2008-03

A comparative analysis of Fortress (ES520) and Mesh Dynamic's (4000 SERIES) networking capabilities during COASTS 2007 field experiments

Tyler, Brian Keith.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A COMPARATIVE ANALYSIS OF FORTRESS (ES520) AND MESH DYNAMICS' (4000 SERIES) NETWORKING CAPABILITIES DURING COASTS 2007 FIELD EXPERIMENTS

by

Brian Keith Tyler

March 2008

Thesis Advisor: Rex Buddenberg
Co Advisor: Tom Hoivik

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2008	Master's Thesis

4. TITLE AND SUBTITLE A Comparative Analysis of Fortress (ES520) and Mesh Dynamics' (4000 Series) Networking Capabilities During Coasts 2007 Field Experiments	5. FUNDING NUMBERS
6. AUTHOR(S) **Brian Keith Tyler**	
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	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited	

13. ABSTRACT (maximum 200 words)

The Cooperative Operations and Applied Science & Technology Studies (COASTS) field experimentation program is a combined Indonesia-Malaysia-Singapore-Thailand-U.S. research and development (R&D) effort to test commercial-off-the-shelf (COTS) Command and Control, Communications Computers and Intelligence, Surveillance and Reconnaissance (C4ISR) technologies to provide real-time situational awareness (SA) for multi-national, tactical and remote decision makers in a cooperative environment.

This thesis evaluated the military suitability of Fortress 802.11 ES520 wireless technology and Mesh Dynamics' 4000 series 802.11 wireless technology by conducting a comparative analysis of the technologies network performance while deployed in a tactical ground, maritime and mobile configuration in support of COASTS 2007 field experiments. Several operational field tests were conducted in California and Thailand in order to evaluate both Mesh Modules and ES520s network performances. Specific military suitability areas evaluated included network availability, throughput, network security, graphical user interface, transportability, connectivity, environmental effects, peripheral support, encryption performance, AP to AP handoff capability and antenna configuration.

14. SUBJECT TERMS IEEE 802.11 Technology, WiFi, COASTS, Fortress ES520 802.11 access bridge, Mesh Dynamics 802.11 4000 series access bridge.	15. NUMBER OF PAGES 177
	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	UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

A COMPARATIVE ANALYSIS OF FORTRESS (ES520) AND MESH DYNAMIC'S (4000 SERIRES) NETWORKING CAPABILITIES DURING COASTS 2007 FIELD EXPERIMENTS

Brian K. Tyler
Lieutenant, United States Navy
B.A., University of the South, 2002

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2008

Author: Brian Keith Tyler

Approved by: Professor Rex Buddenberg
Thesis Advisor

Professor Tom Hoivik
Co-Advisor

Dan C. Boger, PhD
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Cooperative Operations and Applied Science & Technology Studies (COASTS) field experimentation program is a combined Indonesia-Malaysia-Singapore-Thailand-U.S. research and development (R&D) effort to test commercial-off-the-shelf (COTS) Command and Control, Communications Computers and Intelligence, Surveillance and Reconnaissance (C4ISR) technologies to provide real-time situational awareness (SA) for multi-national, tactical and remote decision makers in a cooperative environment.

This thesis evaluated the military suitability of Fortress 802.11 ES520 wireless technology and Mesh Dynamics' 4000 series 802.11 wireless technology by conducting a comparative analysis of the technologies network performance while deployed in a tactical ground, maritime and mobile configuration in support of COASTS 2007 field experiments. Several operational field tests were conducted in California and Thailand in order to evaluate both Mesh Modules and ES520s network performances. Specific military suitability areas evaluated included network availability, throughput, network security, graphical user interface, transportability, connectivity, environmental effects, peripheral support, encryption performance, AP to AP handoff capability and antenna configuration.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACK	Acknowledgement
AOR	Area of Responsibility
AP	Access Point
C2	Command and Control
COASTS	Cooperative Operations and Applied Science & Technology Studies
COTS	Commercial-off-the-shelf
HFN	Hastily Formed Network
IEEE	Institute of Electrical and Electronic Engineers
LOS	Line of Sight
NMS	Network Management System
NPS	Naval Postgraduate School
PoE	Power over Ethernet
RF	Radio Frequency
TOC	Tactical Operation Center
UAV	Unmanned Aerial Vehicle
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First, I would like to thank Professor Tom Hoivik for working with me to ensure my field test objectives supported my thesis. His professional insight was pivotal to my continued success on this thesis, as a student at NPS and to my future as a Naval Officer. Next, I would like to thank Professor Rex Buddenberg for his technical expertise, which helped guide my thesis to answering the right technical questions. A special thanks to LCDR Amy Bleidorn and LT Alex Simmons for their effort in helping me set-up and test the equipment used for my thesis. I also want to thank Mr. Jim Ehlert and Mr. Scott Howard for helping me choose a thesis topic and providing the means to conduct thesis testing. Finally, I thank my wife for enduring my frustrations and the time I spent away from home with the COASTS field experiments.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE

The purpose of this thesis is to evaluate the military suitability of Fortress 802.11 ES520 wireless technology and Mesh Dynamics' 4000 series 802.11 wireless technology by conducting a comparative analysis of there networking performance while deployed in a tactical ground, maritime and mobile configurations in support of COASTS 2007 field experiments.

B. BACKGROUND

The Cooperative Operations and Applied Science & Technology Studies (COASTS) program is a joint project between the Naval Postgraduate School and the Royal Thai Armed Forces (RTAF). The program focuses its research on command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) uses for commercial-off-the-shelf (COTS), state-of-the-art, rapidly scaleable airborne and ground communications equipment, including various wireless network technologies. This research is being conducted in partnership with the RTAF to develop a network and associated devices and applications that potentially may help suppress drug trafficking in the northern Thailand border regions (Russo, p 1). The work that the COASTS program does is paving the way to better tactical awareness solutions through the integration of COTS technologies.

Currently most of the drug smuggling activity occurring in Thailand is concentrated in the northern border areas, while most of the civil unrest is occurring in the south. Both of these regions of the border are quite rugged and require many resources to manage, making these locations ideal for drug and terrorist or insurgent operations. The development of a robust and rapidly deployable network that is equipped with increased bandwidth and modern surveillance technologies can greatly aid the Thai military and law enforcement agencies to accomplish their counterinsurgency and counter-drug missions. The importance of a coalition-oriented focus for

modern Maritime Domain Awareness and Protection operations have become a major priority of U.S. combatant commanders. In a recent naval message, all numbered fleet commanders stated that their number one Command, Control, Computers, Communications, Intelligence, Surveillance, and Reconnaissance (C4ISR) requirement was improved coalition communications (COASTS CONOPS 2006, p 7). Current and future operational capabilities are tightly tied to improved interoperability with U.S. allies in the operational theater. As reflected by the increasing number of requests to the Naval Postgraduate School from foreign partners, there is an immediate requirement for low-cost, state-of the-art, real-time threat warning and tactical communication equipment that is also rapidly scaleable based on operational and tactical considerations (COASTS CONOPS 2006, p 7). This issue has become especially apparent in the face of the overwhelming mission requirements placed on US forces conducting the Global War on Terror (GWOT). The GWOT extends globally where nations are engaged in direct action against numerous forces employing asymmetric tactics. In Thailand, the separatist insurgency in the southern provinces is connected to various transnational terrorist organizations, to include both the Jemaah Islamiyah (JI) and Al-Qaeda, which have struck against both the U.S. and its allies (COASTS CONOPS 2006, p 3).

The 2007 COASTS mission is a continuation of the above excerpts from the 2006 COASTS concept of operation paper. The continued effort is to deter terrorists, provide relief in the wake of natural disasters, secure home ports and provide domestic and foreign security with police and military forces. This requires the use of new communication solutions both technical and non-technical for U.S. and foreign nations in order to combat the above threats to world sovereignty. COASTS 2007 mission is to continue to test and evaluate COTS technology in hope to provide these better solutions.

The COASTS 2007 vision incorporates engaging international and domestic partners at the research and development level in order to satisfy the following objectives:

(1) Investigate net-centric information management in a multi-national environment across tactical, operational, and strategic domains (C2 center integration)

(2) Expand the scope of maritime research into improved command and control technologies for Maritime Interdiction Operations (MIO) and demonstrate ship-to-ship/shore communication packages in robust form factors.

(3) Investigate the deployment issues surrounding hastily formed networks in rugged and varied terrain under adverse climatic conditions and the integration issues surrounding NGO and international partner participation (From COASTS 2007 CONOPS brief).

The operational network performance of Mesh Dynamics and Fortress ES520 was conducted at Fort Hunter Liggett, Fort Ord and Thailand in order to fulfill the above 2007 COASTS objectives. These test sites were used to test and evaluate the devices advertised features such as security, remote management, networking protocol, mobility, transportability, quality of service, and ruggedness. These features were tested while deployed in a mobile and ground application.

C. THESIS OBJECTIVE

The primary thesis objective was to determine Mesh Dynamics and Fortress 802.11 access points operation suitability for COASTS Maritime, Humanitarian and SAR scenario and ultimately military applications. The overall evaluation of military suitability of each product was based on their respective network performance in the COASTS 2007 scenarios conducted in Thailand.

D. THESIS SCOPE

This thesis was limited to evaluating the access points while deployed on hilly, paved, maritime and vegetated terrains. Through an operational comparative analysis, this thesis also evaluated the network performances of the Fortress (ES520) and the Mesh Dynamics (4000 series) 802.11 networking devices in two environmental conditions (Dry, and Humid). The primary objective was to determine operational suitability for COASTS 2007 field exercises and determine suitability for military applications.

The Fort Hunter Liggett site was used to conduct the network mobility tests on flat paved terrain and to observe network performance in a fixed ground deployment.

The Fort Ord site was used to tests the APs' network operations on hilly terrain and the Thailand site was used for the COASTS 2007 scenarios, which included deployment on vegetated and maritime terrain.

E. METHODOLOGY

All tests objectives for the mobile and ground experiments were designed to evaluate the two products' capability to provide the following: 1. High network availability (which was the ability to provide network throughputs of 3Mbps or greater for mobility and 11Mbps or greater for ground experiments). 2. Network security (ability to protect data and access to the network). 3. Quality of service (throughput suitable for operation of attached sensors). 4. Mobility (observe the mobile APs' ability to traverse the area of operation and hop from AP to AP).

Three field experiments were utilized to conduct an operational comparative analysis of the Mesh Modules and the ES520s network performances. In each field experiment, the Mesh and Fortress APs were deployed in various network configurations, network throughput was measured with IxChariot, and results were analyzed and evaluated. Critical issues, Measures of Evaluation and test objectives were determined for each experiment.

Weather, terrain conditions and network throughput were recorded in order to assess performance in the dry and humid environments. Equipment requirements were also observed as to assess labor requirements for deployment of the devices. Additionally, detailed test plans were developed for each test phase in order to control all variables. For instance, both the ES520 and Mesh Modules devices had the same antennas and were mounted at the same heights in each test evaluation. On the other hand, uncontrollable variables such as unfavorable weather, test location, time and equipment failures were limited through pre-tests, and test plans.

The primary software used for data collection throughout the 2007 field experiments was IxChariot. The Ix Chariot software is a product of the Ixia company, a leading provider of performance test systems for IP-based infrastructure and services (from http://www.ixiacom.com/product, MAR 2007). Ixia's IxChariot is the industry's

leading test tool for emulating real-world applications to predict system performance under realistic load conditions (from http://www.ixiacom.com, MAR 2007). With each test, the software sends traffic over the network to evaluate how the network performs. The results of each test include throughput, latency, and transaction rate data, along with a graph that has throughput data points plotted. Figure I-1 gives a visual description of how IxChariot runs a network test.

Each test session required the use of at least two clients (laptops). One client's console was running the IxChariot software while the other client was running IxChariot Endpoint software. The IxChariot console can only communicate with clients that are running the Endpoint software. The IxChariot basic throughput script was used for all network throughput testing. As seen in Figure I-1, this script function sent data packets from endpoint one to end point two and the IxChariot console measure the time it took for the packets to be received and acknowledged. The evaluation then produced the total network throughput based on the time it took the sent packets to be received and acknowledge.

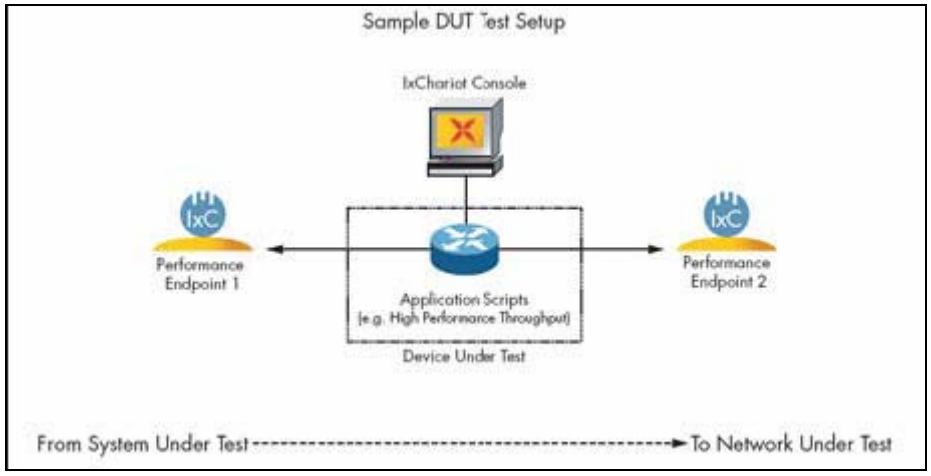


Figure I-1. Sample of IxChariot Test Set-up (from www.ixiacom.com, MAR 2007).

F. ORGANIZATION OF THESIS

The organization of the thesis is as follows:

Chapter II provides an overview of wireless network architectures, IEEE 802.11 standards, and continues with information on the OSI model Data Link and Physical layers. The effects on radio frequency propagation such as Doppler shift, antenna configuration, and blockage of the Fresnel zone are presented. This chapter ends with a discussion on the WEP and WPA/WPA2 standards and their applications to 802.11 technologies.

Chapter III introduces the Mesh Dynamics and the ES520 unique specifications, which include radio layout, network remote management capability, mobility capability, multicast capability, security implementations, and certifications and evaluations.

Chapter IV provides details of the mobile field experiments conducted at Fort Hunter Liggett and Fort Ord. Field experiment objectives, test results, lessons learned and recommendations are discussed and conclude with a comparison between Mesh Dynamics and Fortress network performance in a mobile application.

Chapter V provides details of the fixed ground field experiments conducted at Fort Hunter Liggett and Mgnat Dam in Thailand. The chapter begins with test objectives, results, lessons learned and recommendations and comparison of the Mesh Dynamics and Fortress network performance at Fort Hunter Liggett. Next, Fortress network performance in its deployment in Thailand I for preliminary test trials for the final demonstration is discussed and analyzed. Finally, both Mesh Dynamics and Fortress performance in Thailand II COASTS 2006 and 2007 scenarios is discussed and analyzed.

Finally, Chapter VI summarizes the research, provides conclusions and recommendations, and suggests areas for network improvement and future study.

II. 802.11 WIRELESS ARCHITECTURES AND STANDARDS OVERVIEW

Wireless networks have provided flexible network solutions for many military and civilian applications. The military needs simple, easily implemented and secure method of exchanging data in a combat environment and civilian corporations need the same solutions for business growth. The purpose of this chapter is to provide an overview of different 802.11 wireless network architectures, 802.11 standard protocols, and security implementations.

A. 802.11 WIRELESS ARCHITECTURES

In the 802.11 wireless environments, two basic architectures are utilized to establish a wireless network. The basic wireless architecture is called a Basic Service Set(BSS), which is an independent basic service set used to create an ad hoc network and a group of basic service sets is called Extended Service Set (ESS) (Akins, p 331). The BSS is made up of one AP and one or more laptops as clients or subscriber stations. The ESS is made up of two or more BSS, which allows the laptops to roam or hop from AP to AP within the ESS (Akins, p 331). A service set identifier (SSID) is used to allow access points and laptops to communicate within the ESS or BSS. The SSID should reject association attempts from stations that do not have the same SSID (Akins, p 333). Figure II-1 is a depiction of an ESS.

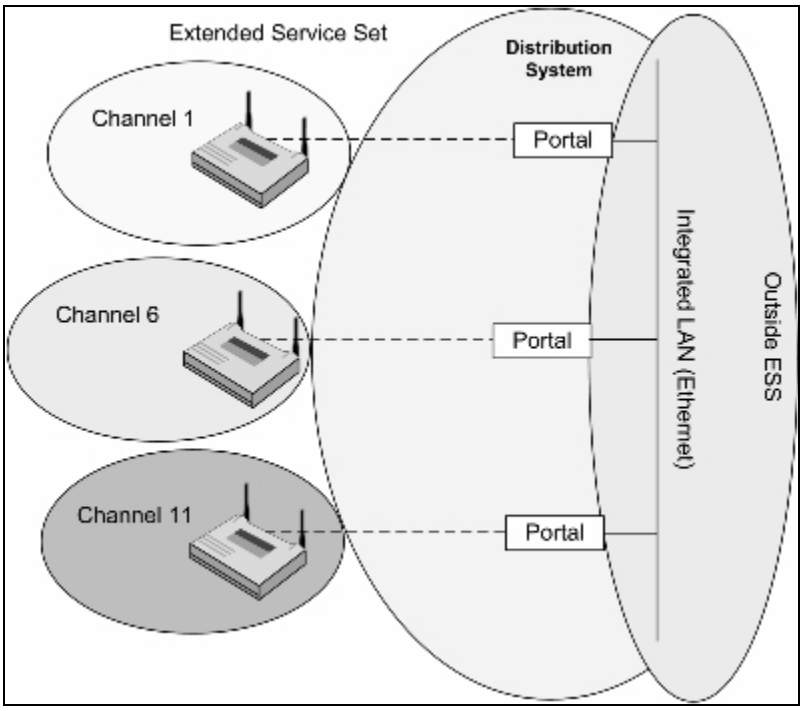


Figure II-1. ESS Display with three Access Points. (From www.cwnp.com, JAN 2008)

The BSS and the ESS are IEEE standardized architectures used for everyday wireless communications.

Conventional mobility is from laptop to AP, which is limited to the laptop or laptops subscribing to one or more APs. The mobile device is the laptop, therefore the network does not move but rather the client. On the other hand, having a mobile AP, the network can be extended wirelessly and create more client access from further distances and allow mobile video surveillance whether it is from ground or maritime vehicles. The above ESS depiction does not show the APs connecting to each other because connectivity between APs is not an IEEE 802.11 standard. This capability is currently only implemented in proprietary applications.

Bridging occurs when two wireless APs connect two wired segments together. See Figure II-2.

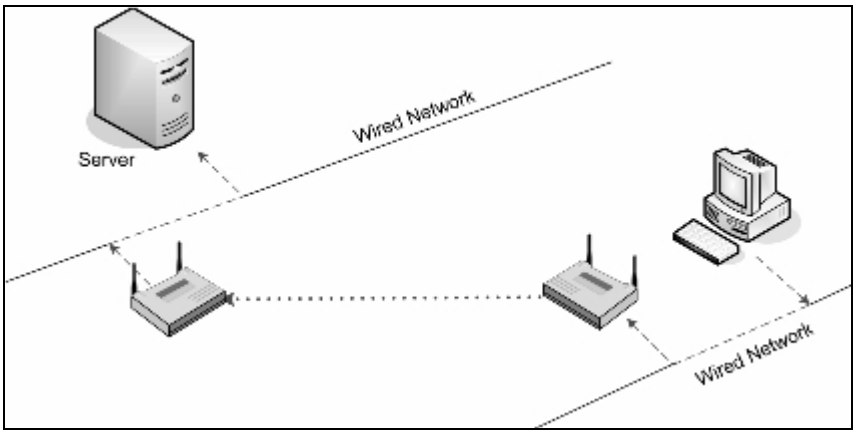


Figure II-2. To wired segments being connected by wireless APs (from www.cwnp.com, JAN 2008)

The 802.11 APs used in the COASTS 2007 deployment were not used to bridge two segments but rather one segment. The APs were deployed in a daisy chain that provided wireless coverage out to 1.5 miles from the tactical operation center. See Figure V-14 for daisy chain set-up.

