NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DEPLOYABLE COMBAT SIMULATIONS VIA WIRELESS ARCHITECTURES

by

Jeffrey S. Lock Sr.

March 2004

Thesis Advisor: Rudolph Darken
Thesis Co-Advisor: Joseph Sullivan

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

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

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

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: **Deployable Combat Simulation Via Wireless Architectures**	**5. FUNDING NUMBERS**
6. AUTHOR(S) Jeffery S. Lock, Sr.	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

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

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

13. ABSTRACT ***(maximum 200 words)***

This thesis details the critical need for deployable combat simulations for training in today's surge force environment. To truly realize deployment of these simulations on Naval vessels and in remote theaters, simulations for training must be wireless. Wireless standards 802.11/a/b/g are presented in detail to highlight the strengths and weaknesses of each. This thesis then investigates the viability of deploying combat simulations for training using wireless devices. To this end, the Joint Semi-Automated Forces (JSAF), combat simulation model and the Virtual Helicopter (VEHELO) training simulation entity are tested in an 802.11a wireless environment against the VEHELO application in a wired environment. 802.11a is proposed as part of an overall solution to deploy combat simulations for training. This is primarily because of its high data rates and ability to co-locate access points without interference. Testing reveals that operating JSAF and Virtual Helicopter via the High Level Architecture (HLA) with User Datagram Protocol (UDP) packets in an 802.11a environment provides ample bandwidth with which to deploy combat simulation for training for the simulations conducted.

14. SUBJECT TERMS JSAF, HLA, RTI, Wireless, Simulation, Training, VEHELO, UDP,	**15. NUMBER OF PAGES** 97
	16. PRICE CODE

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

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DEPLOYABLE COMBAT SIMULATIONS VIA WIRELESS ARCHITECTURES

Jeffrey S. Lock Sr.
Lieutenant, United States Navy
B.S., Hawaii Pacific University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
March 2004

Author: Jeffrey S. Lock Sr.

Approved by: Dr. Rudolph Darken
Thesis Advisor

CDR Joseph Sullivan
Co-Advisor

Dr. Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis details the critical need for deployable combat simulations for training in today's surge force environment. To truly realize deployment of these simulations on Naval vessels and in remote theaters, simulations for training must be wireless. Wireless standards 802.11/a/b/g are presented in detail to highlight the strengths and weaknesses of each. This thesis then investigates the viability of deploying combat simulations for training using wireless devices. To this end, the Joint Semi-Automated Forces (JSAF), combat simulation model and the Virtual Helicopter (VEHELO) training simulation entity are tested in an 802.11a wireless environment against the VEHELO application in a wired environment. 802.11a is proposed as part of an overall solution to deploy combat simulations for training. This is primarily because of its high data rates and ability to co-locate access points without interference. Testing reveals that operating JSAF and Virtual Helicopter via the High Level Architecture (HLA) with User Datagram Protocol (UDP) packets in an 802.11a environment provides ample bandwidth with which to deploy combat simulation for training for the simulations conducted.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION 1
A. PROBLEM STATEMENT 1
B. APPROACH 2
C. THESIS ORGANIZATION 2

II. REQUIREMENTS FOR TRAINING 3
A. PROPOSED REQUIREMENTS 3
B. SIMULATED COMBAT ENTITIES 3

III. FUTURE OF SIMULATION FOR TRAINING 7
A. INTEROPERABILITY 7
B. INCREASING COST OF LIVE TRAINING 9
C. SIMULATION SCALABILITY 10
D. DEPLOYING LARGE SCALE SIMULATIONS 12
E. LEVERAGING WIRELESS TECHNOLOGY 14

IV. OVERVIEW OF 802.11 WIRELESS TECHNOLOGIES 15
A. 82.11 FAMILY 15
1. 802.11 16
2. 802.11b 17
a. Frequency 17
b. Throughput 21
3. 802.11a 23
a. Frequency 23
b. Throughput 26
4. 802.11g 28
a. Frequency 28
b. Throughput 28
B. 802.11 RANGES 29
C. SUMMARY 32

V. MODELS, TOOLS, AND PROTOCOLS 33
A. MODELS AND APPLICATIONS 33
B. NETWORK ARCHITECTURE 36
C. TESTING TOOLS 39
1. AirMagnet Laptop Trio a/b/g 39
2. Solar Winds Professional Edition 41
3. Windows Performance Logs 44
4. Runtime Infrastructure Parser 44
5. Ethereal 45
D. SECURITY 46

VI. JOINT SEMI-AUTOMATED FORCES TESTING 49
A. JSAF COMMUNICATIONS 49

B. PRE-TESTING SURVEY 51
C. ARCHITECTURE 53
D. BACKGROUND NETWORK TRAFFIC 53
E. BANDWIDTH TESTING 55
1. 87 Entity Static Test 56
2. 87 Entity Dynamic Test 65

VII. CONCLUSION 73
A. GENERAL DISCUSSION 73
B. CONTRIBUTIONS 75
C. FUTURE WORK 76
1. Continued Testing of JSAF and VEHELO 76
a. Increasing the Number of Wireless Entities 76
b. Categorically Different Entity Testing .. 77
c. Entity Increases at JSAF 77
2. Modifications to the RTI for Wireless Clients 77
3. Layered Wireless Architectures 78

LIST OF REFERENCES 79

INITIAL DISTRIBUTION LIST 81

LIST OF FIGURES

Figure 1. Range of M&S Embraced by the DoD M&S Vision (From: Ref 1) 8
Figure 2. Historical Government Outlays as percent of GDP 9
Figure 3. Graphic illustration of ISM and U-NII bands. 16
Figure 4. High Rate PHY channel plan. (From: Ref 7) 18
Figure 5. 802.11b channels showing overlap. 19
Figure 6. Maximum non overlapping channels in 802.11b. 20
Figure 7. Three Access Points collocated on three different channels with 802.11b. 22
Figure 8. 802.11a 5 GHz frequencies. 24
Figure 9. 802.11a channel breakout (From: Ref 10) 25
Figure 10.802.11a 5GHz Frequency Scheme (From: Ref 10) 26
Figure 11.OFDM breakdown of 802.11a channel.(From: Ref 10) ..27
Figure 12.Signal Loss Chart 30
Figure 13.Data Link Rate vs. Indoor Range. (From: Ref 11) ...31
Figure 14.Throughput comparison of 802.11a vs 802.11b (From: Ref 11) 32
Figure 15.JSAF screen capture with entities 34
Figure 16.VEHELO screen capture 36
Figure 17.Evaluation architecture 37
Figure 18.Screen capture of AirMagnet Laptop Trio a/b/g 40
Figure 19.Sample SNMP Management Information Base walk results. 42
Figure 20.Hewlett Packard processor use monitor. 43
Figure 21.Panasonic Toughbook processor use monitor. 44
Figure 22.Ethereal screen capture. 46
Figure 23.Internet Group Management Protocol packet. 50
Figure 24.RX protocol packet capture by Ethereal. 51
Figure 25.Air Magnet Survey. 52
Figure 26.Architecture setup with IP addresses shown. 53
Figure 27.HP idle network UDP traffic. 54
Figure 28.Panasonic idle network UDP traffic. 55
Figure 29.Static 87 Entity scenario. 56
Figure 30.Panasonic 87 entity average bps. 57
Figure 31.HP 87 entity average bps. 57
Figure 32.JSAF 87 entity average bps. 58
Figure 33.Panasonic packets received per/s. 60
Figure 34.Panasonic packets sent per/s. 60
Figure 35.Panasonic combined sent and received packets/s. ...61
Figure 36.HP packets received per/s. 61
Figure 37.HP packets sent per/s. 62
Figure 38.HP combined sent and received packets/s. 62

Figure 39.AirMagnet capture during 87 entity static. simulation. 64
Figure 40.87 entity dynamic scenario capture. 65
Figure 41.Panasonic average bps. 66
Figure 42.HP average bps. 66
Figure 43.JSAF average bps. 67
Figure 44.Panasonic packets send per/s. 68
Figure 45.Panasonic packets received per/s. 68
Figure 46.HP packets sent per/s. 69
Figure 47.HP packets received per/s. 69
Figure 48.Wireless versus wired bps. 71

LIST OF TABLES

Table 1. Panasonic and HP packets sent and received per second. 59
Table 2. Wireless versus wired bps. 63
Table 3. Packets sent and received per second. 67
Table 4. Wireless versus wired bps. 70

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my wife Angie and my children, Jeffrey and Justin for being infinitely supportive of my efforts in completing this thesis. I would also like to extend my sincere gratitude for the guidance and education afforded me in completing this thesis by my advisors, Dr. Rudy Darken and CDR Joseph Sullivan.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

Deployable simulations for training are large, wired, systems, which limit the scope of their employability. These trainers allow warriors to hone their skills in some remote theaters and, to some extent, onboard ships. However, training is normally limited to a small number of troops. There are a couple of reasons that these trainers limit the number of troops that can be trained at any one time. First, the systems are deployed in self-contained units that limit the space available to the trainer. Second, systems that aren't self-contained are wired via the Ethernet. Both of these factors reduce the scalability, and training opportunities for the warrior.

Because these systems limit the number of personnel that can be simultaneously trained, they are more costly on an individual training basis and don't afford entire units the ability to conduct combat simulation training as unit. Also, because they are wired, they are not particularly scalable in many operational environments that our forces operate in today, whether it is on ship or on foreign soil.

This thesis will test bandwidth use of a current large-scale combat simulation model. The Joint Semi-Automated Forces (JSAF) model will be evaluated running with wired and wireless simulation entities. This will allow for future simulation and modeling developers to incorporate into their application and interface designs the notion of wireless simulation for training.

B. APPROACH

This thesis begins the process of evaluating the feasibility of deploying combat simulations for training, in whole or in part, via wireless technologies. To do this, wireless technologies are presented, identifying the strengths and weaknesses of current 802.11 technologies. Then, a current wireless technology is selected on which to conduct bandwidth use evaluation. This wireless evaluation will then be compared to wired simulation bandwidth, to begin to determine the feasibility of deploying combat simulations for training in a wireless environment, from a bandwidth perspective.

C. THESIS ORGANIZATION

This thesis is organized in the following chapters:

- Chapter I: Introduction. The problem statement is presented along with an overview of work.
- Chapter II: Requirements For Training: Presents a realistic scenario of the needs for training in a current environment.
- Chapter III: Future Of Simulation For Training. Looks at how we arrived at our current simulation training environment and discusses future needs.
- Chapter IV: Overview of 802.11 Wireless Technologies. Describes the general technology with strengths and weaknesses of each.
- Chapter V: Models, Tools, And Protocols. Presents the models used, the tools, and the communication protocol for JSAF.
- Chapter VI: Joint Semi-Automated Forces Testing. Details the pre-test survey, the architecture used and testing conducted.
- Chapter VII: Conclusion. Contributions and conclusions based on this thesis work are presented, along with proposed future work in the area of wireless simulation for training.

II. REQUIREMENTS FOR TRAINING

A. PROPOSED REQUIREMENTS

This chapter will explore a probable requirement for training that can give some scope and other guidance for deploying wireless combat simulations for training. An environment where wireless combat simulation for training is envisioned as needed and exists today is aboard naval vessels. Specifically, amphibious ships transiting to either a familiar or unfamiliar Amphibious Objective Area (AOA).

Prior to an Amphibious Ready Group (ARG) arriving in an AOA, it will be at sea for long periods of time. During this time, troops could be training in a virtual environment that is built to simulate where they intend to go ashore. The immense value of this advance in training could prove invaluable for our troops.

B. SIMULATED COMBAT ENTITIES

The forces that a Marine Air Ground Task Force (MAGTF) would go ashore against can vary greatly. For instance, if a MAGTF were going ashore against a capable force with significant combat power in the form of tanks, other armored vehicles, and aircraft, the MAGTF would want greater ratio. In this scenario the number of red forces would be significantly less than the number of blue entities. A MAGTF could also be deployed ashore against rebel factions, who have limited combat power, but may have a larger number of personnel. To scope the number of entities a probable scenario might have, a situation that

has a MAGTF deploying ashore against a force, which is capable, and has combat power is presented.

A MAGTF could deploy with 400 tracked or wheeled vehicles. Total personnel strength could be 3,000. Of these 3,000 personnel, a significant number would be assigned to aircraft maintenance and other logistics related duties. The total number of blue entities that would need to be represented would be significantly less than 3,000. This is because maintenance and logistics personnel wouldn't necessarily need to be represented and the pilots would be in their aircraft and the vehicle operators would be their vehicles. A reasonable number of blue entities would be 2,000, based on the above conditions.

Red forces, with combat power and ability on par with ours, that need to be represented in this scenario would be significantly less than the blue numbers. This is because a desirable ratio of blue to red forces in this situation would be 3:1. In these conditions, a conservative estimate would be 1000 red entities.

Given the likelihood of a MAGTF operating in an urban environment, in today's world, it is prudent to include some number of civilian entities. However, it is also reasonable to assume that if two combat units are engaged in battle, enormous numbers of civilians will not be in the middle of the battle. Of course, a scenario could be envisioned where a force is using civilians as a human shield. But, for our probable scenario, we can assume 100 civilians are one the periphery of the engagement.

In our scenario, we have established that 3100 entities would be a reasonable number to represent. Of these 3,100, 1,100 would be represented by a server with entities added to the simulation. The blue forces would typically be embarked in one of three amphibious ships in the ARG. The ARG is typically made up of an Amphibious Helicopter Assault (LHA) ship or Amphibious Helicopter Dock (LHD) ship, a Landing Platform Dock (LSD) ship, and a Dock Landing Ship (LSD). The LHA and LHD are significantly larger than the LPD and LSD. A reasonable scenario would be, 900 troops embarked in the LHA would need to join the scenario and 550 troops embarked on each of the LSD and LPD would need to join the scenario.

This chapter has presented a probable scenario that could be generated in JSAF. It also gives some scope to the possible number of blue and red entities that would need to be represented in either JSAF or by wireless clients running simulation entity applications, such as VEHELO.

THIS PAGE INTENTIONALLY LEFT BLANK

III. FUTURE OF SIMULATION FOR TRAINING

A. INTEROPERABILITY

Traditionally, individual services determined a need for a product and commenced to developing systems without taking into account the desire or need to work with other services or other systems within their service. Interoperability is and will continue to be a critical element for any program or project within DoD. Simulations for training must take this into account, if they are to flourish. To this end, for Modeling and Simulation (M&S), through the Undersecretary of Defense for Acquisition, Technology & Logistics (USD(AT&L)), the DoD stood up the Defense Modeling and Simulation Office (DMSO) in 1991. Specifically, “The DMSO supports the warfighter by leading a defense-wide team in fostering the interoperability, reuse, and affordability of M&S and the responsive application of these tools to provide revolutionary warfighting capabilities and improve aspects of DoD operations.” [Ref 1]

To ensure interoperability, DMSO, through the DoD Modeling and Simulation Master Plan, mandated the initial definition of the High Level Architecture (HLA) for simulation interoperability. The 1996 Master plan delineated the baseline definition of HLA. This action effectively put an end to individual services creating stovepipe projects that were limited in scope and use.[Ref 2]

The Secretary of Defense stresses, in his April 2003 Transformation Planning Guide, the importance of

interoperability.[Ref 3] Figure 1 indicates the breadth and depth of DoD's M&S commitment to inter-service interoperability.

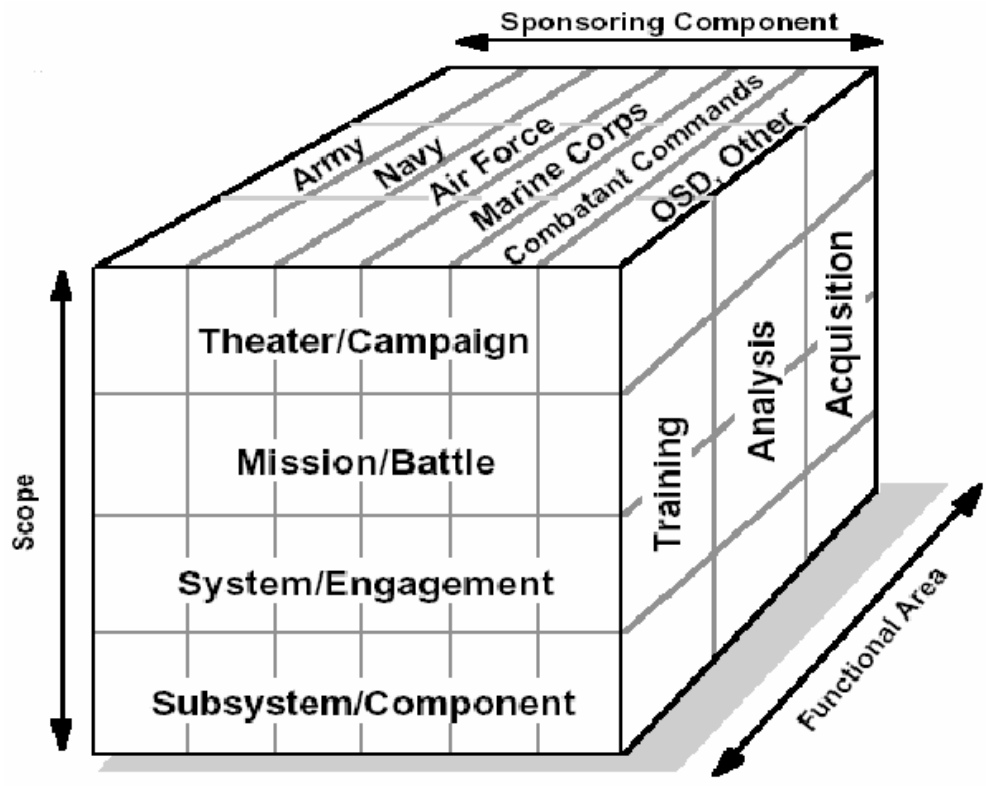

Figure 1. Range of M&S Embraced by the DoD M&S Vision (From: Ref 1)

Outside of the obvious reasons for designing systems based on interoperability, such as, increased flexibility and better return on investment of every M&S dollar spent, it is the right thing to do with the tax payer's money. Through DMSO, DoD has made a commitment to eliminating stove pipe programs that cost too much and do too little and whose useful lives are shortened without interoperability built into the program.

B. INCREASING COST OF LIVE TRAINING

The portion of the Gross Domestic Product (GDP) that is allocated to the DoD has been decreasing since World War II. All indications are that this trend is going to continue. Figure 2 shows this trend over the last forty years.

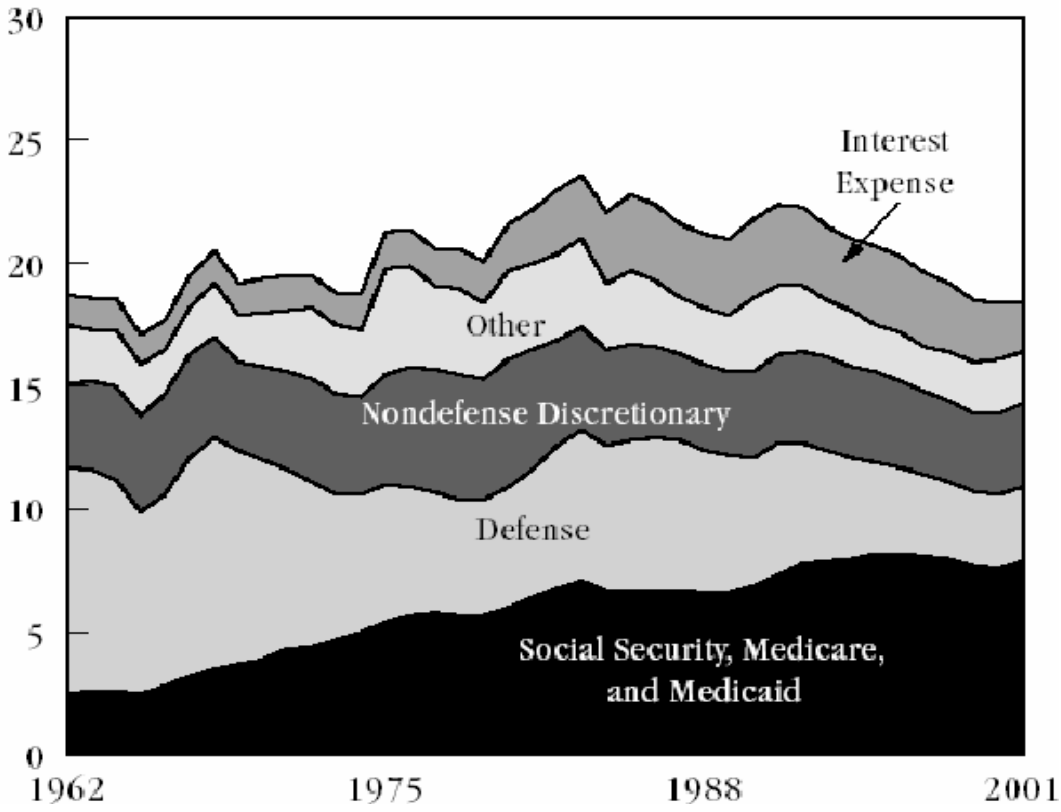

Figure 2. Historical Government Outlays as percent of GDP (From: Ref 4)

With the current and forecast budget deficits the United States is facing, along with the increases in Social Security, Medicare, and Medicaid funding trends, the percentage of GDP allocated to the military is likely to continue to shrink. This means less money to train our forces.

The cost of training personnel in large or small numbers is expensive. Whether training is focused on tank crews or pilots, it may be reduced or eliminated due to budget cuts or operational commitments. Fuel is expensive, military member's time is not cheap and the logistics for affecting real world training continues to increase in cost.

Another cost that cannot be overlooked is the number of lives that are lost during real world training. Families need to be assured that when they send their sons and daughters to defend the country that the DoD is doing everything in its power to keep them safe. This means that any and all methods that allow service members to efficiently and effectively train, while reducing the numbers of lives lost due to training mishaps, need to be exploited.

The increasing costs of live training in terms of dollars as well as the potential for loss of life are in part why we need to use simulations for training. It is generally accepted that simulations can and do allow a significant level of proficiency with a greatly reduced level of overhead costs. This is not to imply that simulations will nor that they should replace all live training

C. SIMULATION SCALABILITY

Simulation scalability is a significant feature that is needed to train large units of combatants in order to mimic the size of forces that trainee's need operate in. This means it is desirable to have a company, for instance, all involved in a battle simulation together in order to realize increased operational proficiency as a unit. Even

greater than a single ground company operating as a unit in a simulation, other units from the MAGTF could be conducting a simulated beach landing with the craft master of a Landing Craft Air Cushioned (LCAC), while pilots simulate taking troops in via helicopter and Osprey.

