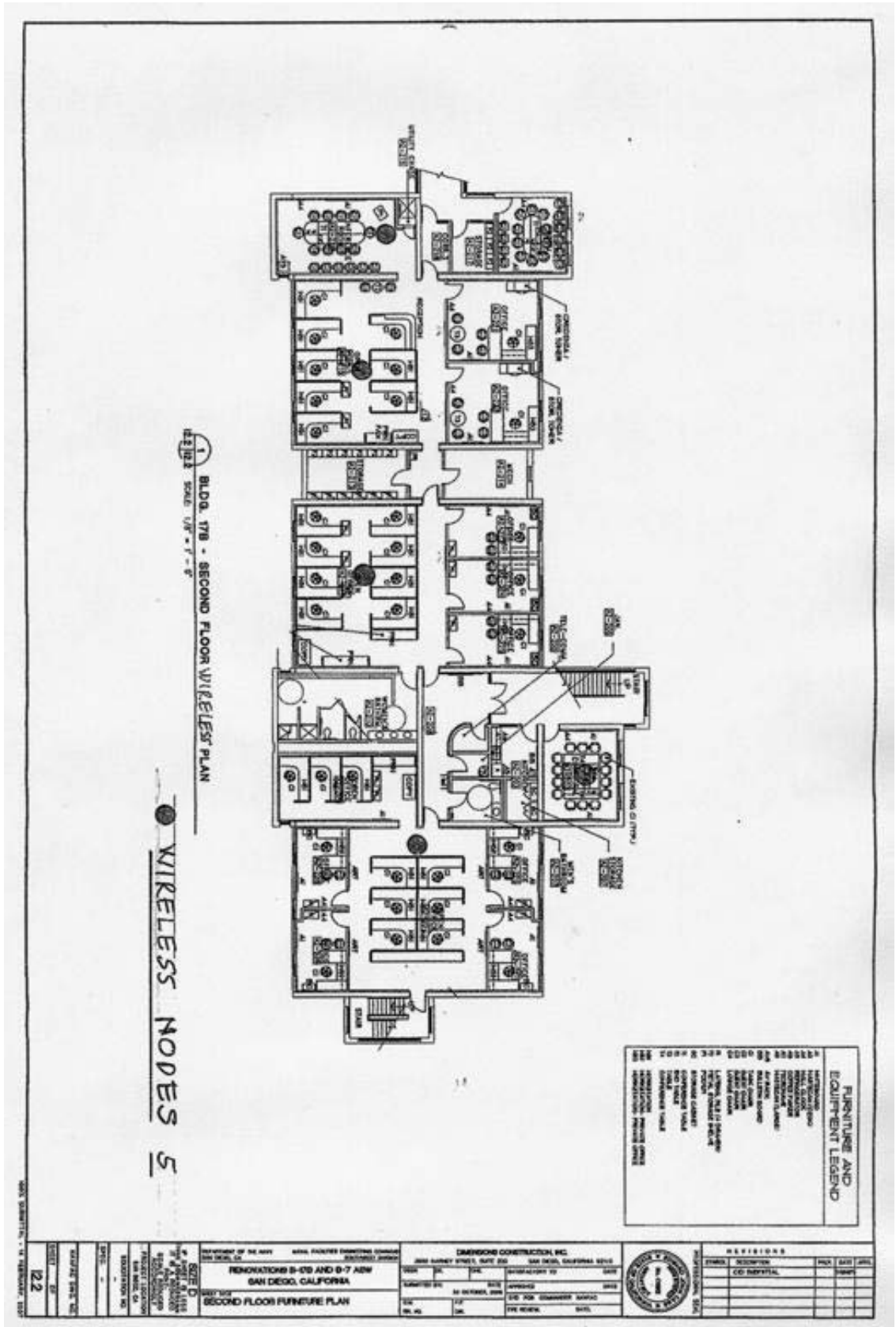


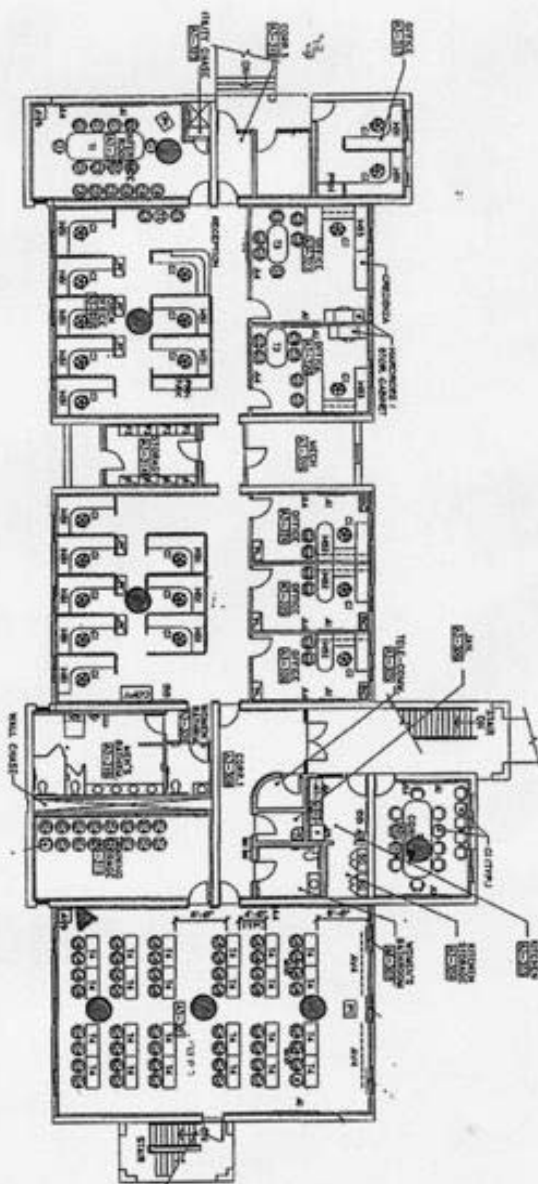
BLDG. 17B - FIRST FLOOR WIRELESS PLAN

- WIRELESS NODES 5
- ▲ WIRELESS PRINTER 1

FURNITURE AND EQUIPMENT LEASED	
1	10. AIRCRAFT
2	11. MARITIME VESSELS
3	12. RAILROADS
4	13. TRUCKS
5	14. BUSES
6	15. TRAILERS
7	16. CRANES
8	17. CONSTRUCTION EQUIPMENT
9	18. OTHER EQUIPMENT
10	19. OTHER
11	20. TOTAL
12	21. TOTAL
13	22. TOTAL
14	23. TOTAL
15	24. TOTAL
16	25. TOTAL
17	26. TOTAL
18	27. TOTAL
19	28. TOTAL
20	29. TOTAL
21	30. TOTAL
22	31. TOTAL
23	32. TOTAL
24	33. TOTAL
25	34. TOTAL
26	35. TOTAL
27	36. TOTAL
28	37. TOTAL
29	38. TOTAL
30	39. TOTAL
31	40. TOTAL
32	41. TOTAL
33	42. TOTAL
34	43. TOTAL
35	44. TOTAL
36	45. TOTAL
37	46. TOTAL
38	47. TOTAL
39	48. TOTAL
40	49. TOTAL
41	50. TOTAL
42	51. TOTAL
43	52. TOTAL
44	53. TOTAL
45	54. TOTAL
46	55. TOTAL
47	56. TOTAL
48	57. TOTAL
49	58. TOTAL
50	59. TOTAL
51	60. TOTAL
52	61. TOTAL
53	62. TOTAL
54	63. TOTAL
55	64. TOTAL
56	65. TOTAL
57	66. TOTAL
58	67. TOTAL
59	68. TOTAL
60	69. TOTAL
61	70. TOTAL
62	71. TOTAL
63	72. TOTAL
64	73. TOTAL
65	74. TOTAL
66	75. TOTAL
67	76. TOTAL
68	77. TOTAL
69	78. TOTAL
70	79. TOTAL
71	80. TOTAL
72	81. TOTAL
73	82. TOTAL
74	83. TOTAL
75	84. TOTAL
76	85. TOTAL
77	86. TOTAL
78	87. TOTAL
79	88. TOTAL
80	89. TOTAL
81	90. TOTAL
82	91. TOTAL
83	92. TOTAL
84	93. TOTAL
85	94. TOTAL
86	95. TOTAL
87	96. TOTAL
88	97. TOTAL
89	98. TOTAL
90	99. TOTAL
91	100. TOTAL

COUNTY OF SAN DIEGO DEPARTMENT OF THE WATER SAN DIEGO, CA	3000 HARVEY STREET, SUITE 200 SAN DIEGO, CALIFORNIA 92108	DATE: 08/15/2011			REVISIONS			
		DRAWN BY: DAVID A. SMITH CHECKED BY: DAVID A. SMITH DATE: 08/15/2011	PROJECT: RENOVATIONS B-076 AND B-077 LOCATION: SAN DIEGO, CALIFORNIA		SHEET: 01 OF: 01	REVISION: CD REVISION	DATE: 08/15/2011	BY: DAVID A. SMITH



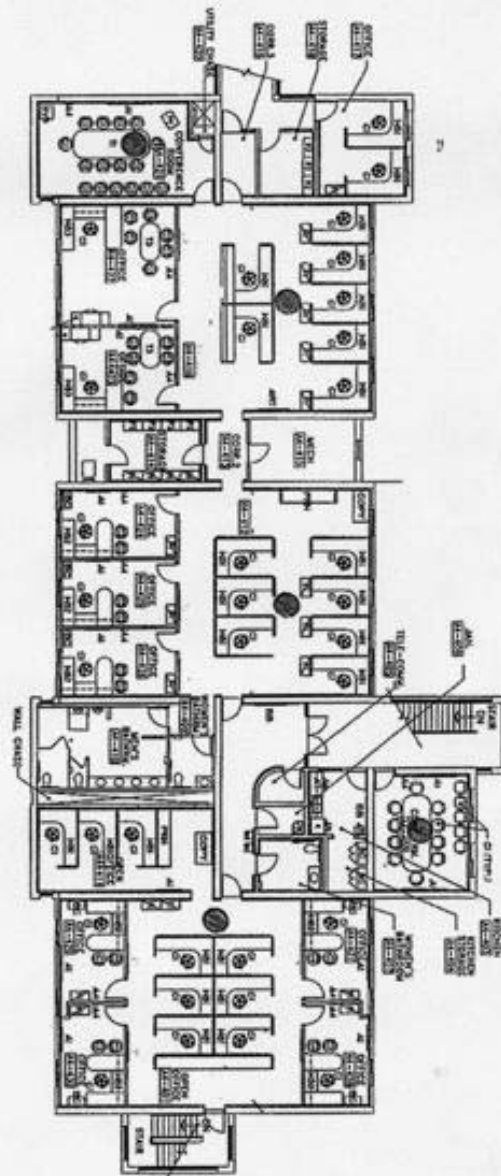


BLDG. 17B - THIRD FLOOR WIRELESS PLAN

- WIRELESS NODES 7
- ▲ WIRELESS PRINTER 1

FURNITURE AND EQUIPMENT LEGEND	
A	APPROXIMATE
1	1.00 CUBIC YARD
2	2.00 CUBIC YARD
3	3.00 CUBIC YARD
4	4.00 CUBIC YARD
5	5.00 CUBIC YARD
6	6.00 CUBIC YARD
7	7.00 CUBIC YARD
8	8.00 CUBIC YARD
9	9.00 CUBIC YARD
10	10.00 CUBIC YARD
11	11.00 CUBIC YARD
12	12.00 CUBIC YARD
13	13.00 CUBIC YARD
14	14.00 CUBIC YARD
15	15.00 CUBIC YARD
16	16.00 CUBIC YARD
17	17.00 CUBIC YARD
18	18.00 CUBIC YARD
19	19.00 CUBIC YARD
20	20.00 CUBIC YARD
21	21.00 CUBIC YARD
22	22.00 CUBIC YARD
23	23.00 CUBIC YARD
24	24.00 CUBIC YARD
25	25.00 CUBIC YARD
26	26.00 CUBIC YARD
27	27.00 CUBIC YARD
28	28.00 CUBIC YARD
29	29.00 CUBIC YARD
30	30.00 CUBIC YARD
31	31.00 CUBIC YARD
32	32.00 CUBIC YARD
33	33.00 CUBIC YARD
34	34.00 CUBIC YARD
35	35.00 CUBIC YARD
36	36.00 CUBIC YARD
37	37.00 CUBIC YARD
38	38.00 CUBIC YARD
39	39.00 CUBIC YARD
40	40.00 CUBIC YARD
41	41.00 CUBIC YARD
42	42.00 CUBIC YARD
43	43.00 CUBIC YARD
44	44.00 CUBIC YARD
45	45.00 CUBIC YARD
46	46.00 CUBIC YARD
47	47.00 CUBIC YARD
48	48.00 CUBIC YARD
49	49.00 CUBIC YARD
50	50.00 CUBIC YARD
51	51.00 CUBIC YARD
52	52.00 CUBIC YARD
53	53.00 CUBIC YARD
54	54.00 CUBIC YARD
55	55.00 CUBIC YARD
56	56.00 CUBIC YARD
57	57.00 CUBIC YARD
58	58.00 CUBIC YARD
59	59.00 CUBIC YARD
60	60.00 CUBIC YARD
61	61.00 CUBIC YARD
62	62.00 CUBIC YARD
63	63.00 CUBIC YARD
64	64.00 CUBIC YARD
65	65.00 CUBIC YARD
66	66.00 CUBIC YARD
67	67.00 CUBIC YARD
68	68.00 CUBIC YARD
69	69.00 CUBIC YARD
70	70.00 CUBIC YARD
71	71.00 CUBIC YARD
72	72.00 CUBIC YARD
73	73.00 CUBIC YARD
74	74.00 CUBIC YARD
75	75.00 CUBIC YARD
76	76.00 CUBIC YARD
77	77.00 CUBIC YARD
78	78.00 CUBIC YARD
79	79.00 CUBIC YARD
80	80.00 CUBIC YARD
81	81.00 CUBIC YARD
82	82.00 CUBIC YARD
83	83.00 CUBIC YARD
84	84.00 CUBIC YARD
85	85.00 CUBIC YARD
86	86.00 CUBIC YARD
87	87.00 CUBIC YARD
88	88.00 CUBIC YARD
89	89.00 CUBIC YARD
90	90.00 CUBIC YARD
91	91.00 CUBIC YARD
92	92.00 CUBIC YARD
93	93.00 CUBIC YARD
94	94.00 CUBIC YARD
95	95.00 CUBIC YARD
96	96.00 CUBIC YARD
97	97.00 CUBIC YARD
98	98.00 CUBIC YARD
99	99.00 CUBIC YARD
100	100.00 CUBIC YARD