Wireless network functionality in a tactical environment required that optimal connectivity and network reliability be established and maintained throughout the tactical operation. In order to establish network reliability and connectivity, the network topology had to be examined.

1. Network Topology

Network topology plays a significant role in how a wireless network will perform. Environmental factors such as, weather, terrain, dust, and technology protocols have to be taken into account when implementing a tactical wireless network because network degradation caused by these factors could limit or disrupt network operations. Further, as the wireless links extend, a fixed amount of total bandwidth is apportioned across multiple end systems and across the overhead necessary to keep the packet forwarding correct.

a. STAR

A STAR topology is a single base station or AP that acts as the central connection point for several other access points or sites (Dean, p 345). Figure II-3 is an example of a STAR Topology for a hard wired local area network. In the wireless representation, the computers would be the APs and the Hub the root AP.

When the root AP is active and all non-root APs are connected to it, they will remain connected as long as the root AP stays active. The advantage of this type of topology in a tactical environment is that the root AP will always be at the tactical operation center or base station were as the non-root APs would not and as long as the root AP stays active, any non-root AP can get its information back to the TOC. The disadvantage to this topology is that the root AP is the single point of failure and the non-root APs are limited to being in line of sight of the root AP in order to pass network traffic.

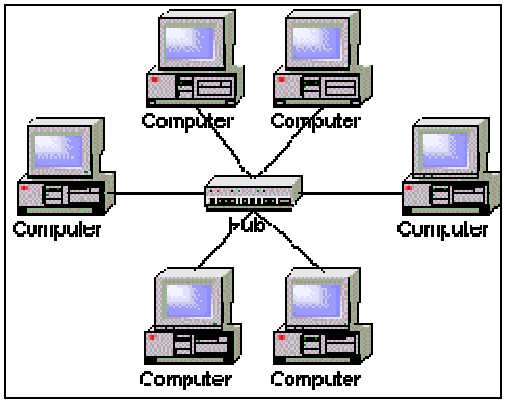


Figure II-3. STAR topology (from www.inetdaemon.com/tutorials/lan/topology.shtml, JAN 2008)

b. Meshed

A Meshed network has multiple paths for data to pass in order to reach its destination. Because every AP is interconnected, data can travel directly from its origin to its destination even when multiple routes have connectivity problems, but one serviceable route must exist. The advantage of this type of topology in a tactical

environment is that it creates the most reliable and efficient data transfer system for network traffic by having multiple routes to the tactical operational center. Therefore multiple APs could suffer casualties and important tactical data can still be routed because no one AP is the single point of failure. The disadvantage with this type of topology for wireless networks is that the implementation of a protocol that does meshing at layer 2 is very difficult. Another disadvantage with the Meshed topology at layer 2 is with network looping, which is a continuous broadcasting of network data packets in a network. Meshed topologies at layer 2 are vulnerable to network loops because all APs in the topology receives all packets and because layer 2 does not route data but rather relay it, loops can be created if an AP that is designated to receive data does not acknowledge the receipt of the data.. Figure II-4 depicts an indoor and outside Mesh topology.

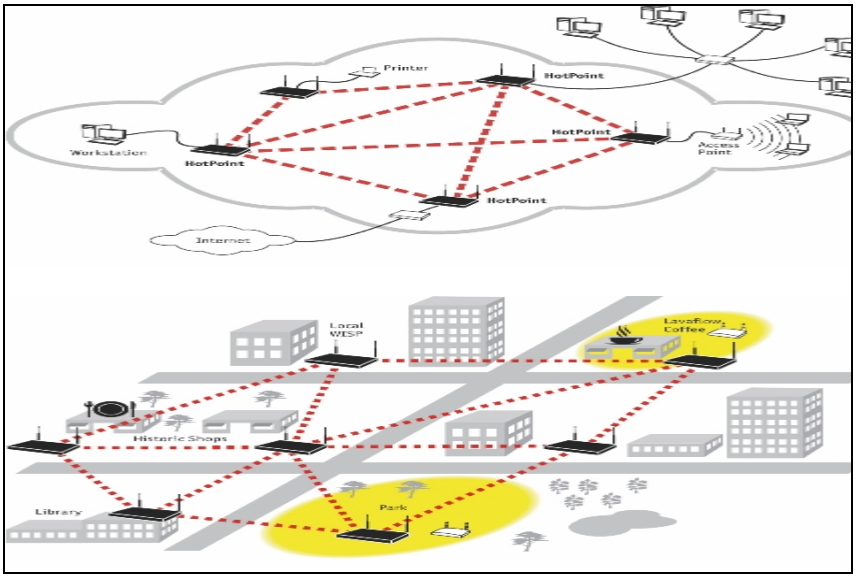


Figure II-4. Indoor and Outside Mesh topology (from www.cwnp.com, JAN 2008)

B. IEEE 802.11 WIRELESS STANDARDS

As mentioned earlier, the IEEE standardized the protocols for most of the information systems in the U.S. and the WiFi alliance ensures that the 802.11 wireless standards are tested and products certified.

1. IEEE 802.11a

The 802.11a standard describes all 802.11 wireless devices operating in the Unlicensed National Information Infrastructure (UNII) bands in the 5GHZ range i.e., 5.8GHZ. In this band, the OFDM or Orthogonal Frequency Division Multiplexing technology boosts the data rates to 54Mbps. This standard takes the place of the 802.11b standard which was limited to a maximum network throughput of 11 Mbps.

2. IEEE 802.11f

The 802.11f standard defines how the management frames used by access points' request re-association with a second access point. The IEEE committee left the implementation of this standard to the vendors. Ability to handoff from one AP to another is an important requirement for mobility in a tactical environment. In a local area network where all APs are on the same network, a mobile AP should be able to associate to the closer of two APs for data transfer.

3. IEEE 802.11g

The 802.11g provides the same maximum throughput as 802.11a and it also uses OFDM technology in the same manner as 802.11a. The 802.11g operates in the Industrial Scientific Medical band which is located at 915 MHz to 2.45 GHz and 5.8GHz (Akins, p 302). Because most of the clients (laptops) that accessed the network in Thailand used 2.4 GHz 802.11g network interface cards, the 802.11g 2.4 GHz radio was used for client access to the network. The 802.11g standard is also backwards compatible to 802.11b network interface cards, which are found in older laptops.

4. IEEE 802.11i

The 802.11 wireless security has being under scrutiny after the realization of how easy it was to gain access to the Wireless Equivalent Protection (WEP) protocol. The 802.11i standard addresses the weakness of the WEP security method. The 802.11i standard includes the use of 802.1X port-based authentication and use of the thought-to-be unbreakable AES encryption algorithm (Akins, p 316). Due to the extreme processor

requirements imposed by the complex AES algorithm, vendors had to come up with innovative ways to implement this standard without jeopardizing network throughput.

C. 802.11 RF PROTOCOLS

The WiFi alliance promotes and tests for wireless LAN interoperability of 802.11 devices and when the product meets the standards released by the IEEE committee, the WiFi alliance grants the product a certification which allows the vendor to use the IEEE 802.11 logo for the certified product (Akins, p 320).

The Institute of Electrical and Electronics Engineering (IEEE) is the key LAN standard maker for most things related to information technology in the United States (Akins, p 311). This organization creates its standards within regulatory guidelines of the countries in which the standards will be applied. In the case of wireless networks, the IEEE develops standards for wireless LAN operation within the framework of regulatory guidelines (Akins, p 11). Figure 5 depicts the layers of the OSI model; this thesis focuses only on the Physical and Data Link Layers.

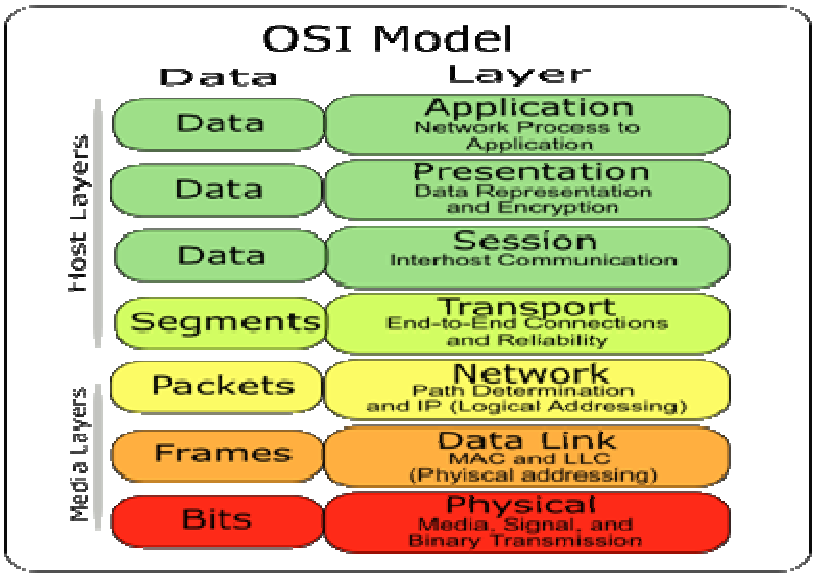


Figure II-5. Open System Interconnection Basic Reference Model (from www. images.google.com/images, JAN 2008).

1. Data Link Layer

Layer 2 access points' network management capabilities occur at the layer 2/Data Link Layer of the Open Systems Interconnection model OSI model (which consists of seven layers that support network communications). See Figure II-5. At each layer, protocols perform services unique of that layer; while performing those services, the protocols also interact with protocols in the layers directly above and below (Dean, p 44). The Data Link layer of the access points determines how the APs function as a network. The Data Link layer is made up of two sub-layers, Logical Link Control (LLC) sub-layer, provides an interface to the network protocols, manages flow control, and issues requests for transmission for data that has suffered errors (Dean, p 53). The second sub layer is the Media Access Control (MAC) layer which is the lower sub layer of the Data Link layer. The MAC layer manages access to the physical medium by appending the physical address of the destination computer onto a data frame (Dean, p 54). Network traffic is also relayed utilizing the Media Access Control Address (MAC) of the connected APs or computers to route information through the network. The MAC address is the physical address of the object connected to the AP i.e., computer, another AP or switch

All 802.11 vendors have to follow IEEE 802.11 standards when building their products for public use if they want interoperability with others' products but there are exceptions that allow the implementation of proprietary functions.

Vendors follow the standards not because there's any coercion but out of enlightened self-interest. They do it because mult-vendor interoperability allows them to sell more products.

The 802.11f standard defines how two APs establish network connection between each other. The standard intentionally left it up to the vendors to create protocols that the access points could use to talk to each other (Akins, p 315). For an access point configured as a mobile AP, the ability to hop AP to AP as it traverse an area of operation is determined by the Data Link layer proprietary functionalities.

2. Physical Layer

The Physical layer is where the bits from the upper layers of the OSI is transformed into a transmit signal and passed either through a hardwire or wireless conduit. The bits that are sent to the Physical layer are in the form of a frame of bytes which can be at most 2304 bytes of payload for wireless local area network (Akins, p 366). The payload carries the layer 3 through 7 information package into a frame for transmission. When receiving data, the Physical layer protocols detect voltage and accept signals, which they pass on to the Data Link layer, which then is forward up the OSI chain (Dean, p 55). Because the Physical layer connects wireless APs and hardwire to computers and routers, the outside environmental effects i.e., power surges, vegetation, water, weather and terrain had the most influence on this area of the 802.11 products that were being evaluated.

a. Doppler Shift

Doppler shift is a very important factor that must be considered in a mobile application. Doppler shift occurs when a radio frequency wave source and a receiver are moving relative to one another; for instance a mobile subscriber station moving from one AP to another; the signal strength of the AP being approached by the mobile subscriber station will be more intense and the signal strength of the first AP would fade as the mobile subscriber station gains distance.

Therefore, as the mobile subscriber station moves towards a ground AP, the signal strength should increase which should result in the mobile subscriber station shifting to the better RF signal and disassociate with the weaker signal.

b. Antenna

The antenna utilization in a mobile application versus a stationary application can be very different. For instance, in a ground application utilizing directional antennas in a point to point configuration provides a better link over long distances and also provides the best network throughput because the RF energy is

focused. On the other hand, utilizing directional and omni-directional antennas in a multipoint configuration provides the best throughput to multiple stations but distance is limited because the omni-direction antennas RF energy is not focused. For mobile applications, an omni-directional to omni-direction configuration provides the most reliable connectivity since the mobile unit can travel in a 360-degree pattern and maintain connectivity. Because the 2007 COASTS deployment required fixed and mobile links in the network architecture both directional and omni-directional antennas were used. In particular, the hyper-link 8dbi 5.8GHZ omni-directional antennas were chosen because of their higher vertical beam width, and because it provided the best connectivity in the mobile operational tests. High gain dipole (Omni-directional) antennas offer more horizontal coverage (distance) and reduced vertical coverage (vertical beam width) (Akin, p 75). In a mobile environment, vertical radiation is more of a concern than horizontal radiation, because the wider the vertical radiation pattern the more likely it is to have a link between two omni antennas when they are not fixed and distances beyond one mile are not required. When a vehicle is in motion, whether it is on paved or non-paved road, the vehicle will always be subjected to dips and valleys due to the imperfection of the road. Therefore, an omni-directional antenna with a large vertical beam width would increase the link stability in a mobile environment with road contour imperfections and that is why the 8dbi omni-directional antennas were used instead of the 12dbi omni-directional. Figure II-6 and II-7 illustrates the 8dbi omni-directional antenna's 10 degree increase in vertical beam pattern over the 12dbi omni-directional antenna.

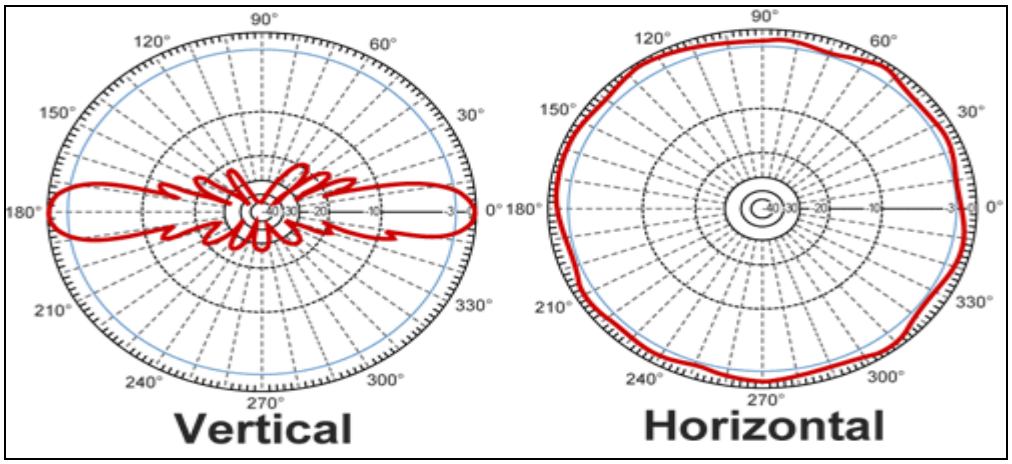


Figure II-6. Hyper-link 8dbi vertical and horizontal beam patterns (from www.hyperlink.com, AUG 2007)

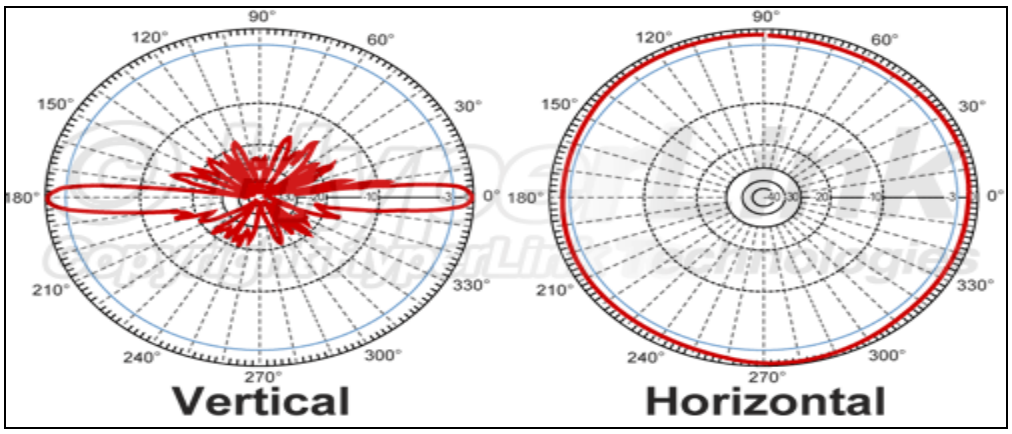


Figure II-7. Hyper-link 12dbi vertical and horizontal beam pattern. (from www.hyperlink..com, AUG 2007)

c. Fresnel Zone

Fresnel zone blockage can have a major affect on network throughput and in a mobile application blockage is most likely unavoidable. The Fresnel zone is an area centered on the visible line of sight between the transmitting and receiving antenna (Akins, p 88). See Figure II-8. When an object obstructs the Fresnel zone, energy is absorbed and prevented from getting to the receiver. If too much of the Fresnel zone is blocked, even if visible LOS exists, there won't be enough energy to get the signal

through to the receiver (Akins, p 88). For the mobile tests conducted at Fort Ord, in order to have 80 percent clearance of the LOS path between the mobile and third ground AP, at least 9.6 feet of the Fresnel zone had to be clear between these two APs. As indicated by the calculations in Table II-1, the Fresnel zone from the third AP to the mobile AP was 12 feet. Figure II-8 is an illustration of what a Fresnel zone would look like between two APs and based on the distance and radio frequency used to establish a link, the Fresnel zone radius was 12 feet.

* denotes a required field	
Calculation Input	
Distance between antennas*	Miles: 0.53
Frequency (f)*	GHz: 5.8
Calculation Results	
Fresnel Zone Radius (r)	Feet: 12
80% of Fresnel Zone Radius (r)	Feet: 9.6

Table II-1. Fort Ord Mobile test Fresnel Zone Calculation (from www.terabeam.com AUG 2007)

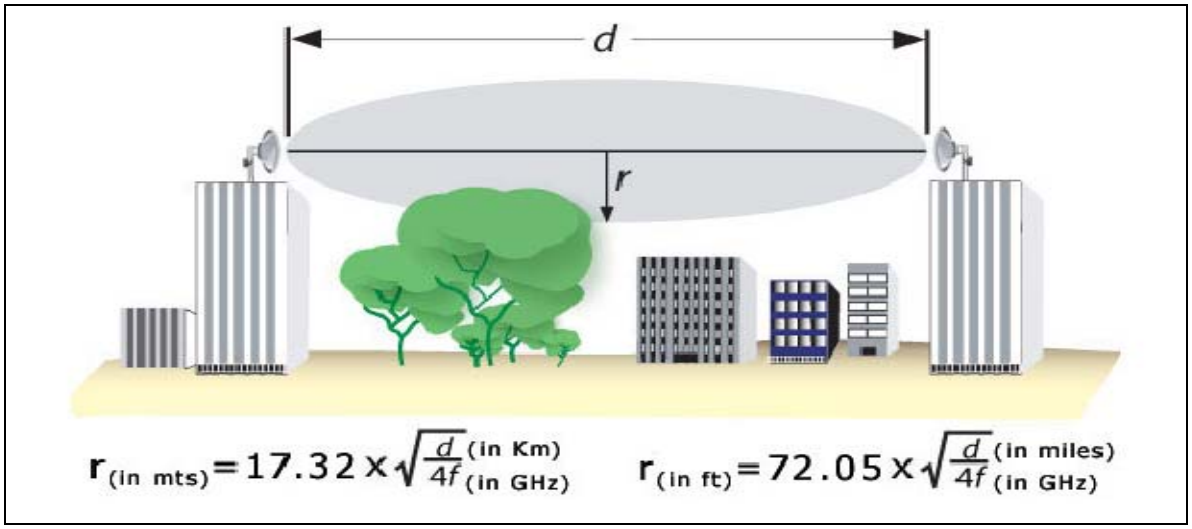


Figure II-8. Fresnel Zone Formula (from www.terabeam.com AUG 2007).