The number of entities (players in a simulation) is going to quickly become significantly large. In order satisfy the capability of placing all or as many units into a simulation as possible the system architecture must be scalable. Scalable, not only from a software stand point where the system needs to host a significant number of entities, but from a connectivity standpoint. It is not feasible to physically connect very large numbers of combatants in a ship board environment. Ship’s do not have enough space to accommodate all the current needs for cabling let alone the additional requirements that would come from wiring a large-scale simulation system.

Ships are not the only environments where there is a need for large scale deployable simulations. These other environments will also be constrained by space available for simulation devices and the infrastructure that supports them. For a system to be considered deployable it must take into account the number of entities allowable, the physical size of the simulation devices and the architecture which will be used to connect the devices. If a system is designed without all three of these elements in mind, it most likely will not meet the needs of the deployed environment.

D. DEPLOYING LARGE SCALE SIMULATIONS

Small and large scale simulators are becoming more prevalent in all aspects of DoD training. This trend will only continue. However, these simulators are, in general limited to large devices that were designed to be immobile. The lack of mobility can either be due to the shear size of the simulator itself or the need to be hard wired into an Ethernet backbone or a combination of the two. Because of the lack of deployable trainers, when a unit completes workups for deployment, whether they are shipping out to a crisis area or as part of a scheduled deployment cycle, their skills begin to degrade as soon as the schoolhouse or field training ends.

A better illustration of this dilemma is with the case of a MAGTF, which deploys aboard ships in an ARG. Typically the MEU will begin training for a deployment a year before they are scheduled to deploy. Just before deployment, everyone in the unit has an opportunity, in a 30 day window, to take leave. During this 30 day period, last minute administrative and logistics issues are being overcome. This means that people are on leave or conducting non-training work for the last 30 days before a deployment.

After the ARG and MEU deploy, it may take up to 45 days to reach the objective. This equates to 75 days that have elapsed from the time large-scale, unit level combat training was conducted. This can significantly reduce the effectiveness of a combat unit.

This dilemma is not experienced by ground forces alone. Aviation units can also experience the same training voids, just before and during the transit to the

objective area, when deploying with an ARG. In general, when aviation units fly while an ARG is transiting to the objective area, they are working on keeping their flight qualifications from lapsing. With little exception, they get almost no combat flight training while en route to the Amphibious Objective Area (AOA).

It is desirable to have these units arrive as soon as possible and in the best possible fighting condition. In the foreseeable future, we are not going to be able to get these forces to the objective area any sooner than we currently do. Simulation training, that reinforces traditional training, which units have undergone in the workup cycle, is the vision for keeping warfighters proficient during these training voids.

Currently, the CNO is sponsoring one such program that is designed to maintain unit and individual proficiency for Marines when on ship en route to an Objective Area. Deployable Virtual Training Environment (DVTE) is a laptop based simulation, with a wired backbone, that allows Marines to select their respective combat vehicles, weapons and leadership position before joining an ongoing battle simulation. This simulation enables Marines to maintain a high level of combat proficiency, regardless of a ship’s transit time or operating environment.

While deploying simulations is a significant benefit to marines and aviators while ships are underway, their benefits can be realized by a much larger audience. Air Force and Army units can conduct an infinite range of training on deployable devices that can be networked together to simulate real world environments. However, there is a significant technological advantage that has yet

to be leveraged to improve the flexibility and benefits provided by deployable simulation systems.

E. LEVERAGING WIRELESS TECHNOLOGY

Using wireless technology to interconnect simulation devices is the best solution for deploying a significant number of devices in the confined space of a naval vessel as well as other space limited operational environments. With a wireless broadband infrastructure for running simulations, a significant number of combatants can be placed in a confined space without being tethered to a bird’s nest of wire, umbilical cords. Even better, these combatants can be in their vehicles in the vehicle storage decks of an amphibious ship with their simulation devices participating in battle scenarios. Aviators can be inside of their aircraft in the hanger bay, also participating in the battle scenario; for instance, conducting Close Air Support (CAS) for the same ground troops that are in the vehicle storage areas, in the simulation from their vehicles.

Training is moving away from the brick and mortar, inflexible icons of the cold war era and into a training environment that allows service members to receive the right training, anytime, and in any place. In order to make these training devices truly deployable we have to move away from wired infrastructures and into the wireless realm. This move will allow simulations to accommodate large numbers of entities within the current environments that many deploying units are subject to.

IV. OVERVIEW OF 802.11 WIRELESS TECHNOLOGIES

A. 82.11 FAMILY

The 802.11 family consists of 802.11, 802.11b, 802.11a, 802.11g, and they share characteristics. However, as these standards have evolved they have taken on distinctly different characteristics, which make some more suitable for specific applications than others. Below is an overview of some of the more significant characteristics of each and how this affects their application domains.

Most notably, some of the 802.11 family members share the same frequency space. The entire spectrum used by the 802.11 family is contained in the bands established by the Federal Communications Commission (FCC) in 1997 and 1999. Beyond the sharing of frequencies is where the differentiation in the technologies is most prevalent.

A significant issue that should be mentioned at this point is that bandwidth in all of the current 802.11 technologies is somewhat deceiving. As with all networking technologies, there is management overhead, this translates to reduced bandwidth. The bandwidth reduction occurs, because a portion of the bandwidth is taken up by management packets as well as sending and receiving headers that are added. Some technologies have higher overhead than others. 802.11 technologies can realize up to 50 percent of the advertised throughput, as actual data throughput.

The operating frequencies for all 802.11 family technologies are contained in one of two unlicensed bands. The Industrial, Scientific, and Medical (ISM) Band and the Unlicensed National Information Infrastructure Band (U-

NII). [Ref 5] In these bands manufacturers and users can develop and use equipment without having to pay licensing fees to the FCC. This is contrary to how the FCC typically allocates frequency space. Generally speaking, frequency space is licensed to users at relatively high cost. The exact location of the ISM and U-NII bands in the radio frequency spectrum are shown in Figure 3.

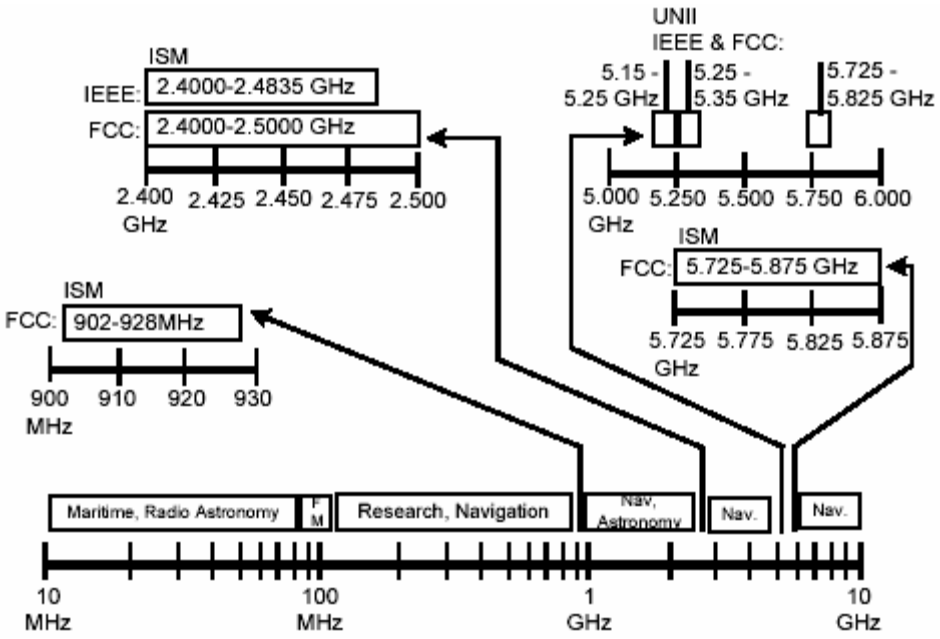

Figure 3. Graphic illustration of ISM and U-NII bands. Used with permission of PLANET3 WIRELESS, INC. (From: Ref 8)

1. 802.11

802.11 was the first in the family of 802.11 technologies to be promulgated by the International Electrical and Electronic Engineers Standards Board (IEEE). [Ref 6] The original designation for this standard was 802.1 but was later changed to 802.11. The need for IEEE to develop the standard became a necessity when the equipment being developed for use in this spectrum turned out to be proprietary, with no interoperability features.

The original 802.11 was only able to realize a relatively low bandwidth of 1 or 2 Mbps. The different bandwidths were achieved by using either Frequency-Hopping Spread Spectrum (FHSS) or Direct Sequence Spread Spectrum (DSSS) technologies. FHSS was limited to 1 Mbps while DSSS could operate at 1 or 2 Mbps. [Ref 6]

It is a useful exercise to divulge the original 802.11 standard and its capabilities. However, because it will not be a technology explored for use in deployable combat simulations due to its low bandwidth we will move onto the next generation of 802.11 technologies.

2. 802.11b

802.11a has not been skipped, the 802.11a standard was being developed before 802.11b, however, 802.11a took slightly longer to get to market, due to technology difficulties. 802.11b is currently the most popular of the 802.11 family.

a. Frequency

The Frequency Plan for 802.11b is depicted below in Figure 4. As shown, the FCC has authorized the use of 11 channels in the United States. Of the 11 channels shown, an access point (AP) will generally operate on only one at any given time. The ISM band used for 802.11b is typically referred to as the 2.4 GHz band.

		Regulatory domains						
CHNL_ID	Frequency (MHz)	X'10' FCC	X'20' IC	X'30' ETSI	X'31' Spain	X'32 France	X'40' Japan	X'41' Japan
1	2412	X	X	X	—	—	—	X
2	2417	X	X	X	—	—	—	X
3	2422	X	X	X	—	—	—	X
4	2427	X	X	X	—	—	—	X
5	2432	X	X	X	—	—	—	X
6	2437	X	X	X	—	—	—	X
7	2442	X	X	X	—	—	—	X
8	2447	X	X	X	—	—	—	X
9	2452	X	X	X	—	—	—	X
10	2457	X	X	X	X	X	—	X
11	2462	X	X	X	X	X	—	X
12	2467	—	—	X	—	X	—	X
13	2472	—	—	X	—	X	—	X
14	2484	—	—	—	—	—	X	—

Figure 4. High Rate PHY channel plan. (From: Ref 7)

1. Overlapping Channels. The 802.11b frequency plan for the United States is not without concerns. Of the 11 channels the FCC has established for use in the US, only three of them can be used simultaneously in close proximity. This is due to the fact that there is a significant amount of overlap in the 2.4 GHz channel plan. Figure 5 shows the 11 channels used for 802.11b in the middle ISM band and their significant overlap.

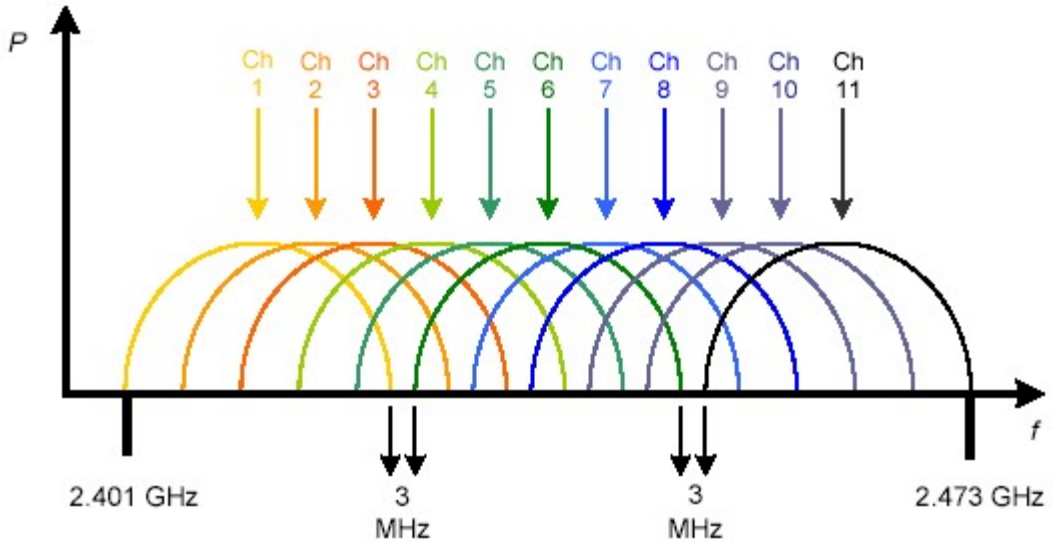

Figure 5. 802.11b channels showing overlap.
Used with permission of PLANET3 WIRELESS, INC. (From: Ref 8)

Figure 6 below shows the maximum number of channels that can be used simultaneously without causing interference with other channels, in the same proximity. These channels are 1, 6, and 11. Other channels can be used without interference; however, these schemes would be limited to two channels. For instance, channels 5 and 10 could be used in the same space without interference, but this would reduce the bandwidth available versus using channels 1, 6, and 11.

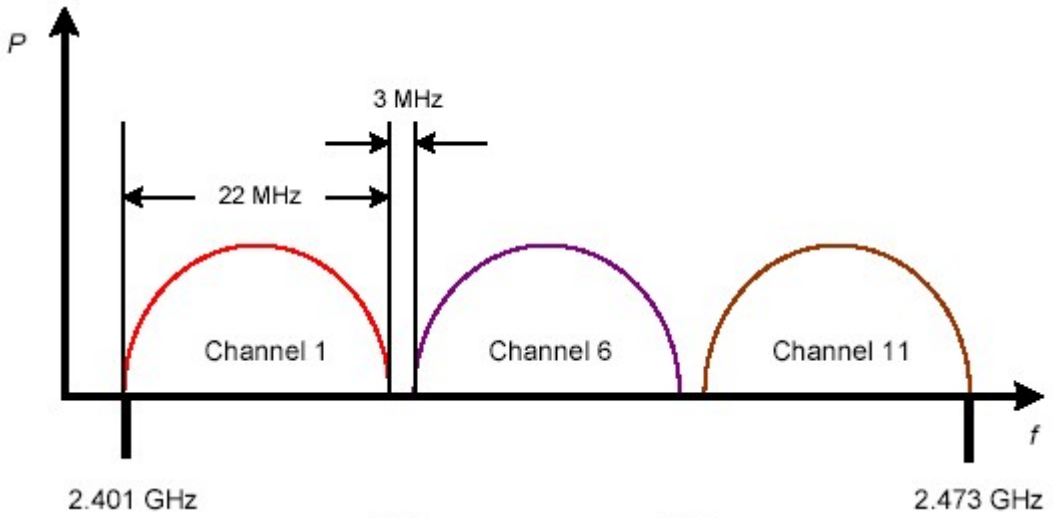

Figure 6. Maximum non overlapping channels in 802.11b.
Used with permission of PLANET3 WIRELESS, INC. (From: Ref 8)

While interference from competing channels in the 802.11b frequency spectrum is a concern, there are also other interference concerns for this spectrum. Microwaves operate in the 2.4 GHz range and will cause significant loss of throughput if used in the proximity of an 802.11b network. Also, cordless phones that operate in the 2.4 GHz range will cause interference in an 802.11b environment. As time goes on, this may be a greater source of interference because 2.4 GHz cordless phones deliver significantly greater performance than previous technologies and are therefore becoming very popular.

Another source of interference for 802.11b technologies can be experienced when systems using FHSS and DSSS are used in proximity. FHSS systems can dominate the DSSS systems if they both are using the same radio space. This will restrict the DSSS system from unfettered access to the 2.4 GHz spectrum, in effect, reducing the throughput of a DSSS system to a very low level or zero.

b. Throughput

Earlier we mentioned that the throughput of any networked system is reduced by the amount of bandwidth taken by the network management protocol that controls the system. This management loss, when subtracted from the bandwidth given, in general, will give the overall throughput characteristics of a system.

802.11b is designed to operate at 4 different levels of throughput, 1, 2, 5.5, and 11 Mbps. As mentioned earlier, this is the maximum theoretical throughput. The actual throughput of user data will be roughly 50 percent of the maximum theoretical throughput due to the control overhead.

For the purpose of deploying combat simulations for training, we are interested in the throughput of a system of wireless access points. This is because we believe that in order to get a large number of entities, who are collocated, training in the same simulation we will need a significant level of system throughput.

When we take the system characteristics of 802.11b technology we can arrive at different schemes for antenna location, which will drive the amount of system throughput that we can expect. For instance, if we were interested in training a rifle company, in the confines of a classroom aboard a ship, using 802.11b technology, we would be able to simultaneously operate on three channels. Figure 7 below indicates the setup and the system throughput we could expect.

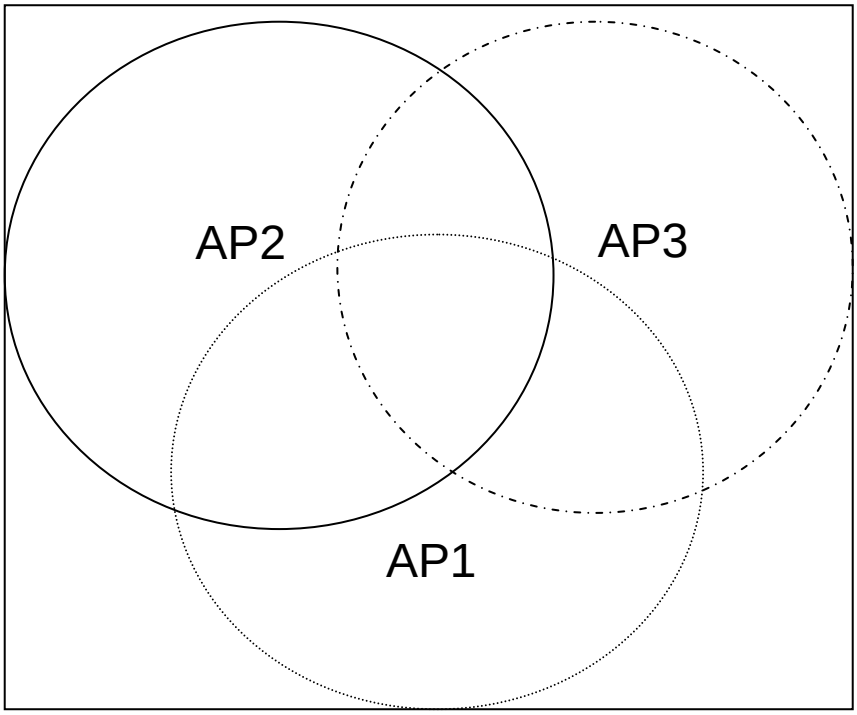

Figure 7. Three Access Points collocated on three different channels with 802.11b.

The throughput of this system would be:

11 Mbps x 3 = 33 Mbps

While the throughput of user data would be:

33 Mbps/2 = 16.5 Mbps.

Figure 7 is to give a rough idea of a hypothetical configuration and is not meant to represent the actual radio propagation of each of the different channels. The range of 802.11b allows one channel to cover all practical classrooms.

At 16.5 Mbps second in the above scenario a number of users could effectively access the medium with relatively good results, for general administrative or internet access work. However, when running simulations, it is anticipated that relatively large throughput

requirements per user will be required to effectively depict the combat environment.

With the limitation of three access points collocated in the 802.11b scheme, we would be severely restricted in our ability to run simulations with larger numbers of entities. This may preclude the use of 802.11b for combat simulations for training in confined spaces.

3. 802.11a

As mentioned earlier, 802.11a is a technology that was being developed prior to 802.11b, however, there were technology difficulties which caused it to arrive at market after 802.11b.

802.11a uses a different frequency than 802.11b. In part, due to the different frequency, it is not compatible with 802.11b. In general 802.11a technology is slightly more expensive today than 802.11b because it does not have the market share that 802.11b enjoys. 802.11a prices are expected to fall to 802.11b levels because; in many ways it is a superior product.

a. Frequency

802.11a operates in the 5 GHz frequency range. Its spectrum is in the U-NII band and is broken up into non-congruent bands. The lower band is broken into two separate bands. The lower half of the lower band is designated for indoor use only due to its possible interference with mobile-satellite service (MSS) and the upper band is allocated for outdoor use. [Ref 9]

Figure 8 below, indicates the locations of the U-NII band in the 5 GHz range, authorized for use by 802.11a technologies.

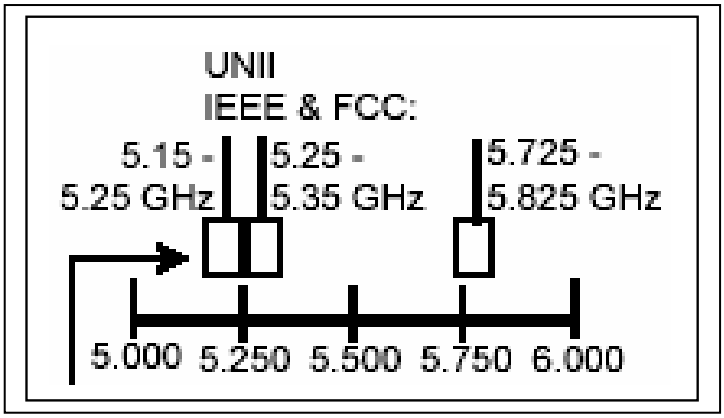

Figure 8. 802.11a 5 GHz frequencies.
Used with permission of PLANET3 WIRELESS, INC. (From: Ref 8)

1. 802.11a Channels. Each of the three distinct bands for use by 802.11a technologies are further broken down into channels. Each band is separated into 4 channels. This allows for a total of 12 channels, 8 of which can be used simultaneously indoors. Figure 9 below depicts the breakout of the channels in the three different bands.

Regulatory domain	Band (GHz)	Operating channel numbers	Channel center frequencies (MHz)
United States	U-NII lower band (5.15–5.25)	36 40 44 48	5180 5200 5220 5240
United States	U-NII middle band (5.25–5.35)	52 56 60 64	5260 5280 5300 5320
United States	U-NII upper band (5.725–5.825)	149 153 157 161	5745 5765 5785 5805

Figure 9. 802.11a channel breakout (From: Ref 10)

2. Non-overlapping Channels. The most significant advantage of 802.11a technology over the other 802 technologies is that the frequency plan does not have channels that overlap. This is significant when compared to the maximum allowable channels in the 802.11 and 11b schemes, which allow a maximum of 3 non-overlapping channels. Figure 10 below depicts the non-overlapping scheme of the 802.11a channelization.