SHEET NO. 121 OF 121 DATE 12/1		PROJECT NO. 121 OF 121 DATE 12/1		DRAWING NO. 121 OF 121 DATE 12/1		REVISIONS NO. DESCRIPTION 1. PRELIMINARY	
CONTRACT NO. 121 OF 121 DATE 12/1		PROJECT NO. 121 OF 121 DATE 12/1		DRAWING NO. 121 OF 121 DATE 12/1		REVISIONS NO. DESCRIPTION 1. PRELIMINARY	
CONTRACT NO. 121 OF 121 DATE 12/1		PROJECT NO. 121 OF 121 DATE 12/1		DRAWING NO. 121 OF 121 DATE 12/1		REVISIONS NO. DESCRIPTION 1. PRELIMINARY	

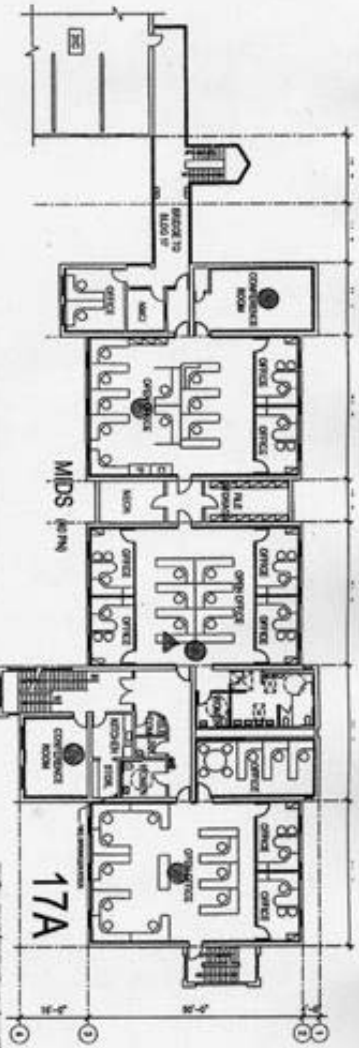


1 BLDG. 77B - FOURTH FLOOR WIRELESS PLAN
SCALE: 1/8" = 1' - 0"

WIRELESS NODES 5

FURNITURE AND EQUIPMENT LEGEND	
1	RECEPTION
2	RECEPTION
3	RECEPTION
4	RECEPTION
5	RECEPTION
6	RECEPTION
7	RECEPTION
8	RECEPTION
9	RECEPTION
10	RECEPTION
11	RECEPTION
12	RECEPTION
13	RECEPTION
14	RECEPTION
15	RECEPTION
16	RECEPTION
17	RECEPTION
18	RECEPTION
19	RECEPTION
20	RECEPTION
21	RECEPTION
22	RECEPTION
23	RECEPTION
24	RECEPTION
25	RECEPTION
26	RECEPTION
27	RECEPTION
28	RECEPTION
29	RECEPTION
30	RECEPTION
31	RECEPTION
32	RECEPTION
33	RECEPTION
34	RECEPTION
35	RECEPTION
36	RECEPTION
37	RECEPTION
38	RECEPTION
39	RECEPTION
40	RECEPTION
41	RECEPTION
42	RECEPTION
43	RECEPTION
44	RECEPTION
45	RECEPTION
46	RECEPTION
47	RECEPTION
48	RECEPTION
49	RECEPTION
50	RECEPTION
51	RECEPTION
52	RECEPTION
53	RECEPTION
54	RECEPTION
55	RECEPTION
56	RECEPTION
57	RECEPTION
58	RECEPTION
59	RECEPTION
60	RECEPTION
61	RECEPTION
62	RECEPTION
63	RECEPTION
64	RECEPTION
65	RECEPTION
66	RECEPTION
67	RECEPTION
68	RECEPTION
69	RECEPTION
70	RECEPTION
71	RECEPTION
72	RECEPTION
73	RECEPTION
74	RECEPTION
75	RECEPTION
76	RECEPTION
77	RECEPTION
78	RECEPTION
79	RECEPTION
80	RECEPTION
81	RECEPTION
82	RECEPTION
83	RECEPTION
84	RECEPTION
85	RECEPTION
86	RECEPTION
87	RECEPTION
88	RECEPTION
89	RECEPTION
90	RECEPTION
91	RECEPTION
92	RECEPTION
93	RECEPTION
94	RECEPTION
95	RECEPTION
96	RECEPTION
97	RECEPTION
98	RECEPTION
99	RECEPTION
100	RECEPTION

REVISIONS NO. DESCRIPTION 1 PRELIMINARY		DATE 1 10/1/00	
APPROVED [Signature]		DATE 1 10/1/00	
DESIGNED [Signature]		DATE 1 10/1/00	
CHECKED [Signature]		DATE 1 10/1/00	
PROJECT 122		DATE 1 10/1/00	



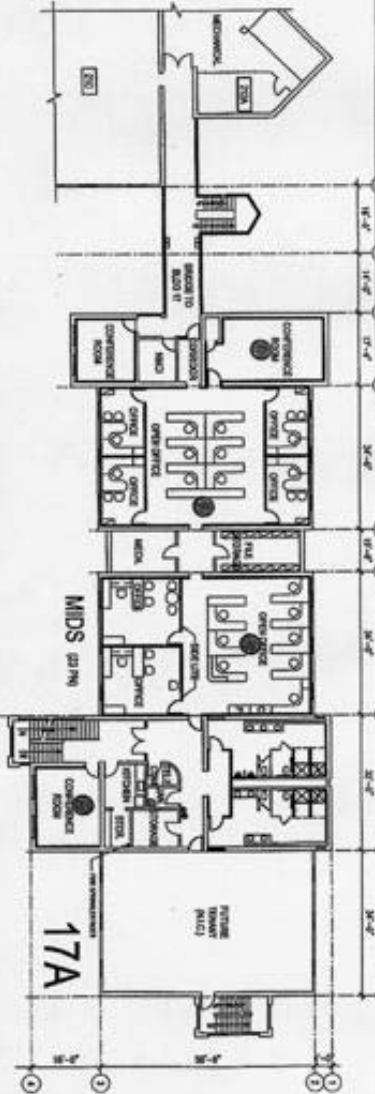
MIDS - PROPOSED 3RD FLOOR PLAN

WIRELESS NODES 5
WIRELESS PRINTER 1

JPEO JTRS - BUILDING 17A



5/7/2008 REVISED



MIDS - PROPOSED 2ND FLOOR PLAN

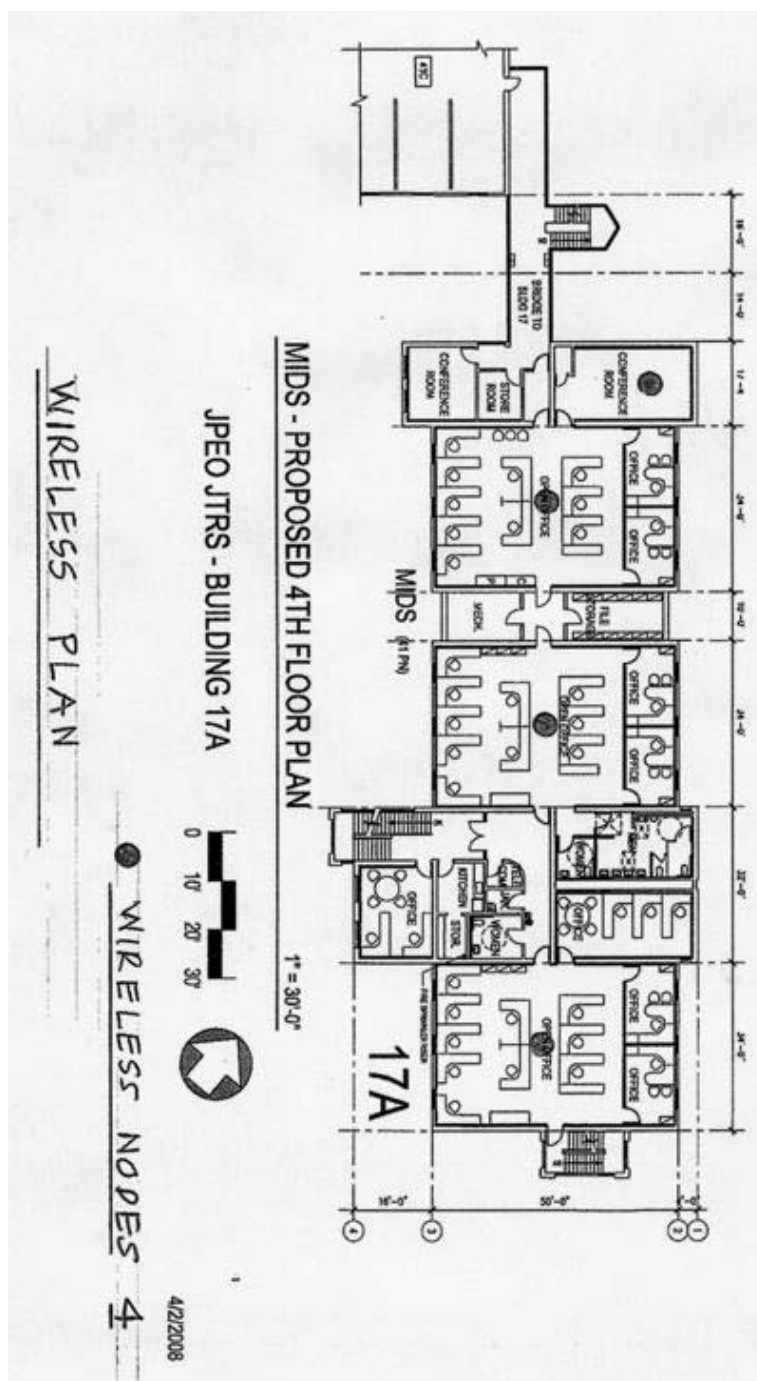
WIRELESS NODES 4

JPEO JTRS - BUILDING 17A



4/2/2008

WIRELESS PLAN



Appendix D

User Agreement

WLAN User Agreement

Name: _____

Program/Directorate: _____ ☐ Military ☐ Civilian ☐ Contractor ☐ Other

Email _____ Phone Number _____

☐ SPAWAR Intranet (CAC enabled) ☐ Un-Restricted Internet (Password required)

Justification: _____

_____ Dates needed: _____ to _____

PLEASE READ THIS DOCUMENT CAREFULLY BEFORE ACCESSING OR USING THE JTRS WIRELESS LOCAL AREA NETWORK (WLAN).

By accessing or using the JTRS WLAN, you agree to be bound by the terms and conditions herein.

- 1) The WLAN is to be used primarily for purposes of fulfilling JPEO JTRS' mission. It is intended to be used as a tool to enhance your job performance. Non-work related use of the WLAN is not authorized.
- 2) The WLAN is comprised of two separate, distinct networks:
 - a) The CAC-enabled SPAWAR Intranet. This network supports PKI verification to access DoD sites and has restricted access to the Internet. This network requires an LDAP account and CAC logon.
 - b) Un-restricted Internet access. Does not support PKI verification and is not suitable for accessing DoD sites. This network requires a user name and password. Usernames and passwords will be specific to an individual, and will expire.
- 3) The WLAN is a shared resource. Therefore, network use or applications which inhibit or interfere with the use of the network by others are not permitted.
- 4) Users of the WLAN must comply with Federal, state, and local laws and ordinances including U.S. copyright law.
- 5) Users of the WLAN must comply with DoD, Navy, and SPAWAR Information Assurance procedures and policies.
- 6) The WLAN shall not be used for sending or receiving classified material.
- 7) WLAN network services and wiring may not be modified, tampered with, or extended. This applies to all network wiring, network jacks, and hardware. If you cause damage by modifying or tampering with network wiring, jacks, or hardware, you may be held financially responsible for such damage and may be subject to disciplinary procedures.
- 8) Malicious use of the network is strictly forbidden. This includes, but is not limited to: sending harassing or threatening messages; attempting to forge messages, crack passwords, intercept data or circumvent server security; sending bulk unsolicited email; or sending data intended to disrupt services.

User Signature: _____ Date: _____

By signing I agree to the conditions contained in this WLAN User Agreement

Requested by: _____ Date: _____

PMO OPS Director or JPEO Deputy Director

Approved: _____ Date: _____

JPEO Operations

WLAN Admin Use Only

Issued by: _____ Date: _____

Expiration date: _____ Extension date: _____

Username: _____ Password: _____

Appendix E

Support Contractor Statement of Work (SOW)

Statement of Work

Government Contract Number: N66001-04-D-5005

Order Number: 0080

Task Title: Systems Engineering and Network Administrative Support for the Joint Tactical Radio System (JTRS) Research, Development, Test and Evaluation (R, D, T, & E) wireless network

1.0 Scope. The purpose of the delivery order is to provide system engineering and integration and network administrative support by designing, implementing, and operating the JTRS wireless network.

1.1 Background. The Joint Program Executive office (JPEO) for the Joint Tactical Radio System (JTRS) has tasked Space and Naval Warfare (SPAWAR) System Center-San Diego (SSC-SD) Code 5525 to provide system engineering/ analysis support and Network Administration for the JTRS enterprise in the form of designing C4I requirements and engineering services to include wireless network services. In August 2008, JPEO JTRS is fielding 60 IEEE-802.11 wireless access points at JPEO JTRS headquarters across three buildings at Naval Station Point Loma. JTRS is a next-generation radio frequency (RF) communications system for use in the Navy communications and the Joint Service communications environment.