D. 802.11 WIRELESS LINK SECURITY

In any wireless network, throughput is most often sacrificed for security. Fortunately, network security can be applied at each layer of the OSI model, which can limit network throughput sacrifices. For COASTS 2007, the scope of the network security applications stopped at layer 2 for network security for the deployed 802.11 wireless network for COASTS 2007.

1. Wireless Equivalent Privacy (WEP)

Wireless Equivalent Privacy (WEP) provides only mediocre wireless security for 802.11 products deployed in the home or office. It was not designed to provide tactical wireless security from professional hackers. Therefore, many vendors became very concerned when their products became useless because this security method did not properly defend against hackers. WEP encrypts all data in the frame from the LLC layer on up the OSI stack, such as IP headers, TCP headers, and application data (Akins, p 427). This encryption occurs only within the network segment not end to end. End to end encryption is accomplished with VPN devices and is only necessary when encryption across the internet is required. But because the layer 2 (802.11) headers were not encrypted an attacker could see the MAC addresses and management frames of a wireless AP that was being relayed to from a laptop. This did not cause the downfall of WEP, but rather it was how the RC4 algorithm was implemented. The RC4 stream cipher is fast and efficient when encrypting and decrypting, which minimizes its impact on network throughput (Akins, p 426). Unfortunately, the way WEP implemented the RC4 encryption algorithm allowed attackers to determine which frames were encrypted using mathematically weak keys (Akins, p 427). Tactically, WEP should not be used as the only source of wireless security. Therefore, while important to the WiFi arena, WEP implementation is outside the scope of this thesis. The defects with WEP apply equally to both wireless devices being tested therefore not treated further.

2. IEEE 802.11 Protected Access (WPA)

The 802.11i committee was formed in 2001 to increase MAC layer security in 802.11 products. The IEEE 802.11 Protected Access (WPA) was released by the IEEE 802.11- Alliance in order to provide better than WEP security until the 802.11i standard was completed. The WPA defined advanced modes of authentication and encryption, including the use of WEP for backwards compatibility with non-WPA stations (Akins, p 438). WPA did provide better wireless access control than WEP.

3. IEEE 802.11 Protected Access (WPA2)

The 802.11i standard defines MAC layer security enhancement for 802.11(Akins, p 441). This security standard utilizes the advance encryption standard (AES) which provided more security at the expense of CPU processing power. WPA2, which is the same as 802.11i standard, was used during the Thailand field exercises because it offered better wireless security against the deployed Red Team who job was to attack the wireless networks.

4. Common Criteria

The common criteria (CC) evaluate the protection of information from disclosure, modification or loss of use (confidentiality, integrity, availability) (Burke, p 2 lesson 25). The CC provides assurance that the process of specification, implementation and evaluation of a computer security product i.e., computers, access points, routers etc… has been conducted in a rigorous and standard manner. The CC has seven predefined assurance packages, on a rising scale of assurance; known as Evaluation Assurance Levels (EALs) (Burke, 9) lesson 25). The common criteria help vendors to develop their products by the defining security requirements for them to build the products too. For the users, the CC ensures that the product security features have been evaluated against standardized security criteria. The CC provides a third party evaluation of a product's security capability claims. Some 802.11 devices are put through this process and if the device meets all established requirements then it receives an EAL number from one being the least rigorous to an EAL 7 being the most rigorous test and evaluation. A product

that has an EAL stamp provides assurance to the procurer that the product is functionally sound. For the products being evaluated in this thesis, one product has an EAL of two and the other does not; therefore, the test and evaluation of these two products should result in the product that received the EAL of two performing better than the product without the EAL stamp.

E. CHAPTER SUMMARY

The 802.11 wireless access points are built with standardized IEEE 802.11 protocols defined by IEEE committee; but the vendor's proprietary protocols make each product unique in its own way. Therefore, through three field operational tests, the IEEE 802.11 technologies proprietary protocols were tested by observing mobile capability, video support capability, security, network reliability, usable throughput capability, remote management capability and transportability. The results were analyzed and compared to determine the suitability of Mesh Dynamics and Fortress 802.11 devices for COASTS 2007 and future military operations. Details of the operational tests and evaluation are contained in Chapters IV, V and VI.

THIS PAGE INTENTIONALLY LEFT BLANK

III. TECHNOLOGY COMPARISON

Both Mesh Dynamics and Fortress claim to be able to provide network connectivity in a mobile application from AP to AP and network connectivity beyond line of sight. These capabilities are beyond the basic capabilities of basic 802.11 WiFi devices. For the test and evaluation of the products ability to perform the above capabilities, a ground daisy chain out to 1.5 mile was used and a mobile capability out to one mile was as the standard distances for the tests.

Mesh Dynamics and Fortress APs topology functionalities are very different. Mesh Dynamics APs interconnect to each other making a fully meshed network where all APs are connected to multiple APs within the network. By contrast, Fortress APs only communicate to the root AP. See Figure V-2 and V-14 in Chapter V. For the 2007 COASTS wireless networks, a fully Meshed topology was desirable but a network that allowed most redundancy and provided the most usable throughput in a tactical operational environment was the main operational goal.

The Mesh Dynamics and Fortress ES520 802.11 wireless devices can function as or with a BSS or an ESS, but in their deployment for mobility and tactical ground operations for COASTS 2006 and 2007, their ability to communicate from AP to AP was tested and not communication from client (laptop) to base station (access point). Currently there are no 802.11 wireless standards that define how an AP communicates to another AP, therefore the testing that was conducted for Mesh Dynamics and Fortress AP to AP functionality was on proprietary system implementations. The objective was to determine mobile AP ability to roam from AP to AP as it traverses the AOR within a single segmented wireless network.

A. MESH DYNAMICS 802.11 WIRELESS NETWORK MODULES (4000 SERIES)

Mesh Dynamics vendor began production of their APs in 2005 and in 2006 the Cooperative Operations and Applied Science & Technology Studies (COASTS) group at NPS began using the Mesh Dynamics APs for network operations. The Mesh Dynamics Mesh Modules ™ are a part of a family of products that provide many improved capabilities in network management, bandwidth and AP configuration. Figure III-1 shows the modules and connectors. There are a total of four N-Female connectors for antenna connection and two Ethernet Ports. Some of the key specifications for Mesh Dynamics Mesh Module ™ APs are listed in Table III-1.

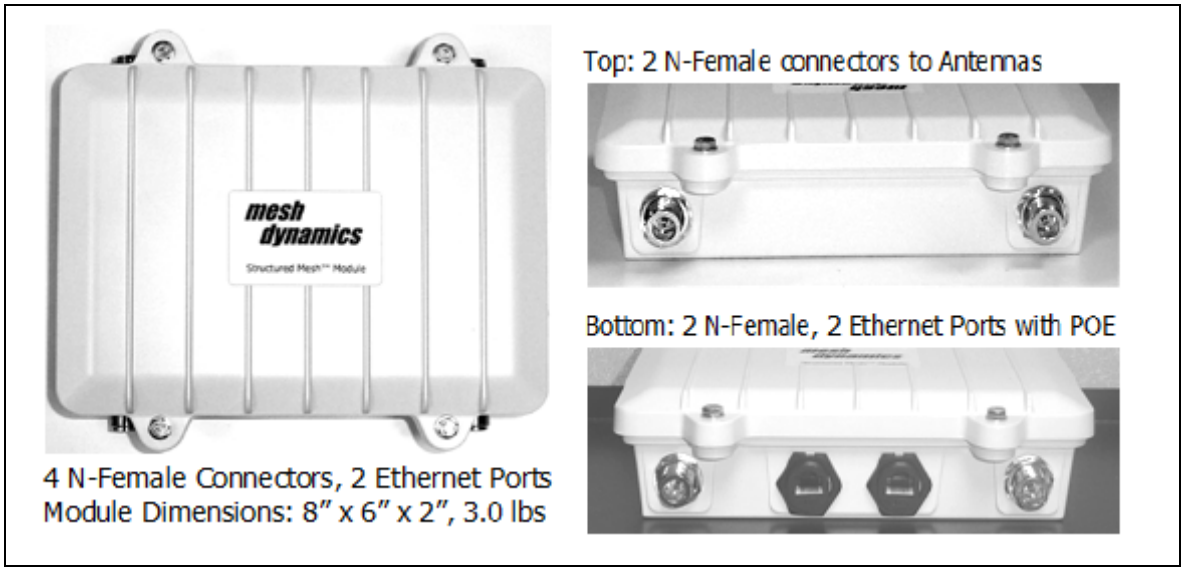


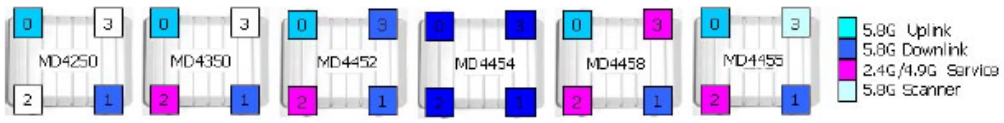
Figure III-1. Mesh Dynamics Mesh Module AP (from www.meshdyanmics.com, SEPT 2007).

MD4000 Specifications/Certifications	
Dimension, weight and weather Rating	8” (length) 6” (width) 2” (height), 3.0 lbs. NEMA 67 weather tight.
System Operating Temperature Range	-40 to + 85 degrees Celsius.
System Power Consumption	5-16 W depending on number of radios (up to 4 in one enclosure)
Supply Voltage Range Supported	12 VDC – 48 VDC. 24 VDC, 2A POE available from Mesh mics.
Ethernet Ports	Two. Power over Ethernet (POE) supported on ETH Port 1. One. May be exposed through second Ethernet Port.
Serial Ports	
Number of Radio card slots in Enclosure	Up to four field upgradeable mini-PCI radios per enclosure.
Radio Frequency Bands Supported.	2.4GHZ, 5.8GHZ and 4.9GHZ Atheros based radios.
Radio Output Power Supported (millwatt)	Each radio is capable of transmission at up to 400 mw.
Radio Transmit Power range (dbm, typical)	21 dbm at 54 Mbps, 25 dbm at 12 Mbps or lower
Radio Receive Sensitivity range(dbm, typical)	-75 dbm at 54 Mbps, -90 dbm at 12 Mbps or lower.
Backhaul Capacity (raw)	54 Mbps raw, 108 Mbps raw, Turbo mode.
Backhaul Capacity TCP/IP	22 Mbps TCP/IP, 44 Mbps TCP/IP Turbo mode. Validated by USAF
Bandwidth Degradation	No degradation over multiple hops. Validated by USAF.
Latency Between hops	Less than 1 millisecond per hop. Validated by USAF.
Maximum number of hops	Field-tested at 18 hops, string-of-pearl, 18 Mbps TCP/IP at end.
128 bit Security/Encryption	Support both WEP and WPA/AES
Secure Backhaul Traffic	128 Bit WPA/AES encryption (e.g. with temporal keys).
Priority Traffic and IEEE 802.11e	Up to 4 IEEE 802.11e compliant categories supported.
Multiple VLANS and Multiple SSIDs	16 standard. Hidden SSID with muted beacons also supported
RF Bandwidth control	Selectable based on settings available for all radios.
RF Transmit Power Control	Slider scale user settable for all radios (0-100%)
RF Adjustable ACK timing for long range	Range: 50 us 500 us, for all radios.
RF Auto Channel Management	Manual overrides/channel exclusions also possible.
GPS radio support in enclosure	Uses serial line connection and one N-FEMALE antenna port
Ability to Change Channel Width	For Non FCC applications channel width settable to 5, 10, 20, 40 MHz
Ability to set custom channel frequencies	Center Frequency of Channel settable via NMS utility
Multi-country support	Country and channel selection, NMS settable.
Module is FCC/CE Compliant	FCC ID: UZU-MD5, UZU-MD2
U.S. Government Supplier Approved	GSA Contract GS-35F-0652T

TableIII-1. Mesh Dynamics Mesh Module AP specifications (from www.meshdynamics.com, SEPT, 2007).

1. Radio Layout

The Mesh Modules are capable of supporting up to four 400mw radios and can be configured to operate in both the 5.8GHZ and 2.4GHZ ranges. As mentioned earlier, the Mesh Dynamics APs have four N-Female slots, which are labeled as slot 0, 1, 2, and 3. Slots 0 and 1 are normally used as backhaul uplink and downlink radios and slots 2 and 3 are used for operating non-interfering channels. See Figure III-2 for a more detailed view.



5GHZ Backhaul Products (operating in 5.250GHz- 5.350 GHz, 5.4000GHz- 5.700GHz, 5.725GHz – 5.845GHz)	
MD4250-AAxx	2-Radio module 5GHz BH uplink and downlink Structured Mesh Backhaul (BH), slots 0, 1.
MD4350-AABx	3-Radio module 5GHz BH in slots 0,1. 2.4GHz AP radio in slot 2. AP client connectivity settable to b, g, b and g.
MD4455-AABA	4-Radio mobile mesh module 5GHz BH in slots 0,1. 2.4G AP radio in slot 2. 5GHz Mobility Scanner radio in slot 3.
MD4452-AABA	4-Radio module 5GHz BH in slots 0,1. 2.4GHz AP radio in slot 2. Second 5GHz Backhaul downlink in slot 3.
MD4454-AAAA	4-Radio module with 4 radios all 5GHz downlinks. Intended as a root node with four 90 degree panel antennas
MD4458-AABB	4-Radio module 5GHz BH in slots 0,1. Two 2.4GHz AP radios in slots 2, 3. AP connectivity settable to b, g, b and g.

Figure III-2. Mesh Dynamics Mesh Module AP Radio layouts (from www.meshdynamics.com, SEPT, 2007).

A single radio 802.11 device provides both client and backhaul services i.e., client laptop to AP and backhaul AP to AP. Within this device, an 802.11a radio is used for backhaul and an 802.11b/g client service radios are used for client access to the AP. In this particular set-up, the backhaul radios have to send and receive information on the same radio were as with the multiple radio configurations of Mesh Dynamics one can send and receive information at the same time. This functionality is like full duplexing, which is receiving and sending information at the same time.

Mesh Dynamics has a patent-pending on the logic that allows the Mesh Dynamics APs to operate with multiple radios.

> Mesh Dynamics' patented and patent-pending solutions begin by adding additional logical- or physical radios to each mesh node. One radio is used to create a link to its upstream (nearer the wired source or "root") node. Another radio creates a link downstream to the next neighbor node. Unlike second-generation solution, these two radios may use different channels - one for the upstream link, another for the downstream links (multiple down links are supported). Using different channels dramatically reduces performance degradation over multiple hops. Mesh Dynamics third generation products are being used in 10+ radio hop networks. Previous generation products typically run out of steam after the third hop (Why Structure Mesh, p 2).

Mesh Dynamics multiple radio configuration should provide a network with throughput advantage because one radio is dedicated to sending and one radio is dedicated to receiving network traffic which should limit bandwidth lost therefore increasing throughput. In conventional AP radio setups, one radio sends and receives the network traffic, which means some bandwidth is lost because of the switching between sending and receiving traffic.

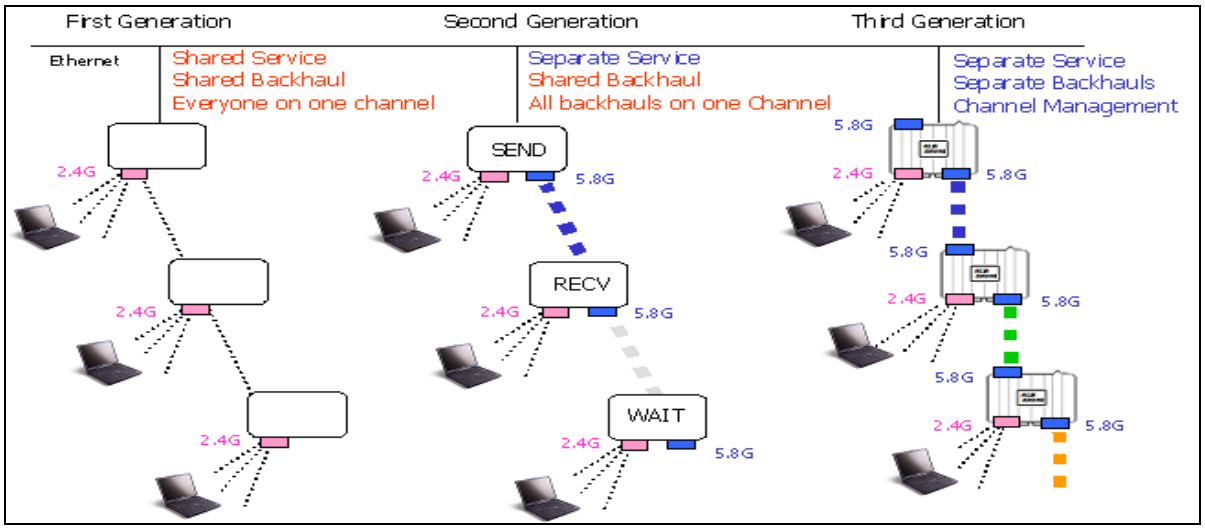


Figure III-3. Two Radios versus Four Radio Network Architecture (from www.meshdynamics.com DEC 2007).

2. Network Management Capabilities

The Mesh Dynamics network capabilities does not follow the accepted standard of using management information bases (MIBS) via the Simple Network Management Protocol (SNMP). Instead, the Mesh Dynamics Mesh Modules have a proprietary network manager called Network Management System (NMS), which provides the ability to configure, monitor and analyze the Mesh Dynamics APs activities locally. Through the use of Java technology, the NMS can run on any PC with Java runtime environment installed. Each activated AP appears as a graphical widget in the NMS and can be individually monitored and configured. Health information such as, throughput, temperature, transmit rate, packets moved and signal strength are all provided on the deployed APs through the NMS on a single console(laptop). Figure III-4 depicts some of the features that the NMS provides for user interface.

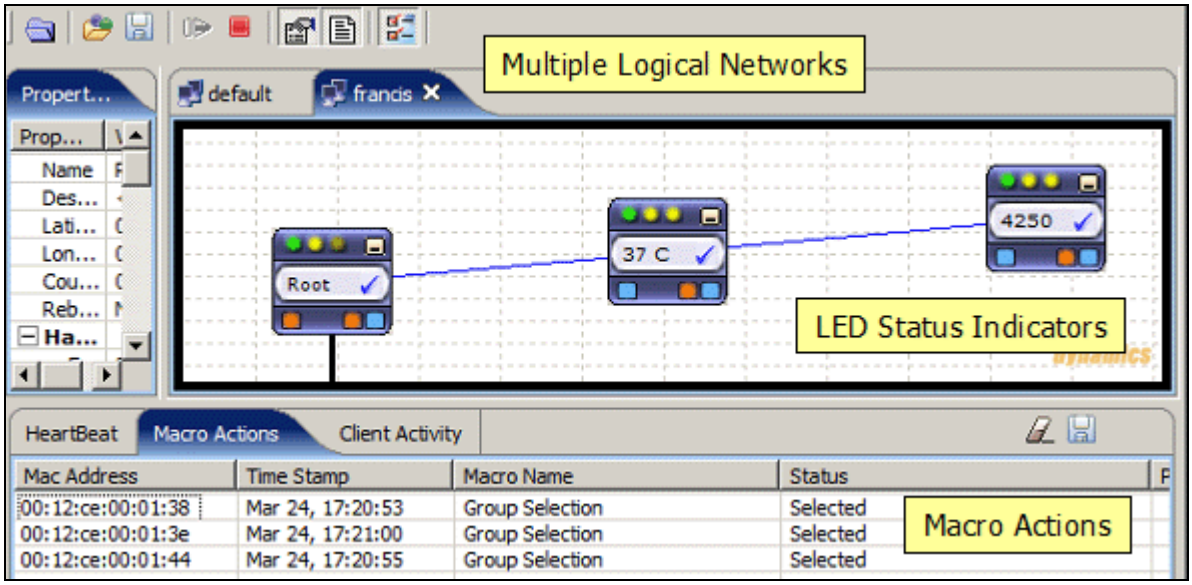


Figure III-4. NMS Display of Three Deployed AP Activity (from www.meshdynamics.com DEC 2007).