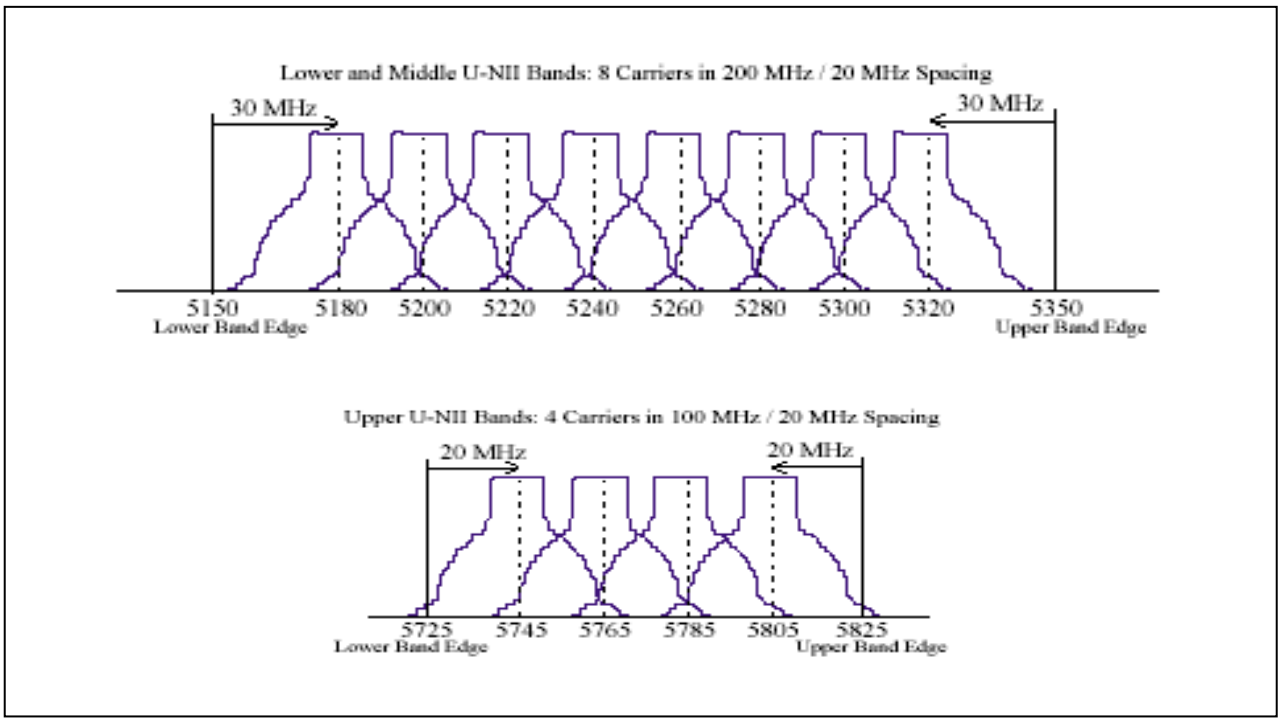

Figure 10. 802.11a 5GHz Frequency Scheme (From: Ref 10)

b. Throughput

802.11a realizes throughput of up to 54 Mbps, per access point, which is per channel. This significantly greater throughput per channel is realized though modulation techniques that differ from 802.11 and 802.11b. The 802.11a standard indicates that 802.11a equipment will operate at 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. Of these, the IEEE standard indicates that operating rates of 6, 12, and 24 Mbps are mandatory. [Ref 10]

802.11a technology leverages modulation techniques that use a combination of Binary Phase Shift Keying (BPSK) and Orthogonal Frequency Division Multiplexing (OFDM) to realize a data link rate of 54 Mbps. Figure 11 below graphically depicts how OFDM breaks down each channel's frequency into 52 distinct subcarriers. Of

these 52 subcarriers, 48 carry data and the remaining 4 are pilot subcarriers. By breaking each channel down into 52 distinct subcarriers, which can be filled with data, 802.11a can realize data rates of up to 54 Mbps. [Ref 10]

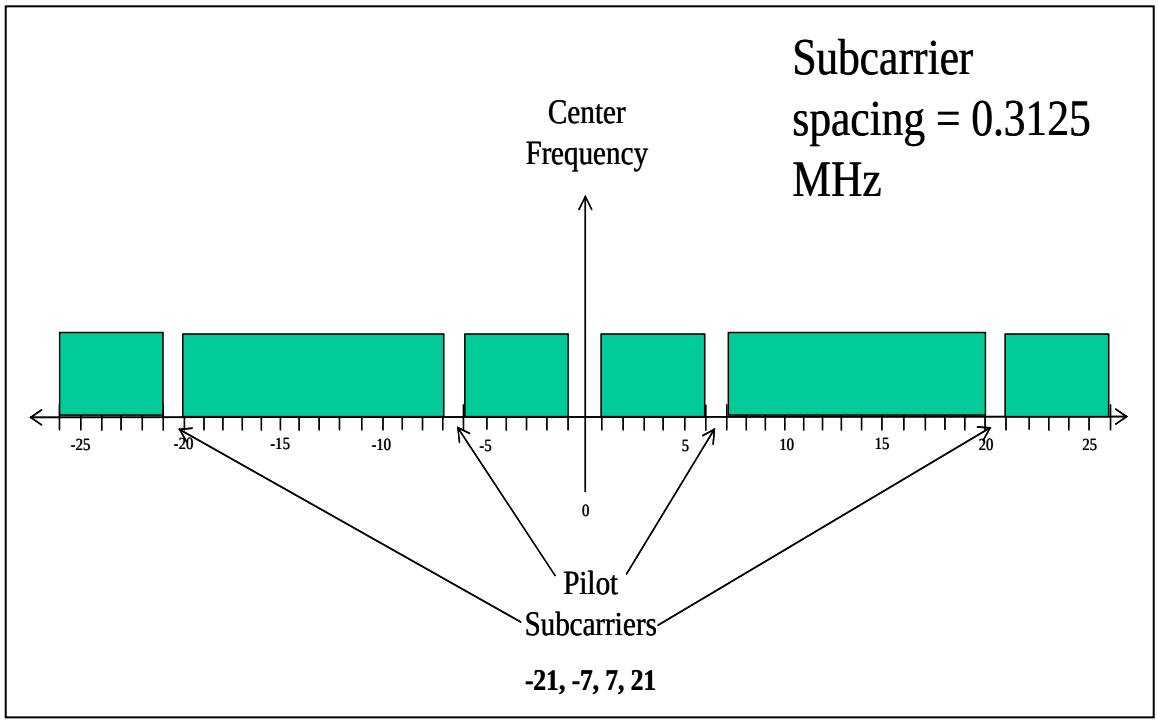

Figure 11. OFDM breakdown of 802.11a channel.(From: Ref 10)

There are manufacturers that have developed and are selling 802.11a equipment that is advertised at a rate of 108 Mbps per channel. However, we are not introducing this proprietary technology as a possible solution for deploying combat simulations for training, due to the risks of implementing a system using proprietary technologies.

Because the 802.11a channels do not overlap, a system could be designed that allows for 8 APs to be collocated, indoors, without interference. With 8 APs collocated, all operating at 54 Mbps, a single classroom,

for instance could realize a system throughput of 432 Mbps. Taking into account the management overhead, the user throughput could be 216 Mbps.

When compared to 802.11 and 802.11b technologies for throughput in a confined space, 802.11a realizes over 13 times the user throughput of 802.11b and over 72 times the user throughput of 802.11.

4. 802.11g

802.11g is a technology that improves on the 802.11b technology by using some modulation techniques used in 802.11a. A significant feature of 802.11g technology is it is designed to be backwards compatible with 802.11b devices. This means that 802.11g access points can operate with 802.11b radio cards and 802.11b access points can operate with 802.11g radio cards. It is worth noting that this is a feature that is not designed into the 802.11a specification.

a. Frequency

The frequency plan for 802.11g is the exact same as that used for 802.11b and 802.11. This means that if 802.11g and 802.11 or 802.11b devices are to be used in the same radio space, channel deconfliction will have to occur. Not more than one device in the three of these technologies can be operated on the same channel simultaneously.

b. Throughput

Earlier it was mentioned that the 802.11g technology builds on the 802.11b architecture and that it used some modulation techniques of 802.11a. Throughput is where this combining of technologies shows up.

The maximum system throughput of three collocated APs increases from 33 Mbps with 802.11b to 162 Mbps using

802.11g. The actual user throughput would be at approximately 81 Mbps or 50 percent of the overall throughput, when taking into account management bandwidth overhead.

When compared to 802.11 and 802.11b this throughput is significantly greater. However, the throughput of collocated APs in an 802.11a environment is still 2.7 times greater than 802.11g technology, 216 Mbps versus 81 Mbps. Again, this is due to the overlapping channel issue, in the 2 GHz ISM frequency band.

B. 802.11 RANGES

802.11 range is being broken out here so as not to be redundant with range issues as they pertain to the 802.11 families because there are only two distinctions between ranges in this family.

The two distinctions are the ranges achieved by the 2 GHz technologies versus the ranges achieved by the 5 GHz technology and the throughput achieved at different ranges.

The range of the 802.11 family of technologies in the 2 and 5 GHz frequency spectrums is affected by objects that are encountered in the operating environment. If they operate in an outdoor environment, greater ranges would be experienced, versus operating inside an office environment. The expected ranges for indoor operating environments can also vary based on the materials the signal is transiting through. Figure 12 shows the loss associated with different types of material that may be encountered by 802.11 frequencies.

Obstruction	Additional Loss (dB)	Effective Range
Open Space	0	100%
Window (non-metallic tint)	3	70
Window (metallic tint)	5-8	50
Light wall (dry wall)	5-8	50
Medium wall (wood)	10	30
Heavy wall (6" solid core)	15-20	15
Very heavy wall (12" solid core)	20-25	10
Floor/ceiling (solid core)	15-20	15
Floor/ceiling (heavy solid core)	20-25	10

Figure 12. Signal Loss Chart
Used with permission from PLANET3 WIRELESS, INC. (From: Ref 8)

The loss of signal strength results in a loss of user throughput. To get and idea of the relative throughput versus range in a typical office environment, Atheros Communications conducted live tests. For this particular test they were comparing popular 802.11a and 802.11b equipment in a typical office environment.

Figure 13 gives an idea of the dynamic frequency changes that occur in 802.11 environments, when signal strength increases or decreases. It also shows the results of Atheros' test of 802.11a versus 802.11b data link rate versus distance from the sources.

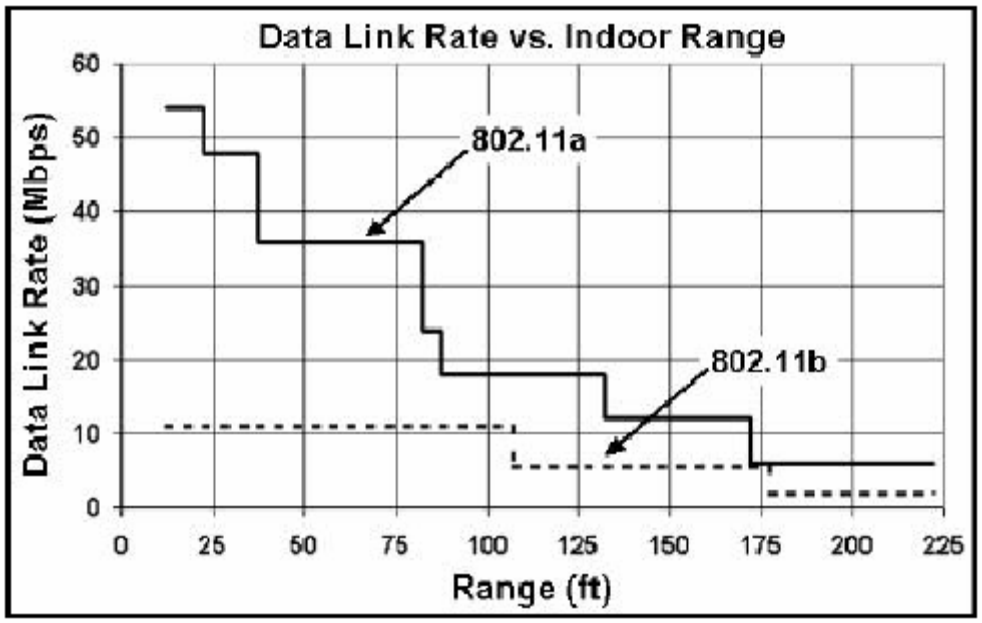

Figure 13. Data Link Rate vs. Indoor Range. (From: Ref 11)

Figure 14 shows throughput at the different ranges for 802.11a and 802.11b. Atheros conducted this test using a packet size of 1500 bytes. The results of their test indicate, that out to 225 feet in a typical office environment, 802.11a technology will deliver greater throughput, when compared to 802.11b. The throughput, as indicated by Atheros' test, also shows that 802.11a ranges from 2 to 4.5 times higher than that of 802.11b. This data link rate advantage is per AP and would have to be multiplied by the number of collocated APs in order to get the system throughput for a confined space. The data link rate of 802.11g would be expected to be equal to or be greater than 802.11a.

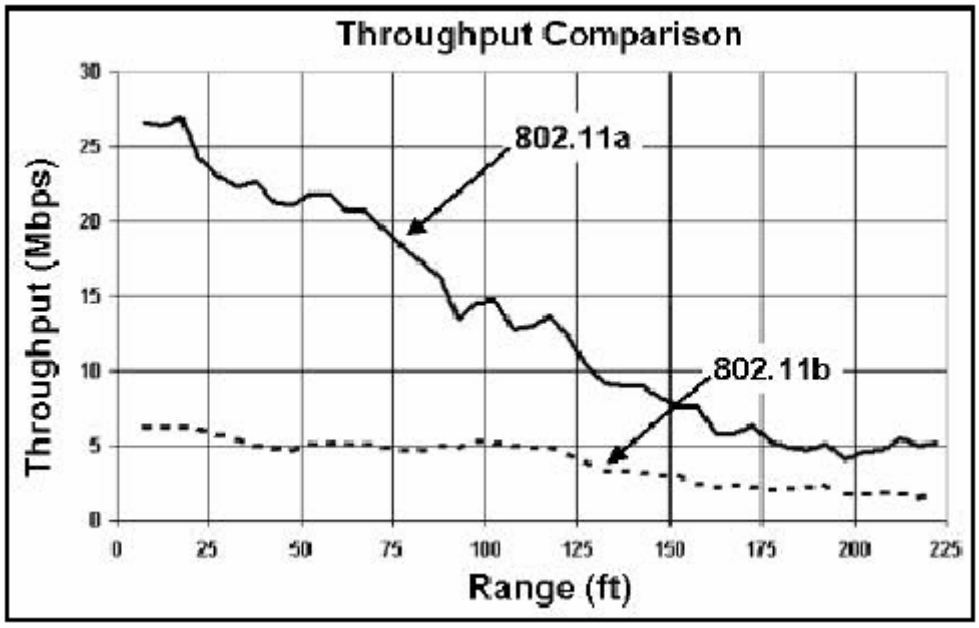

Figure 14. Throughput comparison of 802.11a vs 802.11b (From: Ref 11)

The throughput per system of collocated APs with 802.11a technology will still be significantly greater than 802.11b due to the limitation of having three 2.4 GHz APs collocated.

C. SUMMARY

802.11a offers the greatest throughput of the wireless standards discussed when considering a system of access points. 802.11g advertised data link rate and throughput are significantly greater than 802.11b. System throughput for 802.11b and 802.11g is hampered by operating in the 2.4 GHz ISM band. 802.11a, 802.1b, and 802.11g all have strengths and weaknesses. It is envisioned that a wireless implementation of deployable combat simulations could use one or more of these technologies to maximize wireless' strengths and minimize its weaknesses.

V. MODELS, TOOLS, AND PROTOCOLS

A. MODELS AND APPLICATIONS

To evaluate the potential bandwidth use of a large scale combat simulation model, Joint Semi-Automated Forces (JSAF) model will be used. "JSAF is a Modeling and Simulation system that generates entity level platforms, interactions, and behaviors in a Synthetic Natural Environment (SNE). JSAF is used in support of joint command and staff training, mission rehearsal and other DoD simulation requirements. JSAF started out as a Defense Advanced Research Projects Agency (DARPA) Advanced Concept Technology Demonstration (ACTD) formerly called Synthetic Theater of War (STOW) and has evolved into a mature M&S tool used by the U.S. Joint Forces Command J9 Experimentation and Engineering Lab in Suffolk VA. It was recently used in Millennium Challenge 02 with outstanding results and has been distributed to numerous foreign countries." [Ref 12]

Figure 15 shows a screen capture of JSAF with a Camp Lejune, South Carolina scenario with miscellaneous entities present. For testing purposes JSAF version 5.26 is being used. This is not the newest version of JSAF, however, it is stable and was used as the interoperability standard for the Office of Navy Research's (ONR) Virtual Technologies and Environments (VIRTE).

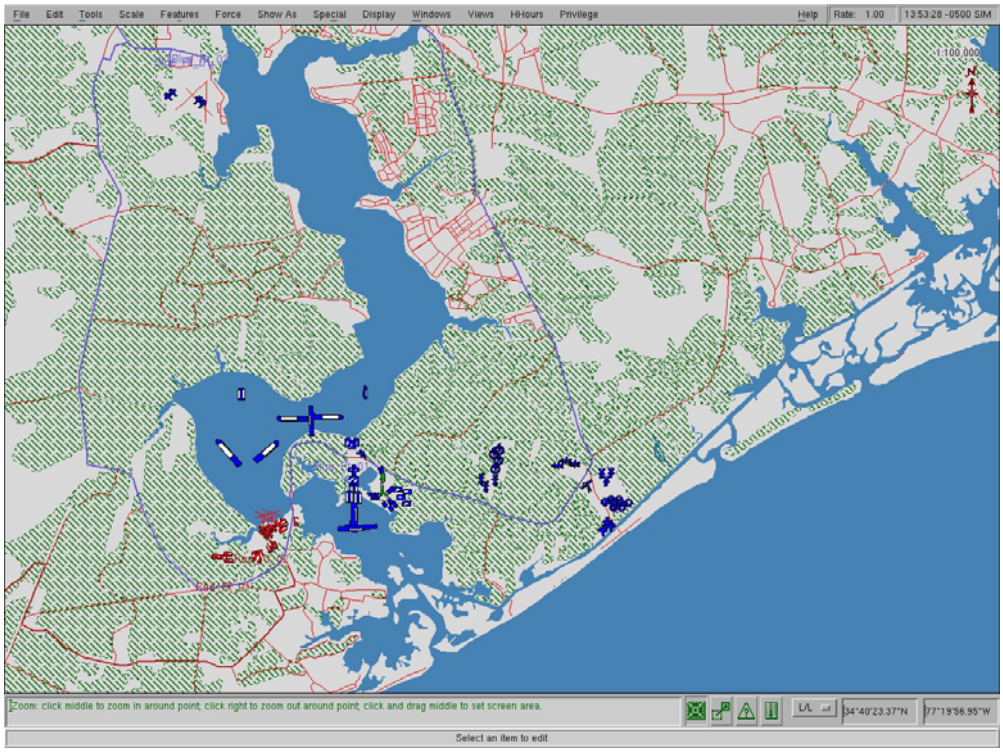

Figure 15. JSAF screen capture with entities

JSAF is built to operate with the DMSO's mandated High Level Architecture (HLA) standard. "The High Level Architecture for simulations is a DOD-wide initiative to provide architecture to support interoperability and reuse of simulations. The HLA is part of the DOD common technical framework for simulations as required in Objective 1 of the DOD Modeling and Simulation Master Plan.

The Department of the Navy's overarching goal for the implementation of the HLA, is to enhance modeling and simulation (M&S) capabilities while making best use of current and future investment." [Refs 1, 13]

Our version of JSAF uses Runtime Infrastructure-s version 1.3 D3 (RTI-s version 1.3 D3) which is implemented in accordance with HLA. The RTI-s is what allows JSAF to communicate with other, appropriate simulation models via

a network or the Internet. If a simulation application is interested in joining a JSAF simulation it must also be using the exact same version of RTI. The RTI acts as a translator and without the correct version, an entity application or other JSAF server will not be able to join a simulation.

To evaluate the bandwidth used by JSAF and the RTI-s, an entity or another JSAF server is required. The Virtual Helicopter (VEHELO) application is the entity vehicle with which we will test JSAF environment throughput. VEHELO is a simulation application designed to run on a Windows machine, using the exact same interface used by our version of JSAF. Figure 16 below is a screen capture of VEHELO running on one of our test machines. Incidentally, the helicopter in the background is from another machine also running the VEHELO application.

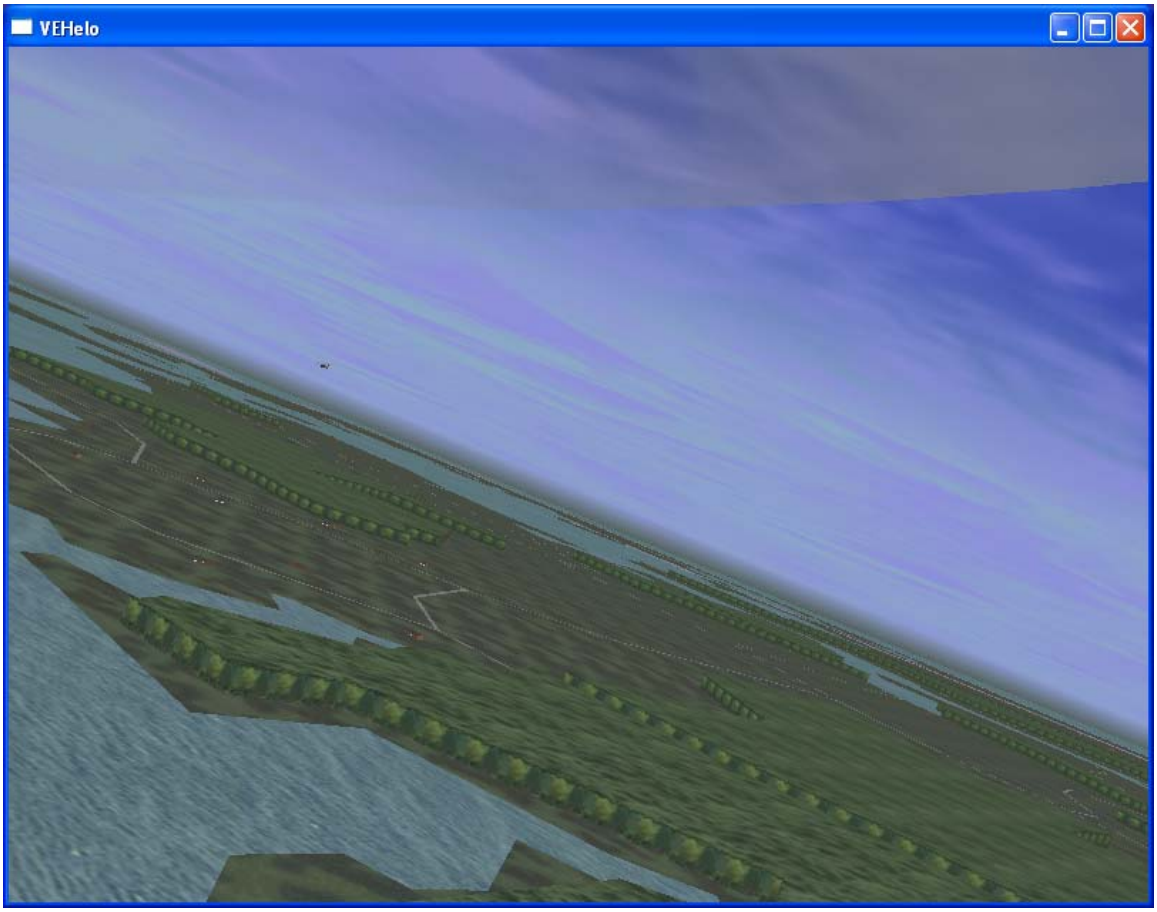

Figure 16. VEHELO screen capture

The VEHELO application was developed by a number of organizations, including Lockheed Martin and the Naval Postgraduate School. The graphics are generated by Vega, a commercial graphics engine.