2.0 Technical Requirements

2.1 Contract Status Report. The Contractor shall prepare and deliver monthly Contract Status Reports (CSR) that accurately and completely document accomplishments, deliverables, performance indicators, past-due deliverables and any planned corrective actions, relevant issues and concerns as well as cumulative travel costs.

2.2 System Engineering and Integration. The contractor must be an expert in managing and designing 802.11 networks and have a thorough understanding of DOD network wired and wireless security policies. Services shall include setting up accounts, troubleshooting the infrastructure (Application, Radio Frequency, and Network), and training users how to connect to the network, configure their systems and follow DOD, DON and SPAWAR security policy. The contractor shall also develop training and implementation plans, and analyze capabilities (vague). The contractor shall coordinate between JPEO JTRS and SSC on all technical, policy and budgetary issues that in any way impact the successful operation of the JTRS wireless network. The contractor shall write a one page bi-weekly report on the health of the network describing all wireless network issues in terms supportability, usability and security (A003). The contractor shall participate in both JTRS and SPAWAR meetings, conferences, working groups and program reviews by answering technical and progress related questions and providing presentation materials, briefs, and documentation.

4.0 Government Furnished Information. The government will provide the contractor access to information and documentation relative to the requirements and evaluation within 10 days of contractor's request.

5.0 Travel. None

6.0 Other

6.1 Technical Point of Contact. LCDR Joe Roth 619-553-0413 SSC San Diego Code 5525

6.2 Inspection and Acceptance. Mr. Chris Horne 619-553-6821 SSC San Diego Code 5523

6.3 Place of Performance. Work will be performed at SPAWARSYSCEN San Diego and at government selected sites in San Diego, CA. The remainder of the work will be performed at the contractor's facility in San Diego.

Appendix F

Customer Service Survey

SSC-PACIFIC Customer/Sponsor Interview

Fax Completed Form to (619) 524-5204 Date: May 12, 2009

Customer/Sponsor

Name Keith Kaufman
 Organization JPEO JTRS
 & Code
 E-mail Keith.kaufman@navy.mil

SSC-PACIFIC Code

Project(s) Wireless LAN

*For the code and project being rated,
 please indicate your satisfaction with the following areas:*

1. *Quality of products and/or services*

Extremely Dissatisfied	Very Dissatisfied	Slightly Dissatisfied	Adequately Satisfied ("No complaints")	Well Satisfied	Very Satisfied	Extremely Satisfied	Not Applicable
-3	-2	-1	0	+1	+2	+3	99

2. *Time and schedule performance*

Extremely Dissatisfied	Very Dissatisfied	Slightly Dissatisfied	Adequately Satisfied ("No complaints")	Well Satisfied	Very Satisfied	Extremely Satisfied	Not Applicable
-3	-2	-1	0	+1	+2	+3	99

3. *Budget and financial performance*

Extremely Dissatisfied	Very Dissatisfied	Slightly Dissatisfied	Adequately Satisfied ("No complaints")	Well Satisfied	Very Satisfied	Extremely Satisfied	Not Applicable
-3	-2	-1	0	+1	+2	+3	99

4. *Overall Performance*

Extremely Dissatisfied	Very Dissatisfied	Slightly Dissatisfied	Adequately Satisfied ("No complaints")	Well Satisfied	Very Satisfied	Extremely Satisfied	Not Applicable
-3	-2	-1	0	+1	+2	+3	99

5. *Consider how you work with the SSC-SD Project team.*

How satisfied are you with that relationship?

Extremely Dissatisfied	Very Dissatisfied	Slightly Dissatisfied	Adequately Satisfied ("No complaints")	Well Satisfied	Very Satisfied	Extremely Satisfied	Not Applicable
-3	-2	-1	0	+1	+2	+3	99

Appendix G

Wireless Configuration Instructions

Connecting to the SSCSD Wireless Government LAN & JTRS guest commercial wireless network

The SSCSD WLAN conforms to the following security standards:

WPA2 (a.k.a. 802.11i) “Enterprise”
802.1x authentication using protocol EAP-TLS
AES Encryption

The alternative protocols (WEP, WPA, WPA2 PSK) will not work.

This is in conformance with DoD Directive 8100.2: *Use of Commercial WLAN Devices, Systems, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)*.

Laptop (or other WLAN client) requirements:

You **must** have a wireless (802.11 a/b/g) NIC that is WPA2 compliant, supporting AES encryption.

You **must** have an 802.1x “supplicant.” There is one in MAC OS X that works quite well, and there is one in Windows XP which can be made to work. There are alternative supplicants that work better in Windows XP, such as the Funk Odyssey client, or the one that comes with your NIC manufacturer such as the “Dell TrueMobile WLAN Card Utility.”

You **must** have a DoD CAC, or other DoD PKI certificate, and your computer must be able to access it and use it. Go to <https://pkitest.spawar.navy.mil> to verify.

Your DoD PKI certificate **must** be registered in the SPAWAR LDAP directory. Use <https://directory.spawar.navy.mil> to find your record and look at the certificate details to see if your certificate is registered. Some people have more than one certificate. Make sure that the one you are using is registered properly and has not expired and has not been revoked.

If you are running Windows XP, make sure you are running with Service Pack 2 (SP2) and be sure to install the Wireless Client Update as described in KB917021 <http://support.microsoft.com/kb/917021>.

For MAC OS X, make sure you’re running the latest 10.4 (Tiger) release.

DoD Directive 8100.2 mandates that laptops and other wireless clients employ FIPS 140-2-validated file encryption for data at rest.

Location requirements:

You must be near (within about 100 meters of) one of the SSCSD WLAN Access points at Point Loma or Old Town campus. All of these support 802.11 b/g (2.5 Ghz), and some support 802.11a (5.0 Ghz) as well.

Support:

This is currently a Pilot effort. You cannot call the help desk for support, or find any information online. This will be fixed in the future.

References:

The following reference (and the references it points to) can be very helpful:

- http://en.wikipedia.org/wiki/IEEE_802.11i

Points of Contact:

CDR Joe Roth, SSCSD 5525, Joseph.Roth1@navy.mil, 619.553.0413
 Ron Broersma, SSCSD 21403, Ron@spawar.navy.mil, 619.553.2293

Configuring an Apple MAC running OS X:

Make sure your Airport interface is turned on. From the wireless network pick list, select “SSCSD” if it is listed; otherwise choose “Other.”

In the “Closed Network” panel that pops up, select the following:

- For “Network Name” enter SSCSD.
- For “Wireless Security” select WPA2 Enterprise.
- For “User Name” and “Password,” you can leave these blank, because it is using your certificate for authentication. However, if you do leave it blank, then the popup window will ask you for your userid/password every time, even though you don’t need to enter anything. So, enter your SPAWAR userid and password if you want to get it to stop prompting you every time. It will still use your certificate for authentication.
- For 802.1X Configuration, choose Automatic.
- For “TLS Certificate,” select a valid DoD PKI certificate. If you don’t see any, then you need to load your PKI certificates into your keychain.

Configuring a Windows PC (using the built-in wireless configuration tool):

Launch the wireless configuration tool (Start -> Connect To -> Show All Connections and then double-click the line matching your wireless NIC) shown below in Figure G-1.

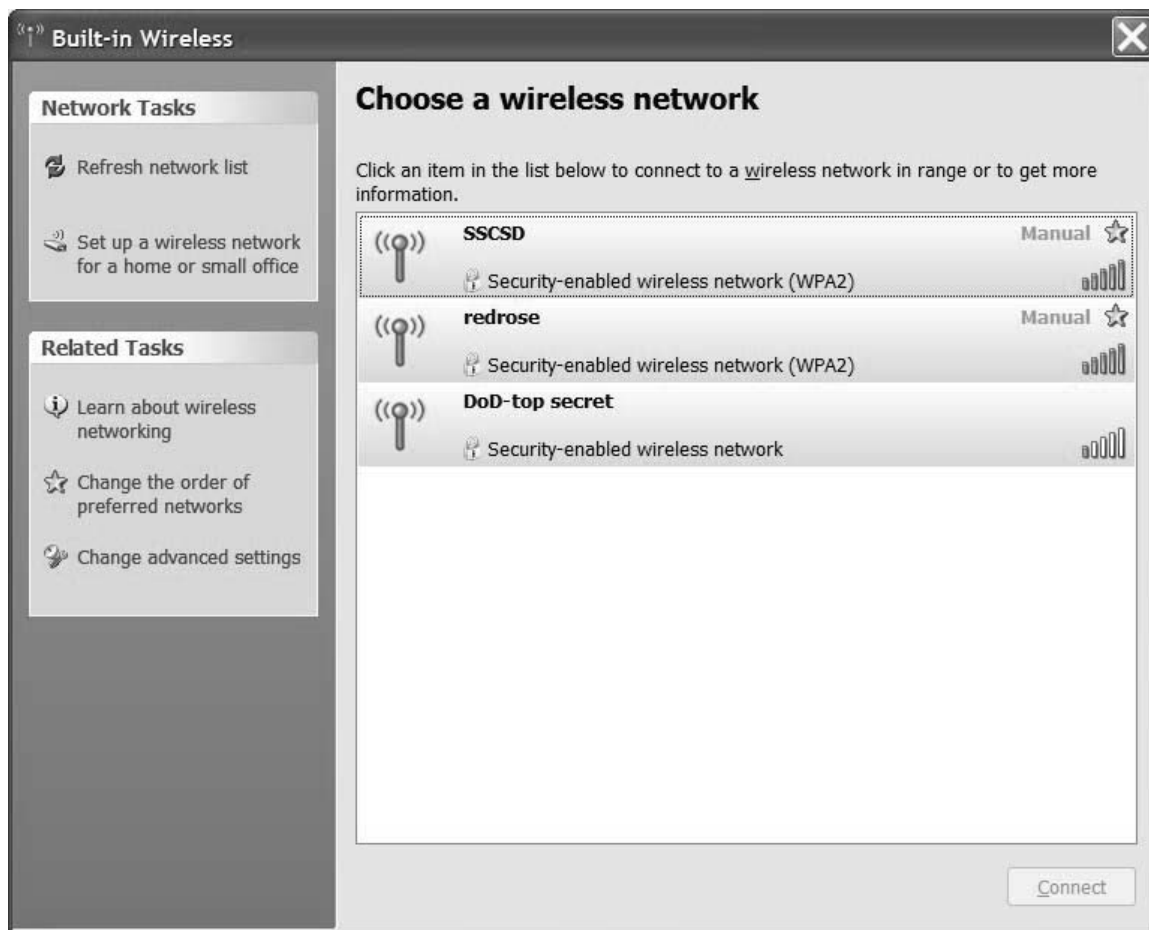


Figure G-1. Microsoft Wireless Configuration SSID Selection Tool

If you don't see "SSCSD" in the list, you'll have to add it.

Select "Change advanced settings" where Figures G-2 and G-3 shown below will appear.

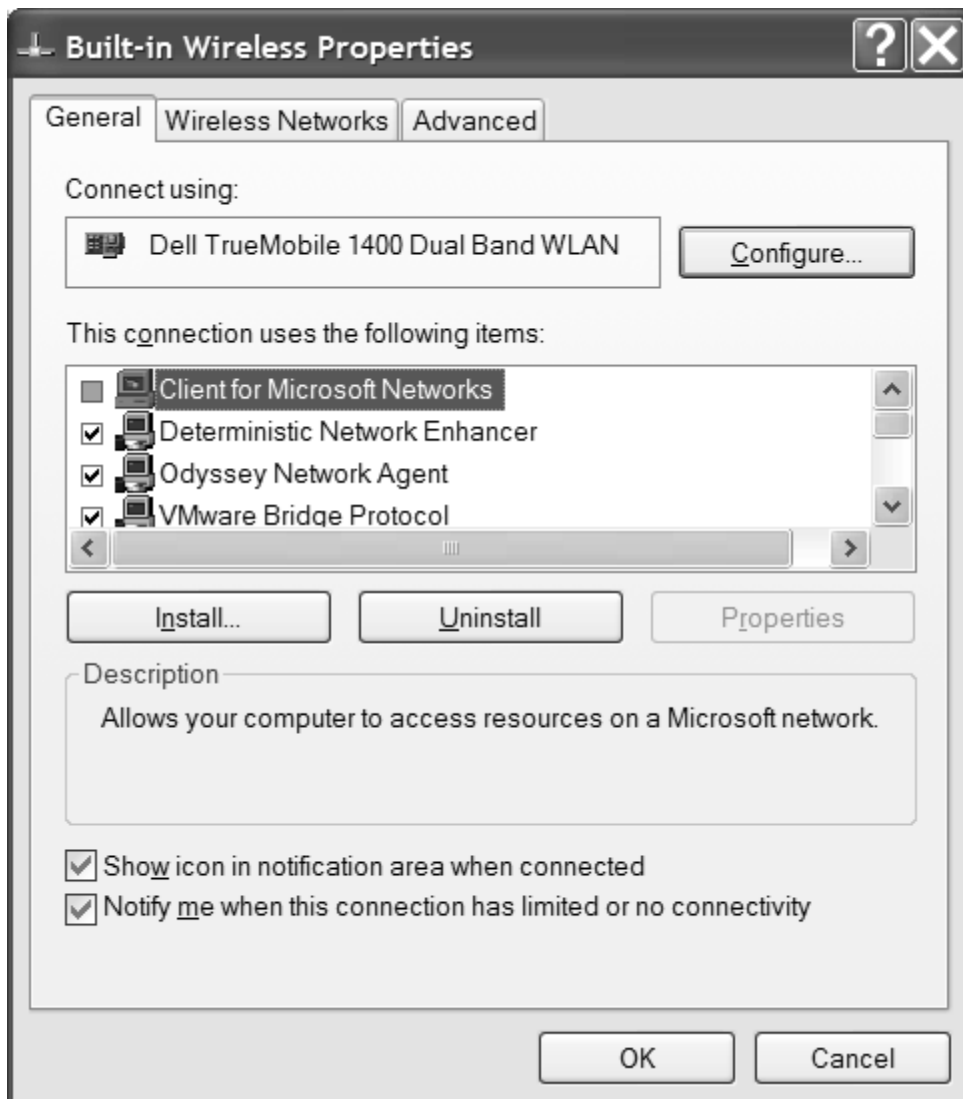


Figure G-2. Microsoft Wireless Configuration Tool Advanced Settings General Tab

Select “Wireless Networks” tab:

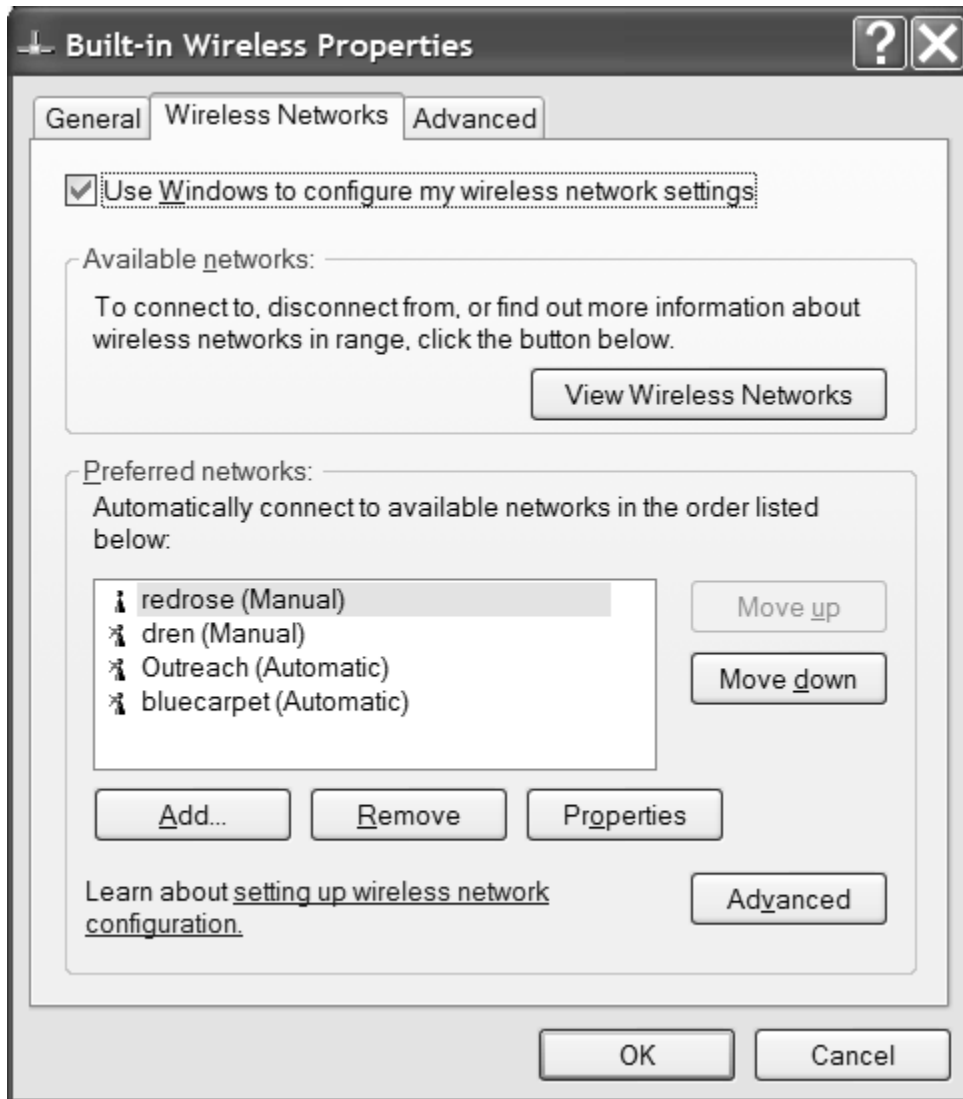


Figure G-3. Microsoft Wireless Configuration Tool Advanced Settings Wireless Networks Tab

If you don't already have "SSCSD" configured, then select "Add" as shown in Figure G-4:

The screenshot shows a window titled "Wireless network properties" with three tabs: "Association", "Authentication", and "Connection". The "Association" tab is selected. It contains the following fields and options:

- Network name (SSID):** A text input field.
- Wireless network key:** A section containing:
 - This network requires a key for the following:**
 - Network Authentication:** A dropdown menu set to "Open".
 - Data encryption:** A dropdown menu set to "WEP".
 - Network key:** A text input field.
 - Confirm network key:** A text input field.
 - Key index (advanced):** A spinner box set to "1".
 - ☒ **The key is provided for me automatically**
- ☐ **This is a computer-to-computer (ad hoc) network; wireless access points are not used**

At the bottom are "OK" and "Cancel" buttons.

Figure G-4. Microsoft Wireless Configuration Tool Advanced Settings Association Tab

Set the SSID to SSCSD as shown in Figure G-5.:



Figure G-5. Microsoft Wireless Configuration Tool Advanced Settings Association Tab

Look at the choices for “Network Authentication”. You should see the following shown in Figure G-6:



Figure G-6. Microsoft Wireless Configuration Tool Association Tab Data Encryption Menu

If you don't see the WPA2 selections, then either you didn't install the hotfix that was mentioned earlier, or your NIC doesn't support WPA2.

You want to choose **WPA2**. Do NOT choose WPA2-PSK.

Also choose **AES** encryption as shown in Figure G-7:



Figure G-7. Microsoft Wireless Configuration Tool Association Tab Data Encryption AES setting

Next select the “Authentication” tab as shown in Figure G-8:

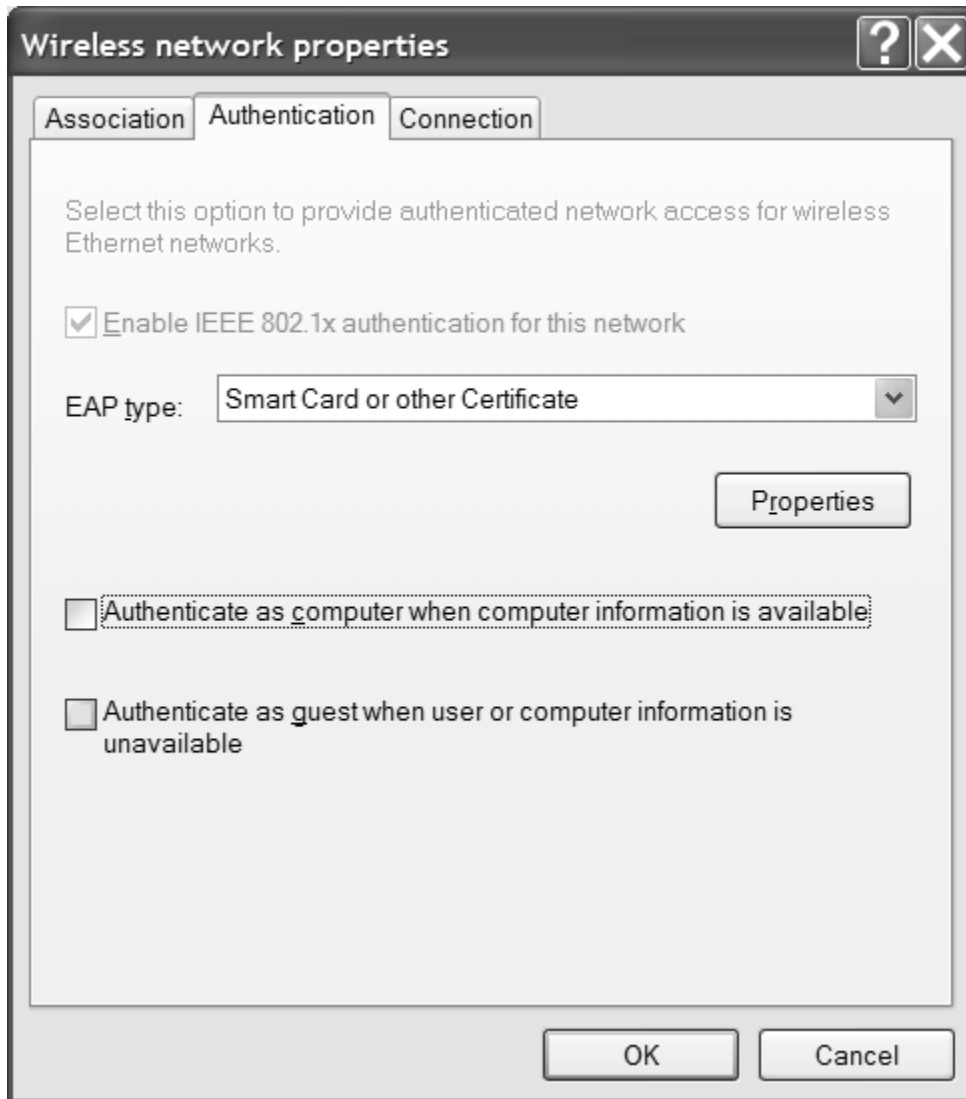


Figure G-8. Microsoft Wireless Configuration Tool Authentication Tab

Make sure the “Authenticate as computer...” and “Authenticate as guest” boxes are NOT checked.

For EAP type, select “Smart Card or other Certificate”.

Then hit “Properties” as shown in Figure G-9:



Figure G-9. Microsoft Wireless Configuration Tool Smart Card Screen

Configure as shown above: Select “Use my smart card.” Note that “Use a certificate on this computer” should also work for selecting a soft certificate, but doesn’t for some reason. Microsoft doesn’t like DoD soft certs. Also note that “Validate server certificate” should also work, but doesn’t for as-yet-unknown reasons. In the future we will want to check that box.

Then hit “OK” on all the windows. You should now be able to connect to SSCSD.

On the original screen listing all the wireless networks, you should see SSCSD as shown in Figure G-10:

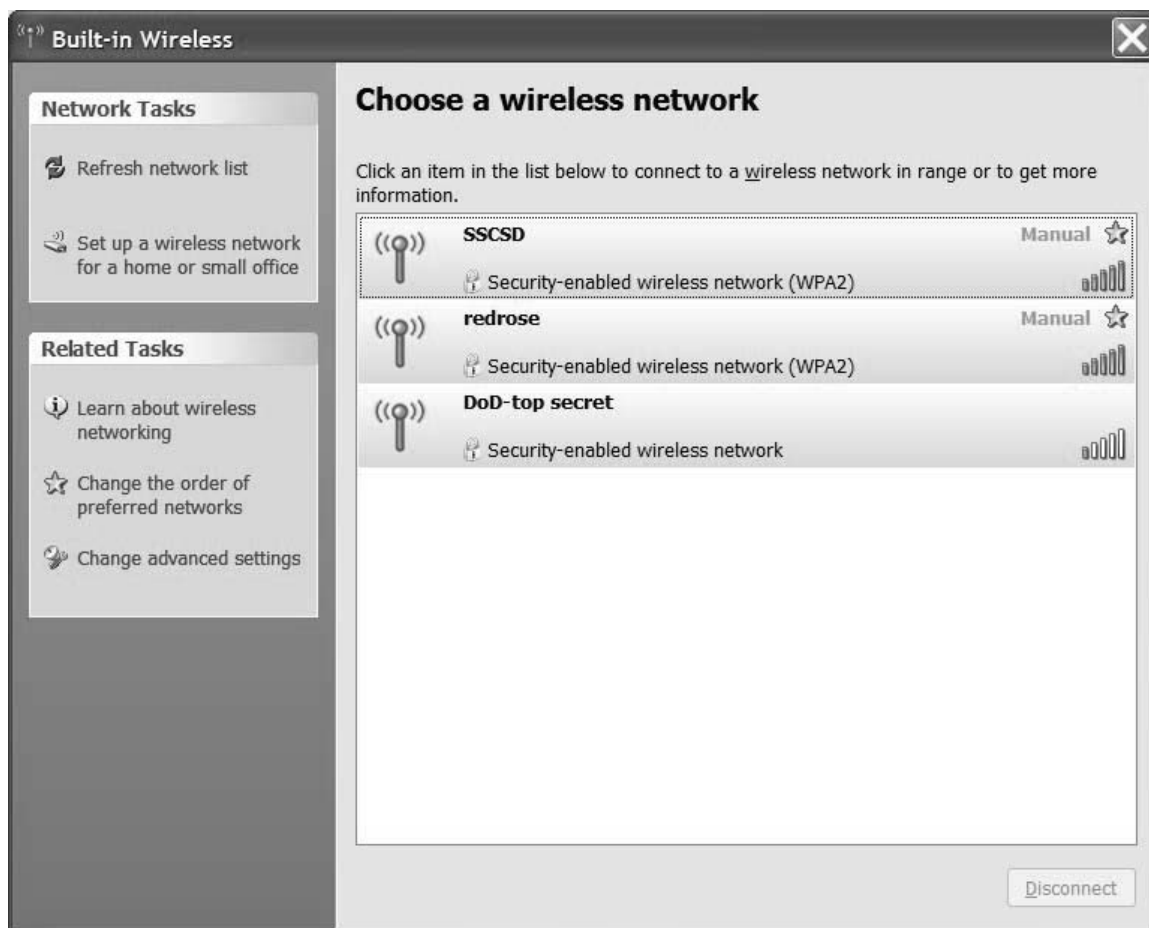


Figure G-10. Microsoft Wireless Configuration SSID Selection Tool

Click on “SSCSD” to connect as shown in Figures G-11 and G-12:

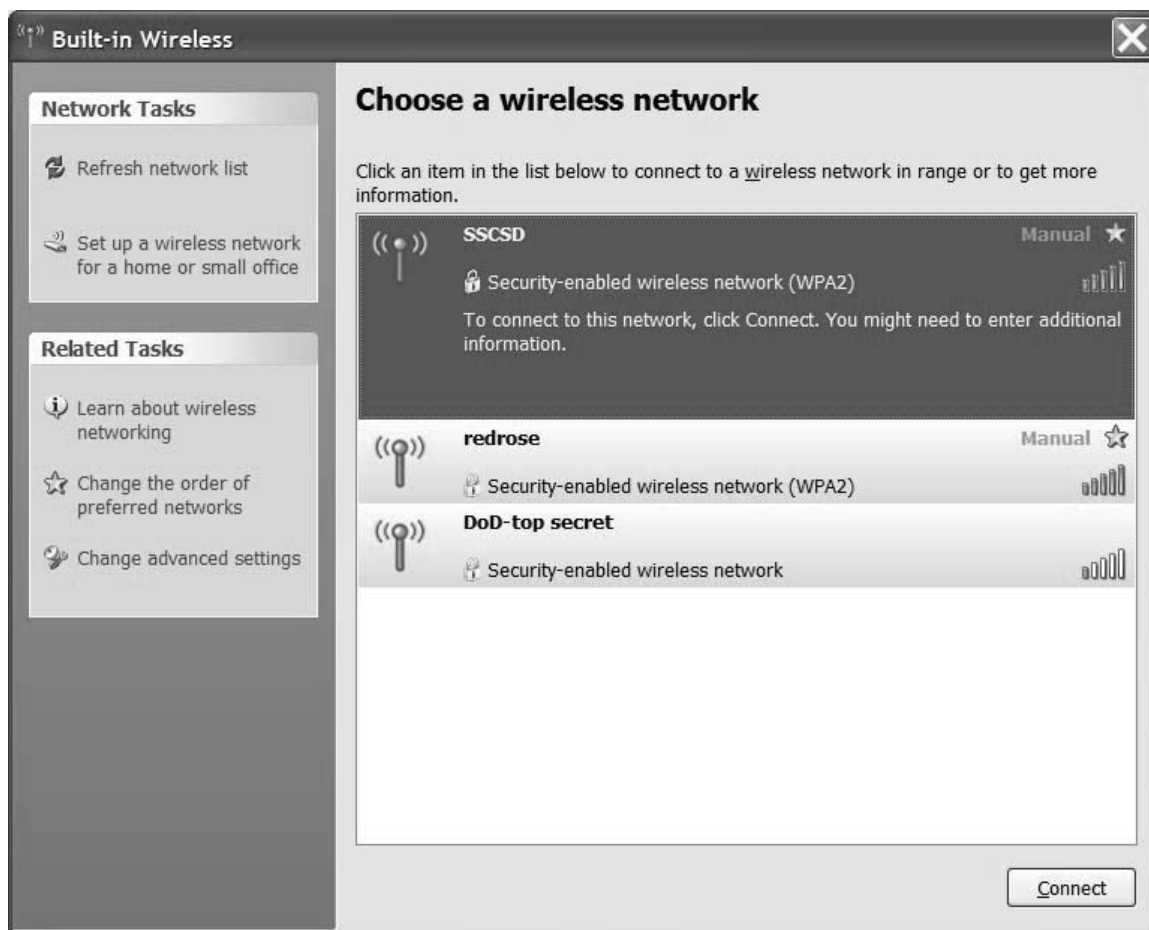


Figure G-11. Microsoft Wireless Configuration SSID Selection Tool

Then hit “Connect.”



Figure G-12. Microsoft Wireless Configuration SSCSD Connection Screen

It should then ask for your CAC PIN as shown in Figure G-13:



Figure G-13. Pin Entry Screen

Enter your PIN and hit “OK”.

It will attempt to authenticate as shown in Figure G-14:

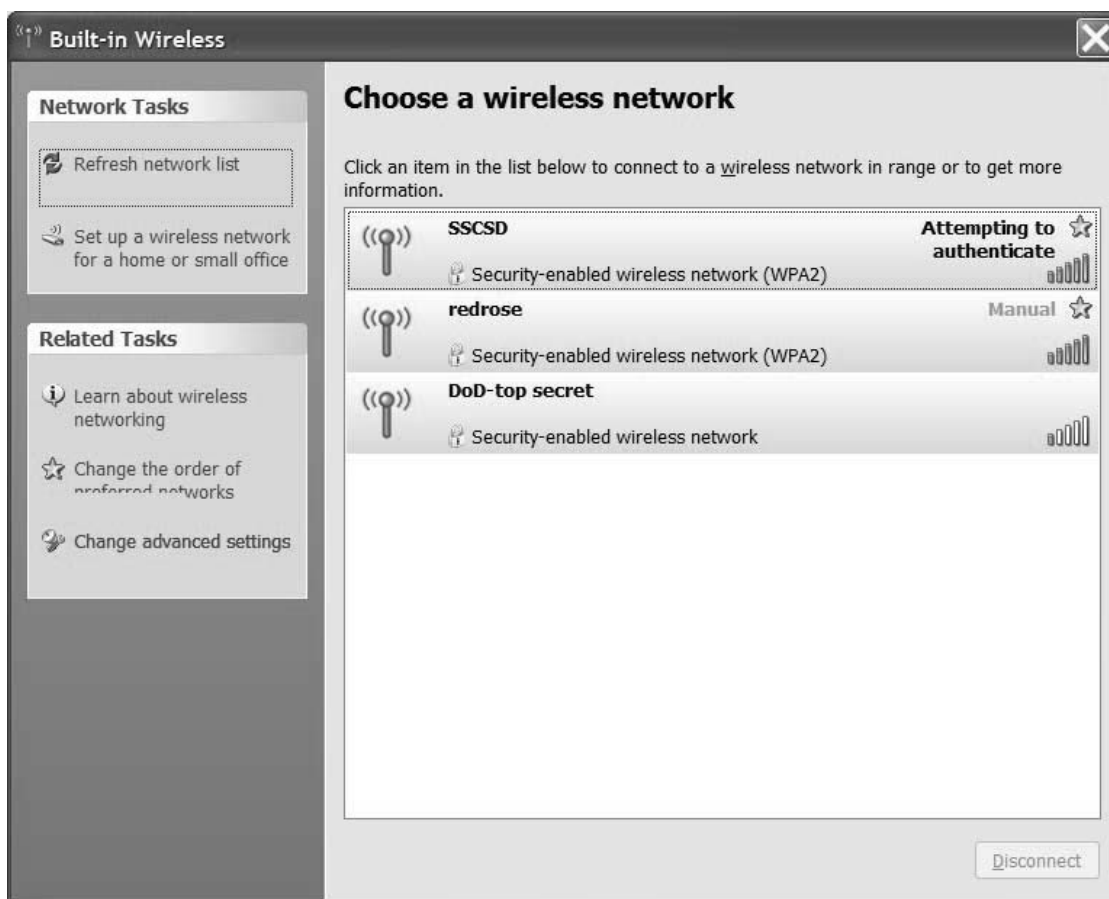


Figure G-14. Microsoft Wireless Configuration SSID Selection Tool SSCD Authentication Feedback screen

After successfully negotiating a DHCP address, it will connect as shown in Figure G-15:

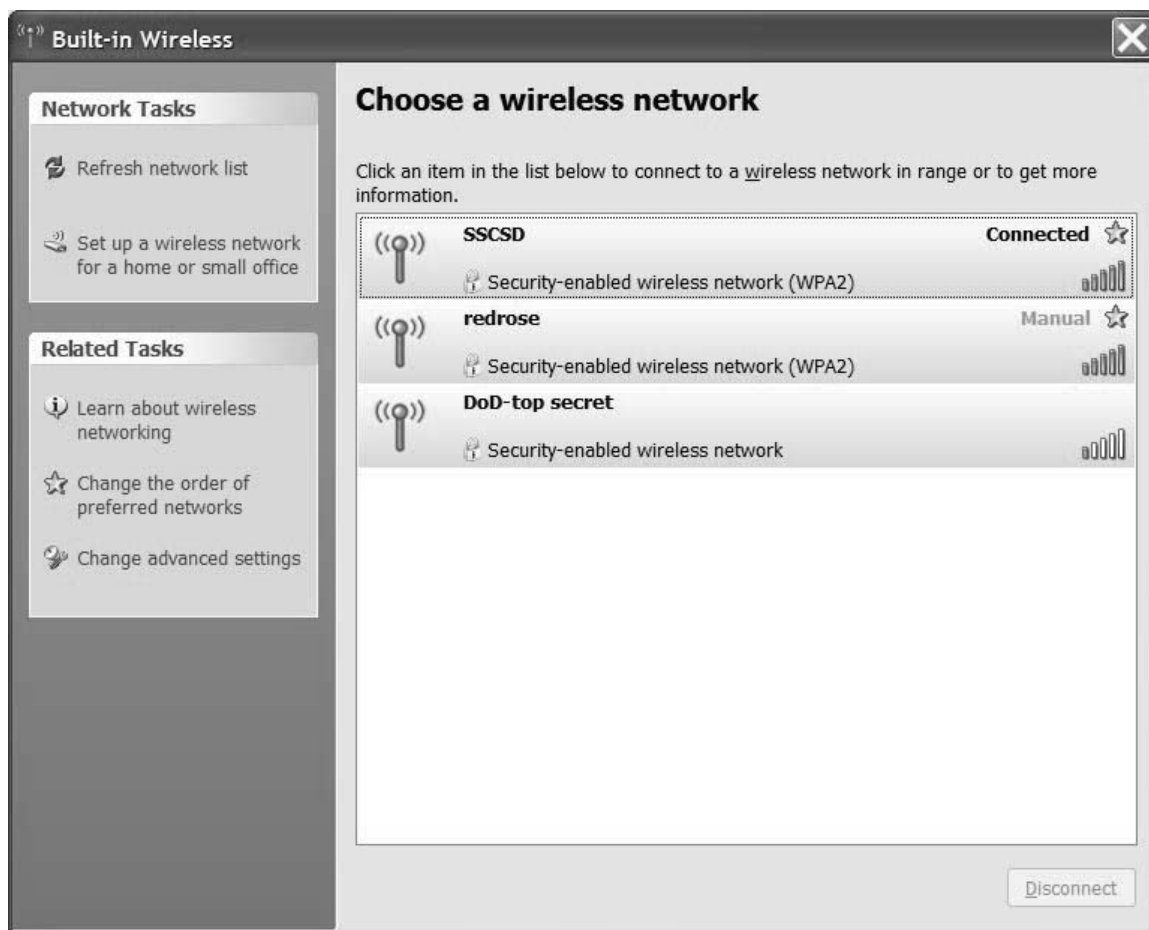


Figure G-15. Microsoft Wireless Configuration SSID Selection Tool Connection feedback Screen

You have now successfully connected to the government wireless network

In order to connect to the jtrs-guest commercial network do the following procedures.

Access the “View Available Wireless Networks” as shown in Figure G-16

Control Panel > Network Connections > Right Click on your wireless NIC

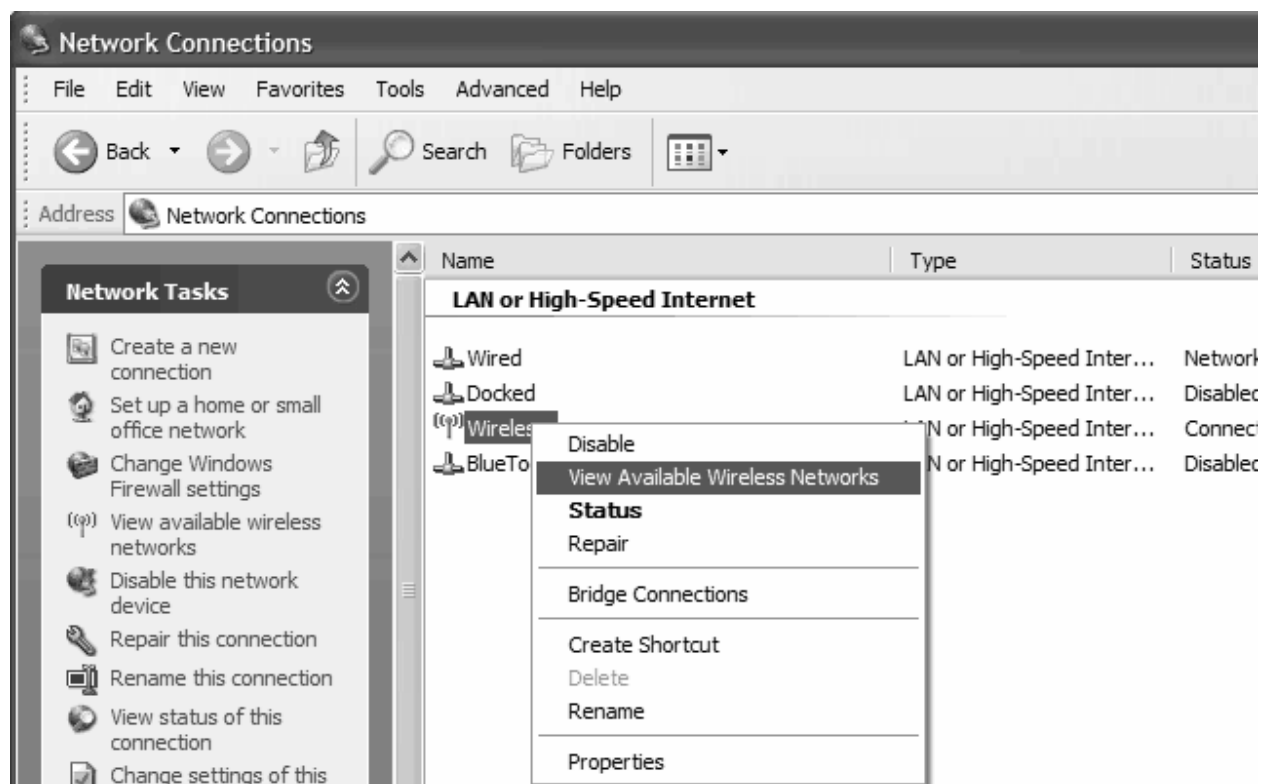


Figure G-16. Microsoft Network Connection Screen

Select jtrs-guest from the list of networks, and click on Connect as shown in Figure G-17.