This remote manager is proprietary, and the excerpt below is from the Mesh Dynamics NMS user guide explains how the NMS was developed.

> The network manager is written in Java on top of IBM's Open Source Eclipse Development Platform. The look and feel has been changed to support OEM customer requirements. Customization projects include branding – OEM customer logos on the screen and Help page. Additionally, specialized features on the mesh modules require their own custom interfaces. These dialog boxes are merged with the menu system. Contact your Sales Engineer regarding your NMS customization requirements (Mesh Dynamics NMS User Guide, p 27).

The Mesh APs also have a special feature that automates RF channel selection for RF interference avoidance. For instance:

> Mesh Dynamics' third-generation Structured Mesh TM algorithms detect and avoid RF interference from non-Mesh Dynamics products. Each node contains the equivalent of a radio spectrum robot, monitoring other radio traffic, tracking its neighbor Mesh Dynamics mesh nodes, and adjusting the topology and channel mapping on the backhauls automatically, and without disturbing users' sessions. The backhaul radios switch channels to provide consistent backhaul performance -- automatically! (Why Structured Mesh, p 5)

This capability is proprietary and makes the Mesh APs very unique in that they can avoid RF interference without network manager intervention.

3. Mobile Capabilities

The Mesh Dynamics APs utilizes a proprietary protocol that acts like a router by utilizing the MAC addresses of the connected Mesh Modules to form a local meshed topology. The Mesh Dynamics vendor does not define how their APs handle loops. Instead they advertised that each AP has the ability to sense the optimal route for data transfer and if a AP that is designated to receive data suffers a casualty, the self-healing and dynamic control mechanism implemented in the Mesh Modules will shift to the second best AP to route the information. Figure III-5 depicts Mesh Dynamics APs' mobility characteristics. As the mobile AP, node 4455 pass from the root AP, node 4452 to second ground AP, node 4350, the signal strength of the second AP would be greater resulting in the mobile AP shifting connectivity from the root AP to the second ground

AP. Because the Mesh Dynamics connects to more than one AP at a time, bridging availability is higher and multiple segments can be connected with multiple network routes. See Figure III-5.

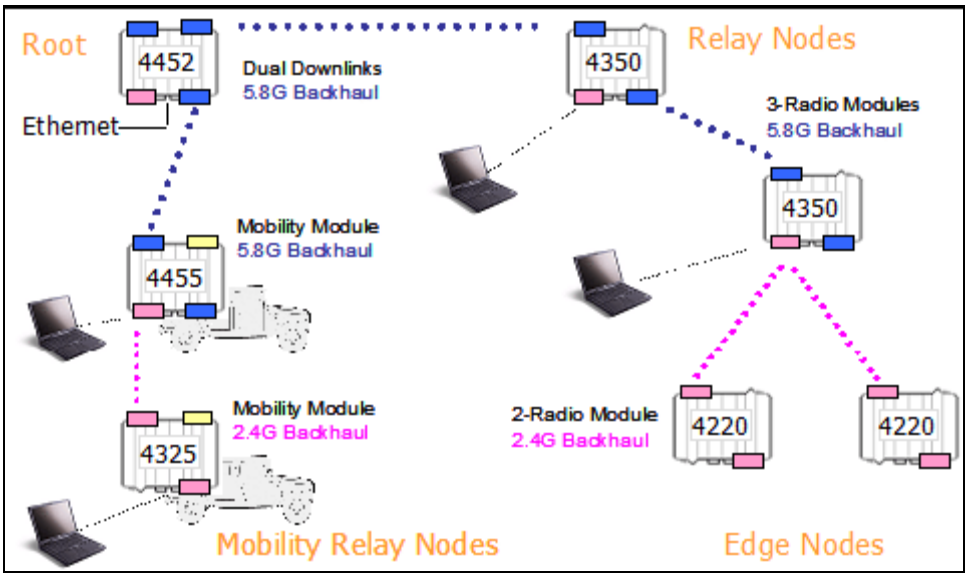


Figure III-5. Depicts AP to AP Mobility. (from www.meshdynamics.com, DEC 2007)

4. Multicast Capabilities

Multicast occurs when each packet is sent from one sender to multiple receivers with a single "transmit" operation (Multicast Conformance and Performance Testing from www.ixiacom.com). Mesh Dynamics does not have a multicasting capability; instead Mesh Dynamics uses the following method:

> Mesh Dynamics' patented and patent-pending solutions begin by adding additional logical- or physical radios to each node. One radio is used to create a link to its upstream (nearer the wired source or "root") node. Another radio creates a link downstream to the next neighbor node. Unlike second-generation solution, these two radios may make use of different channels.
>
> This increases the bandwidth of the network in two ways.
>
> Firstly, each node may be sending and receiving simultaneously to its upstream and downstream neighbors, unlike first-or second-generation nodes, which must continually "turn around" between sending and receiving upstream and downstream.
>
> Secondly, because each link is managed independently, the available channels may be re-used across the network. This expands the available spectrum, increasing performance of the network 50 times or more compared to first- and second-generation solutions.
>
> Distributed intelligence in each node allows for agile channel switching to avoid interference sources while still permitting rapid set-up and additions to the wireless mesh network (Why Structured Mesh, p 2).

The second-generation solution as referenced in the first paragraph is referring to how conventional access points receive and send information via the same radio. Multicast for these types of access points increase the send and receive efficiency by transferring information to all APs at one time. Mesh Dynamics on the other hand does not have a multicast capability but by having two backhaul radios vices one allows each AP to receive and send information at the same time. The two backhaul radios implementation eliminates the requirement for a multicast capability for network efficiency because each AP has a radio dedicated to receiving information and sending information. Therefore the Mesh Dynamics APs do not multicast but rather duplex which is ability to receive and send information at the same time.

5. Security Capabilities

Mesh Dynamics APs have all of the latest wireless security standard requirements implemented ranging from WEP to WPA2 (IEEE802.11i) which provides client side encryption and the backhaul traffic is encrypted at all times with 128 bit WPA/AES

encryption. This security implementation provided security at layer 2 for network access control and data protection The Orthogonal Frequency Division Multiplexing (OFDM) algorithm provides more network throughput by using a low transmit power and wider-than-necessary bandwidth (Akins, p 197). The low transmit power capability provides transmission security against eavesdropping from the enemy. The wide bandwidth makes it very difficult for the enemy to degrade single strength during transmissions See Figure III-6 for more details.

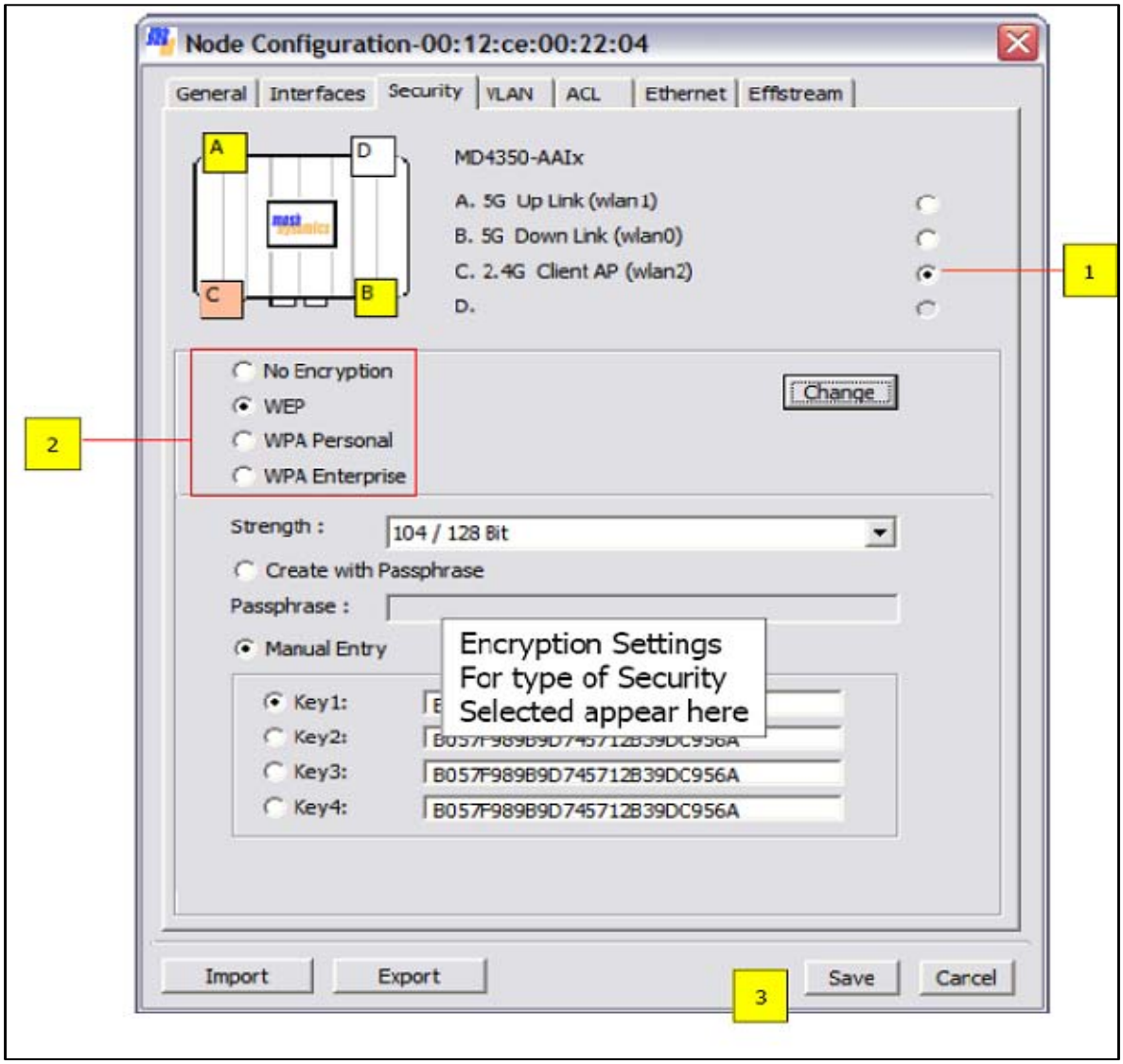


Figure III-6. Security Management Feature for Mesh Dynamics (from www.meshdynamics.com DEC 2007).

6. Certifications and Evaluations

The Mesh Dynamics APs were evaluated by the U.S. Air Force and in their evaluation, the following line items were evaluated: Bandwidth preservation over multiple hops, Bridge Latency over multiple hops, Rapid Self-Healing, Dynamic control of topology, and Dynamic Interference Avoidance. The evaluation resulted in the determination that the Mesh Dynamics two radio backhaul provided a distinct advantage over the traditional single radio solutions. See Mesh Dynamics website at www.meshdynamics.com for more details.

The Mesh Dynamics has a GSA contract which means the Mesh Dynamics APs can be procured by the military.

The Air Force evaluation and the GSA contract does not give Mesh Dynamics the proper certification and evaluation for military field operations. On the other hand certifications such as the WiFi alliance and FIPS-142-2 certifications gives the user the assurance that the product has gone through a legitimate operational test and evolution.

Federal Information Processing Standards (FIPS 140) were established in 1995 to provide assurance that encryption products deployed in US government applications performed properly, and that they provide appropriate levels of data protection (from www.fortresstechnologies.com, JUN 2007). The use of FIPS 140-validated encryption modules is mandated for all Federal network and communications systems that handle sensitive information. FIPS 140 has four levels which include the following: level one is the lowest which imposes very limited requirements, level two, provides requirements for tamper resistance, level three provides requirements for identity-based authentication, and for a physical or logical separation between the interfaces by which critical security parameters enter and leave the module and finally level four makes the physical security requirements more stringent, and requires robustness against environmental attacks (Burke, lesson one p 52). Therefore without this certification the product can only be used in non-sensitive deployments.

Mesh Dynamics has not been through the FIPS process and they claim to implement the WPA2/802.11i standards. They also claim that all traffic is encrypted but

do not indicated whether only the payload (Data, IP addresses, routing INFO) or the entire layer 2 payload (which include the addition of the MAC addresses) is encrypted.

The WiFi alliance guarantees to the user that the 802.11 device met the IEEE 802.11a/b/g/i standards. Mesh Dynamics unfortunately does not have neither the WiFi nor the FIPS 140-2 certifications and with its multiple proprietary implementations require that user understand where the device stands in regards to validity as an 802.11 product.

B. FORTRESS ES520 802.11 WIRELESS ACCESS BRIDGE

Fortress Technologies began production of the ES520 APs in 2006 and in 2007; the Cooperative Operations and Applied Science & Technology Studies (COASTS) group at NPS began using the ES520 APs for network operations. The ES520s are equipped with dual radios that allow simultaneously wireless backhaul and access. The eight port Ethernet switch ports make this AP idea for voice and video peripheral devices (from www.fortresstechnolofies.com, JUN2007). The ES520 achievement of FIPS-140-2 approval, IEEE 802.11 certification, and military ruggedness set it apart from the average AP. See Figure III-7. Some of the key specifications for Fortress Es520 APs are listed in Table III-2.

Figure III-7. ES520 AP by Fortress Technologies (from www.fortresstechnologies.com JUN 2007)

.

ES520 SPECIFICATIONS

FEATURES AND PERFORMANCE

range	· tested up to 32 miles (directional antenna) · tested up to 7 miles (omnidirectional antenna)
performance	· up to 100 secure clients
encryption	· AES-128, 192, 256 · WPA2 (802.11i) · NSA Suite B Cryptography upgradeable
authentication	· internal or external RADIUS, PKI/CAC · network, user and device
management	· secure browser-based GUI, CLI or SNMP
SSID support	· up to 4 SSIDs

HARDWARE

enclosure	· rugged .125" aluminum · NEMA 4
mounting	· mast mounting kit and weatherizing kit included
chassis dimensions	· 2.7"H x 8.8"W x 8.2"D (6.9 cm x 22.4 cm x 20.8 cm)
with connector ends	· 2.7"H x 8.8"W x 10"D (6.9 cm x 22.4 cm x 25.4 cm)
weight	· 4.9 lbs. (2.2 kg)
connections	· eight RJ-45 10/100 LAN ports w/ auto-MDIX and PSE · RJ-45 10/100 weatherized WAN port with PoE receiver · two RJ-45 serial ports (1 console port) · USB port for future functionality
radios	· 200mW 802.11a/b/g radio (max transmit power 23 dBm) · 400mW 802.11a radio (max transmit power 26 dBm)
antenna support	· 2 N-style external antenna connectors (female)
radio modes of operation	· wireless access point or bridge · 802.11h
power supply	· variable 7-30 or 36-60 VDC (AC adapter included) · PoE (injector included) · weatherized power connector with tethered cap · polarity protection
power draw	· 13W maximum (not including PSE)
power sourcing	· PSE, maximum power draw 55W
port LEDs	· link, activity, status, PoE
radio LED	· strength and association
warranty	· includes 1 year of maintenance and support

ENVIRONMENTAL

cooling	· convection (no fans)
operating temperature	· -10 to 55°C
humidity	· 5 to 95%
weather resistance	· water-resistant front panel cover plate included · IP56 · NEMA 4 · lightning arrestor
vibration, bounce & shock	· MIL-STD 810F

CERTIFICATIONS

safety & emissions	· CE, FCC, UL 60950-1, IEC 60529 (CB Test)
NIST	· FIPS 140-2 level 2
common criteria	· EAL3 submitted

www.fortresstech.com

Fortress Technologies Inc. Corporate Headquarters
4023 Tampa Road, Suite 2000, Oldsmar, FL 34677
Phone: 813.288.7388 or 1.888.4PRIVACY [477.4822]

FORTRESS® TECHNOLOGIES

Table III-2. Fortress ES520 Specifications (from www.fortresstechnologies.com, JUN 2007)

1. Radio Layout

The ES520 has the standard two N-Female ports connected to a 5.8GHZ and 2.4GHZ radio. The 5.8GHZ radio is used to backhaul wireless data and the 2.4GHZ radio is used for client access.

2. Network Management Capabilities

The ES520 does not follow the standard network management protocol provided by SNMP, instead, the Fortress ES520 has a basic graphical user interface used to configure different functions such as security, radio, and set authentication parameters to the AP. See Figure III-7 for more details. The ES520 securely propagates the configuration from one node to other nodes over both the wired and the wireless interfaces. With the 2.1.5 firmware upgrade, the operator is able to take new ES520 (slave) units and have these units receive their configuration securely from other nodes (master) in the network without the need to use a Command Line Interface (CLI) or GUI on the slave units(from www.fortresstechnologies.com, JUN 2007). The 2.1.5 firmware capability was not available during the COASTS 2007 deployment.

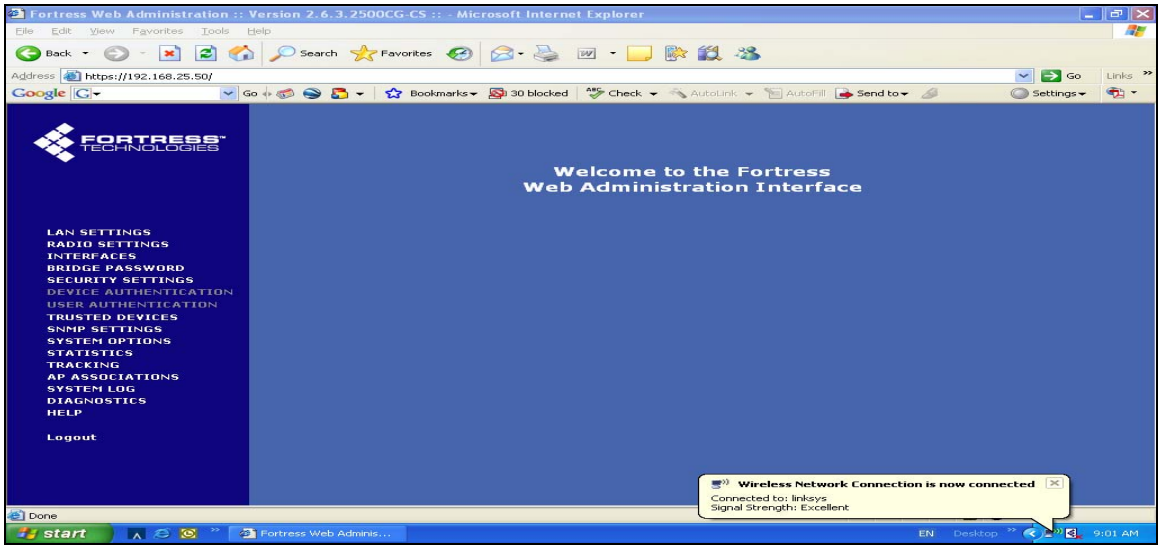


Figure III-8. ES520 Graphical User Interface (from www.fortresstecnologies.com, JUN 2007)

3. Mobile Capabilities

The ES520's were originally designed to connect to only the AP that was configured as the root AP. During the 2007 mobile test and evaluation period, the Fortress engineers upgraded the ES520's firmware to allow connection to the nearest available AP. This upgrade allowed the mobile AP to roam out of the RF view of the root AP and still send its network traffic through the closer non-root AP. The ES520 mobile capability is from AP to AP but the mobile AP can only connect to one AP at a time. This product does not have a network meshing capability; instead, the single mobile AP connects to the closer ground AP with the highest RF signal strength.