B. NETWORK ARCHITECTURE

The network architecture used to evaluate JSAF and VEHELO was arrived at based on the decision to use existing equipment possessed by the research group. The goal was to get an early understanding of JSAF and VEHELO requirements to establish future needs for appropriate testing and deployment architectures.

The architecture consisted of the JSAF server running on a PC connected via cat 5 to a 4 port hub. To the hub we

also connected a laptop used for gathering data. The hub was then connected to a 4 port gigabit switch. Also connected to the switch were an access point controller (APC), an access point (AP), and a wired laptop running the VEHELO application.

Figure 17 is a graphic depiction of the above described architecture. The following lists describe the components used.

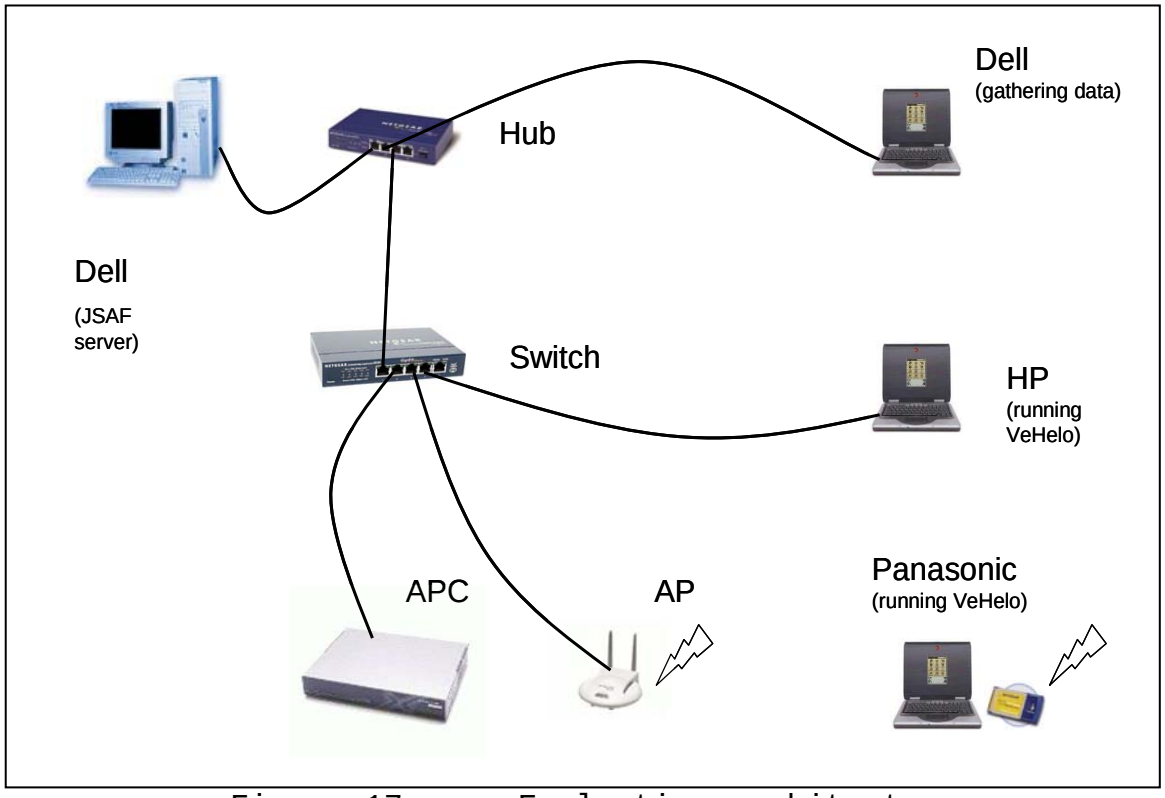

Figure 17. Evaluation architecture

JSAF Server

Dell Dimension 4100
OS: Redhat 7.3 with a 2.4 kernel
Processor: Intel P-1 1.6GHz
Ram: 256 MB
NIC: 3 Com Corporation 3c905c 10/100 Network Interface

Wired VEHELO

Hewlett Packard
OS: Microsoft Windows XP Professional version 2002
Processor: Pentium VI 2.2 GHz
Ram: 1.00 GB
Video Card: Mobility M6 with 32MB of RAM
NIC: National Semi-Conductor Corp DP83815 10/100

Wireless VEHELO

Panasonic Toughbook
OS: Microsoft Windows XP Professional version 2002
Processor: Intel Pentium M 1400 MHz
Ram: 768 MB
Video Card: Mobility Radeon 9000 with 64MB of RAM
NIC: NetGear Dual Band Wireless Adapter WAB501
2.4GHz and 5GHz 802.11a/b

Hub

NetGear 10/100 base-tx Fast Ethernet Hub
Model FE104

Switch

NetGear 4 port 100/1000 Gigabit Switch
Model GS504T

Access Point Controller

Proxim Harmony Access Point Controller
Model 7560

Access Point

Proxim Harmony Access Point

The Proxim access point controller exists on a network and is designed to manage up to 10 access points. A network manager interfaces with the access point controller and the access point through a network pc using their web

browser. The PC used to gather the data, as the figure indicates, is Dell C840 and is tethered to the hub.

C. TESTING TOOLS

A number of different tools designed to analyze network traffic were evaluated to try and establish which would work best for our research. Of the many tested, 4 were selected. Below is a description of each along with some of their limitations, which were discovered in our particular test environment.

1. AirMagnet Laptop Trio a/b/g

AirMagnet Laptop trio is capable of scanning all 802.11a/b/g channels. However, we were only interested in capturing packets on channel 36, the lowest channel in the 802.11a, 5GHz, lower U-NII band as indicated in Chapter VI. AirMagnet does have the ability to allow only one channel to be continuously scanned. AirMagnet can capture all packets it receives on all scanned channels and give specific details about access points and infrastructure. This information can be saved to capture files for later analysis.

Figure 18 below is a screen capture of the one of the many panes available for viewing Wireless Local Area Networks (WLAN) management and traffic analysis information.

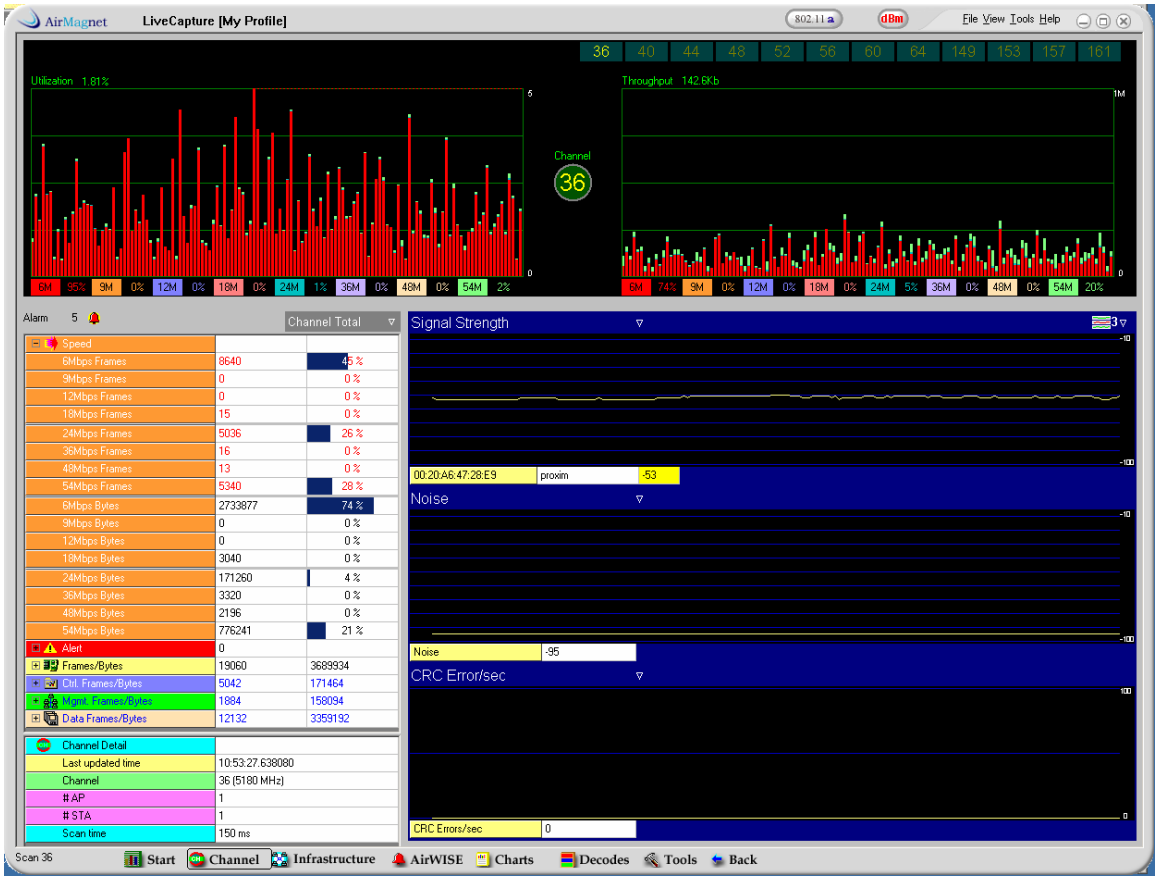

Figure 18. Screen capture of AirMagnet Laptop Trio a/b/g

In working with AirMagnet Laptop Trio a/b/g, a couple of issues occurred with the product that made data analysis somewhat difficult and held up testing were discovered. The first issue was that multicast packets were not recognized as such when sent from our wireless VEHELO laptop. This was only discovered after packet-by-packet analysis between this and other tools, when multicast packet totals weren't matching but data packets totals were. Second, the original AirMagnet NetGear wireless card sent with the product became problematic and ultimately stopped working causing the manufacturer to have to send a replacement.

2. Solar Winds Professional Edition

Solar winds products allow for a relatively robust array of network monitoring, analysis, and management tools. Most of Solar Winds tools rely heavily on Simple Network Management Protocol (SNMP) and its Management Information Base (MIB) calls. SNMP is typically disabled on newer computers and has to be manually started. This is primarily for security, because SNMP version 1 was shipped with a default password of “public” and if shipped in an enabled status, hackers could cause security issues through buffer overflow attacks. Also, with version 1, if a default password was changed, it didn’t help all that much because when passwords were sent across the network they were in the clear. SNMP version II has some security features, such as hashing passwords before sending them. Simply put, SNMP queries a host using User Datagram Protocol (UDP) packets for information from MIB tables that hosts dump information to. This information includes, but is not limited to things such as system information and network data.

Figure 19 below is a sample SNMP MIB walk that one can get using Solar Winds if the host IP address is known along with the SNMP password. MIB tables can have thousands of possible queries. Some table information is static; however, other information, such as network statistics, is dynamically updated and can be queried once or repeatedly. Dynamic updates and repeated queries are what allow Solar Winds to update information in real time.

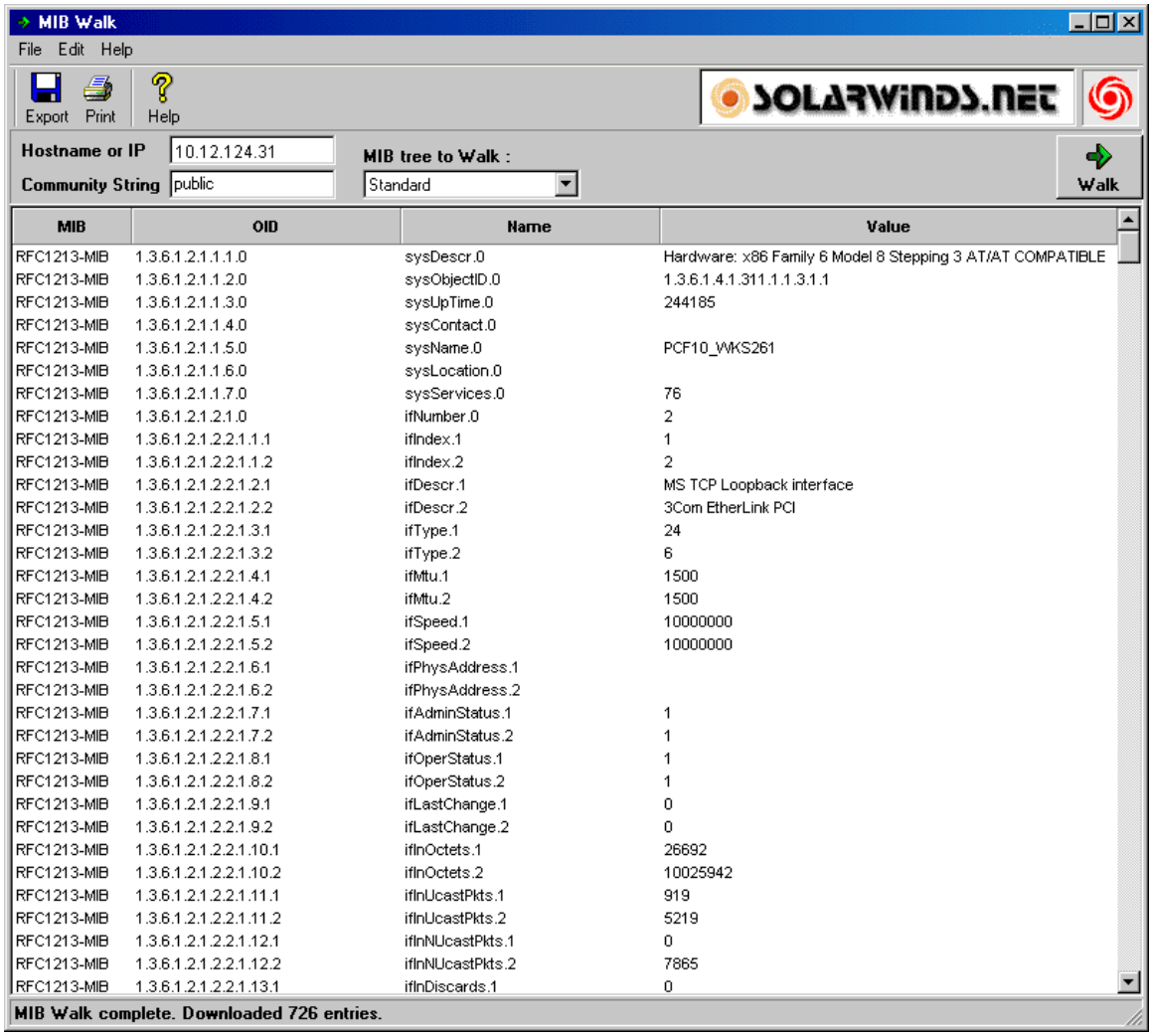

Figure 19. Sample SNMP Management Information Base walk results.

Solar Winds proved to be a very reliable tool for many things. However, charts will be presented later that were created using Performance Monitor and almost without fail there is a gap in the graphed data. This is possibly due to the fact that all three processors were working relatively hard to execute the scenarios and when Solar Winds queried for the information, the host refused the

request. Figures 20 and 21 are screen captures of the processor monitors on the two VEHELO laptops during the simulations.

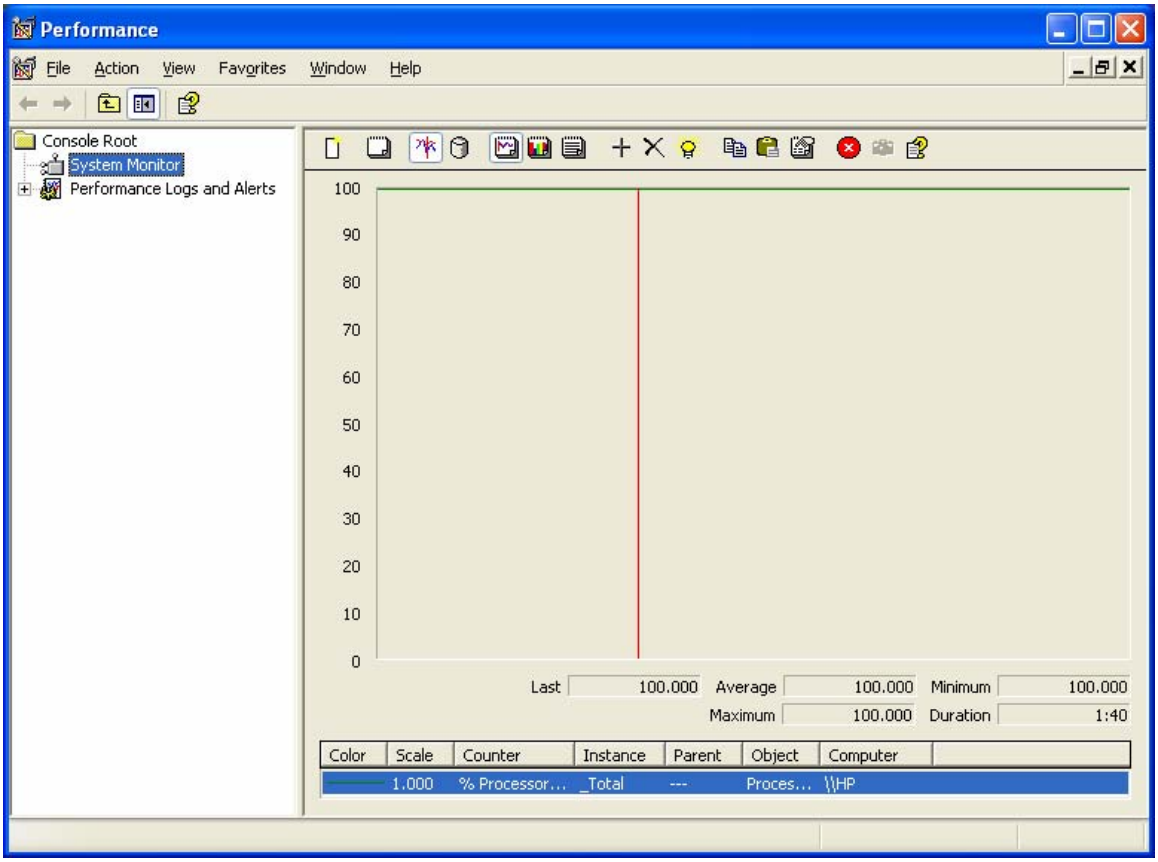

Figure 20. Hewlett Packard processor use monitor.

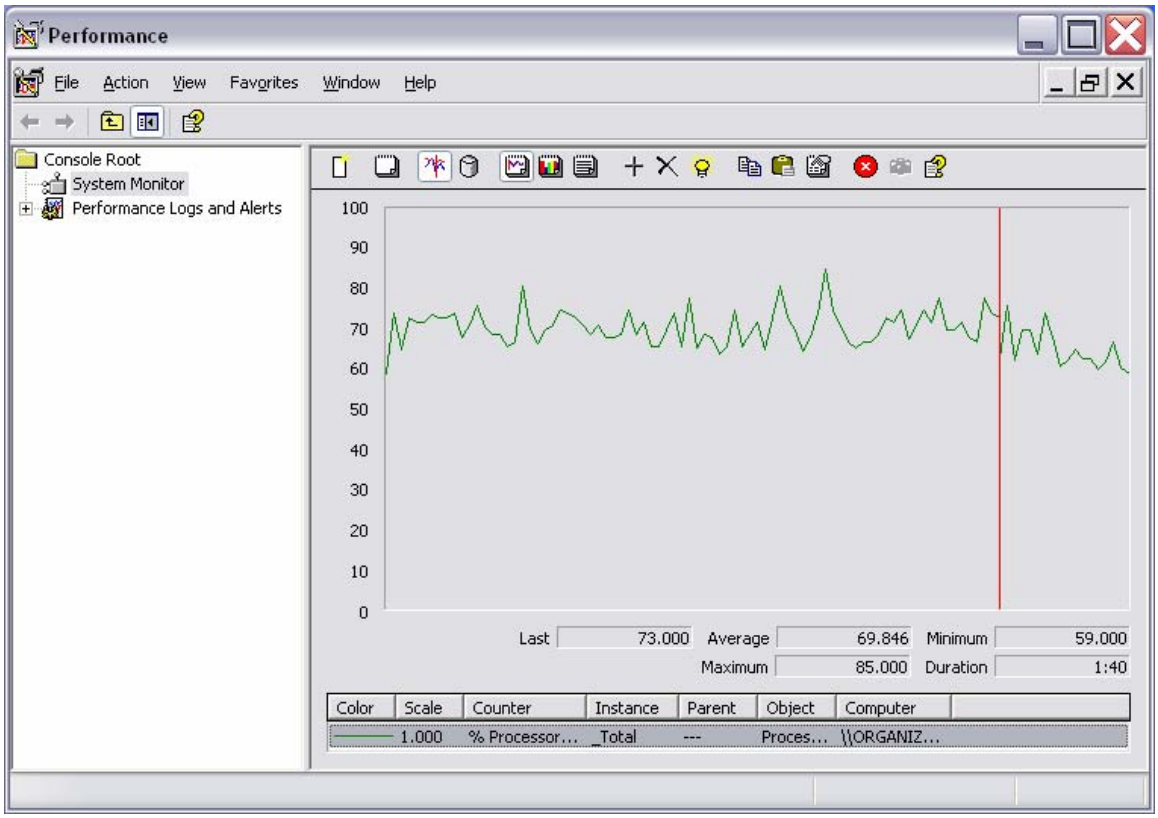

Figure 21. Panasonic Toughbook processor use monitor.

3. Windows Performance Logs

Microsoft Windows XP professional, along with previous version of Windows, are delivered with the ability to log a myriad of system events. These events or statistics can be logged at intervals as small as 1 second. On both VEHELO laptops, Windows performance monitors were used to gather data. Windows performance logs worked well and could be saved as text, comma delimited files which could then be dumped into Microsoft Excel.