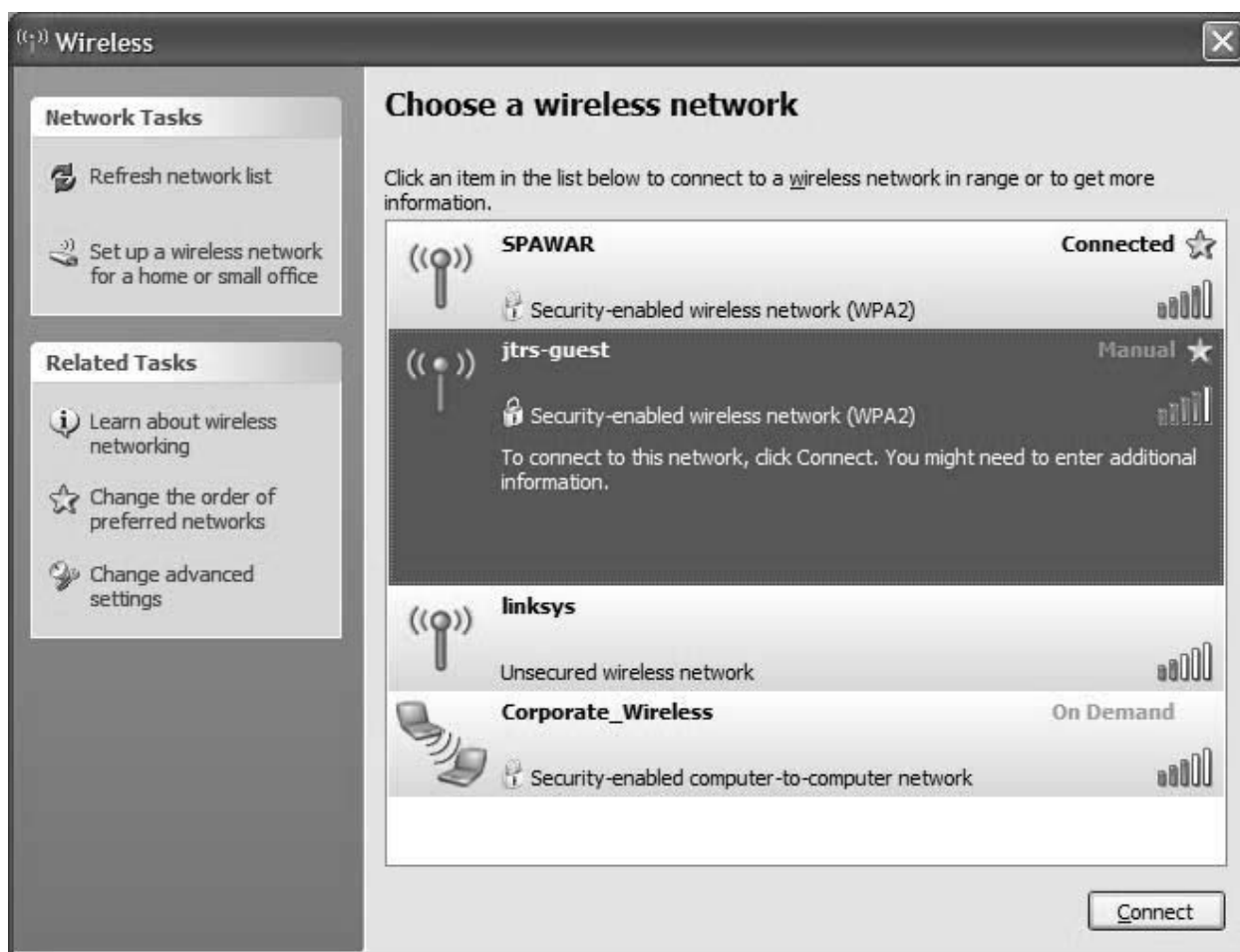


Figure G-17. Microsoft Wireless Configuration SSID Selection Tool “JTRS-Guest” screen

It will prompt you for a Network Key as shown in Figure G-18:



Figure G-18. Network Key Entry Screen

The key is “**REDACTED**”. No quotes. Capitalization is important. The space is important. (You should only have to enter this once. Windows should remember it after the first good connection.)

It will return the following shown in Figure G-19:

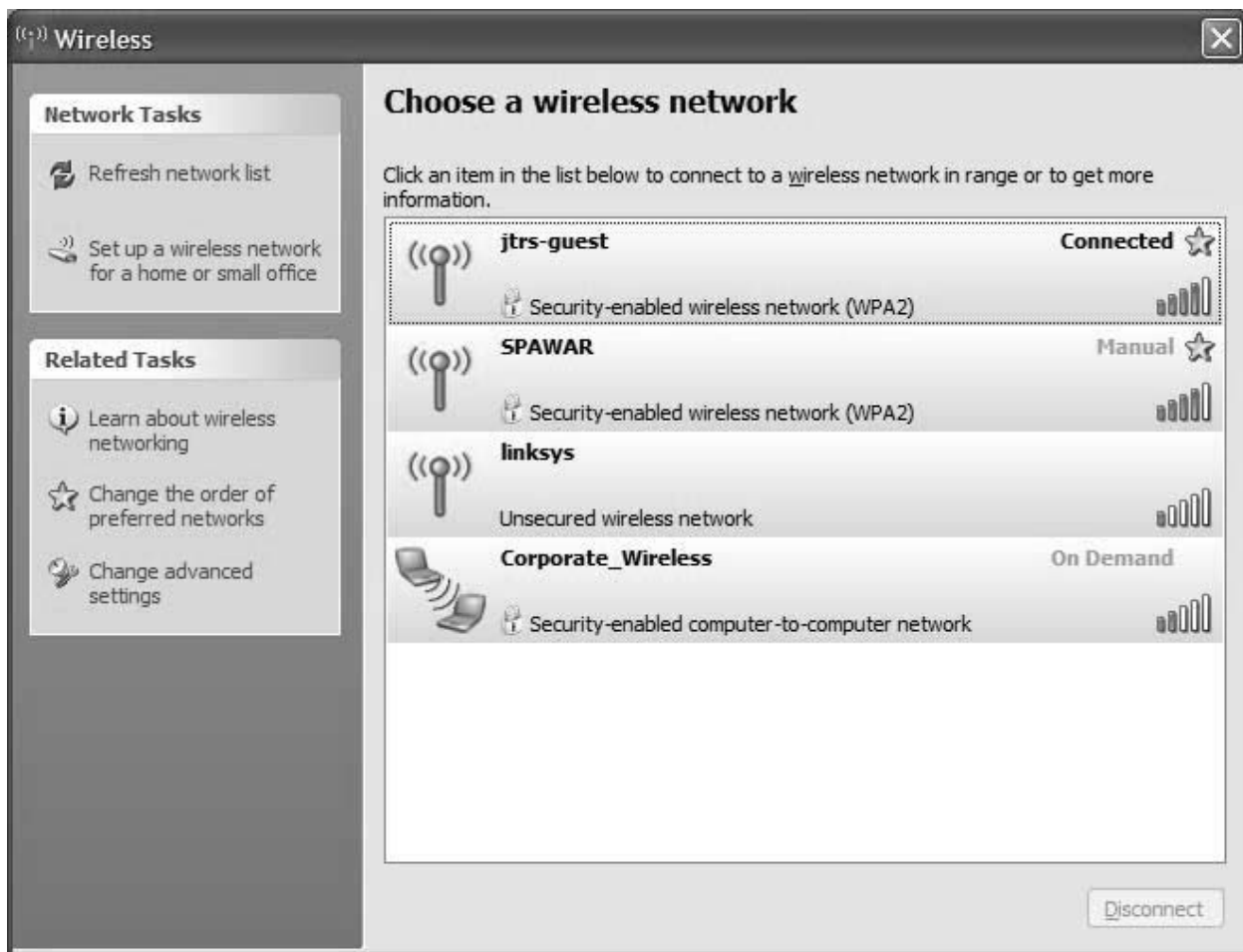


Figure G-19. Microsoft Wireless Configuration SSID Selection Tool “JTRS-Guest” Connection Screen

Note: Even though it says connected, you can not do anything until you have opened a browser and authenticated.

Open a browser as shown in Figure G-20:



Figure G-20. Aruba Authentication Screen

It does not matter what your homepage is, you will be redirected here. Use the username and password that you received to login.

Note: Both the username and the password are case sensitive.

The next screen you will be connected as shown in Figure G-21:

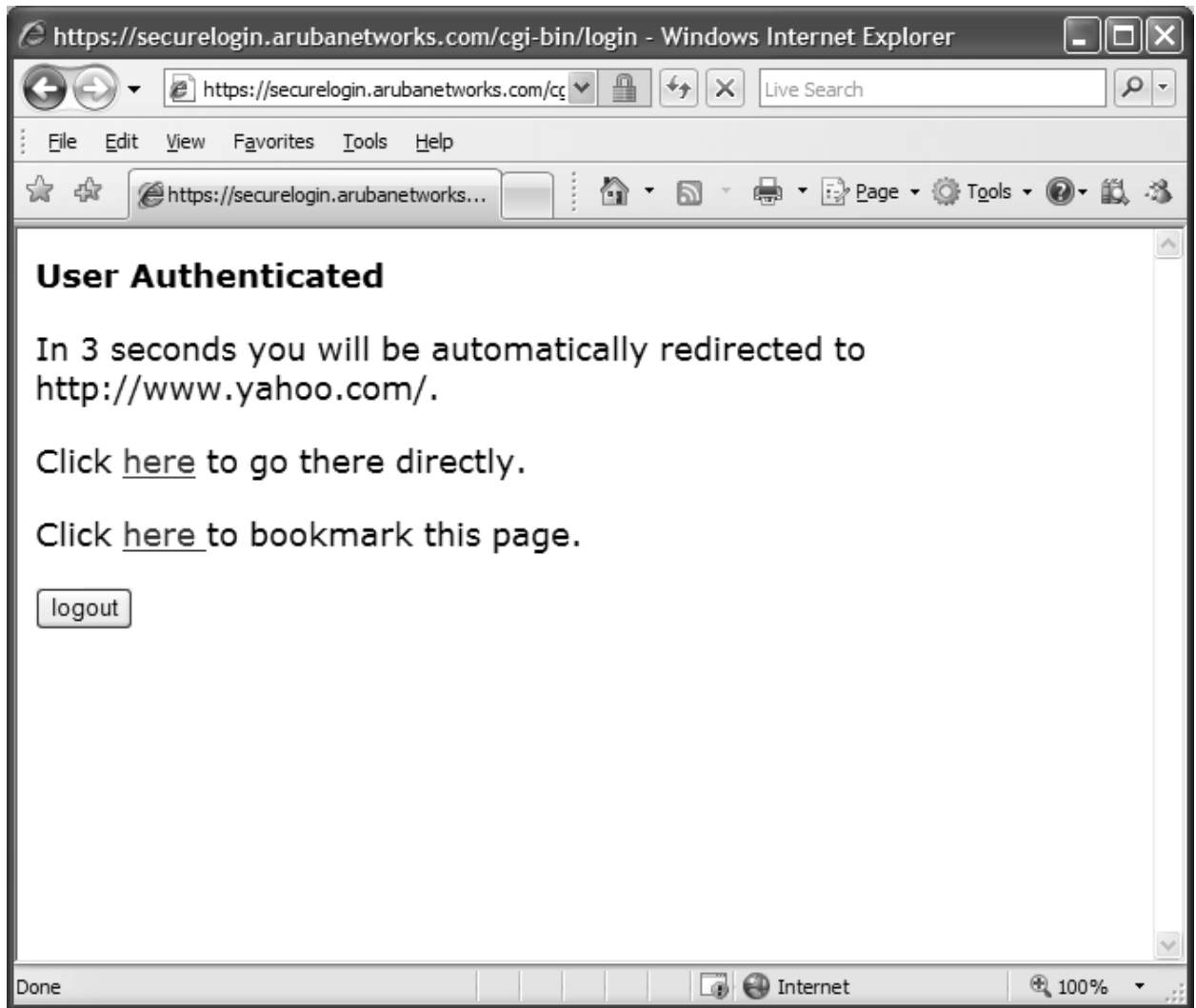


Figure G-21. Microsoft Wireless Configuration SSID Selection Tool

You can now do other things that do not require a browser. (E.g. SSH, VPN, update anti-virus software or other programs, check email if it is configured...)

In order to print do the following procedures:

CONNECTING TO A PRINTER VIA THE WIRELESS:

This procedure will work with both commercial and Government wireless networks.

Determine the IP of the printer that you would like to connect to.

Examples:

128.49.104.126	jtrs-17b-301-a.sd
128.49.104.132	jtrs-b50-222-a.sd

You will need to download a driver.

[http://www.support.xerox.com/go/getfile.asp?Xlang=en_US&XCntry=USA&objid=59796&EULA=0&prodID=6360&Family=Phaser&ripId=&langs=English\(US\)&plats=Windows_XP&Xtype=download&uType=](http://www.support.xerox.com/go/getfile.asp?Xlang=en_US&XCntry=USA&objid=59796&EULA=0&prodID=6360&Family=Phaser&ripId=&langs=English(US)&plats=Windows_XP&Xtype=download&uType=)

Once the Driver is downloaded, run the file as shown in Figure G-22:



Figure G-22. Xerox Driver Run Screen

Click Install as shown in Figure G-23



Figure G-23. Xerox Initial Driver Configuration Screen

Add a new printer.

The program should have automatically launched the Add Printer Wizard as shown in Figure G-24.