The ES520 APs differ from the standard commercial bridging APs in that it can shift from one bridge to another automatically. The below figure depicts Fortress Vehicle Area Network solution. The picture can be misleading in that the ES520s does not have mesh capabilities but they are semi-mesh capable in that the APs can be configured to shift to the closet available AP automatically.

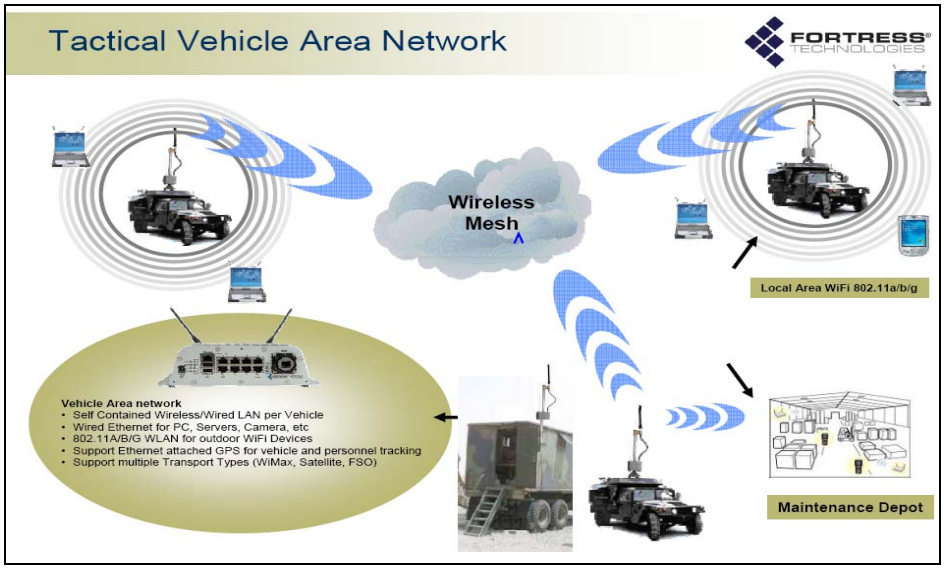


Figure III-9. Fortress Mobile Vehicle LAN Solution (from www.fortresstecnologies.com, JUN 2007).

4. Multicast Capabilities

The Fortress ES520s have a multicast configuration setting in its' GUI, and it was used in all network tests conducted for the 2007 COASTS operations. The multicast feature can only be used with a non-root AP because the root AP is responsible for broadcasting network traffic. The description of the multicast feature is described below.

> Wireless is an inherently broadcast medium. A multicast packet, like any other, is broadcast (by the root Bridge) to all nodes (non-root Bridges) on the wireless network. Each non-root bridge then examines the packet and:
>
> If the Bridge is an intended receiver, it accepts the packet. If the Bridge is serving as a repeater for an outlying bridge that is an intended receiver, it passes the packet along this route. If the Bridge is neither an intended receiver nor the repeater for an intended receiver, it drops the packet. Non-root Bridges on which Multicast is disabled will drop all multicast packets.
>
> The Multicast function applies exclusively to non-root bridges, and so can only be Enabled on Bridges with a Radio Mode setting of Bridge and a Bridge Mode setting of Non-Root (ES520 Bridge Guide, p 28).

All non-root APs were configured with the multicast feature activated as to allow the most efficient traffic flow. The multicast feature increased the network's reliability by broadcasting the information at one time to all APs connected to the root AP which resulted in a reliable network that supported video and data transfer.

5. Security Capabilities

The Fortress ES520 has a very robust security suite. At layer 2, the ES520 provides FIPS AES-256 encryption and protection against timing attacks (from www.fortresstechnologies.com, JUN 2007). The ES520 provides standard-based 802.1x port based authentication and allows for easy integration with Remote Authentication Dial In User Service (RADIUS) and DOD CAC PKI based on EAP-TLS protocols. The ES520 modular flexibility also allows it to be easily integrated with wireless intrusion detection (WIDS). The ES520 security capabilities have made it a highly procured

802.11 wireless device for many DOD organizations. The ES520 is also equipped with the standard WPA/WPA2 encrypting features for client to AP encryption.

The Fortress ES520 vendor claims to have strong encryption at the MAC layer, they state the following:

> Fortress ensures network privacy at the Media Access Control (MAC) sublayers, within the Data Link Layer (Layer 2) of the Open System Interconnection (OSI) networking model. This allows a transmission's entire contents, including the IP address and any broadcast messages, to be encrypted. Additionally, Fortress supports encryption algorithms: DES, 3DES, AES-128/192/256(from www.fortresstechnologies.com, JUN 2007).

6. Certifications and Evaluations

The ES520 has met all security and operational requirements that the DOD requires for wireless devices. Unlike most 802.11 wireless devices, the ES520 is FIPS 140-2 approved, IEEE 802.11 certified, conforms to Defense Information Systems Agency (DISA) JTIC standards, has been evaluated with the common criteria at EAL 2 with EAL 3 submitted (from www.fortresstechnologies.com).

The ES520's robust layer 2 security helped COASTS 2007 maintain a robust wireless defense against the Information Warfare Red Team from the Joint Electronic Warfare Center in San Antonio, Texas. More details of the ES520 performance is provided in Chapter V

C. CONCLUSION AND COMPARISON

The Mesh Dynamics APs have a distinct advantage over the ES520s in that they can connect to more than one AP at a time and automatically adjust network connectivity based on health of connected APs. This ability increases network availability and quality of service, which is highly beneficial in tactical applications. Mesh Dynamics also has a defined mobile capability, in that the vendors produced an AP with a scanner radio that scans the RF space for available Mesh APs. While scanning, the mobile AP's logic can shift to the available AP without user inputs. The Mesh Dynamics APs also have a very

user friendly graphical user interface. All APs can be monitored from one laptop; the network manager reports APs temperature, link status, security configuration, and throughput status.

On the other hand, Fortress ES520 has a very strong encryption solution at layer 2 with AES – 256 encryption, hardened rugged casting, basic graphical user interface, and has been tested a ranges up to seven miles using omni-directional antennas. The strong encryption and rugged casting makes the ES520 idea for harsh environment deployments. The ES520 also has gone through recent firmware update which has increased its network mobile usability. The GUI is user friendly but does not provide a consolidated interface that manages all APs at one time.

The Mesh Dynamics APs and Fortress ES520s have their own unique features that benefit the tactical user. Both products conform to the standard application of an ESS with two APs bridging two wired segments as seen in Figure II-2. The only difference is that the bridging capability is not standardized by 802.11 IEEE; therefore any wireless device with bridging capability will have proprietary implementations.

In comparing the two products Mesh Dynamics has the advantage in the categories of quality of service, remote management, and mobility. But as mentioned in this chapter, Mesh Dynamics products have not gone through a certification and accreditation process which makes the user vulnerable to procuring an incompatible product. In the case of the ES520, it has gone through the 802.11 WiFi alliance and FIPS 140-2 certification processes which ensure usability, ruggedness, security and interoperability.

Both products are not compliant with the standard SNMP for network management. Each product has a proprietary implementation for this functionality which limits network management to the local segment that the products are attached too.

The difference between Mesh Dynamics and the ES520 APs lie in how they extend the network segment through relaying from one AP to the next. End systems in

both cases, still attach to the last AP in the conventional IEEE 802.11 manner. Therefore subscriber station parts of these network segments are identical to each other and to a conventional WiFi segment.

Mesh Dynamics and Fortress unique capabilities were tested in a tactical application while deployed as part of the COASTS 2007 field experiments. All advertised advantages were stressed in mobile and ground applications which required that the devices be able to pass video, defend against network attacks, provide usable throughput in a mobile application, withstand high heat and humid environments, and be transportable. The detail of the devices network performance is provided in the following chapters.

IV. MOBILITY PERFORMANCE TESTS

The purpose of this chapter is to present the test objectives, evaluation methodology, field test results of the Fortress (ES520) and Mesh Dynamic (4000 series) access point (AP) mobile performance trials. Tests were conducted at Fort Hunter Liggett, CA from 16 JAN 2007 thru 21 JAN 2007 and at FORT ORD, CA conducted 30 JAN and 2 FEB 2007. The main operational test objective was to determine mobile capability by observing both Fortress ES520 and Mesh Dynamics 4000 series access points' ability to provide usable network throughput while deployed on flat and hilly terrain.

A. OBJECTIVE OF TEST

The main test objective was to evaluate mobile capability, as defined in Chapter II, by observing both Fortress ES520 and Mesh Dynamics Mesh Module access point ability to provide usable network throughput while deployed on flat and hilly terrain. Once usable throughput was established, a comparative analysis of Mesh Dynamics and the ES520 networks performance was conducted to determine suitability for COASTS 2007 MIO scenario and military mobile applications. The mobile test results for the ES520 and Mesh Dynamics networks are in the Results and Discussion section.

Because these products had different proprietary implementations at the Data Link Layer, results of the tests varied. So, the objectives established in this section were not only to support what the COASTS 2007 team required for mobility but also to discern which product had the most potential to provide uninterrupted network mobility within a 1.5 mile corridor and provide mobility for military applications i.e., pier surveillance, base security, and maritime operations.

As discussed in Chapter III, traditional access point mobility is from a subscriber station (laptop) to an AP. This form of mobility is limited to the power of the laptop and the AP. On the other hand, mobility from AP to AP is currently created through proprietary implementations, which is an advanced form of bridging. This form of

mobility extends the fixed ground network by making one AP mobile therefore extending the fixed network out via mobile means. In order to do this, the mobile AP has to be able to hop from AP to AP just like a laptop hops from AP to AP to maintain network connectivity.

As discussed earlier, bridging occurs when two wired segments are connected via two wireless APs. By taking the bridging concept and making one AP mobile, you create a mobile network, which gives user the capability to attach cameras to the mobile AP for surveillance operations, have multiple clients (i.e., cameras, PDAs, laptops, UAVs) send information in a mobile application from further distances from the fix network. The COASTS 2007 scenario required that a boat be outfitted with a mobile wireless AP to pass video and biometric information. Both Mesh Dynamics and Fortress advertise that their products are mobile capable so, in order to determine suitability for military mobile applications, and COASTS 2007 Maritime Interdiction Operations the objectives in this section were developed to test the devices mobile capability.

The following supporting objectives were utilized in both the Fort Hunter Liggett and Fort Ord mobile network performance test trials:

- To evaluate network connectivity in a mobile configuration while deployed on flat and hilly terrain.
- To evaluate network stability while traversing the area of operations.
- To evaluate maximum distance with an attached wireless ES520/Mesh Dynamics mobile network bridge to a mobile unit on flat and hilly terrain.
- To evaluate usable throughput in a mobile environment conducted on hilly and flat terrain.
- To evaluate mobile AP handoff capability while deployed on flat and hilly terrain.
- To evaluate remote management capability.
- To evaluate Mesh Dynamics frequency management protocol in a low RF environment.
- To establish a mobile network by configuring the ES520 mobile node as the root.

1. Evaluation Measures for the Tests

The tools used for testing the above objectives included IxChariot throughput script, see Chapter I for detailed discussion, Internet Control Message Protocol (ICMP), and visual observation. The details of how each objective was measured are as follows:

a) Network connectivity in a mobile configuration was measured by utilizing IxChariot throughput scripts and ICMP (ping). A minimum of 3Mbps was required in order to support network requirements for the COASTS scenario.

b) Network stability while traversing the area of operations was measured by visually observing breaks in mobile node links with ground nodes.

c) Maximum useful distance with an attached wireless ES520/Mesh Dynamics node to a mobile unit on flat and hilly terrain was measured by observing the distance at which the mobile node link became unstable.

d) Usable throughput in a mobile environment conducted on hilly and flat terrain was measured by utilizing IxChariot throughput script. In order to support the COASTS 2007 network requirements, a minimum of 3Mbps had to be maintained during the IxChariot script runs.

e) Mobile node's ability to associate to the nearest ground AP on flat and hilly terrain was measured by observing the time it took the mobile node to shift to the nearest ground node.

f) Network Management capability was measured by observing time and task requirements for operating, managing and configuring the nodes for operations.

g) Mesh Dynamics frequency management protocol functionality was measured by visually observing the mobile node's connectivity to ground nodes while the auto frequency management feature was active.

h) In order to establish mobile network architecture for the ES520, the root node or base station was configured as the mobile node. The ES520's ability to maintain a stable network with the root node attached to a vehicle as the mobile node was measured by observing mobile node connectivity to the ground nodes as it traveled through the AOR.

B. TEST METHOD

Mesh Dynamics and the ES520 access points' set-up, configuration and deployment were conducted in the same manner. The Fort Hunter Liggett and Fort Ord mobile field tests method was to deploy ES520 and Mesh Dynamics nodes/access points in order to test their Data Link layers' mobile capability from AP to AP utilizing the APs backhaul radio (802.11a) in unencrypted mode. See Chapter II for more details on the 802.11a protocol. While in the mobile configuration, Mesh Dynamics and the ES520 802.11 networks ability to pass data was measured utilizing IxChariot throughput script. Due to the video and data support requirement for COASTS 2007, no less than 3Mbps of network throughput was required for all mobile test runs.

The Fort Hunter Liggett test site was used to test the networks mobile performance while deployed on flat terrain and the Fort Ord site was used to test network mobile performance on hilly terrain. The objectives that were not completed at Fort Hunter Liggett were retested at the Fort Ord test site. The measurement of these eight test objectives are detailed in the evaluation measure section. The tests that were applicable to measuring network throughput were conducted in unencrypted mode so as to allow the maximum throughput for each test run.

C. FORT HUNTER LIGGETT TESTS

Fort Hunter Liggett location was used for three COASTS 2007 field tests because it offered the best layout and conditions for testing unmanned aerial vehicles(UAVs), wireless networks and camera devices that were used in the COASTS 2007 Maritime Humanitarian and SAR scenarios conducted in Thailand.

1. Test Conditions

This section will describe the terrain, weather conditions and topology during the Fort Hunter Liggett mobile test trials.

a. Terrain

Fort Hunter Liggett's terrain consisted of light vegetation with an overall flat layout. The mobile test was conducted along the main paved road (Mission RD) that runs through the base. Figure IV-1 is a Google Earth snapshot of the area of operations for the mobile test.

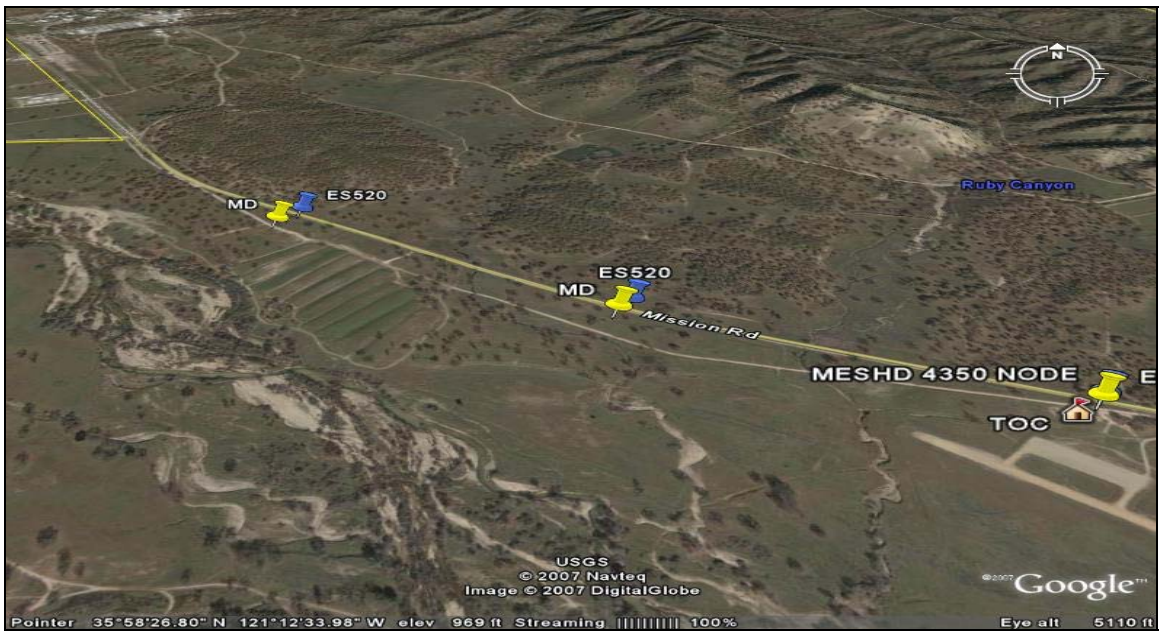


Figure IV-1. Fort Hunter Liggett Mobile AOR. (from Google Earth NOV 2006)

b. Weather

The weather was very suitable for wireless network testing in that the elements such as rain, fog and heavy wind were non-existent throughout the testing phase. The temperature remained at a constant level throughout the duration of the

mobile test trials. The early morning temperatures averaged in the mid to low 40(F)'s. The temperature gradually increased throughout the day peaking at mid to upper 50's. The terrain also offered a perfect topology for the mobile tests in that the paved road utilized for the testing was smooth and free of imperfections.

The two frequencies used for all field tests and the scenario in Thailand included 5.8GHZ (used to backhaul the data and video traffic) and 2.4GHZ (used to allow clients to access the network). The 5.8GHZ band was used because its RF spectrum was the least saturated and most laptops i.e., clients came with 2.4GHZ wireless cards. The 5.8GHZ and 2.4GHZ RF bands are not negatively affected by normal weather conditions but harsh conditions such as heavy rain, snow, fog and heavy wind can have an adverse affect on these frequencies which would cause degradation in network performance. For instance, snow, when collecting on trees and obstacles normally in part of the RF path(like fresnel zone), can act as a wall of water which can effect an RF signal and the same can hold true for leafy trees that hold lots of rain water (Akins, p 416). In the first test trials at Fort Hunter Liggett, it appeared weather did not affect network performance; nevertheless, weather data were recorded as a background variable to monitor conditions at all test sites. Weather data were also recorded because network degradation occurred previously in Thailand due to overheating during the COASTS 2006. Weather data were taken in the COASTS 2007 deployments in order to observe possible network degradation and possible factor comparative analysis. See appendix A for more detailed weather information.

c. Topology

Three modes in which an access point typically can be configured, are root, repeater and bridge modes. In all mobile and ground tests conducted with the ES520 and Mesh Dynamics nodes, at least one node was configured as the root node, which is used when a access point is connected to a distribution system through a wired interface and more than one node was configured as a bridge/non-root node which creates a wireless distribution link between two or more access points (Akin, p 222-223).

The mobile topology for the Mesh Modules and ES520s consisted of a total of two ground APs configured in non-root mode, one mobile AP configured in non-root mode, and one root AP. The ground APs were set at a lateral separation of 0.5 miles, starting with the root AP that was located at the Tactical Operation Area and the last ground AP was one mile from the root AP. (See Figure IV-1 for the layout) Each AP was attached to a tripod at a height of ten feet with an 8dbi omni-directional antenna attached to the 5.8GHZ backhaul antenna port and an 8dbi omni-directional antenna attached to the 2.4GHZ antenna port. Details of Mesh Dynamics and Fortress ES520 AP configurations can be found in Appendix B.