4. Runtime Infrastructure Parser

The version of RTI-s we used during our simulation testing has a built in parser that allows the retrieval of information from the RTI. In particular, the number of UDP multicast packets sent and received, “streams sent” and

“received” (which correlate to the different multicast addresses information is being sent and received on), and the number of object (entity) “updates” and “receives”. Unfortunately the version of the parser on JSAF and the version on the VEHELO machines has to be the same and in the version we have, RTI-s 1.3 D3, the parser was not compatible with Windows.

5. Ethereal

Ethereal is a free tool that was developed in 1998 by Gerald Coombs to track down network problems. It is an extremely powerful tool that can detect and analyze a staggering array of network protocols, on all major platforms. The tool is now maintained and upgraded by a core of twelve people. The code is open source and fixes, recommendations, and new code are developed regularly by users groups. [Ref 14]

Figure 22 shows a screen capture, which is very typical of the information displayed by Ethereal during any packet capture event. In the first pane, packets scroll up as they are received. If a particular packet is selected in the top pane, its layers are depicted in the second pane. The third pane is the hexadecimal representation of the specific bytes of each protocol.

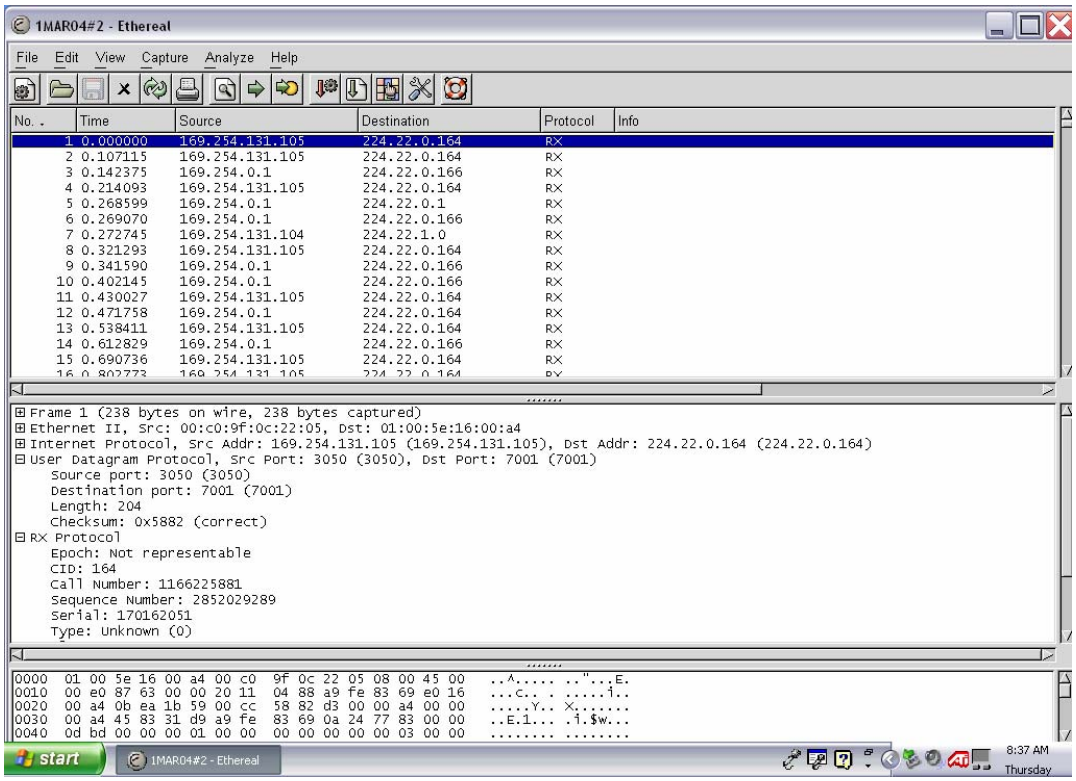

Figure 22. Ethereal screen capture.

By comparison, Ethereal worked extremely well, particularly, when evaluated against non-free tools. One possible problem that was detected with Ethereal in our case was that it would detect multicast packets, when not in promiscuous mode, when we had no multicast application running that had subscribed to said packets. This could have been due to IP physical and logical routing tables at lower levels, not being updating when multicast groups are joined or released.

D. SECURITY

Networked systems of computers have security concerns that must be taken into consideration during design and certainly before deployment. Wireless security issues are perhaps more prominent because data, control, and management frames are conveyed through air. To mitigate

the security threat of wireless environments, encryption of wireless communications is considered essential. Encryption will add some measurable amount of overhead to wireless operations. While determining overhead associated with encrypting wireless communications is not the focus of this thesis, it is a concern.

The Naval Postgraduate School has a group which is conducting some preliminary testing of Harris Corporation's, Secure Wireless Local Area Network (SecNet 11) equipment for 802.11b technologies. This technology uses National Security Agency, Type I approved crypto for classified and unclassified information transfer. In the following months, data should be available that will provide some metrics that indicate the amount of added overhead due to encrypting wireless communications.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. JOINT SEMI-AUTOMATED FORCES TESTING

A. JSAF COMMUNICATIONS

JSAF communicates with other JSAF servers or simulation entities using UDP multicast. UDP multicast is managed on the Internet or larger networks using Internet Group Management Protocol (IGMP). Multicast addresses are class D addresses and are between 224.0.0.0 and 239.255.255.255.[Ref 15] In order for multicasting to work effectively, routers in a network or Internet have to be multicast enabled and running IGMP. IGMP prevents multicast producers from flooding the Internet or network with packets by, only establishing traffic routes for those applications that ask for it. This is especially true for IGMP version 3, which further reduces multicast related traffic while getting all subscribers the traffic they are interested in.[Ref 16] JSAF version 5.26 uses IGMP version 2. This is most likely because the global Internet routers were not all IGMP version 3 enabled when JSAF version 5.26 was developed. Figure 23 shows an IGMP membership message sent out from the Panasonic machine running VEHELO during testing.

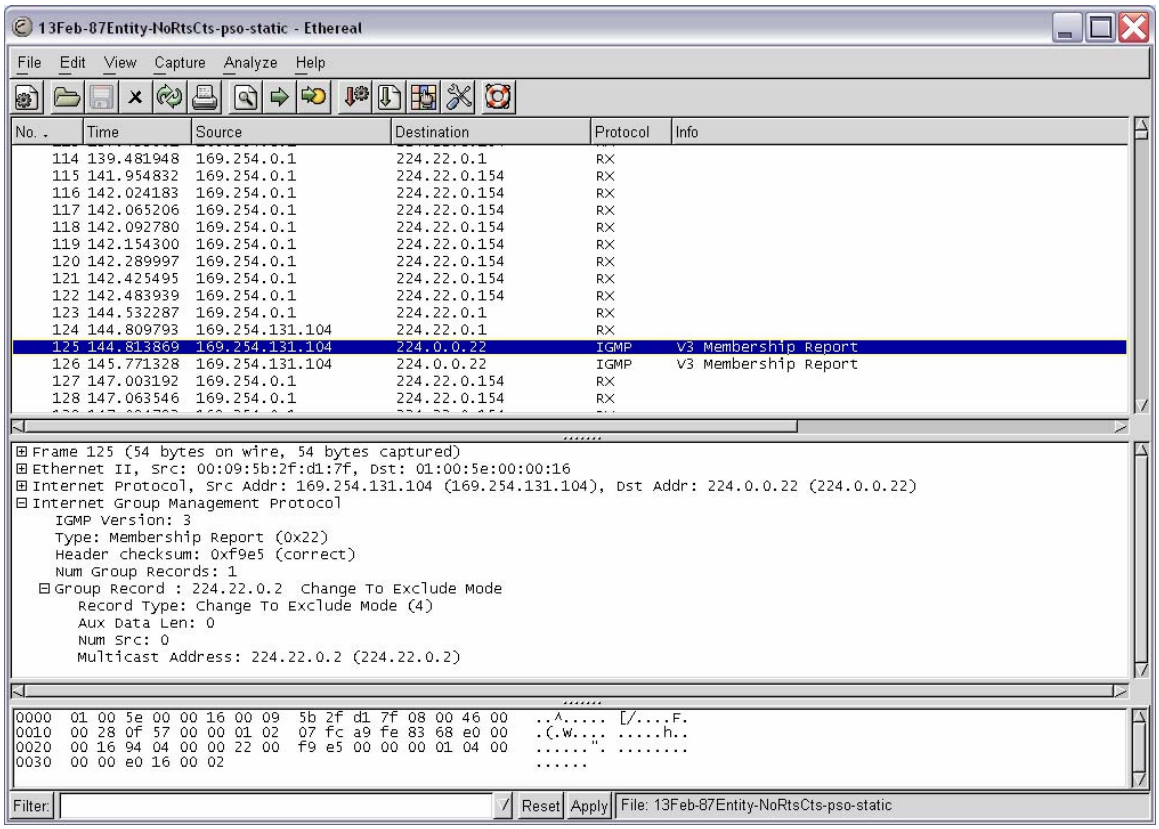

Figure 23. Internet Group Management Protocol packet.

When JSAF or VEHELO applications are launched, they look for a simulation in progress and also send out IGMP membership packets that tell the upstream routers to forward specific multicast traffic to them. The RTI-s, implemented in accordance with HLA, is the originator of the UDP packets, with entity information from JSAF. When a host, simulation server, or entity in our case, shuts down it sends out IGMP packets telling everyone not to forward to said host anymore. When the host sending the multicast traffic receives the message indicating the entity has resigned, the entity will be removed from the simulation.

JSAF also uses another protocol on top of the UDP packet. Figure 23 shows the expanded view of the RX protocol packet which reveals the settable flags. This RX

protocol is on top of the UDP packet and is only revealed to the RTI-s once the packet gets to the application level.

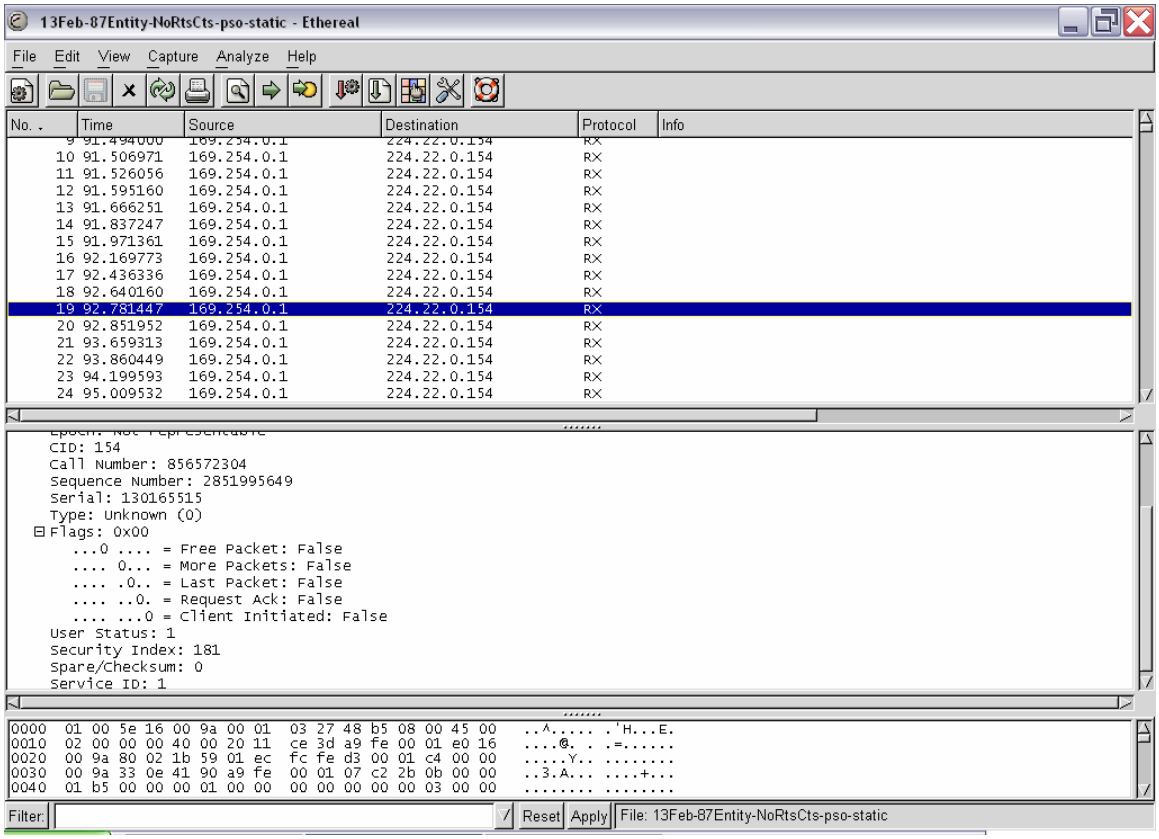

Figure 24. RX protocol packet capture by Ethereal.

B. PRE-TESTING SURVEY

To ensure that we wouldn't be testing on channels and frequencies that the school is currently using for the wireless side of its network infrastructure, a survey was conducted. Two tools were used to survey the area surrounding our test lab; Berkley Varitronics Systems, Inc's Yellow Jacket handheld analysis tool and AirMagnet's, AirMagnet Laptop Trio a/b/g. Both tools revealed that there was traffic on 802.11b/g channels in or near our test lab. They showed no signals from 802.11a equipment. Figure 25 below is the screen capture of the survey done using AirMagnet.

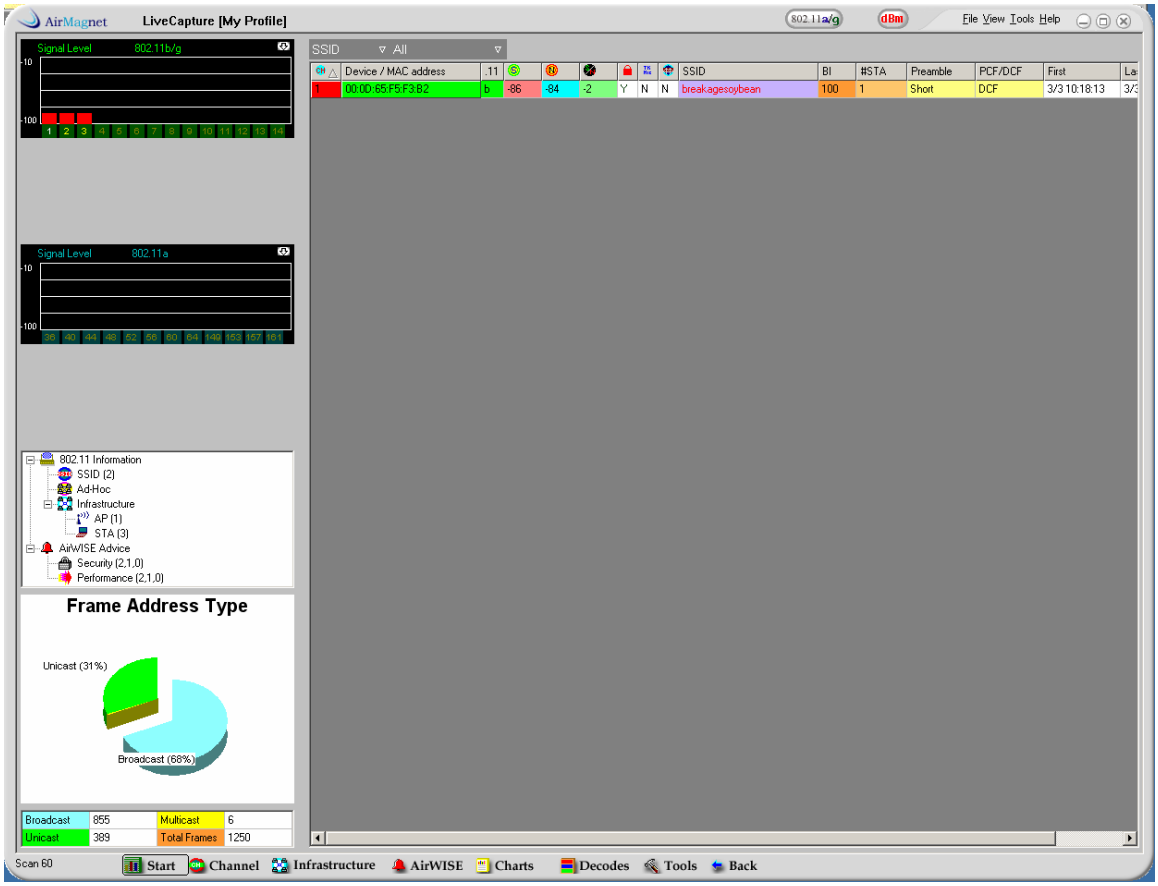

Figure 25. Air Magnet Survey.

Figure 25 indicates that there was utilization on channels 1 and most likely bleed over onto channels 2 and 3; as previously mentioned, this occurs in b/g environments (Chapter VI). Based on the results of the survey we chose to conduct testing with 802.11a. Also, 802.11a has 12 available channels and if the school were interested in placing an 802.11a access point in the vicinity, or even in the same space, because of the non-overlapping structure of 802.11a, this would not have posed a problem for testing.

C. ARCHITECTURE

The Architecture for the evaluation is shown below in Figure 26 and includes the non-routable IP addresses used at each interface.

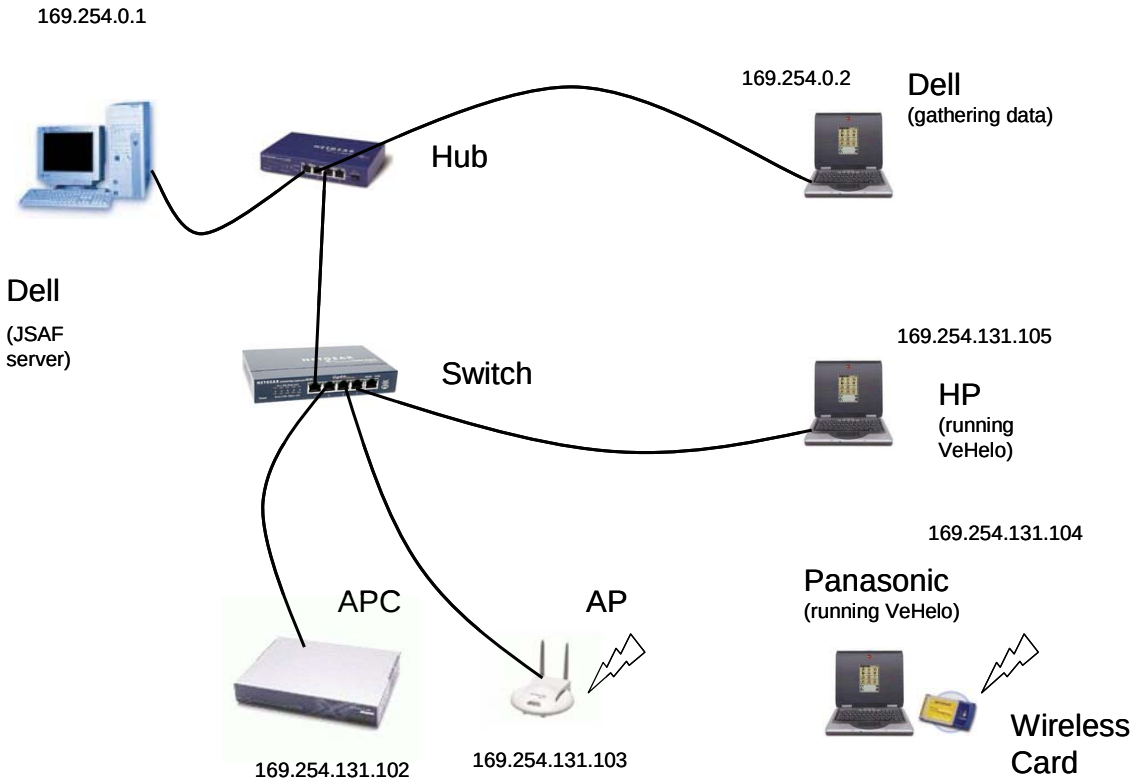

Figure 26. Architecture setup with IP addresses shown.

The access point and access point controller were placed about 20 feet from the Panasonic machine. Signal strength of the access point at the Panasonic averaged 75 percent of transmitted strength. Where signal strength from the Panasonic to the access point was 20 percent of transmitted strength. There were no obstructions in between the access point and the Panasonic machine.

D. BACKGROUND NETWORK TRAFFIC

Prior to testing, the background network traffic of the above architecture was evaluated for consideration

later when analyzing JSAF and VEHELO traffic. Since JSAF primarily uses UDP, the UDP traffic for each is graphed. The UDP traffic that existed on the network without JSAF and VEHELO running was minimal and would be inconsequential in bandwidth measurements of JSAF and VEHELO. Therefore, graphs of the traffic will be presented, but no further analysis of the background traffic will be discussed as it relates to bandwidth measurements of JSAF and VEHELO. Figures 27 and 28 are graphic depictions of the idle network traffic that exists in the evaluation environment.

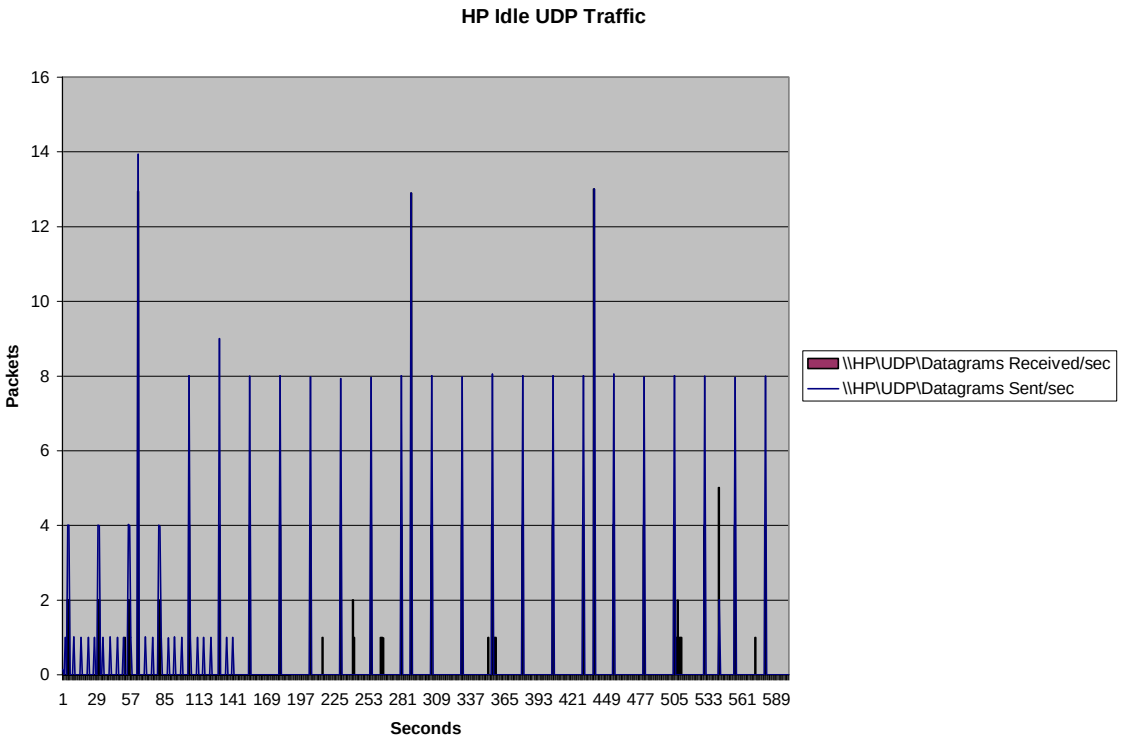

Figure 27. HP idle network UDP traffic.