Click on Next



Figure G-24. Printer Wizard

Select “Local printer attached to this computer”, WITHOUT the “Automatically...” as shown in Figure G-25:

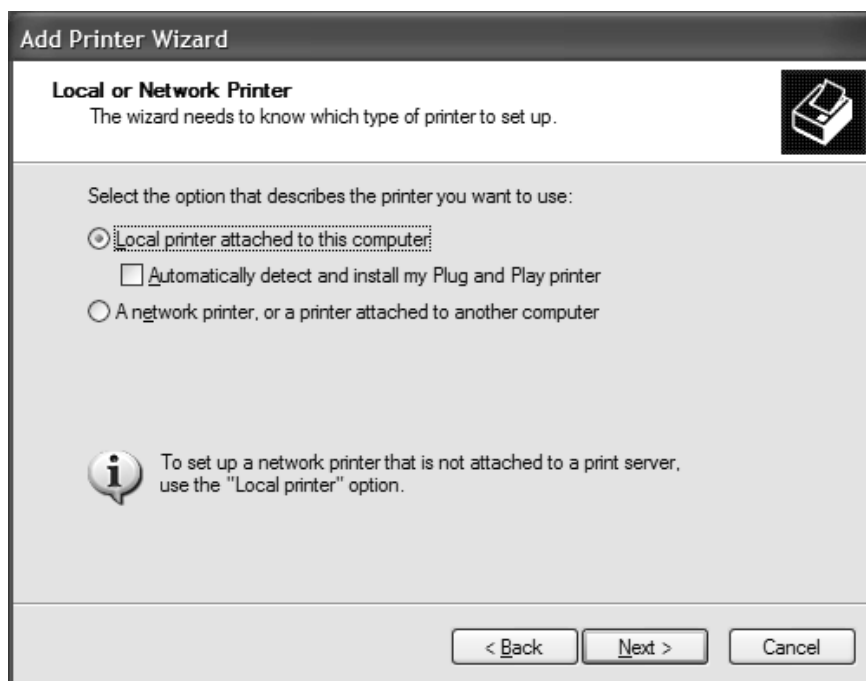


Figure G-25. Local Printer Configuration Screen

Select “Create a new port” and “Standard TCP/IP Port” then click Next as shown in Figure G-26

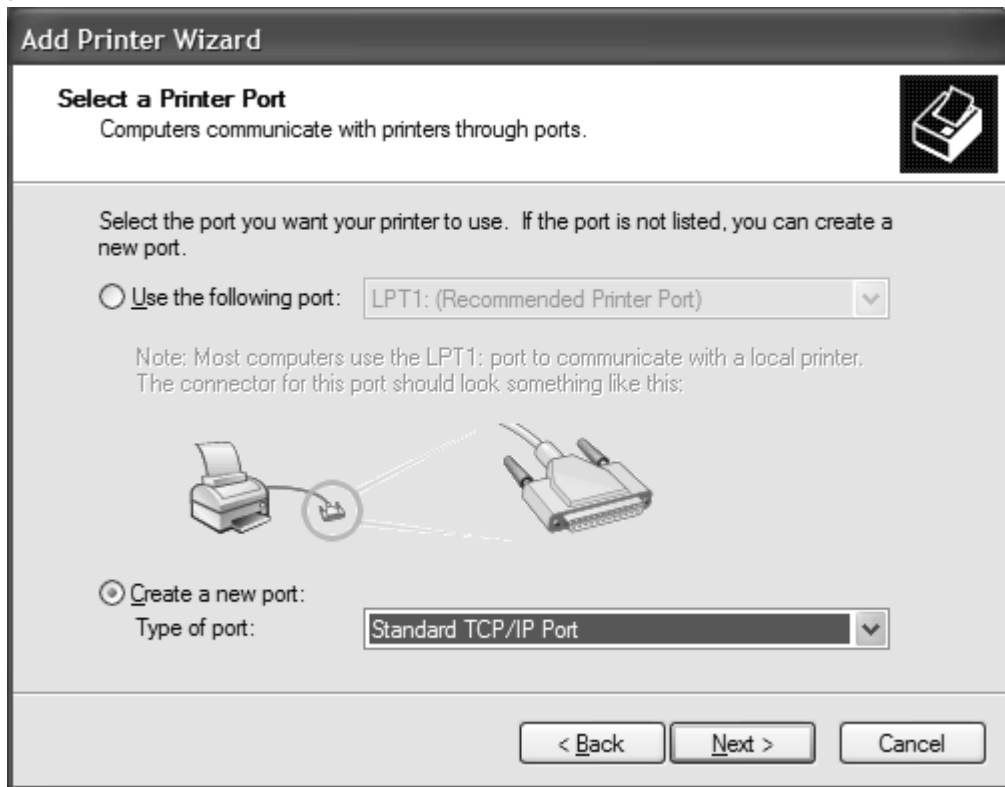
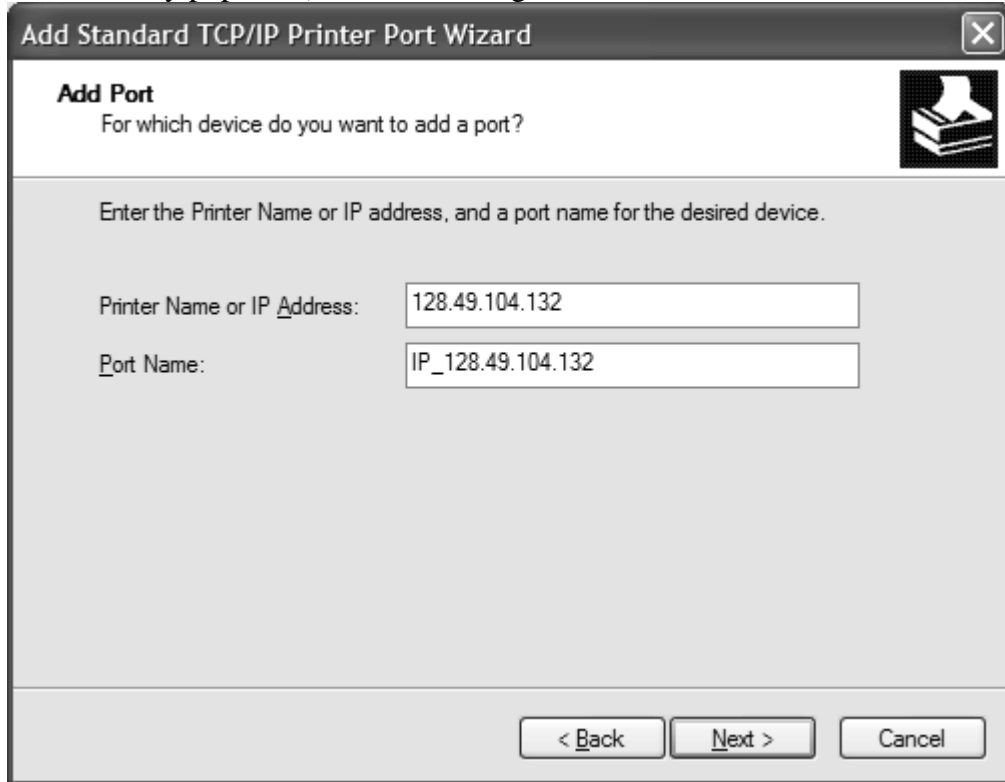


Figure G-26. Printer Port Configuration Screen

Click Next twice.

For the Printer Name or IP Address, enter the IP of the printer (The Port Name will automatically populate.) as shown in Figure G-27. Click Next.



Add Port
For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 128.49.104.132

Port Name: IP_128.49.104.132

< Back Next > Cancel

Figure G-27. Printer IP Configuration Screen

Use the defaults and click Next twice.

Select Finish as shown in Figure G-28:

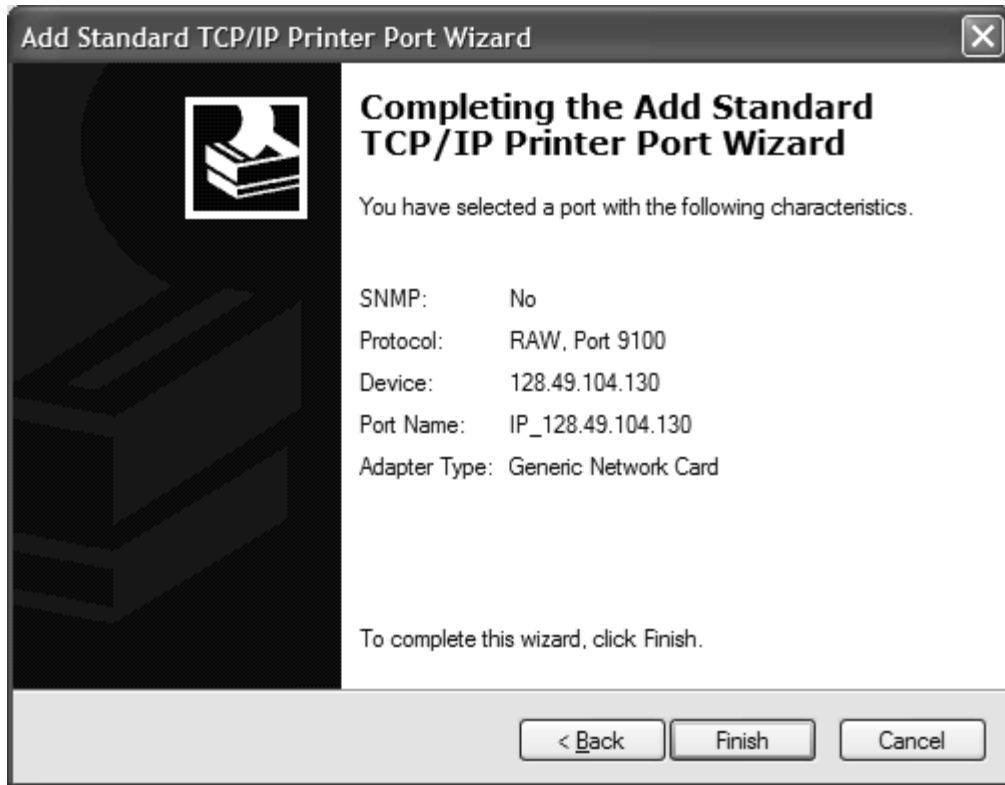


Figure G-28. Xerox Driver Configuration Finish Screen

Select Xerox Phaser 6360N PS as shown in Figure G-29. (If it is not present, select Have disk and navigate to the folder you extracted the files to, usually, C:\Xerox\6360_Driver and select the file: X26360.inf)

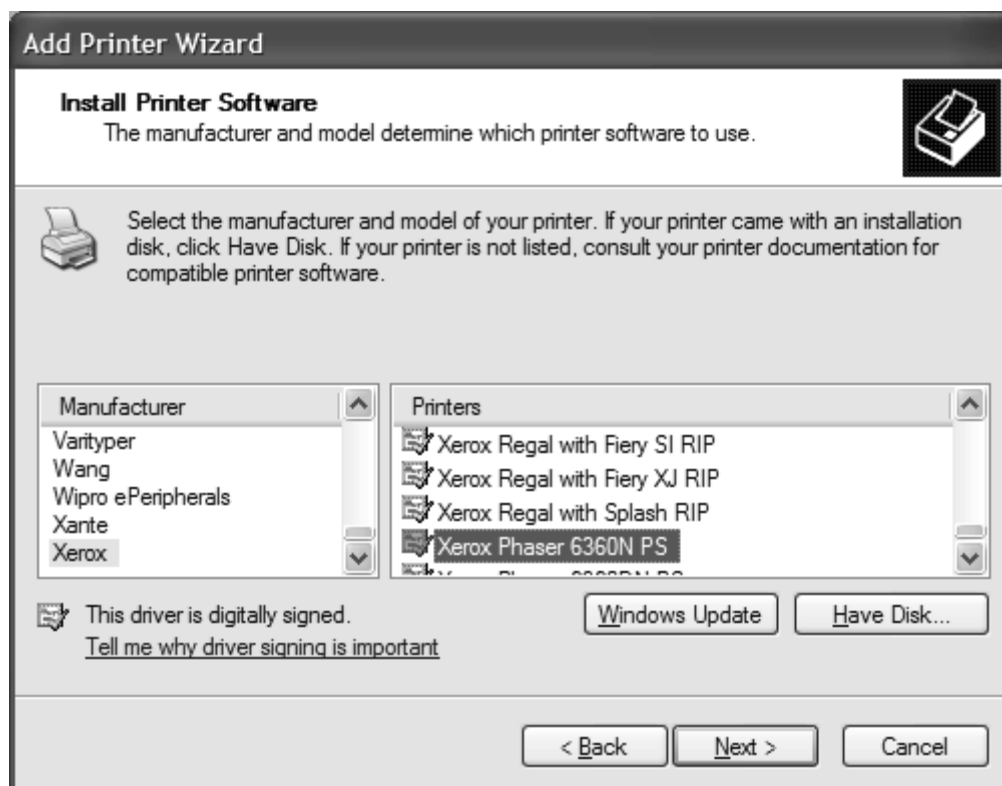


Figure G-29. Printer Selection Screen

Continue to click Next and Finish using the default values.