2. Mesh Dynamics Test Results

This section will present the test results for Mesh Dynamics network performance in the mobile tests conducted at Fort Hunter Liggett.

a. Results and Discussion

(1) Remote Management**.** The Mesh Dynamics Graphical User Interface network manager made network trouble shooting and configuration very easy during the Fort Hunter Liggett mobile test trials. All Mesh Dynamics APs used for the test trial were easily configured utilizing the Mesh Dynamics Network Management System. Mesh Dynamics NMS consolidates all connected access point's health, connectivity, power and data route information onto the managing laptop's screen. Figure IV-2 illustrates this connectivity. The AP with the solid black line is the root AP and the Meshed network connectivity to the internet starts at this connection point. This point also marks were the wireless network meets the wired network. Each AP can be managed by clicking on the icon displayed on the screen. This all in one display and reporting of deployed APs network information made network management very efficient for AP deployment for the test trial.

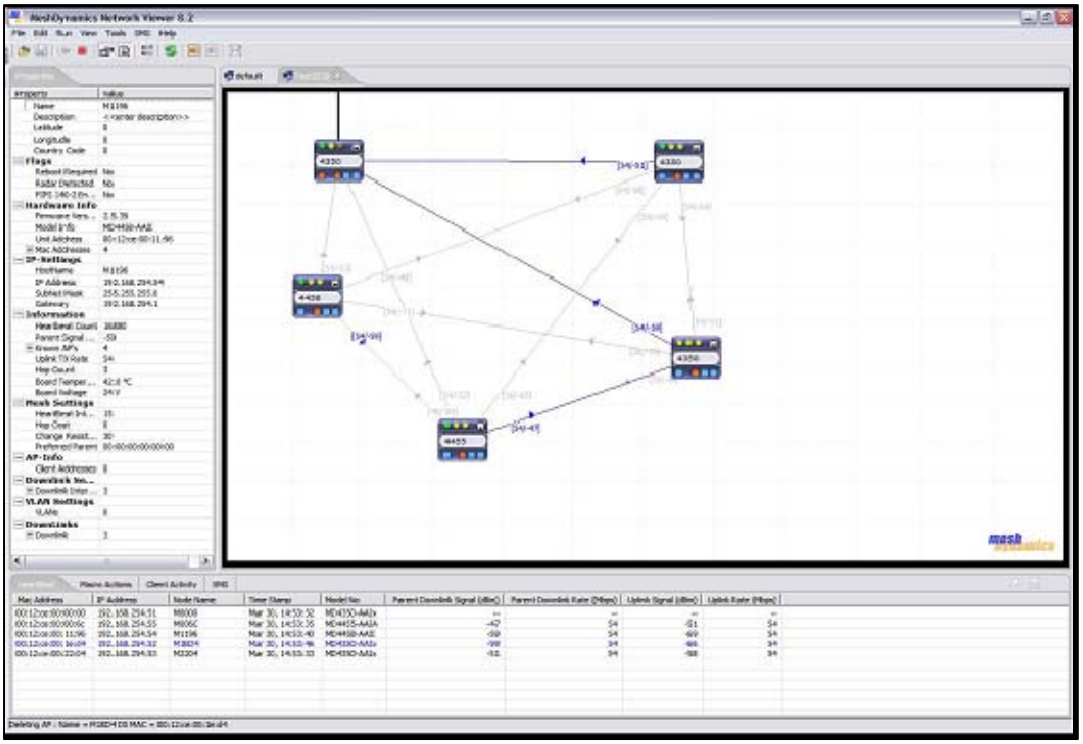


Figure IV-2. Mesh Dynamics NMS viewer displaying active nodes/APs (Mesh Dynamics NMS guide, JUN 2007).

(2) Network connectivity tests in a mobile configuration deployed on paved terrain. All non-root APs connected with the root node at the TOC during the initial connectivity test. However, when the first ground node was placed at 0.5 miles from the root AP, connectivity was lost and unrecoverable. In order to troubleshoot the connectivity problem, the ground node was brought back to the TOC for another connectivity test with the root AP and it reconnected with no problems. After a successful link test at the TOC, the ground AP was placed at the 0.5 mile mark again which again resulted in a broken link with the root AP. The Mesh APs have a proprietary protocol implemented in hardware that gives all APs the ability to shift to the less busy RF channel when frequency conflicts are detected. This feature was activated as recommended by a Mesh Dynamics engineer. However, the connectivity between the APs still failed. The reason for the connectivity failure was unknown.

b. Test Limitations and Conclusion

Inability to establish a network connection prevented the evaluation of the following test objectives:

(1) Evaluation of network connectivity in a mobile configuration while deployed on flat and hilly terrain.

(2) Evaluation of network stability while traversing the area of operations.

(3) Evaluation of maximum distance with an attached wireless ES520/Mesh Dynamics mobile network bridge to a mobile unit on flat and hilly terrain.

(4) Evaluation of usable throughput in a mobile environment conducted on hilly and flat terrain.

(5) Evaluation of mobile node handoff capability while deployed on flat and hilly terrain.

The remote management feature made configuring and troubleshooting the Mesh Dynamics APs very easy. This network manager allowed the Mesh Dynamics APs to be deployed in less than 30 minutes which is very beneficial to the tactical user. On the other hand, the incompletion of the above objectives resulted in an unsatisfactory network performance for Mesh Dynamics mobility test trial. Mesh Dynamics poor network performance also made it unsuitable for further testing in the COASTS 2007 MIO scenario and other military applications due to the product's inability to establish a stable link in order to complete the above objectives. It appears that the link instability came from the auto radio frequency dynamic channel management feature. When this feature is set to auto RF channel management mode, the access point automatically chooses the channel with the least RF interference upon boot-up. While in operation, the RF manager also adjust RF channels as the current channel becomes saturated. The RF channel manager is implemented slightly above the MAC/Data Link layer. The Mesh Dynamics manual states that the:

> Frequency agility is taken one step further in Mesh Dynamics Modular Mesh products. The mesh control "RF robot" software runs above the MAC layer of the radio: the same mesh control software supports radios operating on different frequency bands. Decoupling the logical channel-selection and topology-definition processes from the specific physical radio in this fashion delivers distributed dynamic radio intelligence benefits for current as well as emerging radio standards. (Why Structure Mesh, p 4)

The Media Access Layer or Data Link Layer in the program logic described above monitors and coordinates channel de-conflictions at this layer and communicates the adjustments to the physical layer for a mechanical shift to a different RF channel. Because the RF channel manager feature is a proprietary implementation for the Mesh Dynamics access points the vendor must conduct an in depth review of this protocol and assess the access point's ability to support mobility with this feature activated. As a result of Mesh Dynamics poor network performance at Fort Hunter Liggett, the Mesh Modules were re-deployed at Fort Ord in order to re-assess mobile capability, determine if the RF management feature caused the network instability, and to determine network mobility in a hilly environment.

c. Recommendations

(1) The Mesh Dynamics access points are equipped with an auto frequency management protocol. This protocol gives the Mesh Dynamics APs the ability to shift to the less crowed frequency when the RF space is saturated in the 2.4GHZ and 5.8GHZ space. This feature could make RF management more efficient for the tactical user in that the frequency management would not have to be changed manually. Mesh Dynamics should conduct more field tests to evaluate the effectiveness of the above frequency management protocol. Efficient RF Management is needed, because as the RF space in the 5.8GHZ and 2.4GHZ spectrum becomes more crowded, the more CPU processing will be required from the Mesh Dynamics APs to de-conflict opposing frequencies.

d. Mesh Dynamics Testing Lessons Learned

The Mesh Dynamics Mesh Modules [TM] are advertised as being capable of performing in a mobile configuration. As a result of its performance in the Fort Hunter Liggett mobile test trials, the Mesh Modules required further testing before mobile capability could be determine to be legitimate. The below lessons learned were applied at the next mobile test which was conducted at Fort Ord.

(1) Determine RF space use prior to network deployment. As mentioned earlier in this section, the 5.8GHZ band was used as the backhaul frequency for the 802.11 networks because it was the least saturated frequency band. For the COASTS 2007 Fort Hunter Liggett mobile test trial, only the 802.11 network and the 802.16 networks used this frequency band and channel assignments were de-conflicted as to eliminate RF interference. As a number of un-scheduled vendors arrived, they plug-in their devices in order to demonstrate its ability to support the COAST 2007 scenario requirements. Because of poor RF management, the RF space became saturated but ironically only Mesh Dynamics experienced RF interference. The other deployed 802.11 and 802.16 networks deployed in the AOR did not experience a total link degradation during the test trial. This fact helped narrow the possible cause of the Mesh Dynamics network degradation to the RF management feature. When the Mesh Modules were in close proximity to the root access point, which was around 15 feet, connectivity was immediately established, but once the AP were set at its operation distance of 0.5 and one mile, link connectivity was dropped. Therefore in the case of Mesh Dynamics, poor RF space management can cause major network degradations. The Mesh Dynamics Mesh Modules were deployed at Fort Ord utilizing the same configuration used at Fort Hunter Liggett in a very light RF environment in order to determine if the RF management feature inability to adjust to the RF environment at Fort Hunter Liggett caused the network degradation.

(2) Manually set RF channel if RF space is saturated in the 5.8GHZ domains. When the Mesh Dynamics APs began to experience connectivity issues, the deployed APs should have been set to the pre-defined RF channel, but due to

the recommendation made by the Mesh Dynamic engineers, the RF management feature remained activated. For the next deployment of Mesh Dynamics, the manually setting of the RF channels needs to be tested if network connectivity does not occur with the RF management feature activated.

3. Fortress ES520 Test Results

This section will present the test results, conclusions, recommendations and lessons learned, for the Fortress ES520 network performance in the mobile tests conducted at Fort Hunter Liggett.

a. Results and Discussion

(1) Remote Management It took over three hours to configure four ES520s for deployment. Because of the ES520s lack of a GUI network manager that manages all APs at the same time, each AP had to be configured independently of each other. Configuring each AP by plugging directly into the unit was time consuming and resulted in deployment delays. Once the APs were deployed, each AP required individual wireless logging into or local connection in order to troubleshoot the AP. See Figure IV-2 for a screenshot of the ES520 GUI.

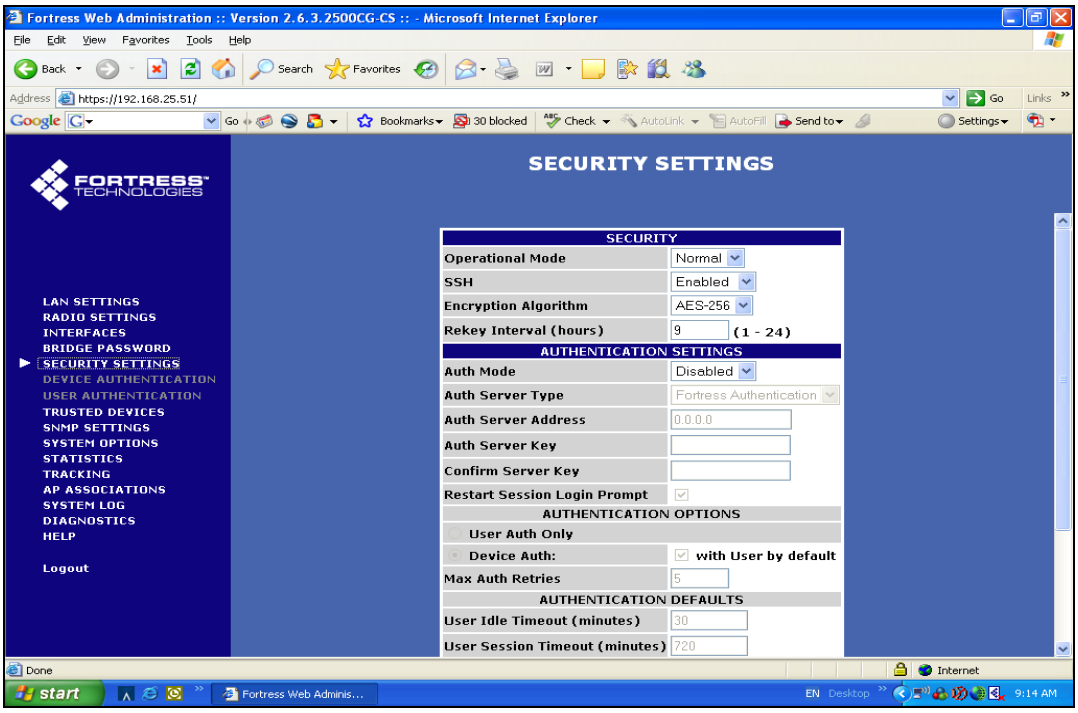


Figure IV-3. Fortress ES520 GUI displaying the security settings (ES520 manual, 2007).

(2) Network connectivity in a mobile configuration while deployed on flat terrain. The mobile AP connected to the root AP promptly, but did not connect to the non-root ground APs/relaying APs during the mobile test. Discussions with Fortress vendors revealed that the ES520s networking protocol does not associate and re-associate automatically. Therefore, once the mobile AP connected to the root AP at the TOC, it stayed connected until line of sight was lost. Nevertheless, throughput data was recorded utilizing IxChariot throughput script and the results are recorded in Table IV-1 This throughput data was taken at a stop in order to test the IxChariot application.

	ES520 AVG Throughput/Light Vegetation/ Paved Road/ Mobile				
Distance	Run 1	Run 2	Date	Weather	Terrain
1 mile	MAX: 4.189 Mbps MIN: 1.643 Mbps	MAX: 6.838 Mbps MIN: 2.312 Mbps	18-Jan-2007	Clear/53(F)	Flat/light vegetation

Table IV-1. Fort Hunter Liggett ES520 mobile throughput test results.

(3) Network link stability while traversing the Area of Operation. The mobile AP did connect to the root AP at a stop, but could not connect to non-root APs while in motion. Therefore when the mobile AP was out of line of sight, which occurred at one mile, the root AP link to the mobile AP dropped. The mobile AP's link to the root AP remained solid while the vehicle moved down the road at speeds up to 45 mph. Doppler shift did not appear to be the cause of the link instability, but rather the fact that once the mobile AP lost LOS of the root AP connectivity back to the TOC was impossible. The purpose of having the other two ground APs/relaying APs was to extend the network out to one mile from the TOC because this distance was the minimum distance requirement for the MIO scenario. The link stability from the root AP to the mobile AP was stable but the ES520's protocol at layer 2 that manages AP to AP associations did not allow links between the mobile AP and the ground APs/relaying APs which were all configured as non-root APs. Because the implemented software at the time of this test did not support AP to AP associations (between non-root configured APs) in a mobile application for the ES520, link stability throughout the network was not achieved.

(4) Maximum distance with an attached wireless ES520/Mesh Dynamics AP attached to a mobile unit. The ES520 mobile AP was able to connect with the root AP at one mile. The mobile AP was stopped at the last ground AP and rebooted. Once the mobile AP rebooted it acquired the root AP, which was one mile away. The throughput data in Table IV-1 was recorded from this position. For mobile operations in Thailand, a 1.5 mile mobile connection distance was the optima required distance for mobility. The ES520 was able to meet the minimum requirement of one

mile with one non-root AP (mobile AP) and the root AP. For the Thailand MIO scenario the other non-root ground APs had to be able to connect to the mobile AP as well in order to establish a stable and redundant mobile network out to 1.5 miles.

(5) Usable throughput in a mobile environment conducted on flat terrain. The minimum acceptable operational throughput needed for the mobility test trial out to 1.5 miles from the root AP was 3Mbps. Due to the mobile AP inability to hop to the closer ground AP when out of line of sight of the root AP, network mobility was determined to be unsatisfactory. Usable throughput was obtained but only at a one mile distance and this data was not recorded while in motion because as the mobile AP transferred towards and away from the root AP the link intermittently dropped when LOS was lost. When LOS was lost while the mobile AP was in motion, the vehicle with the attached mobile AP was then turned towards the root AP in order to regain the link. After the link dropped, the mobile AP did not reconnect as it moved towards the root AP. In order to regain the link, the vehicle had to be at a stop and the mobile AP had to be rebooted. The throughput was usable but it was only usable at a stop not in motion so this objective was partially completed.

(6) Mobile AP to Ground AP handoff capability. As the mobile AP traversed the Area of Operation, it should have connected to the AP with the strongest RF signal. So as the mobile AP moved away from the root AP, the first ground AP should have been acquired. This did not happen because the ES520 when in non-root mode only seeks association with the root AP. When LOS was lost, it took over eight minutes for the mobile AP to reacquire the root AP when rebooted. Because the protocol does not support AP hopping, this test was not feasible for the ES520.

b. Conclusion

The ES520 was able to establish connectivity between the root AP and mobile AP at a distance of one mile and at least 4Mbps of network throughput was achieved during the test trial. Remote management was satisfactory. The Fortress GUI does not have a feature that consolidates all deployed AP information onto one console. Therefore, each AP had to be individually logged into in order to make configuration

changes and to troubleshoot On the other hand, the mobile AP inability to hop to the strongest RF signal as line of sight of the root AP was lost greatly hindered the completion of all test objectives. The ES520 implemented software at the time of this test only supported RF links from the non-root AP to the root AP. The ES520's network architecture did not meet the COASTS 2007 802.11 mobile network operation requirements. Because the mobile AP does not hop to the AP with the strongest RF signal, the path from the mobile AP to the root AP is limited to one route which is to the root AP. This resulted in the ES520's inability to achieve mobility out to 1.5 mile as it traversed AOR. A true mobile and redundant network was not achievable, and this fact made the ES520 unsuitable for COASTS 2007 and military deployments for the Fort Hunter Liggett test trials.

The ES520 does not have an efficient implementation for multi access point remote management. During the test trials, all four APs had to be individually logged into for configurations. Because there were only four APs used, this task was doable yet was not the most efficient way to manage the APs. In a situation that requires more than five access points, the current method used by Fortress to manage the ES520 APs will be very difficult for the network administrator. Because there was no way to monitor the entire network health of the deployed ES520s during this test trial, four Internet Explorer browsers had to remain open in order to display all deployed APs graphical user interfaces. Because one laptop had to be dedicated to displaying four GUIs, it became very time consuming shifting from GUI to GUI just to check AP statuses. The lack of a more efficient network management capability did not affect the ES520 ability to support operations in Thailand and should not affect military deployments but it is a very inefficient way to manage the ES520s.

c. Recommendations

(1) Fortress engineers should investigate the ES520's ability to hop from AP to AP. The ES520 protocol should be adapted for mobility by creating a new protocol or applying a firmware upgrade that allows the ES520 to hop to strongest RF signal when in a mobile configuration. The ES520 needs a better remote management

solution. The configuration and deployment of the four APs became very difficult to manage because when connectivity was lost, each AP had to be logged into wirelessly or locally in order to troubleshoot the issue. Incorporating a GUI that tied in all APs functionalities i.e., health status, connection strength, temperature, should make the network administrator's job easier.

(2) The non-root APs do not connect to each other, rather they only connect to the root AP. This is a weakness in the ES520s networking capability and it limits the APs ability to be configured for mobility. This implementation would increase network reliability and availability.

(3) New software or hardware should be implemented to allow the ES520s to hop to the nearest AP while mobile and shift to the non-root AP with the strongest RF signal.

d. Fortress ES520 Lessons Learned

As a result of its performance in the Fort Hunter Liggett mobile test trials, the ES520 required further development before mobile capability could be determined to be legitimate. The below lessons learned were applied at the next mobile test which was conducted at Fort Ord.

(1) Configure the ES520 APs a day prior to deployment. Because of the remote management limitations discovered during deployment of the ES520s; time can be saved by configuring all APs prior to deployment until a better remote management solution is developed.

(2) Deploy the Root AP as the mobile AP. A more reliable network architecture can be developed in this configuration because the ES520s configured in non-root mode seek association to only the root AP.