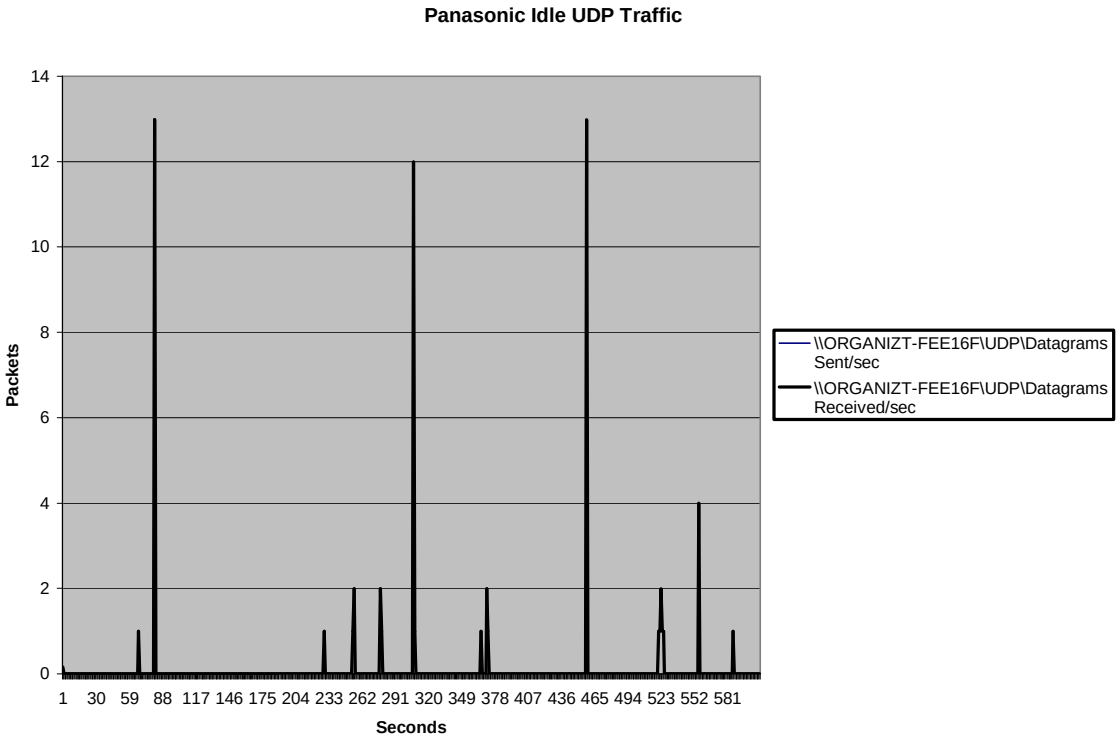

Figure 28. Panasonic idle network UDP traffic.

E. BANDWIDTH TESTING

The JSAF simulations for testing included two scenarios tested in a two different configurations. The first simulation was populated with 87 static entities, made up of 12 surface vessels, 33 aircraft, and 42 ground or other entities. Static in the context of JSAF indicates that the entities are in the simulation but without orders to take any action. We used the 87 entity scenario because it was one that had previously been used for a VIRTE demo. The second simulation kept the same 87 entities but was given a dynamic element to allow for evaluation of traffic increases between static and dynamic simulations. To do this, action orders were given to 45 of the entities. Also, in the second scenario, weapons status was set to "weapons free" to encourage entities to engage one another

even if they hadn't been given specific orders to engage a specific target. Furthermore, the action of all entities in the dynamic simulation was set to automatic, which uses artificial intelligence to guide the actions of the entities. Entities proficiency level for orders assigned was set at 50 percent. For all testing 802.11a on channel 36 was used.

1. 87 Entity Static Test

Tests were set up to take measurements of bandwidth use at each of the three machines, by observing the average bps. Also, packets per second sent and received were captured. Figure 29 below shows a screen capture of the static simulation.

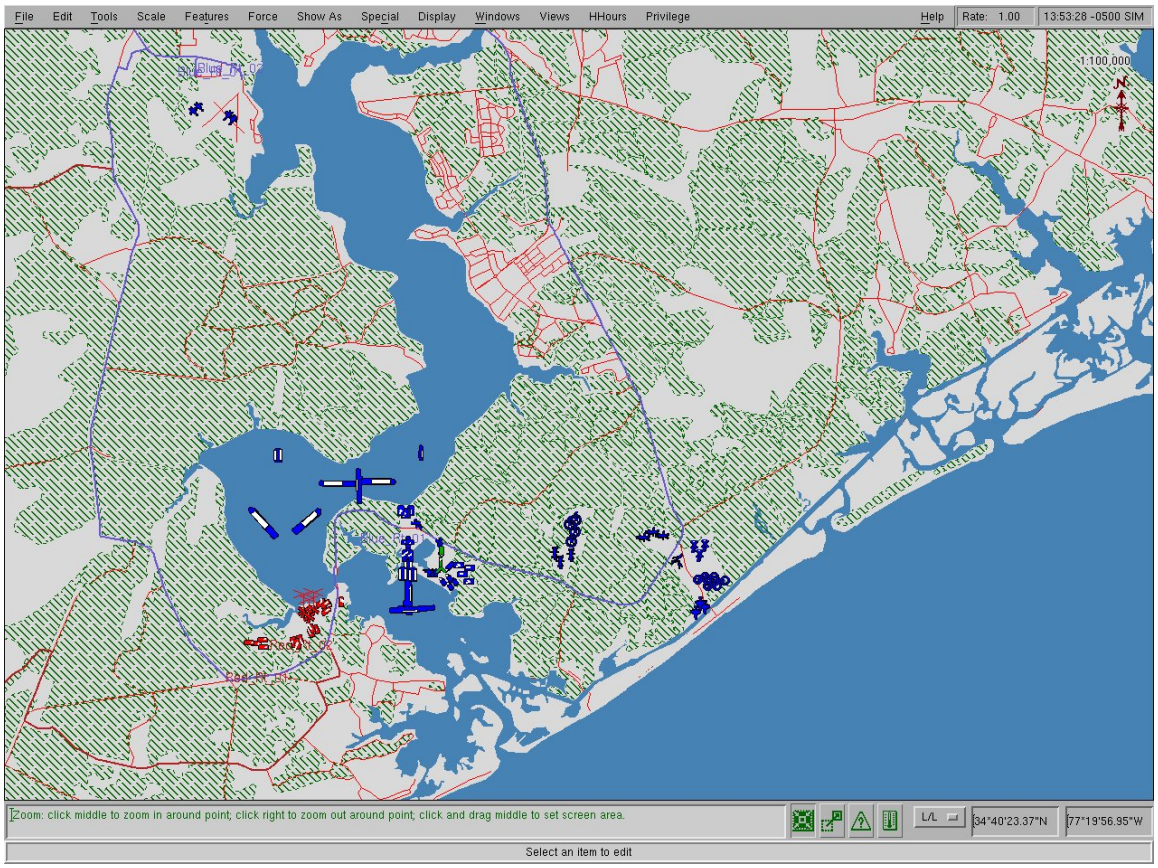

Figure 29. Static 87 Entity scenario.

Bandwidth measurements taken at all three machines are depicted in the graphs below in Figures 30-32. Four tests of the bandwidth used with the 87 entity static scenario were conducted and yielded the same results.

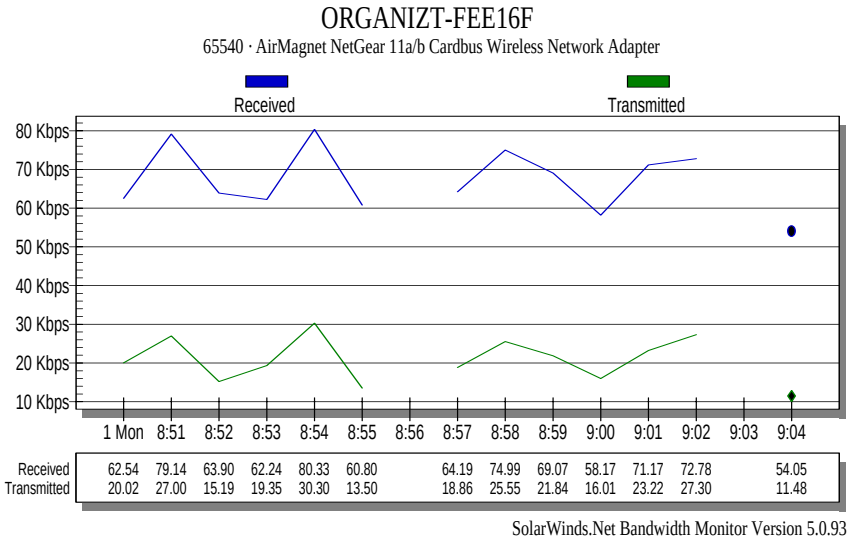

Figure 30. Panasonic 87 entity average bps.

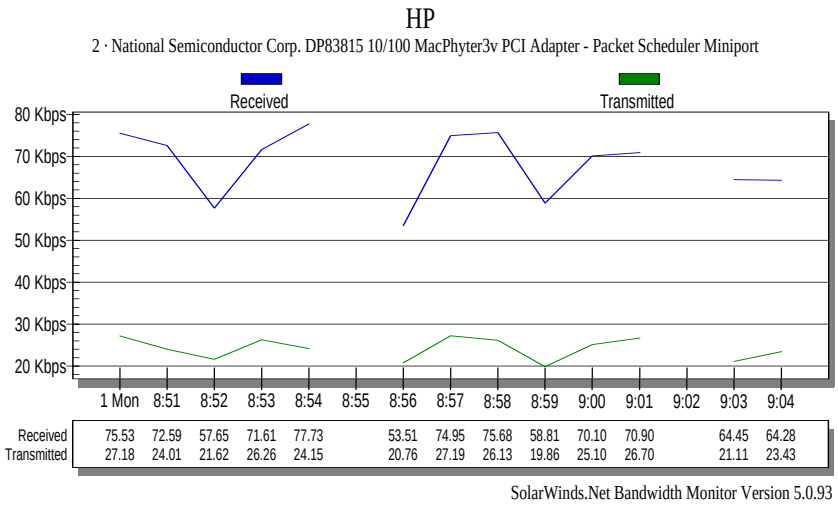

Figure 31. HP 87 entity average bps.

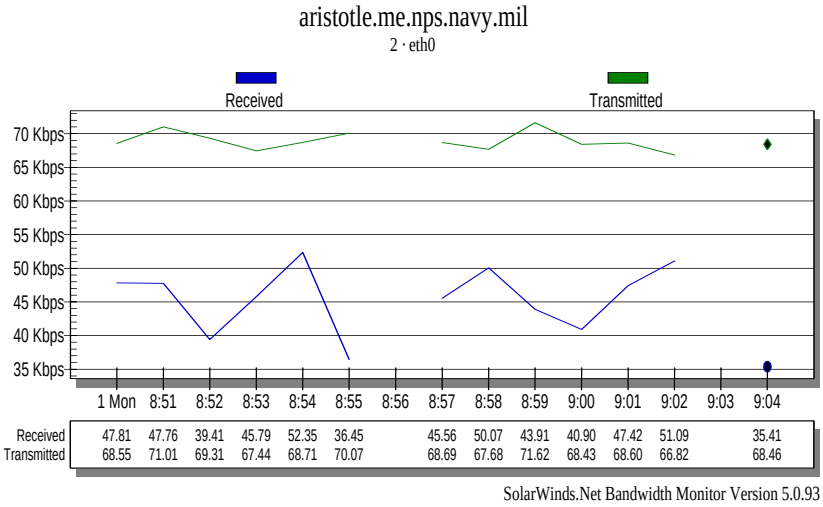

Figure 32. JSAF 87 entity average bps.

To correctly interpret the above charts, another fact about how the RTI works is in order. The RTI we are using has UDP multicast loopback enabled. Loopback enabled is a feature in multicast that can be useful for trouble shooting out going traffic. With loopback enabled, just prior to a UDP multicast packet being sent, the IP layer recognizes it as such and makes a copy and places it into the input queue, as if it had just been received off the wire. [Ref 16] The deviation from this is that while the Panasonic and HP machines report both loopback of UDP packets and their associated octets, the JSAF server only reports the loopback of the UDP packets.

Table 1 shows the average bits per second sent and received at both the Panasonic and HP machines. Received packets per second have to be reduced by the number sent per second, to get the actual average number of packets per second recorded, again, due to multicast loopback.

	Run 1		Run 2		Run 3		Run 4	
	Pkts sent/s	Pkts recv/s	Pkts sent/s	Pkts rent/s	Pkts sent/s	Pkts recv/s	Pkts sent/s	Pkts recv/s
HP	10.93	31.96	9.57	29.5	11.25	33.49	10.55	32.79
Panasonic	13.01	32.28	11.55	29.97	13.08	33.96	12.78	33.25

Table 1. Panasonic and HP packets sent and received per second.

Figures 33-38 below show the average packets per second received and transmitted for the first run for the Panasonic and HP. All runs mirrored this traffic flow pattern.

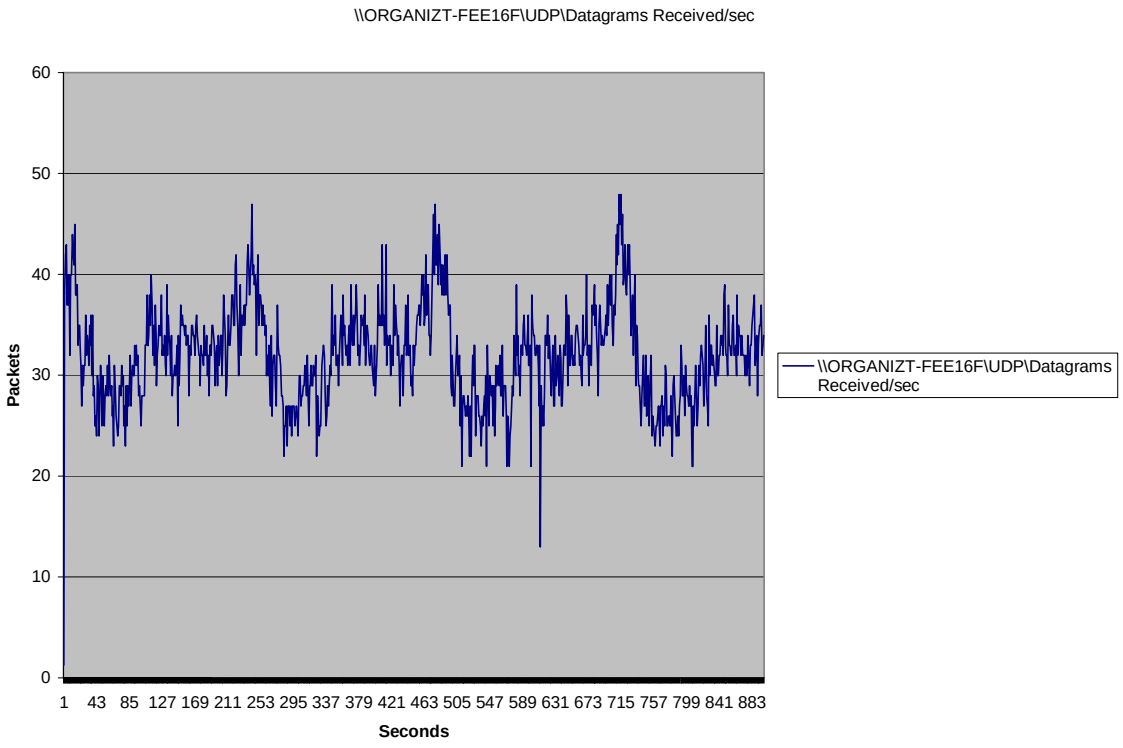

Figure 33. Panasonic packets received per/s.

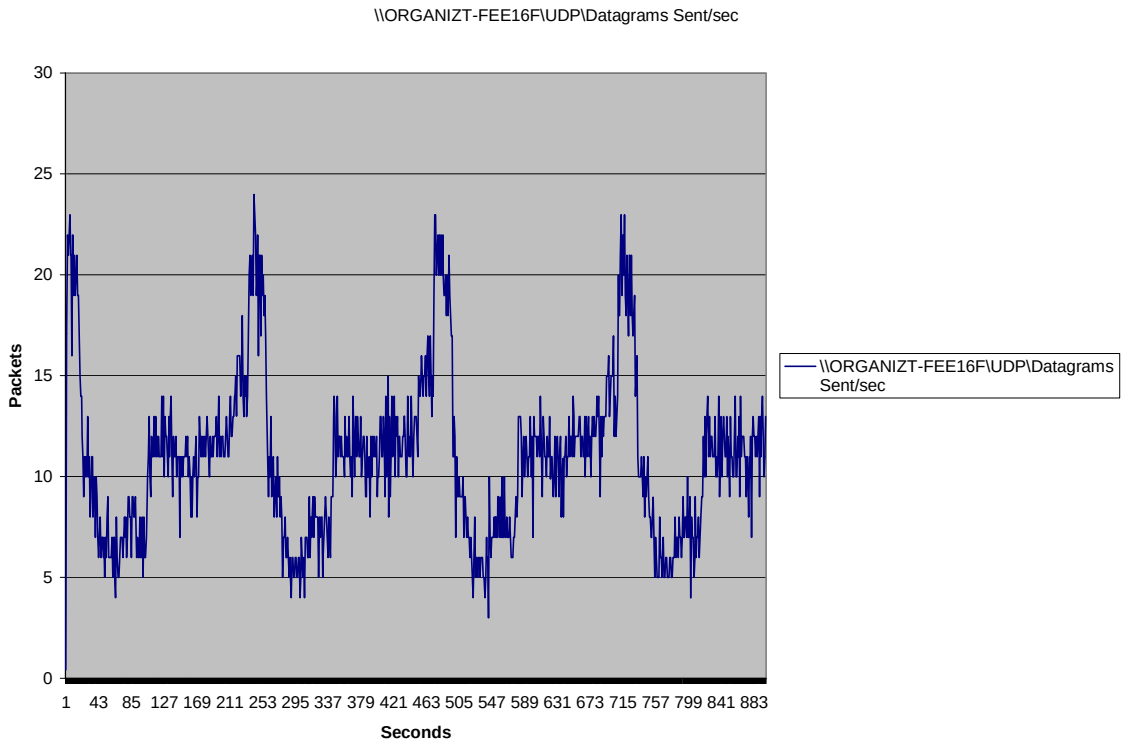

Figure 34. Panasonic packets sent per/s.

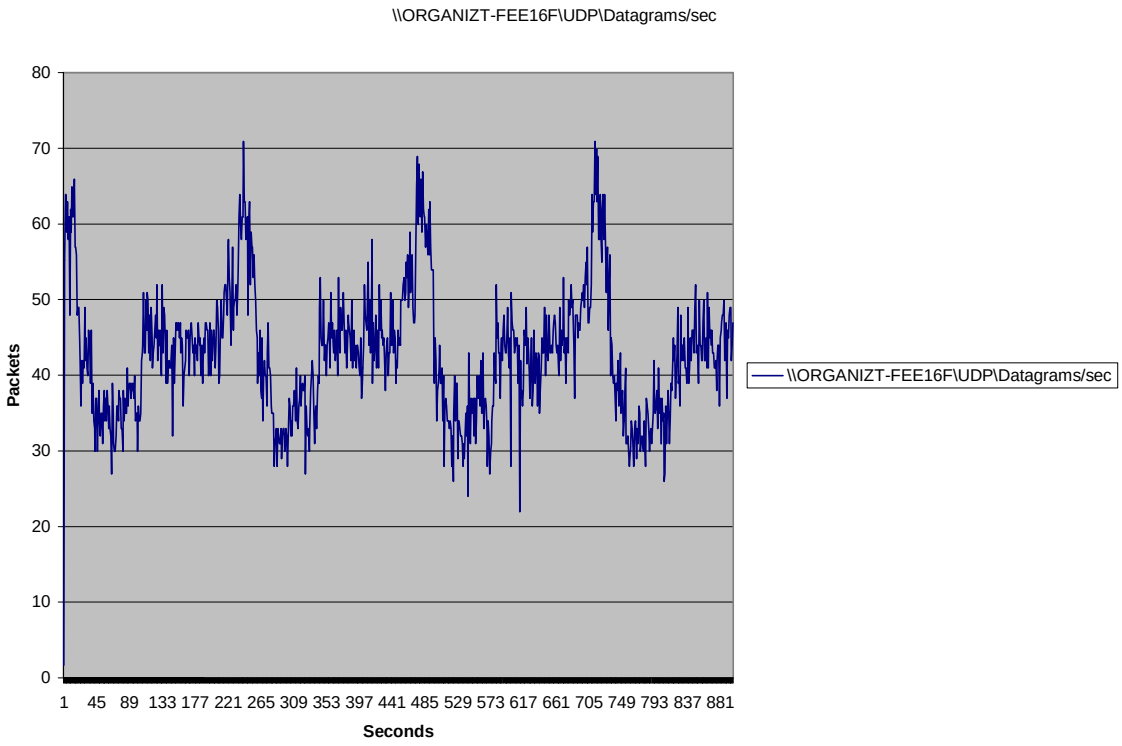

Figure 35. Panasonic combined sent and received packets/s.