Reference List

- Allen, P. (2006). *Service orientation, winning strategies and best practices*. Cambridge, UK: Cambridge University Press.
- Arbaugh, W. (2001). *Your 802.11 network has no clothes*. Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks, 131-44.
- Arbaugh, W. (2003a). WLAN problems and solutions. *Communications of the ACM*, 7(46), 31-34.
- Arbaugh, W. (2003b, August). Wireless security is different. *IEEE Computer*, 36(8), 99-101.
- Arbaugh, W. (2004). Security issues in IEEE 802.11 wireless local-area networks: A Survey, *Wireless Communications and Mobile Computing Journal*, 4(8), 821-833.
- Arbaugh, W. (2006, February). *Wireless network security and interworking*. Proceedings of the IEEE, 94(2), 3.
- Bertino, E., & Ruth, S. (2006, May/June). Municipal wi-fi: Big wave or wipeout. *IEEE Internet Computing* 10(3), 66-71. Retrieved June 25, 2008, from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1631980
- Boessenkool, A. (2008). *Ready for Life after NMCI?* Retrieved January 19, 2009, from http://www.navytimes.com/news/2008/06/navy_nmci_061608w/.
- Briefing to the House on the challenges and risks associated with the Joint Tactical Radio System program. (2003, August). *GAO Briefing*.
- Bueno, R. (2004, April). Global information grid—questions and answers. *Software Tech News*, 7(1). Retrieved June 25, 2008, from https://www.softwaretechnews.com/stn_view.php?stn_id=10&article_id=52.
- Carey, R. (2008, September). *NGEN Industry Day Briefing*. Powerpoint briefing.
- The case for SOA: A roundtable discussion. (2008, January 25). *Federal Computer Week*. Retrieved December 1, 2008, from <http://www.fcw.com/soa/>.
- Challenges associated with the implementation of the Joint Tactical Radio System. (1999, September). *GAO Report*
- Chebrolu, K., Bhaskaran, R., & Sayandeep, S. (2006). Long-distance 802.11b links: performance measurements and experience. ACM Special Interest Group on Mobility of Systems, Users, Data and Computing. *Proceedings of the 12th Annual*

- International Conference on Mobile Computing and Networking*, 74-85. Retrieved May 20, 2007, from <http://portal.acm.org/citation.cfm?id=1161099>.
- Cheng, Y. (2006, October). Jigsaw: Solving the puzzle of Enterprise 802.11 analysis. *ACM SIGCOMM Computer Communication Review*, 36(4), 39-50. Retrieved June 25, 2008, from <http://portal.acm.org/citation.cfm?id=1151659.1159920>.
- Chong, F. (2006). Architectural strategies for catching the long tail. *Microsoft MSDN Architecture Center*. Retrieved September 25, 2007, from <http://msdn2.microsoft.com/en-us/library/aa479069.aspx>
- Creswell, J. (2008). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (3rd ed.). Thousand Oaks, CA: Sage Publications.
- Dalaklis, D. (2004). Monitoring the progress of the Navy and Marine Corps Intranet (NMCI): Implementation, performance and impact. Unpublished master's thesis, Naval Postgraduate School.
- Davis, A. W., & Greenberg, A. D. (2004). *The managed services conundrum: Demystifying conferencing managed services*. Duxbury, MA: Wainhouse Research. Retrieved December 14, 2008, from <http://www.wainhouse.com/files/papers/wr-managedsvcs.pdf>
- Defense acquisition guidebook (DAG)*. (2004). Retrieved June 25, 2008, from <https://akss.dau.mil/dag/DoD5000.asp?view=document>.
- Defense Acquisition University (2007). *Advanced systems planning, research, development and engineering*. SYS 301: Defense Acquisition University.
- Defense information superiority progress made, but significant challenges remain. (1998, August). *GAO Report*.
- The Department of the Navy. (2008). Enterprise mobility 2008. Retrieved December 1, 2008, from <http://www.doncio.navy.mil/Products.aspx?ID=663>
- Dev, S. (2006). *The evolution of managed HR services*. Retrieved June 25, 2008, from <http://www.expresscomputeronline.com/20060403/technologylife01.shtml>
- Diaz, R. (2008). *SOA Core Services PMW 160.5* [PowerPoint]. U.S. Navy presentation.
- DOD needs to ensure that Navy Marine Corps Intranet Program is meeting goals and satisfying customers. (2006, December). *GAO Report*.
- EDIMAX (2009). *EW-7206APG Wireless 802.11APg manual*. Retrieved July 26, 2009 From http://www.edimax.com/tw/produce_detail.php?pd_id=18&pl1_id=3&pl2_id=77

- The Evolution of managed security services: ISS virtual-SOC solution, security the way you need it. (2006). Retrieved June 25, 2008, from http://www.iss.net/documents/whitepapers/ISS_Virtual_SOC.pdf
- Fahrenthold, A. (2002). Network survivability analysis of the Navy and Marine Corps Intranet (NMCI). Unpublished master's thesis, Naval Postgraduate School.
- Federal information processing standard publication 140-2*. (2001). Retrieved June 25, 2008, from <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>
- Foster, I. (2005). *Describing the elephant: The different faces of IT as a service*. Retrieved March 30, 2008, from http://www.ggf.org/documents/Diff_Faces_foster.pdf
- Geier, J. (2003, February 21). Student sailors go wireless. *Wi-Fi Planet*, Retrieved June 25, 2008, from <http://www.wi-fiplanet.com/columns/article.php/1593021>.
- Geier, J. (2005, May 9). *Removing barriers to wireless LAN deployment*. Retrieved December 12, 2008, from <http://research.ittoolbox.com/white-papers/networking/wireless/removing-barriers-to-wireless-lan-deployment-2957>.
- Grantham, D. (2005, May 30). *The evolution toward managed services*. *Sun System News*. Retrieved June 25, 2008, from <http://sun.systemnews.com/articles/88/1/sev/14556>.
- Graves, G. (2005). The United States Navy Reserve component's account management challenge in a Navy and Marine Corps Intranet (NMCI) environment. Unpublished master's thesis, Naval Postgraduate School.
- Hoffman, M. (2007). *Waiting on NMCI*. Retrieved January 19, 2009, from http://www.marinecorpstimes.com/news/2007/12/marine_NMCI_071208w/.
- IBM (2007). *Fiducia enhances banks' responsiveness with IBM content management solution*. Retrieved June 25, 2008, from ftp://ftp.software.ibm.com/software/studies/Fiducia_G225_4309_01.pdf
- Institute of Electrical and Electronics Engineers, Inc. (2001). *IEEE 802.1X port-based network access control* (IEEE Specification). Retrieved June 25, 2008, from <http://standards.ieee.org/getieee802/download/802.1X-2001.pdf>
- Institute of Electrical and Electronics Engineers, Inc. (2003). *IEEE 802.11g specification amendment 4: Further higher data rate extension in the 2.4 GHz band*. (IEEE Specification). Retrieved June 25, 2008, from <http://standards.ieee.org/getieee802/download/802.11g-2003.pdf>

- Institute of Electrical and Electronics Engineers, Inc. (2004). *IEEE 802.11i specification amendment 6: Medium access control (MAC) security enhancements* (IEEE Specification). Retrieved June 25, 2008, from <http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>
- Internet Engineering Task Force (IETF) (2001). *Request for comment (RFC) 2764: A framework for IP based virtual private network*. Retrieved June 25, 2008, from <http://tools.ietf.org/html/rfc2764>.
- Jones, S. (2005). Toward an acceptable definition of service. *IEEE Software*, 22(3), 87-93.
- Koch, C. (2005, April 8). A new blueprint for the enterprise. *CIO Magazine*. Retrieved June 25, 2008, from <http://www.cio.com.au/index.php/id;1350140708;pp;1>.
- Linthicum, D. (2007, June 26). *Small firms take on big SaaS integration woes*. Retrieved June 25, 2008, from http://www.intelligententerprise.com/blog/archives/2007/06/smb_take_on_sa.html
- Macioce, G. E. (2007). *Managed services*. Retrieved May 4, 2008, from http://en.wikipedia.org/wiki/Managed_services.
- Managed Ethernet: Sherman ISD chooses Verizon's managed TLS service*. (2004). Retrieved June 25, 2008, from http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns465/net_customer_profile0900aecd802119b2.html
- Managed services in an IP world: New opportunities for wireless and wired networks 2006–2011*. (2006). Retrieved June 25, 2008, from <http://www.insight-corp.com/reports/manserv06.asp>
- Marks, M. (2006). *Managed services: Business efficiency and growth through infrastructure management solutions*. Retrieved June 25, 2008, from http://ca.com/files/WhitePapers/managed_srvcs_wp.pdf
- Marsan, C. (2006, September 27). Navy touts benefits of enterprise architecture for big IP nets. *Network World*. Retrieved June 25, 2008, from <http://www.networkworld.com/newsletters/isp/2006/0925isp1/html>
- McCafferty, D. (2006, May 10). State CIOs' wish lists include wireless, SOA. *Information Week*. Retrieved June 25, 2008, from <http://www.informationweek.com/showArticle.jhtml?articleID=187202130>.
- McCafferty, J. (2002, October). Talk, or walk? Whistle-blowing. *CFO Magazine*. Retrieved December 15, 2008, from <http://www.cfo.com/article.cfm/3006590>.

- Meredith, J., & Mantel, L. (2006). *Project Management: A Managerial Approach* (6th ed.). Hoboken, NJ: John Wiley and Sons.
- Miller, J. (2007a, September 28). *DISA sees managed services as the future*. Retrieved June 25, 2008, from <http://www.fcw.com/online/news/150272-1.html>
- Miller, J. (2007b, February 21). *Managed networks are the future*. Retrieved June 25, 2008, from http://www.gcn.com/online/vol1_no1/43191-1.html?topic=it_management.
- Mullen, M. (2006). *Sea power for a new era 2006: A program guide to the U.S. Navy*. Retrieved June 25, 2008, from <http://www.chinfo.navy.mil/navpalib/policy/seapower/spne06/top-spne06.html>
- Net Centric Enterprise Services. (2008). *Net centric enterprise services user guide*. Retrieved March 25, 2008, from <https://www.disa.mil/nces>.
- Newcomer, E., & Lomow, G. (2005). *Understanding SOA with Web services*. Upper Saddle River, NJ: Addison Wesley.
- Navy/Marine Corps Intranet Public Affairs (2005). *NMCI High-Speed Remote Access Delivery Begins*. Retrieved July 19, 2008 from <http://www.globalsecurity.org/military/library/news/2005/09/mil-050909-nns02.htm>
- NOP Research (2001). *Wireless LANs productivity and benefits: A research study*. Retrieved June 25, 2008, from http://newsroom.cisco.com/dlls/corp_111201b.html
- Onley, D. (2004). *Six degrees of worldwide integration*. Retrieved June 25, 2008, from http://www.gcn.com/print/23_25/27067-1.html
- Onley, D. (2005). *NMCI Survey finds most users satisfied with Portal*. Retrieved January 19, 2009 from <http://gcn.com/Articles/2005/03/29/NMCI-survey-finds-most-users-satisfied-with-portal.aspx>
- Padhye, S. (2004, February 11). *Managed services: The road to future profits*. Retrieved June 25, 2008, from http://telephonyonline.com/backoffice/infocus/telecom_managed_services_road/index.html
- Piarulli, V. (2004). *Naval WLAN overview from concept to acquisition*. Naval Wireless Network Summit SPAWAR/NETWARCOM.
- Prensky, M. (2005, June/July). *What can you learn from a cell phone? Almost anything! Innovate, 1(5)*. Retrieved June 25, 2008, from <http://www.innovateonline.info/index.php?view=article&id=83>.

- Rauch, J. (1996, August/September). *Eternal life: Why government programs won't die*. Retrieved June 14, 2008, from <http://www.reason.com/news/show/29984.html>
- Restructuring JTRS program reduces risk, but significant challenges remain. (2006, September). *GAO Report*.
- Richter, C. (2007). The evolution of managed security services: A virtual reality. *Information Systems Security*. Retrieved June 25, 2008, from http://www.infosectoday.com/Articles/Managed_Services.htm
- ROI case study Echopass Outrigger Hotels and Resorts*. (2006, July). Retrieved June 25, 2008, from http://www.echopass.com/g31_Echopass_ROI_case_study.pdf
- Roth, J. (2002). Enterprise Implementation of wireless technologies at the Naval Postgraduate School and other military educational institutions. Unpublished master's thesis, Naval Postgraduate School.
- Rozier, J. (2002). An analysis of current and proposed oversight processes for the acquisition of large-scale services as seen through the eyes of the Navy Marine Corps Intranet program. Unpublished master's thesis, Naval Postgraduate School.
- Sage Research (2001, May). *Wireless LANs: Improving productivity and quality of life*. Retrieved June 25, 2008, from http://newsroom.cisco.com/dlls/sage_report.pdf
- Schmeltzer, R. (2004). *SAIC SOA Case Study: The Navy Marine Corps Intranet*. Waltham, MA: Zapthink Press.
- Schuller, S. (2007, March 6) *Repealing the SaaS Tax*. Retrieved June 25, 2008, from http://itmanagement.earthweb.com/article.php/31771_3663266_2.
- Simpson, E. (2007, January). *An introduction to managed services*. American Institute of Certified Public Accountants. Retrieved December 12, 2008, from http://findarticles.com/p/articles/mi_hb5865/is_ai_n23807969.
- Sorenson, J. (2008, March). *Transforming to a Services-Orientated Enterprise*. Retrieved February 2, 2009, from <http://www.army.mil/CIOG6/briefings.html>
- Swanton, B. (2006, November 15). *B2B E-business: The murky evolution to managed service*. Retrieved June 25, 2008, from <http://www.amrresearch.com/Content/View.asp?pmillid=19891>.
- Tsai, W. T., Cao, Z., Wei, X., Paul, R., Huang, Q., & Sun, X. (2007, January). Modeling and simulation in service-oriented software development. *Simulation Transactions*, 83(1), 7-32.

- Use of commercial wireless local area network (WLAN) devices, systems, and technologies in the Department of Defense (DOD) Global Information Grid (GIG).* (2006). Assistant Secretary of Defense Office. Retrieved June 25, 2008, from <https://acc.dau.mil/CommunityBrowser.aspx?id=103529>.
- Vaughan-Nichols, S. J. (2006, October). Will the new wi-fi fly? *IEEE Computer*, 16-18. Retrieved June 25, 2008, from <http://csdl2.computer.org/comp/mags/co/2006/10/rx016.pdf>
- Walker, J. (2000). *Unsafe at any key size: An analysis of the WEP encapsulation*. IEEE Tech Report #03628E IEEE 802.11 Committee.
- WebSphere application server version 6.1: Advancing SOA for greater business flexibility.* (2006, April). Retrieved June 25, 2008, from ftp://ftp.software.ibm.com/software/webserver/appserv/v61/06_04_10_WebSphere_WP_Final.pdf
- Wetherbe, J. & Vitalari, N. (1994) *Systems Analysis and Design: Traditional Best Practices* (4th ed.). St. Paul, Minesota: West Publishing
- Whitten, J. & Bentley, L. (2005). *Systems analysis and design methods* (6th ed.). New York, NY: McGraw Hill.
- Wi-Fi Alliance (2007). *About the Alliance*. Retrieved June 25, 2008, from http://wi-fi.org/about_overview.php
- The Wi-Fi Navy? (2006, January 23). *Federal Computer Week*. Retrieved May 7, 2008, from http://www.fcw.com/print/12_2/news/92037-1.html
- Yang, H., Ricciato, F., Songwu, L., & Xhang, L. (2006). Securing a wireless world. *Proceedings of the IEEE*, 94(2), 442-453.
- Yin, R. (2003). *Case study research. Design and methods* (3rd ed.). Applied social research method series, vol. 5. Thousand Oaks, CA: Sage Publications.