4. ES520 and Mesh Dynamics Network Mobility Comparison

The Fort Hunter Liggett test revealed concerns with both Fortress' and Mesh Dynamics' 802.11 technologies mobile capabilities. Considering the test results, neither product could satisfy COASTS 2007 and military mobile application requirements. Both Mesh Dynamics and Fortress vendors should review their layer 1 and 2 protocols and reassess the implemented protocols ability to support mobile applications.

a. Network Performance in a Mobile Application

Mesh Dynamics inability to establish a usable link resulted in the incompletion of the objectives listed in the Mesh Dynamics conclusion section. Overall Mesh Dynamics completely failed the mobility test trial, but troubleshooting indicated that the RF management protocol that allows the Mesh Modules to automatically switch to a less saturated RF channel could have been the cause of the connectivity issues. On the other hand, Fortress ES520 partially met the mobility objectives for the Fort Hunter Liggett test trial, but the lack of an efficient AP management tool and the fact that the ES520 implemented protocol is not capable of establishing communication between APs, while in non-root mode greatly hindered the mobility testing. The mobile AP was able to maintain a solid network link with the root AP out to one mile, but due to the loss of line of sight and the mobile AP inability to re-associate with the fixed ground APs, network mobility was not achieved.

b. Overall Conclusion

Some of the possible causes of the network issues that plagued the Mesh Dynamics and Fortress network performance in this test iteration could include prototype mesh algorithms, lack of a decent user interface for network management, lack of attention to standard simple network management protocols (SNMP) and poor human factors. The Fortress ES520 had only been in production for about nine months at the time of this test, so early production flaws could have caused most of the network issues explained in the objective section. On the other hand, Mesh Dynamics Mesh Modules had been in production for over a year and they were also used in COASTS 2006

deployment in Thailand. However, the network link still was very unstable when the APs were deployed at its test distances to the point where network throughput testing could not be retrieved.

As a result of the above network performance at Fort Hunter Liggett, both Fortress ES520 and Mesh Dynamics Mesh Modules were re-deployed at Fort Ord in order to apply the lessons learned from the Fort Hunter Liggett field test and to evaluate network mobility performance while deployed on hilly terrain.

D. FORT ORD TEST

The Fort Ord location was used to test mobility in a hilly terrain because it offered the best layout and conditions for testing Mesh Dynamics RF management protocol, and the effects that hills and valleys have on network connectivity with the Mesh Modules and the ES520. Due to time constraints, the ES520 and Mesh Modules ability to perform in a maritime configuration was postponed until the Thailand field experiment and the results are detailed in the Thailand section.

1. Test Conditions

This section will describe the terrain, weather conditions and topology during the Fort Ord mobile test trials.

a. Terrain

The Fort Ord terrain was surrounded by abandoned military buildings and had more hills and valleys than Fort Hunter Liggett. The mobile test was conducted on a paved road that covered a distance of 1.2 miles. The road had light vegetation and abandoned buildings to either side. The obstructions did not have a negative affect on the mobile test. On the other hand, the hilliness of the paved road did play a factor. The network topology was structured to accommodate for the hilly terrain. Detail of the deployment is explained below in the topology section. Figure IV-4 is a Google Earth snapshot of the area of operations for the mobile test.

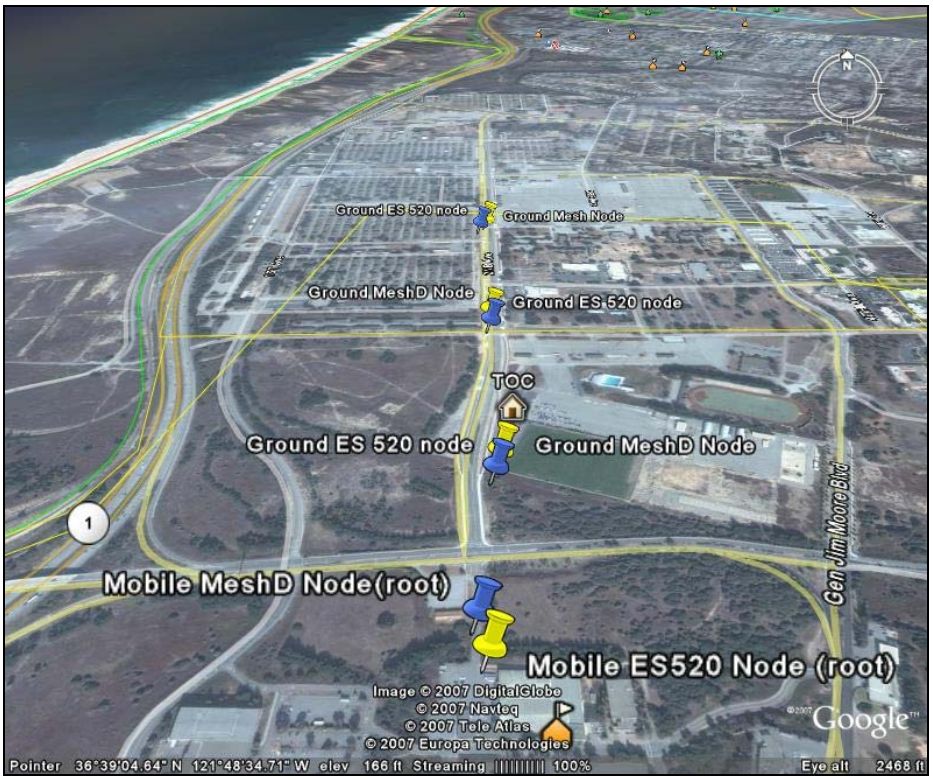


Figure IV-4. Fort Ord Mobile AOR. (from Google Earth JAN 2007)

b. Weather

The weather condition at Fort Ord was very good and on both days of testing, the sky remained clear and free of precipitation. See Appendix C for more details.

c. Topology

The mobile topology for Mesh Dynamics and Fortress consisted of a total of three ground non-root APs with the root AP configured as the mobile AP. The APs were set at a lateral separation of 0.25 miles, starting with the first non-root AP which was located at the Tactical Operation Area and the end AP was 0.50 miles from the TOC. See Figure IV-4 for the layout. Each AP was attached to a tripod at a height of ten feet with an 8dbi antenna attached to the 5.8GHZ backhaul antenna port and an 8dbi antenna attached to the 2.4GHZ antenna port. The AP network configurations for Fort Ord were

the same as Fort Hunter Liggett, but changes were made with AP separation, the ES520 root AP and terrain. For instance a 0.25 mile lateral separation between APs was used at Fort Ord instead of the 0.5 lateral separation because Fort Ord had hills and valleys. The Fort Hunter Liggett flat terrain allowed the APs to be placed further apart. Furthermore, in order to establish mobility between the mobile ES520 and the ground ES520s, the root AP was deployed as the mobile AP, because while in non-root mode the ES520s only seek to acquire the root AP. This fact did not allow the ES520 mobile AP (which was in non-root mode) at Fort Hunter Liggett to acquire the other ground non-root APs because the implemented ES520 network protocol only looked for the root AP when configured to be a non-root AP. At Fort Ord, the ES520 mobile AP was configured to be a root AP because the ground non-root APs automatically connected to the root AP. Figure IV-5 depicts the first ground AP set-up. The second ground AP was placed to left of the arrow in Figure IV-5. The ground AP depicted in Figure IV-5 was in direct line of sight of the second AP. The third ground AP was not in LOS of the first AP due to the hilly terrain, see Figure IV-6. The orientation of the third AP was toward the second AP and the second AP was in LOS of the first and third AP. This set-up allowed the network connection to extend over the hill down into the valley see Figure IV-8. The location of all three ground APs provided RF coverage for the length of the paved road. Figure IV-7 depicts the furthest point of the network from the first AP.

Figure IV-5. First ground AP. (Fort Ord mobile test JAN 2007).

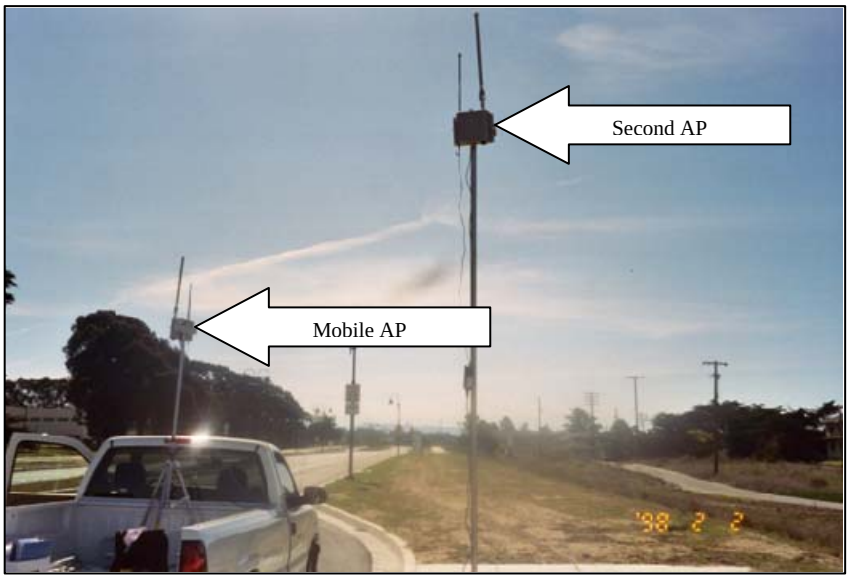


Figure IV-6. Mobile AP connecting to Third ground AP. (Fort Ord mobile test JAN 2007).

Figure IV-7. End of RF reception 1.2 mile from first AP. (Fort Ord mobile test JAN 2007).

2. Mesh Dynamics Test Results at Fort Ord

This section will present the test results, conclusions, recommendations and lessons learned, for the Mesh Dynamics network performance in the mobile test trial conducted at Fort Ord.

a. Results and Discussion

(1) Usable throughput in a mobile environment conducted on hilly terrain. Once all ground APs were activated and showed linkage, a ping test was conducted from the first non-root AP to the mobile AP as it traveled away. As the vehicle with the attached mobile AP dipped into the valleys; the ICMP test intermittently stopped, but started back up as the motion of the vehicle continued. The ping test latency averaged 2ms to 6ms out to one mile. At one mile the ping test totally stopped. Considering the hills and valleys, the signal eventually became too weak to reach the mobile AP.

After conducting a successful ping test, IxChariot clients were attached to the mobile AP and the first ground AP for the network throughput test. 10 successful throughput runs were completed as the mobile AP transverse the area of operations. The Mesh Modules maintained a max throughput of 13Mbps throughout the test runs which was more than enough throughput to support data and video transfer for COAST 2007 field operations. IxChariot throughput test results are listed in Appendix D.

(2) Network link stability while traversing the Area of Operation. Connectivity between the mobile AP and ground APs were stable. After a successful ping test through the APs, 10 throughput runs were recorded gaining max throughput of 13 Mbps and a min of 0.2 mbps. All ten runs were conducted through completion and the only breakage in the network link occurred as the mobile AP dropped into the valley depicted in Figure IV-5, but the break was not long enough to prevent throughput testing. Because the Mesh Modules were able to maintain a stable link throughout the test trial, all throughput tests conducted were completed successfully.

(3) Maximum distance with an attached wireless ES520/Mesh Dynamics AP attached to a mobile unit. In this particular terrain layout, one mile from the first ground AP was the cutoff point for a stable network. As the mobile AP dropped into the valley, throughput decreased and as the mobile AP arose from the valley, the throughput increased. See appendix D for details. The height of eye at the third AP including the height of the tripod was 150ft. The lowest point in the valley was 85ft with the truck and tripod that equates to 95ft. (see Figure IV-7 for details). The lowest LOS difference between the third AP and the mobile AP was 55ft which exceeded the fresnel zone limit and resulted in breakage in the link. More details on how the Fresnel zone affects wireless networks is provided in Chapter II.

When the mobile AP dipped into the valley which is shown in Figure IV-8, due to the Fresnel zone blockage brought on by the height of eye difference, which was 55ft between the mobile AP and the third ground AP marked the point where the link connectivity began to degrade. The max usable network distance achieved with an attached Mesh Dynamics AP in this particular environment was one mile because the Fresnel zone blockage caused by the height of eye difference between the mobile AP and third ground AP.

Figure IV-8. Mobile height difference Fort Ord Mobile test (Google Earth 2007).

(4) Mobile AP to Ground AP Handoff Capability while deployed on hilly terrain. Because the mobile AP was configured as the root, all non-root ground APs immediately connected while the mobile AP passed through the terrain. The Mesh Dynamics ground APs connected to both the mobile root-AP and surrounding ground APs at the same time, which created a full meshed network throughout the AOR. As the mobile AP passed the ground APs, it successfully re-associated to the nearest ground with no network interruptions. The Mesh Dynamics Mesh Modules successfully completed the above operational test.

(5) Evaluate Mesh Dynamics frequency management protocol in a low RF environment. Network link problems observed at Fort Hunter Liggett with the auto RF management feature activated were not experienced at the Fort Ord test site. This fact suggests that the RF saturation that occurred at Fort Hunter Liggett overtaxed

the auto frequency management protocol of Mesh Dynamics. This feature will be tested again while deployed in the COASTS 2007 Thailand Maritime/Humanitarian/SAR scenario.

b. Conclusions

Mesh Dynamics 802.11 Mesh Modules ™ performed well at the Fort Ord mobile field test. All APs connected seamlessly resulting in completion of all mobile operational test objectives.

The Mesh Dynamics APs ability to interconnect with other deployed Mesh Modules, created redundancy in the network and increased the efficiency of traffic transfer, resulting in a maximum network throughput of 13Mbps. See Appendix D for network throughput details. Network redundancy is vital in the deployment of tactical networks and Mesh Dynamics 802.11 Mesh Modules seemed to create the required redundancy needed for a tactical mobile network. However, the network instability experienced at Fort Hunter Liggett field test, makes the Mesh Dynamics Mesh Modules less suitable for military mobile applications because of the RF management channel manager's inability to function properly in a heavy RF environment. This instability causes issues with network reliability.

All test objectives were completed for Mesh Dynamics mobile deployment. In order to test network performance in a ground configuration, Mesh Dynamics was deployed in Thailand with the auto RF management activated to re-examine suitability for COASTS 2007 scenarios.

c. Recommendations

Until the auto RF manager protocol is updated, the Mesh APs should be deployed utilizing the manual RF configuration, because the auto RF protocol is still problematic. As shown in Figure IV-9, the 5.8 GHZ frequency band had multiple vendor products utilizing it for network connectivity at the Fort Hunter Liggett deployment. When the Mesh Dynamics auto frequency management protocol was active, it had to de-conflict 5.8 GHZ frequencies with the other deployed networks, for example the 802.16

network. The Mesh Dynamics engineers said that the Mesh Modules are designed to operate with the RF manager active and that the modules would operate more efficiently in this configuration. Therefore, this feature was activated for the tests, but network connectivity could not be achieved. It appeared that due to multiple devices utilizing the 5.8 GHZ frequency, the RF management protocol was over tasked and could not adjust frequency fast enough to maintain network connectivity for Mesh Dynamics. Therefore, the Fort Ord test trial was used to verify that the RF manager was the cause of the network degradation that occurred at Fort Hunter Liggett.

The Mesh Dynamics Modules should not be utilized in military mobile applications until the vendor can ascertain the faults in the RF management protocol. It appeared that the activation of this feature caused the major network failures at the Fort Hunter Liggett mobile test trial which was conducted in a heavy RF environment. At Fort Ord with the auto RF channel manager activated in a more moderate RF environment, the mobile test was successful.

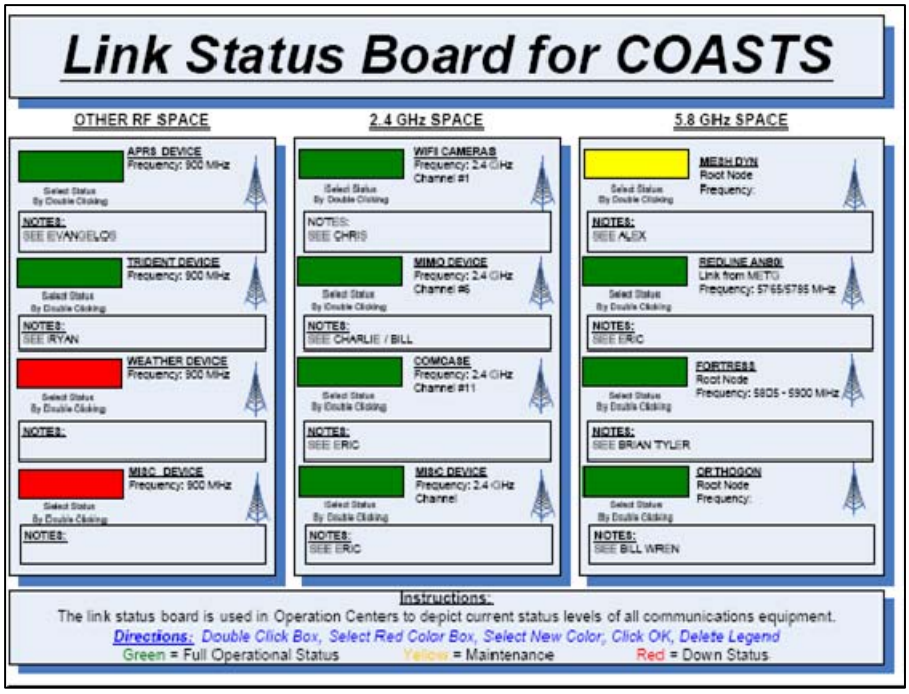


Figure IV-9. Frequency Board for Fort Hunter Liggett Network Deployment COASTS 2007.

d. Mesh Dynamics Lessons Learned

At Fort Ord, the tripod and poles used for the deployment of the ground APs were limited to an antennae height of ten feet. When they were placed at heights higher than ten feet, the tripod became unstable. For heights greater than ten feet, a more stable tripod should be used.

(1) Site surveys should be conducted in order to determine number of AP required to cover the area of operations.

3. Fortress ES520 Test Results at Fort Ord

This section will present the test results, conclusions, recommendations and lessons learned for the Fortress ES520 network performance in the mobile test trial conducted at Fort Ord.

a. Results and Discussion

The observed test results for Fortress are as follows:

(1) Usable throughput in a mobile environment conducted on hilly terrain. The throughput data collected for the ES520 was close to the minimum acceptable throughput of 3Mbps but it was still usable. The ground AP connected to the root AP promptly after configuration operation tests. As mentioned the earlier, the ES520s networking protocol does not associate to the nearest AP automatically. So, once the ground APs connected to the root AP (mobile), they stayed connected. This resulted in 10 uninterrupted IxChariot throughput runs. The maximum throughput achieved for the ES520 was 6Mbps, which was adequate for data and video traffic. The ES520 ability to provide video coverage in a mobile configuration was verified in the Maritime scenario conducted in Thailand. See appendix D for throughput details.

(2) Network link stability while traversing the Area of Operation. Connectivity between the mobile AP and ground APs was stable throughout the operational test. After a successful ping test, 10 throughput runs were recorded with a max throughput of 6 Mbps and a min of 0.01 Mbps. All ten runs were conducted through

completion and the only breakage in the network link occurred as the mobile AP dropped into the valley but the break was not long enough to prevent throughput testing. The third ground AP marked the point where the road dipped into the valley. See Figure IV-8. As the mobile AP began its decent, the link became unstable but it did not completely drop until the 1 mile mark from the first ground AP was reached which is depicted in Figure IV-8.

(3) Maximum distance with an attached wireless ES520/Mesh Dynamics AP attached to a mobile unit. In this particular terrain layout, one mile from the first ground AP was the cutoff point for maintaining a stable network. As the mobile AP dropped into the valley, throughput decreased and as the mobile AP arose from the valley, the throughput increased. See Appendix D for details. The height of the antenna at the third AP including the height of the tripod was 150ft. The lowest point in the valley where the mobile AP traveled was 95ft. (see Figure IV-8 for details) The lowest LOS difference between the third AP and the mobile AP was 55ft which exceeded the fresnel zone limit and resulted in breakage in the link. More details on how the Fresnel zone affects wireless networks is provided in Chapter II.