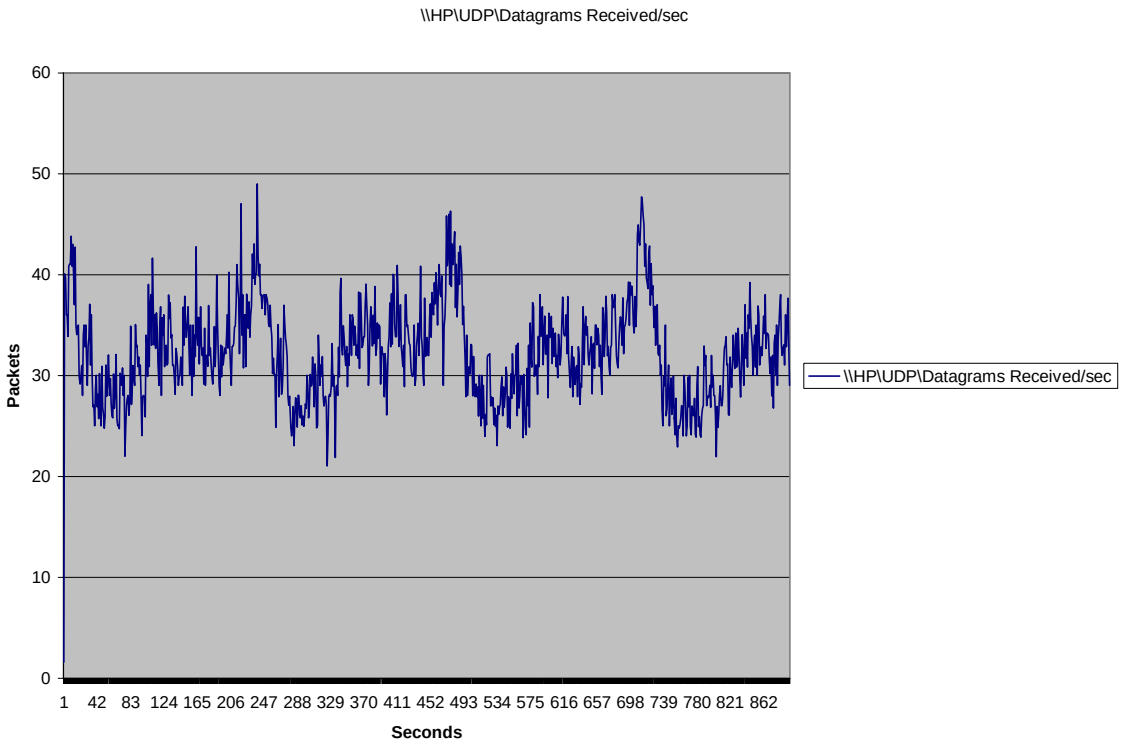

Figure 36. HP packets received per/s.

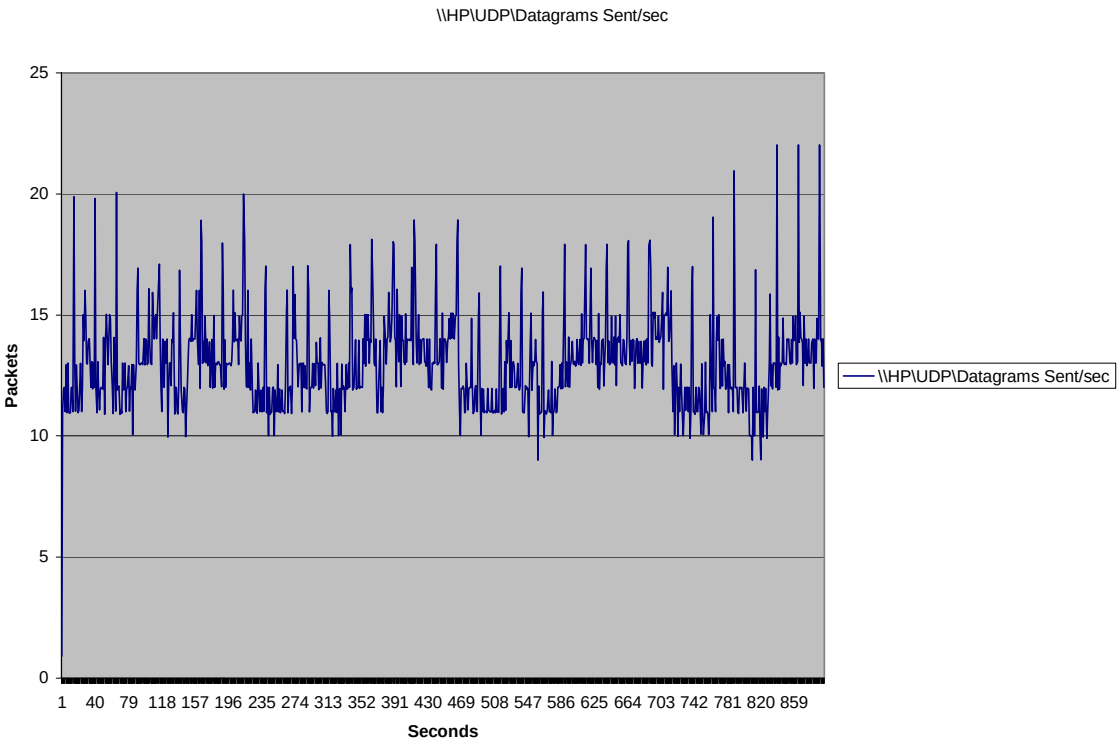

Figure 37. HP packets sent per/s.

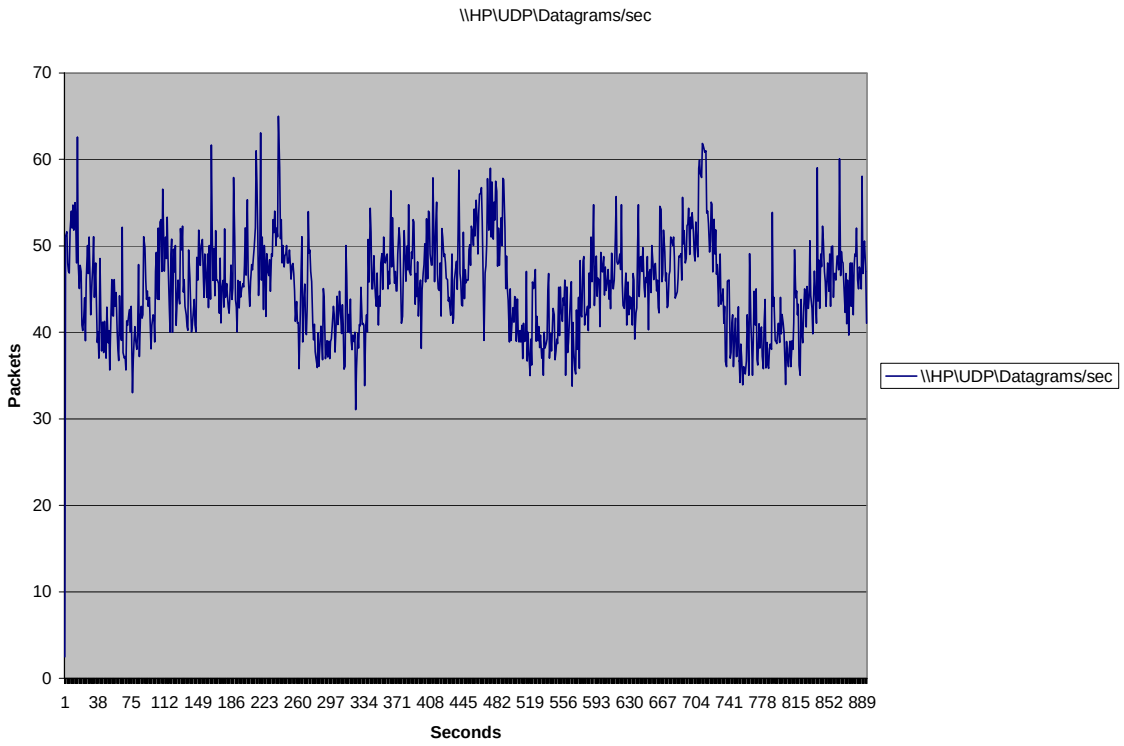

Figure 38. HP combined sent and received packets/s.

The cyclical nature of the received and sent packet graphs is due to the AP not responding to the Panasonic at 60 second intervals. When this occurs the Panasonic will send out a UDP multicast packet, a null function packet or some of both, 35 times each. Traffic then resumes as if nothing had occurred. Observing packets sent from JSAF and HP before and after the cyclical sending events, indicates that no packets from either are missed. Also, the receive logs indicate that both HP and JSAF receive the packets that Panasonic is sending, even though the AP doesn't send out an acknowledgement. The cyclical nature of these graphs is also exhibited in the Solar Winds graph of the JSAF transmit and receive average bps (Figure 32).

Wireless bps versus wired bps seconds is shown in Table 2. The additional 28-35 percent of overhead in the wireless environment is expected, and can be as high as 50 percent. Because JSAF and the RTI use UDP multicast and not TCP/IP, where every frame is acknowledged, they realize lower wireless overhead.

	Run 1	Run 2	Run 3	Run 4
Wireless bps	143,455	138,837	156,842	146,775
Wired bps	106,931	108,357	118,089	109,202
Additional overhead	34 percent	28 percent	33 percent	34 percent

Table 2. Wireless versus wired bps.

A portion of the additional overhead in the wireless environment is caused by packet loss. For the first four runs, AirMagnet indicated that packet loss from the Panasonic machine ranged from 21.2 percent, when it was in power save mode, to 7 percent with power save off. Figure 39 is a screen capture of AirMagnet which shows the utilization and throughput during the static 87 entity simulation. Utilization at the time of the capture was less than 5 percent, with throughput at 146 kbps. This was typical of the entire 15 minute simulation.

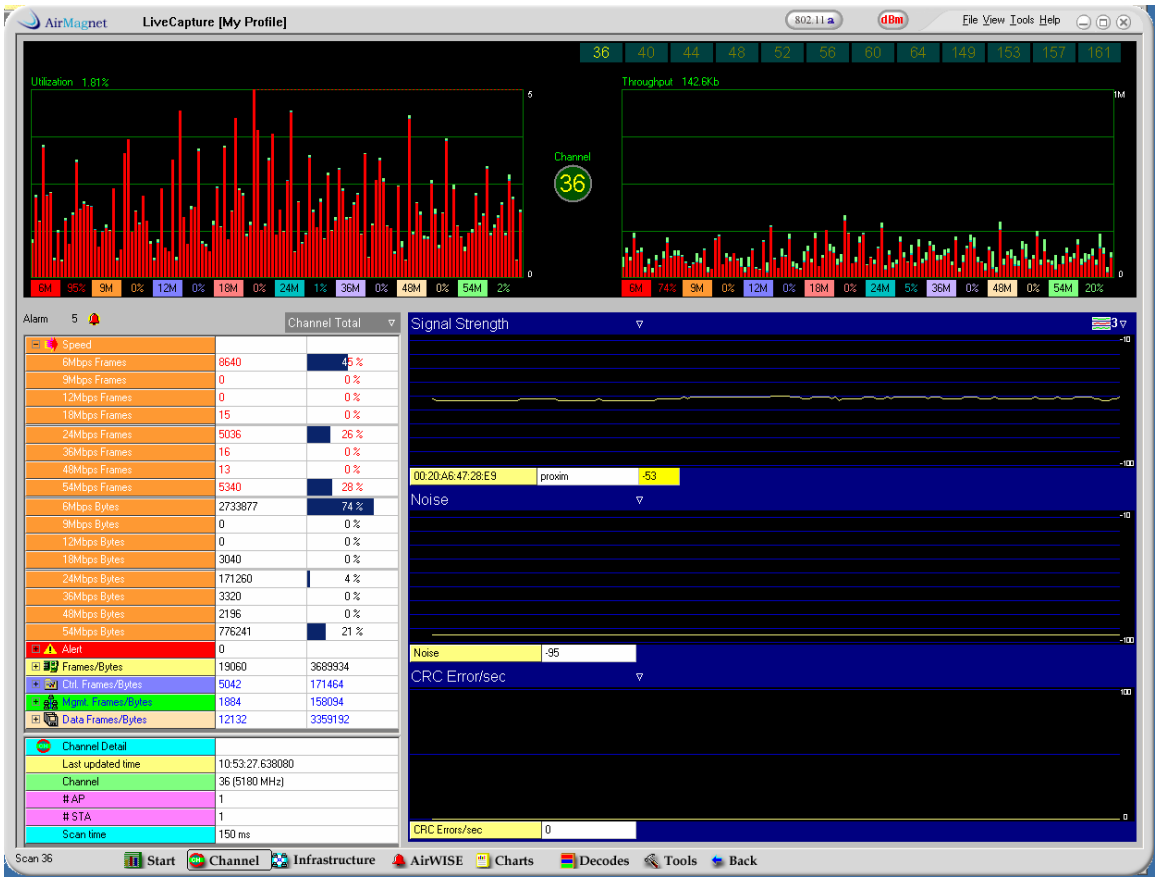

Figure 39. AirMagnet capture during 87 entity static simulation.

The third and fourth simulations were conducted with Request to Send (RTS) and Clear to Send (CTS) on at the access point. As expected, with no other wireless devices associated with the access point, the management overhead went up very little. Because of this, the 87 entity dynamic testing was conducted with RTS/CTS on.

2. 87 Entity Dynamic Test

Dynamic testing was conducted with the same architecture and wireless settings as the third and fourth static tests. Dynamic testing was conducted by giving orders to 45 entities. These orders included aircraft attacking ground targets, surface vessels transiting, and ground vehicles in combat. Below, in Figure 40, is a screen capture of the simulation running.

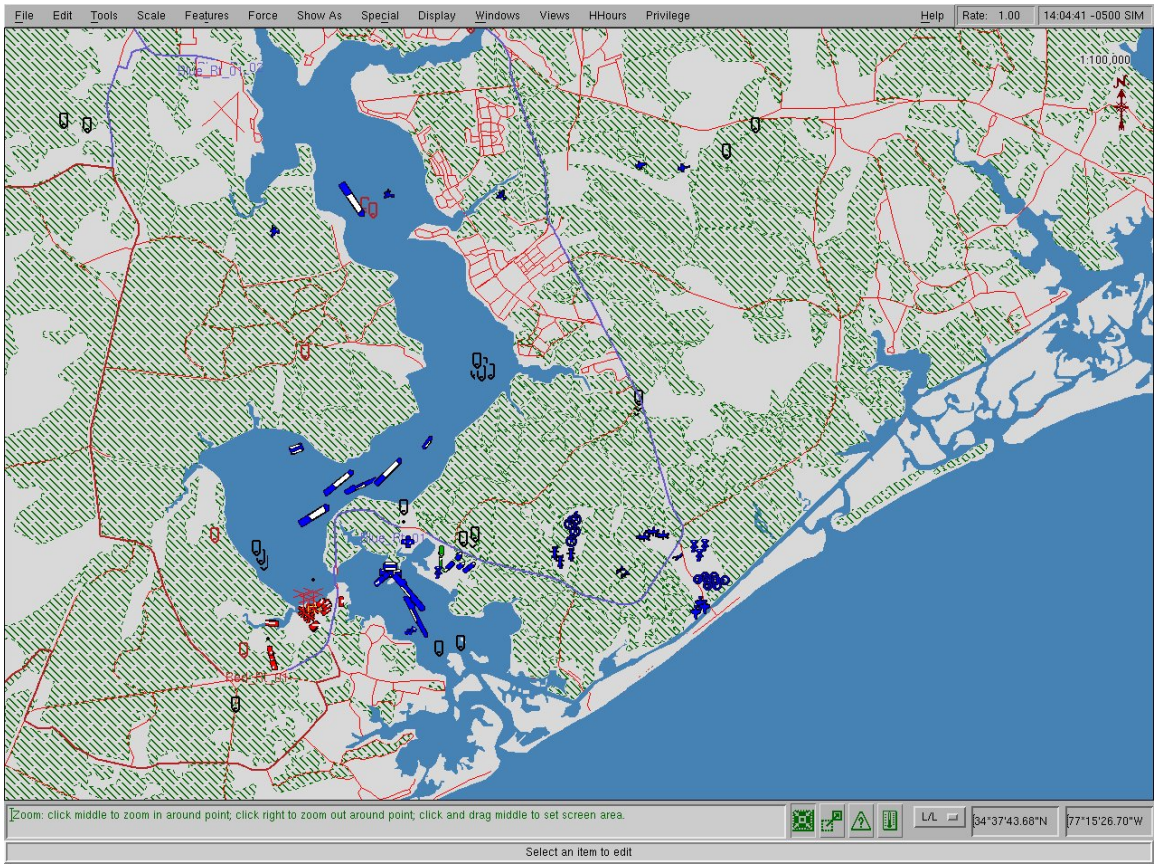

Figure 40. 87 entity dynamic scenario capture.

Bandwidth measurements taken at all three machines are depicted in the graphs below, Figures 41-43. Two tests of the bandwidth used with the 87 entity dynamic scenario were conducted, yielding the same results.

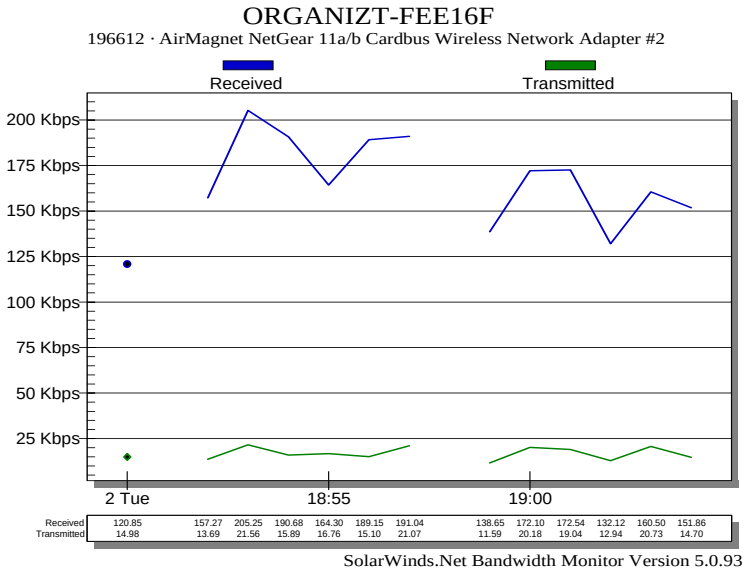

Figure 41. Panasonic average bps.

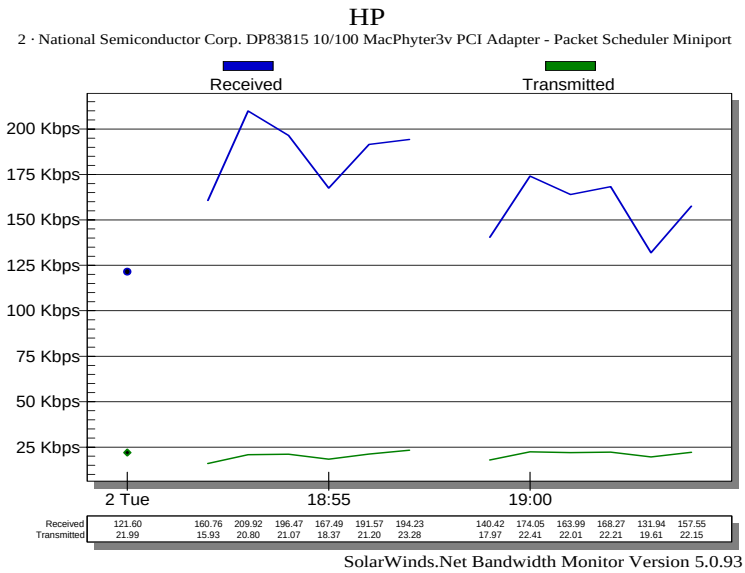

Figure 42. HP average bps.

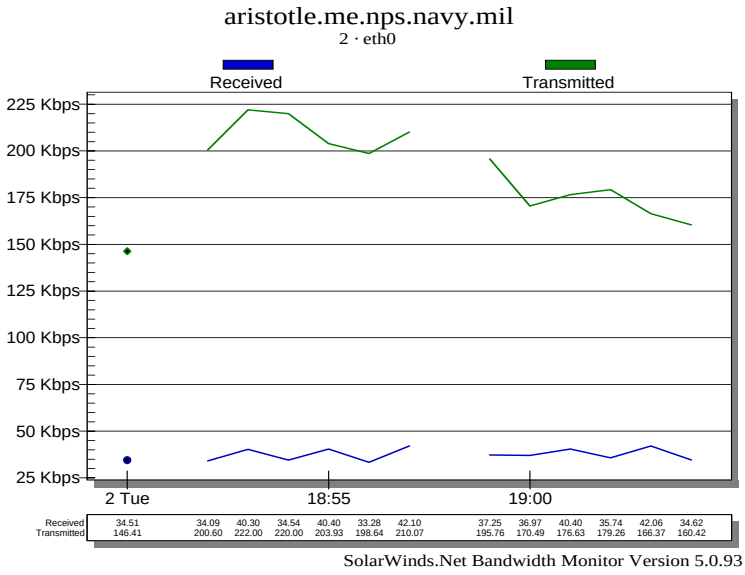

Figure 43. JSAF average bps.

The sharp increase then decline in transmitted traffic depicted in all graphs is expected. This is due to executing all orders for the 45 dynamic entities simultaneously, at the start of the simulation, which coincides with the beginning of the data capture. The decline is a result of many of the aircraft missions completing their tasking halfway through the scenario. Table three shows the packets per second sent and received by Panasonic and HP. Figures 44-47 show packets sent and received by Panasonic and HP.

	Run 1		Run 2	
	Pkts sent/s	Pkts recv/s	Pkts sent/s	Pkts rent/s
HP	11.03	55.06	11.54	54.65
Panasonic	8.865	54.19	8	54.05

Table 3. Packets sent and received per second.

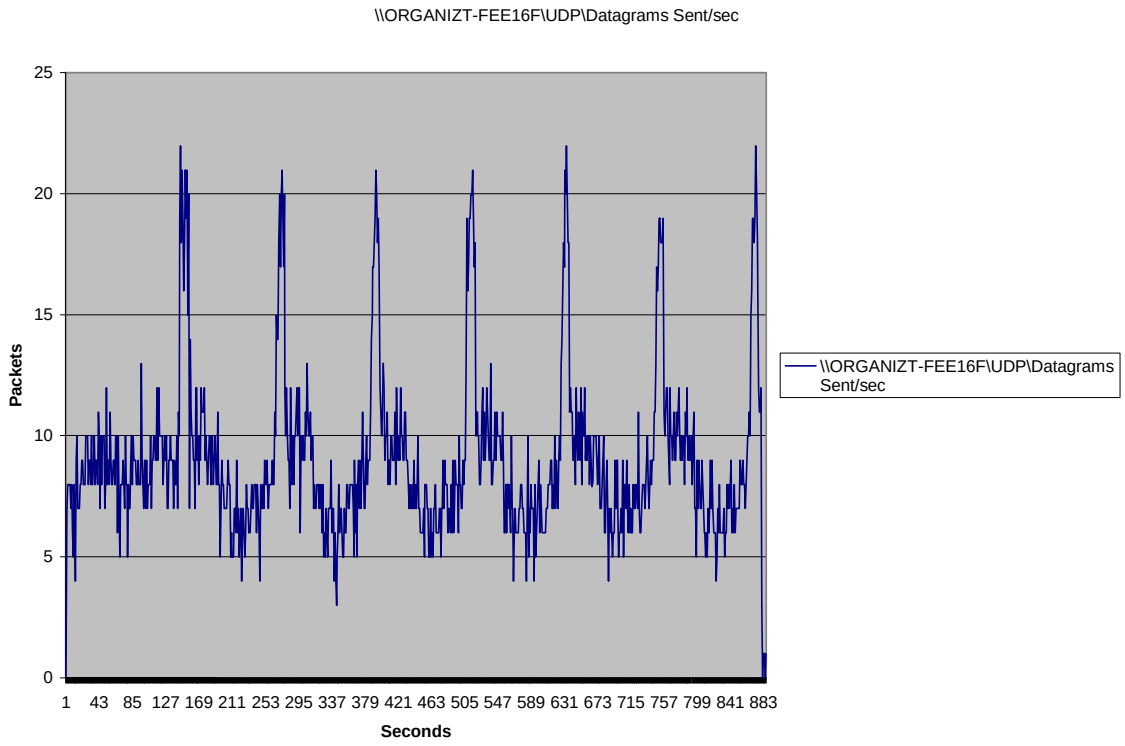

Figure 44. Panasonic packets send per/s.

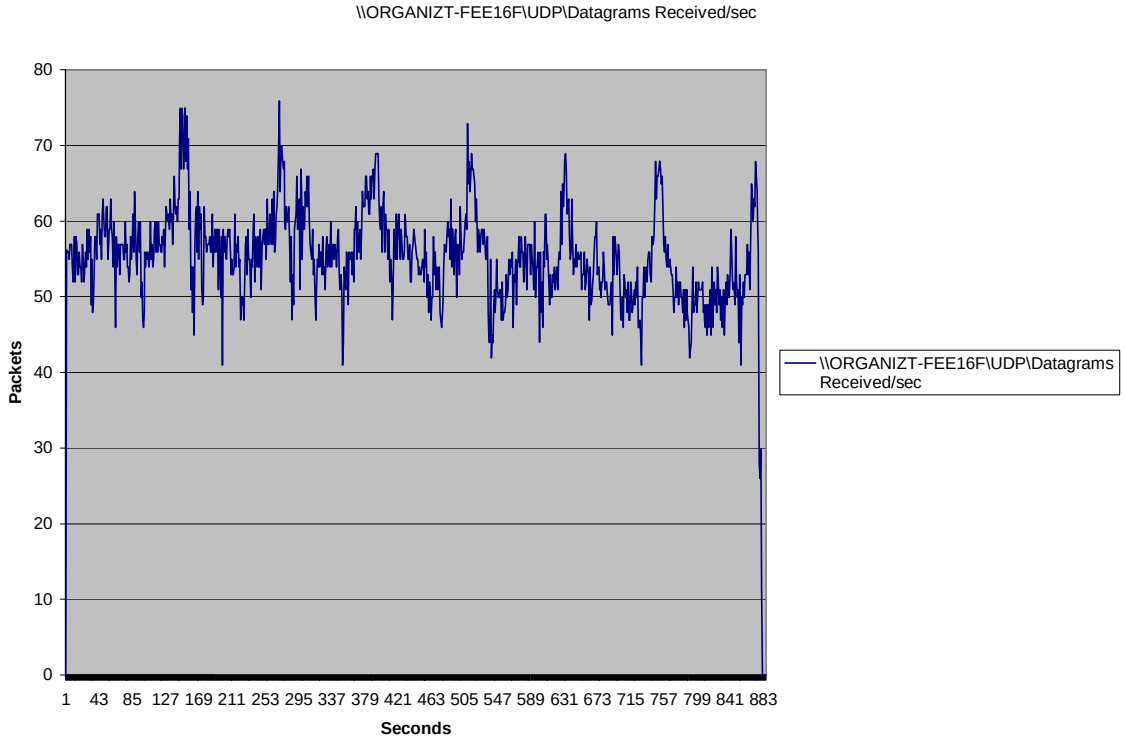

Figure 45. Panasonic packets received per/s.

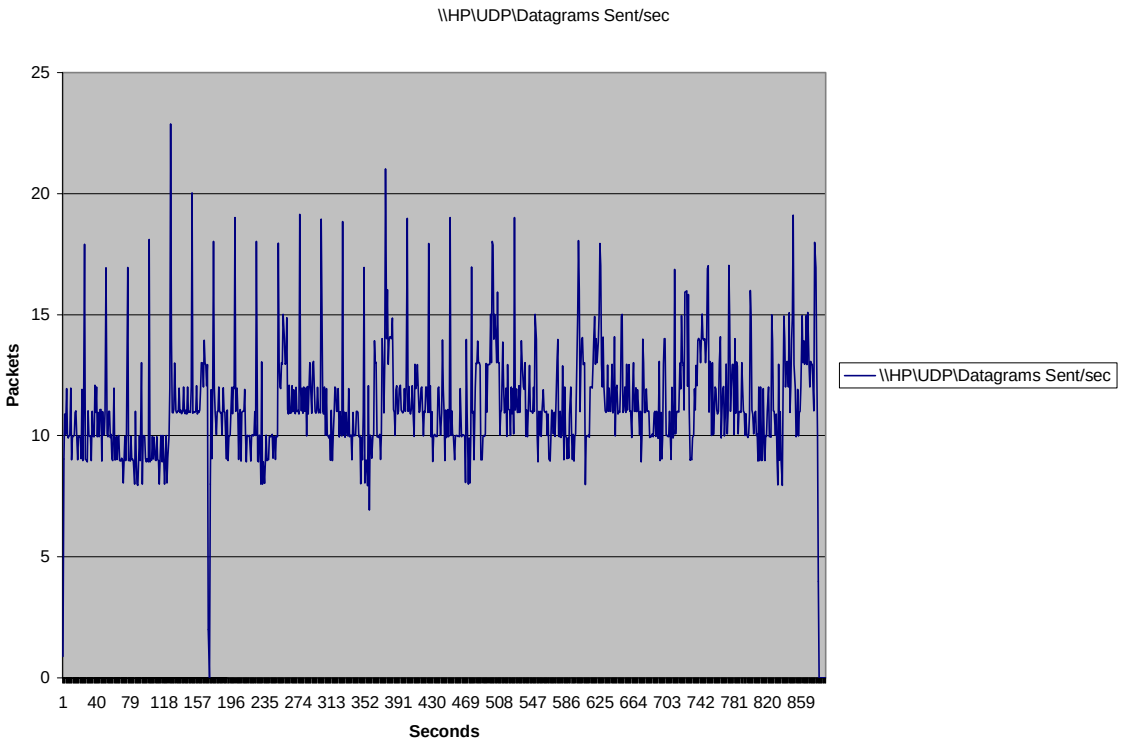

Figure 46. HP packets sent per/s.

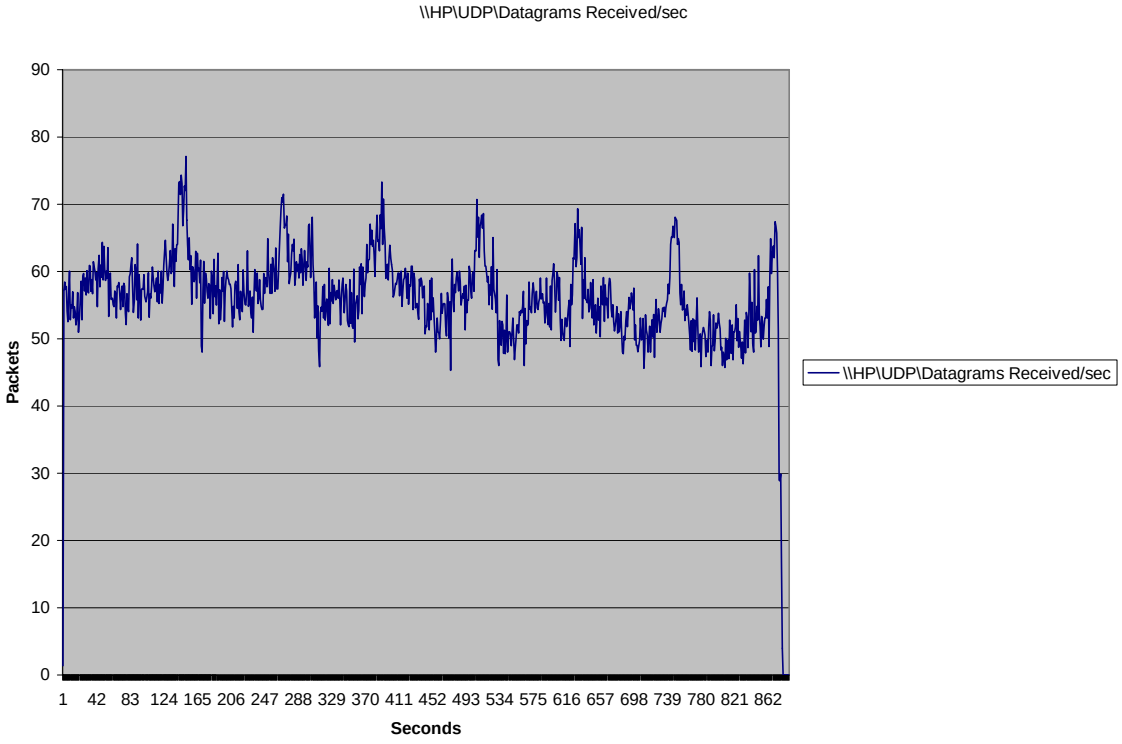

Figure 47. HP packets received per/s.

Wireless bps versus wired bps seconds is shown in Table 4. The additional 22-25 percent of overhead in the wireless environment is expected.

	Run 1	Run 2
Wireless bps	267,122	273,763
Wired bps	218,819	219,608
Additional Overhead	22 percent	25 percent

Table 4. Wireless versus wired bps.

The additional overhead is reduced in the dynamic scenarios because JSAF is sending more traffic. Traffic from JSAF and the wired VEHLO does not get acknowledged on the wireless link. The only traffic that gets acknowledged is the traffic from the wireless node, and the wireless node’s traffic remains the same. The size increase is due to the entities executing orders, which causes more entity updates per packet. The packet loss as reported by AirMagnet from the Panasonic machine for both runs was 12 percent. In all testing, a review of the packet loss from the access point to the Panasonic was very low or non-existent based on the traffic reported as received by the HP, the Panasonic, and AirMagnet. Packet loss was an issue from the Panasonic because of the signal strength being at 20 percent and the issue of the access point not acknowledging traffic at 60 second intervals. Figure 48 below is a graphic depiction of the wireless versus wired kbps from our tests.

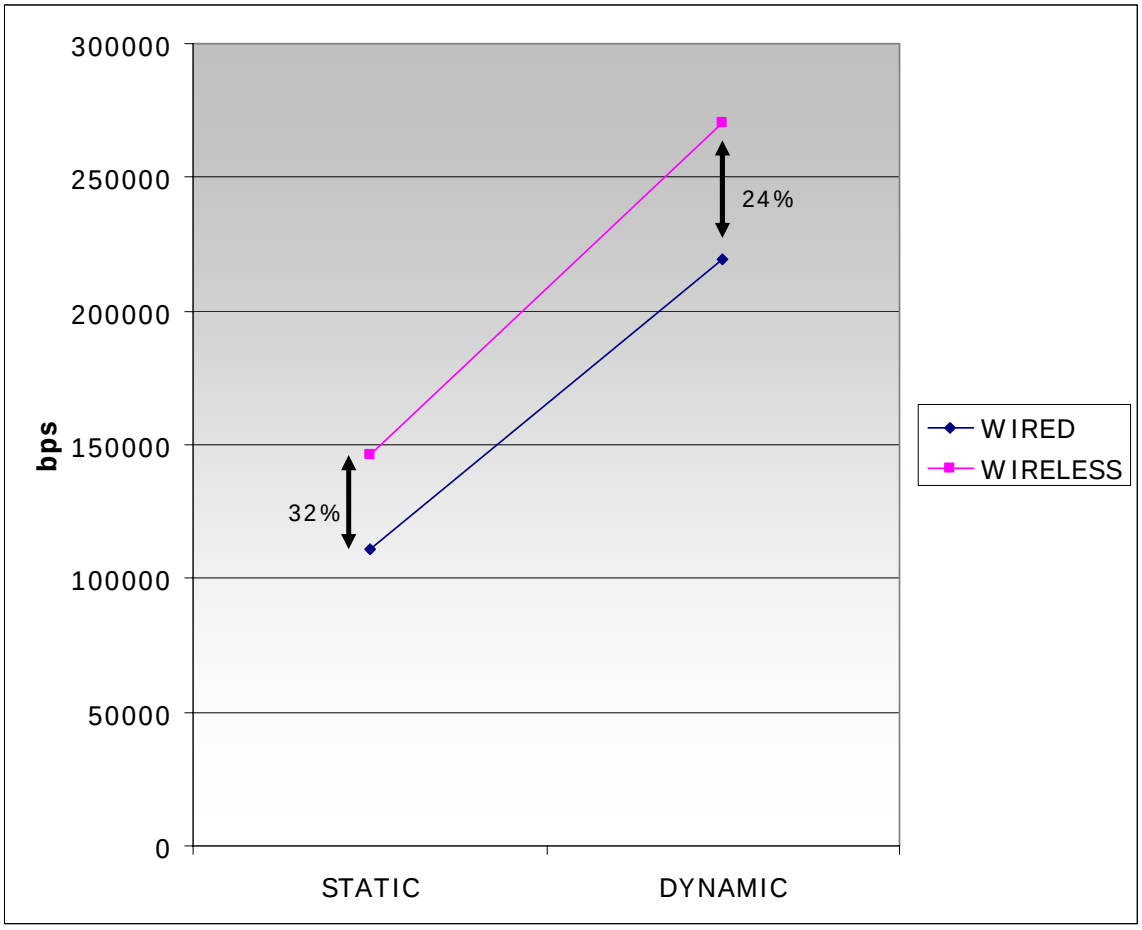

Figure 48. Wireless versus wired bps.

The static tests have a lower bps because in the static simulations, entities were entered but were inactive, therefore there is less network traffic. As mentioned previously, the percentage decrease in overhead from wired to wireless when going from static to dynamic scenarios is because there is more traffic on the wireless link that is not being acknowledged. This reduces the overhead of each byte of data sent.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSION

A. GENERAL DISCUSSION

The goal of this thesis was to identify current IEEE 802.11 wireless technologies as possible candidates for deploying large scale combat simulations for training. This thesis also sought to select a current standard with which to conduct testing of bandwidth use by the JSAF simulation server running with two VEHELO application entities. To do this, JSAF communicating with one wired, and one wireless entity were set up. Both the wired and wireless entities were running the same VEHELO application, on the same OS. All three were on a small, non-routable network.

In our scenarios, we averaged less than 274 Kbps in the wireless environment and less than 219 Kbps in the wired environment. This equates to .005 or less than one percent of the available bandwidth of the 54 Mbps wireless pipe. Of the wired 100 Mbps pipe, only .002, again less than one percent, was used. While many more entities could be added on the wireless or wired side of our environment, the number would not be a linear increase up to the bandwidth being filled. This is because as network traffic increases, contention for the medium increases and therefore collisions (packet loss) increase. Without further testing on the wireless side, it would be difficult to predict the maximum number of wireless clients that could co-exist in any given scenario.

In our testing architecture we did not have a router. Because of this, all traffic was seen at the physical layer of all devices, which means that the observed traffic was

higher than it should have been. A router in our testing would have reduced network traffic. With a router in the architecture, traffic would only be passed to a particular entity or the JSAF server if it were interested in seeing traffic on a particular multicast address. Further testing and deployment of JSAF and the VEHELO should include a router as part of the architecture.

Packet loss in our environment was higher than expected because of the access point not acknowledging packets from our wireless client on a 60 second cycle. Otherwise, packet loss was not unacceptable, even though we were operating on the lowest power 802.11a channel. Had our testing been conducted on other equipment, either higher power 802.11a channels, or 802.11b or g technologies, packet loss would be expected to have been close to or equal to zero. Prior to any wireless combat simulation for training being deployed, surveys to establish the appropriate equipment and frequencies for the particular environment would be required to manage packet loss and overall connectivity.

During our testing we determined that wireless clients operating in the power save mode was not desirable. This is because the client, as ours did, could have trouble joining an ongoing simulation. Clients in power save mode would be asleep at times when the JSAF server was sending traffic that the VEHELO application needed to see to join the scenario. The client doesn’t see this traffic due to a client in power save mode causes the network interface to turn off intermittently. When our client was successful in joining the scenario it operated normally. This is because

the client tells the access point it is going to be off and the access point then stores the traffic for the client until the client is back on.

B. CONTRIBUTIONS

The contributions made by this thesis provide an initial understanding of the bandwidth requirements of a JSAF sever running with VEHELO entities, using UDP multicast, in a wired versus wireless environment. This thesis provides a framework from which future testing of deployable combat simulations for training in a JSAF environment can be based. Identifying some of the peculiarities observed with the relatively new technologies associated with 802.11 standards, highlights the diligence that will be required of the personnel who deploy these technologies for simulations for training for the warrior. Testing and measurement of bandwidth requirements for JSAF and VEHELO show that wireless simulation for training is does not add prohibitive amounts of overhead in the environment tested.

To begin to establish the deployability of simulation for training, whether wired or wireless, bandwidth requirements must be established. Analytically determining expected bandwidth requirements for JSAF or any HLA based simulation would be very difficult at best. The number of variables that can affect bandwidth utilization is enormous. The same scenario, run multiple times, could produce vastly different bandwidth requirements. The differences are based, in part, on: entity manipulations by humans, semi-automated force interaction, probability of successful engagement with different weapons systems, and operator proficiency. These variables are just a small

subset of the very large number that could impact bandwidth requirements for any given scenario.

Taking this into consideration, to further establish the deployability of simulations for training, models for scoping the bandwidth requirements of prospective simulations need to be developed.

C. FUTURE WORK

Numerous areas exist for continued study in this realm of deployable combat simulations for training via wireless architectures. Included would be further testing of JSAF and VEHELO, evaluation of modifications to the RTI in wireless environments, and a layered approach to providing complete wireless coverage.

1. Continued Testing of JSAF and VEHELO

For this thesis a one wireless and one wired entity were tested running simultaneously with JSAF, which was running a limited number of entities. This was because the server was limited by the processor and memory. More testing of the wireless environment, in more robust setting needs to be conducted. This should include more entities on the server along with more wireless entities.

a. Increasing the Number of Wireless Entities

Testing of a wired JSAF server with many (6 or greater) wireless devices running VEHELO, would provide valuable knowledge of UDP multicast characteristics when using JSAF. Having multiple devices contending for the same wireless bandwidth can cause usage to go up dramatically. Available bandwidth will be a concern in this environment, because it will be dynamically reduced if the entities near the fringe of wireless coverage.

b. Categorically Different Entity Testing

Further testing should include other wireless entity applications running with VEHELO in a JSAF environment. This is because multiple entities of different types are envisioned in large-scale deployable simulations for training. Entity types of different categories will have different bandwidth requirements. It is critical to understand the dynamics of entities of different categories, with differing bandwidth requirements, on the same wireless network.

c. Entity Increases at JSAF

It is important to know the types and numbers of entities that are best suited for wireless environments. As simulations get large, wireless entities may need to be tailored to maximize the added flexibility afforded by wireless in combat simulations for training. In this testing, the wireless environment was not taxed from a bandwidth/entity perspective. To greater understand the wireless dynamics in this environment, more entities must be generated by the server.

2. Modifications to the RTI for Wireless Clients

In large-scale combat simulations, bandwidth will become a problem on wireless nodes before it becomes a problem for wired nodes. This is based on the typical wired network running on 100 Mbps links while current wireless technologies are generally compatible up to 54 Mbps. The goal would be to reduce bandwidth from the wireless entities by increasing bytes sent per packet. This would have to occur while keeping an acceptable update rate. The overhead associated with wireless traffic can be reduced if the packet size is increased. This could be

done by increasing the number of entity updates per packet, therefore reducing the total number of packets sent.

3. Layered Wireless Architectures

Large numbers of entities running in a wireless environment is envisioned. With this in mind, layered wireless architectures will need to be investigated. Layering in a wireless environment could include such scenarios as high bandwidth entities close to an access point operating on one or more 802.11a channels, medium range, medium bandwidth entities operating on 802.11g channel/s, and medium range, low bandwidth entities operating on non-interfering 802.11b channel/s. This would leverage all current 802.11 standards to maximize wireless architectures in combat simulation for training environment.

LIST OF REFERENCES

1. Department of Defense, Defense Modeling and Simulation Office (DMSO), (online) Available: <https://www.dmso.mil/public/> (5 Feb. 2003)

2. Department of Defense, Under Secretary of Defense for Acquisition and Technology, Modeling and Simulation (M&S) Master Plan, October 1995.

3. Rumsfeld, Donald, Department of Defense, Transformation Planning Guidance, April 2003.

4. Congressional Budget Office, 125-Year Picture of the Federal Government's Share of the Economy, 1950 to 2075, 3 July 2002

5. Federal Communications Commission Spectrum Policy Task Force, Report of the Unlicensed Devices and Experimental Licenses Working Group, 15 November 2002.

6. Institute of Electrical and Electronic Engineers (IEEE), Std 802.11, 1997.

7. Institute of Electrical and Electronic Engineers (IEEE), Std 802.11b-1999/Cor 1-2001 (Corrigendum to IEEE Std 802.11b-1999.

8. Planet3 Wireless, Certified Wireless Network Administrator Official Study guide, 2002.

9. Federal Communications Commission, Amendment of the Commission's Rules to Provide for Unlicensed NII/SUPERNet Operations in the 5GHz Frequency Range, May 6 1996.

10 Institute of Electrical and Electronic Engineers (IEEE), Std 802.11a, 1998.

11. Chen, James C. PhD, Atheros Communications, Measured Performance of 5-GHz 802.11a Wireless LAN Systems, 27 August 2001.

12. Navy Modeling and Simulation Management Office, Joint Semi-Automated Forces index, (online). Available: http://navmsmo.hq.navy.mil/index.cfm?page_to_go=resources.cfm (4 March 04).

13. Navy Modeling and Simulation Management Office, Joint Semi-Automated Forces index, (online). Available: <http://navmsmo.hq.navy.mil/index.cfm?page_to_go=resources.cfm> (4 March 04).

14. Coombs, Gerald, Ethereal presentation, (online). Available: <http://www.ethereal.com/~gerald/presentations/Ethereal_Intro/> (5 March 04).

15. Deering, S., Network Working Group, Request for Comments: 1112, Host Extensions for IP Multicasting, August 1989.

16. Quinn, B, Almeroth, K., Network Working Group, Request for Comments: 3170, IP Multicast Applications: Challenges and Solutions, September 2001.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California