The maximum usable network distance achieved with an attached Mesh Dynamics AP in this particular environment was one mile. The test was limited to a one mile distance because of Fresnel zone blockage caused by the height of eye difference between the mobile AP and third ground AP. See Chapter II for the Fresnel zone calculation for the Fort Ord test trial.

(4) Mobile AP to Ground AP Handoff Capability while deployed on hilly terrain. Because the mobile AP was configured as the root AP, all non-root ground APs immediately connected while the mobile AP passed through the terrain. The re-acquiring time delay that occurred once LOS was lost and regained was not significant enough to halt the IxChariot throughput test. Technically, the ES520s did not physically perform handoffs as the mobile AP passed through the AOR. Instead, the non-root ground APs individually sought the root AP and did not connect to the other non-root ground APs.

Network mobility was lost because the ground APs did not connect to each other. The lack of interconnectivity between the non-root APs, made the root AP the single point of failure in the network.

b. Conclusion

The ES520 was only able to produce 6Mbps of throughput in an unencrypted mode for the Fort Ord mobility test. 6Mbps is usable for data transfer but may be too low for video streaming with encryption activated. Having the root AP as the mobile unit did allow for throughput testing but this was not a true mobile network or reliable network. The non-root APs do not connect to each other, so when the root AP was out of LOS, the ground APs became isolated from the network because they do not connect to the closer AP . The inability to hop AP to AP and to the nearest AP while in a mobile configuration prevents using the ES520 for mobile operations. The results from this test and the Fort Hunter Liggett test prompted the Fortress engineers to develop a revision for the non-root AP associating flaw. This firmware update was applied and tested in Thailand and the results are in the Thailand section below.

c. Recommendations

The ES520 currently lacks reliability and network redundancy with its current firmware implementation. Recommend developing a firmware update that gives the mobile configured AP the capability to roam from AP to AP.

d. ES520 Test Lessons Learned

While deployed on the hilly terrain of Fort Ord, antennae height was limited to a height of ten feet. The tripod and poles used for the deployment of the ground APs were stable at ten feet and when they were placed at heights higher than ten feet, the tripod became unstable. For heights greater than ten feet, a more stable tripod should be used.

(1) Site surveys should be conducted in order to determine number of AP required to cover area of operations.

(2) The ES520 should be configured prior to field operations. It took about one hour to fully deploy the ES520s due to configurations problems.

4. ES520 and Mesh Dynamics Network Mobility Comparison

a. Network Throughput

Mesh Dynamics had the best throughput recordings for the mobility test. During the ten test runs, Mesh Dynamics was able to maintain a maximum throughput of 13 Mbps while the ES520 was only capable of maintaining 6Mbps. Mesh Dynamics APs were also capable of connecting to each other which established multiple paths to pass information through the network, resulting in a more reliable network. The mesh viewer shown in Figure IV-3 made configuring and monitoring the active APs very easy. See Chapter III for more details on the mesh viewer. The RF channel manager did not cause any network connectivity issues as it did in the Fort Hunter Liggett test trial. Therefore the Mesh Dynamics Mesh Modules seemed to be suitable for the mobility requirements for COASTS 2007 Thailand deployment and military mobile applications.

b. Network Connectivity

The ES520 on the other hand did maintain a connection at Fort Hunter Liggett when Mesh Dynamics failed but the ES520 protocols do not support mobility from an AP management and mobile AP to fixed ground AP point of view. The Mesh Dynamics APs connectivity failure at Fort Hunter Liggett appeared to be due to a faulty RF manager protocol. When an ES520 was configured for non-root mode it seeked to connect only to the root AP. At Fort Hunter Liggett, all APs connected to the root including the mobile AP. As the mobile AP moved out of LOS of the root, it lost connectivity and did not acquire the closer non-root APs which limits the ES520 mobile capability. In order to make the ES520 function in a mobile configuration, the root AP was configured to be the mobile AP at the Fort Ord mobile test. This configuration

change worked and a mobile AP to ground AP architecture was established which allowed for network throughput testing. The drawback to this set-up was that the non-root ground APs did not connect to each other and the network was only connected from mobile AP to the in LOS ground AP which does not constitute a true mobile/reliable network where all APs are connected to each other.

c. Network Overall Performance in a Mobile Application

The network mobility performance at Fort Hunter Liggett was unsatisfactory for Mesh Dynamics and for the ES520. Network redundancy for Fortress was not achievable because of the non-root limitation to communicating only to the root AP. Concurrently, Mesh Dynamics inability to maintain a stable network connection resulted in the inability to conduct the mobile tests.

The Fort Ord mobile test trials showed that the Mesh Dynamics connectivity issues observed at Fort Hunter Liggett were contributed to the RF manager's inability to function in a heavy RF environment. The auto RF manager was activated at Fort Ord and network connectivity remained stable throughout the entire test trial. The ES520 network mobility was partially successful. Throughput data was collected in a mobile application, which was only made possible by configuring the mobile AP as the root AP. As the root AP traversed the AOR, the ground non-root APs automatically connected to the root AP as it passed. This was not a true reliable mobile network because the non-root APs did not communicate between each other, so when the root AP was out of line of sight, the non-root APs became isolated from the network.

Although the vendors are constantly making updates to the above units, at the time of this field test Mesh Dynamics seemed to be more suitable for mobile applications where as the ES520 seemed to be totally unsuitable. The RF management feature on the Mesh Dynamics APs still needs further testing in a heavy RF environment before it can be completely suitable for mobility. However, in the low RF environment of Fort Ord, the Mesh Dynamics Mesh Modules performed flawlessly. The ES520s network performance was good as well but the wireless architecture of the ES520s is not reliable because the root AP is the single point of failure and there was no way of

monitoring AP health. Therefore the network administer would be operating the ES520s in the blind with no way of preventing total network failures. As a result of the network performance in the two mobile operation tests, Mesh Dynamics seemed to provide the most reliable, manageable and functional capability for mobile applications.

d. Overall Conclusion

In regards to conventional WiFi mobility from a laptop to AP, which was beyond the scope of this thesis, both Mesh Dynamics and Fortress APs comply with the standards. As for maintaining a mobile network from AP to AP, while in a tactical environment remains an issue. In theory, the mobile AP should hop from AP to AP as required and do it seamlessly without dropping network connectivity. At Fort Hunter Liggett, both products failed in this category because they could not maintain network connectivity in a mobile application. At Fort Ord, making the ES520 root AP the mobile unit allowed throughput data to be taken, but this was not a realistic mobile network because the AP configured as the root is designed to be wired into a switch or router.

The Mesh Dynamics unique protocol that gives the APs the ability to self-heal, self-form and auto shift frequency channels seemed to have caused the network connectivity issues at Fort Hunter Liggett. At Fort Ord, the APs completed all objectives successfully and the connectivity problems from Fort Hunter Liggett did not resurface.

The next phase of this thesis will be to determine network capabilities while deployed in a fixed ground configuration. While in this configuration, network security, video support, multicast and network availability will be evaluated.

THIS PAGE INTENTIONALLY LEFT BLANK

V. GROUND PERFORMANCE TESTS

The purpose of this chapter is to present the test objectives, measures of evaluation, methodology, and field test results of the Fortress(ES520) and Mesh Dynamics(4000 series) access point(AP) fixed ground performance at Fort Hunter Liggett, CA and at Mae Ngat Dam, Thailand in support of 2007 COASTS field exercises.

Due to time constraint for preparation for the final deployment in Thailand, Mesh Dynamics network performance in the COASTS 2006 demonstrations conducted at Fort Hunter Liggett and Thailand was used to compare the ES520 2007 network performance. For the Thailand II field test, the Mesh Dynamics APs were deployed in order to test operations in an operational scenario and to retest the auto frequency management protocol. The results of its performance are provided in the Thailand II section.

A. OBJECTIVE OF TEST.

The ES520 2007 network performance was compared with the 2006 throughput data from Robert Lounsbury's thesis entitled "Optimum Antenna Configuration for Maximizing Access Point Range of an IEEE 802.11 Wireless Mesh Network in Support of Multi-Mission Operations Relative to Hastily Formed Scalable Deployments" June 2007 and Anthony Russo's thesis entitled "Test and Evaluation of Mesh Dynamics 802.11 Multi-Radio Mesh Modules in Support of Coalition Riverine Operations" June 2006. Although the environmental conditions were not exactly the same for COASTS 2006 and 2007 at Fort Hunter Liggett and in Thailand, they were generally similar and did not appear to have significantly different effects between the two experiments. In the Thailand section, the Information Warfare Red Team (IWRT) 2006 Mesh network and 2007 ES520 network security performance reports were used to compare Mesh Dynamics and the ES520 network security capabilities and limitations.

The main test objective for the Fort Hunter Liggett field test was to evaluate throughput in the unencrypted mode for Fortress ES520 and Mesh Dynamics and to

determine their ability to support COASTS 2006 and 2007 Maritime Interdiction Operations, Aerial Surveillance, Ground Sensors and Video for the Thailand demonstration**.**

The Thailand I 802.11 main test objectives were to; 1) determine the exact number of ES520 required to provide 802.11 coverage over the Dam area of operations, 2) determine antenna configuration requirements, and 3) evaluate ES520 operations in high a temperature environment.

The main 802.11 network objective for the Thailand II demonstration was to evaluate the ES520's network performance and compare it to Mesh Dynamics 2006 network performance while supporting the COASTS scenarios. The networks ability to provide network availability, network security, peripheral support(i.e., video, ground sensors, UAV video feeds) during a live scenario were the final test objectives for Mesh Dynamics 2006 and Fortress 2007 deployments. The following supporting objectives were used to determine which product was more suitable for future COASTS deployments and military tactical environment deployments:

- To evaluate network ability to support peripherals for scenario i.e., cameras, sensors and UAV video.
- To evaluate throughput capacity in unencrypted mode.
- To evaluate Network performance in high temperature environment.
- To determine the number of ES520s required to provide 802.11 coverage over the DAM area of operations and to support peripheral devices.
- To determine antenna configuration.
- To evaluate availability.
- To determine usable throughput in a high temperature environment.
- To evaluate network security capability and limitations against Red Team's network security attacks.
- To evaluate availability
- To determine military usability
- To determine transportability requirements.

1. Evaluation Measures for the Tests

The tools used for testing the objectives in the mobile applications were used for the ground deployment tests. Those tools included IxChariot throughput script, see Chapter III for detailed discussion, ICMP ping, and visual observation. The details of how each objective was measured are as follows:

a) Network ability to support peripherals for scenario i.e., cameras, sensors and UAV video was measured by visually observing quality of the video as it is streamed through the network.

b) Throughput capacity in unencrypted mode was measured by utilizing IxChariot throughput scripts.

c) Network performance was measured by utilizing IxChariot, Ping, and ES520 GUI.

d) The Number of ES520s required for deployment was assessed by observing RF coverage requirement.

e) Antenna configuration requirement was assessed by observing throughput quality while in encryption mode with peripheral devices attached.

f) Operational Availability (Ao) is usually expressed as a percentage and is defined as: (up time – down time) / total time (Buddenberg, p 1). The goal was to achieve a 100% operational uptime with no failures. Therefore in order to measure network availability the below calculation was used.

$$Ao = \frac{uptime - downtime}{total\ \ operational\, time}$$

g) Security capability was measured by utilizing tools/methods deployed by the Red Team for Fortress. Mesh Dynamics security

was measured in COAST 2006 and the after action report provided by the Red Team was utilized to compare to the ES520 results.

h) Military suitability was measured by observing network performance in Thailand maritime, humanitarian and search and rescue scenarios conducted at Mgnat Dam. The scenarios consisted of a maritime interdiction operation, ground sensor detection, UAV video surveillance, ground camera video surveillance and video surveillance from a 1,000ft balloon.

i) Transportability requirements (Logistics required for deployment) was measured by observing weight, number of Pelican cases, power, and configuration required to fully deploy the network.

B. TEST METHOD

Both Mesh Dynamics 2006 and Fortress 2007 802.11 network APs were configured along the air field in the same manner as detailed in figures V-1 and V-2. The same AP radio configuration used in the mobile tests was used in the ground tests for Mesh Dynamics and Fortress network deployed at the second Fort Hunter Liggett and the two Thailand tests. The second Fort Hunter Liggett field test method was to deploy both Mesh Dynamics and Fortress 802.11 APs and test network ability to support all peripherals i.e., ground cameras, sensors, UAV video and balloon video for the COASTS 2006 and 2007 scenarios. Four APs including the Root AP were deployed along the dirt runway at Fort Hunter Liggett with the last AP stationed at one mile for both Mesh Dynamics and Fortress. The ground tests were conducted at Fort Hunter Liggett utilizing the APs' 802.11a backhaul radio in unencrypted mode. While in the ground configuration, Mesh Dynamics and Fortress 802.11 network APs throughput capacity in unencrypted mode was measured utilizing IxChariot throughput script. Eleven Mbps was determined to be the minimum required throughput to maintain usable throughput for data and video transfer for the live scenarios for the 2007 COASTS 802.11 network. This

minimum throughput requirement was based on the number of peripheral devices that were attached to the 802.11 network and being in encryption mode. As for Mesh Dynamics, network throughput data was taken utilizing the 8dbi omni-directional antennas in the 2006 deployment. The same antennas were used for the ES520 in the 2007 deployment. Therefore the Mesh Dynamics' network throughput data taken with the 8di omni-directional antennas was used for comparison with the ES520 network throughput.

The ES520s were the only deployed 802.11 network for the first Thailand trip because of time constraint. While deployed, network performance was measured via IxChariot and visually via GUI and ping tests. Based on the network performance, the exact number of ES520s required to support the final scenario was determined. The optimal antenna configuration was also determined based on the topology of the dam face and client service requirements. All APs were deployed on a 30ft light pole out to 1.2 miles. IxChariot throughput script was run in order to ascertain network throughput in the humid environment of Thailand. This throughput script was also used to determine the numbers of APs required to maintain usable 802.11 coverage over the dam face. The optimal required throughput for the fixed ground network was 11Mbps.

For the final Thailand deployment, the ES520 and the Mesh Dynamics APs were set-up along the Mae Ngnat Dam Face in Thailand in order to test operational performance in a tactical scenario. The ES520 APs were the chosen 802.11 device to provide the 802.11 coverage for COASTS 2007 since Mesh Dynamics APs were used in 2006. However, Mesh Dynamics network performance in Thailand still was evaluated. Network throughput data was taken on the deployed 802.11 devices while in encryption mode, and network attacks were conducted by the IWRT. Multiple scenario profiles were run with full peripheral activation in order to determine suitability for future COASTS deployments and ultimately military applications.

C. FORT HUNTER LIGGETT II

The Fort Hunter Liggett ground test conducted on 16 March to April 1 2007 was in preparation for Thailand demonstration. The main objective was to evaluate the integration of all peripherals including ground cameras, sensors, UAV video and balloon video into the 802.11 network (ES520) This was the same main objective for the Mesh Dynamics network in the COASTS 2006 Fort Hunter Liggett test.

1. Test Conditions

This section will describe the topology, terrain and weather conditions during the Fort Hunter Liggett II fixed ground network tests conducted in 2006 and 2007 with Mesh Dynamics and Fortress 802.11 wireless devices.

a. Terrain

The ground test was conducted on a one mile dirt runway. The surrounding terrain, mountains were to the South of the runway, while light woody trees surrounded the entire area, but overall the runway topology was flat and free of obstructions. Figure V-1 is a 2007 Google Earth layout of the area of operations and Figure V-2 is a 2006 Google Earth layout of Mesh Dynamics layout.

Figure V-1. ES520 Ground AP Layout at Fort Hunter Liggett (from Google Earth FEB 2007).

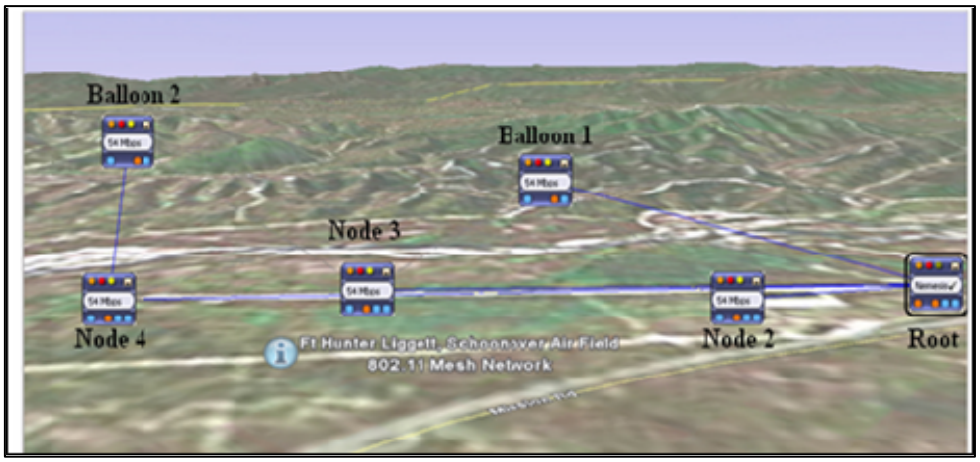


Figure V-2. Mesh Ground AP Layout at Fort Hunter Liggett (from Google Earth MAR 2006).

b. Weather

The weather conditions for the 2006 Mesh network deployment were similar to the weather conditions at Fort Hunter Liggett for the ES520 network deployment. The details of the weather conditions are provided in Appendix E.

c. Topology

Four ground APs were deployed for both Mesh Dynamics and the ES520. The APs for Mesh Dynamics and Fortress were arranged with a 0.4 mile separation between each non-root AP out to one-mile. The details for the ES520 and Mesh Dynamics ground set-up are detailed in Appendix F.

2. Mesh Dynamics Test Results

The test results for Mesh Dynamics 2006 network performance in a fixed ground configuration at Fort Hunter Liggett is presented in Appendix J.

3. Fortress ES520s Test Results

This section will detail the test results, of Fortress ES520 network performance in a fixed ground configuration at Fort Hunter Liggett.

a. Results and Discussion

(1) Network ability to support peripherals for scenario i.e., cameras, sensors and UAV video. The ES520 support of the attached peripherals for the 2007 Fort Hunter Liggett field test was satisfactory. High definition quality video was passed through the network via a mobile router made by Western Data Systems called Grizzly see Figure V-3. The Grizzly was attached to a ground ES520 AP and HD video passed from the Grizzly backhauled through the ES520 to the switch in the TOC. Live video from the balloon also provided an encompassing view of the AOR via an ES520 AP see Figure V-4 for a snapshot. The STS-1400 area surveillance radar system made by ICX provided full 360 degree coverage of the AOR and backhauled live video and radar tracking data successfully through the ES520 ground APs. See Figure V-5 for a snapshot of the radar and camera. The highlight of the Fort Hunter Liggett field test was the ES520 backhauling video from the deployed Unmanned Aerial Vehicles (UAVs) during flight operation tests. Overall, the ES520's network performance was satisfactory for the ground surveillance mission. The information that the attached peripherals provided were seamlessly passed through the ES520 network.

Figure V-3. Grizzly Fort Hunter Liggett 2007 (from http://www.western-data.com, FEB 2007)

Figure V-4. Screen Shot of Surveillance Video Taken by AXIS 213 PTZ Camera attached to Aerial ES520 Node Fort Hunter Liggett 2007.

Figure V-5. Screen Shot of ICX ground radar from www.ICX.com used for tracking ground targets at Fort Hunter Liggett 2007 field exercise and Thailand demonstration.

(2) Throughput capacity in unencrypted mode**.** As mentioned in Appendix J the best possible throughput that could be achieved based on the OFDM protocol is 54Mbps. The minimum acceptable required throughput for 2007 COASTS 802.11 fixed ground network was 11Mbps. The ES520 averaged a network throughput of 28Mbps in the IxChariot throughput tests at a distance of one-mile, which was very suitable for the ground surveillance mission. See Table V-1 for more throughput details.

8dBi to 8dBi 802.11a (backhaul radio) Fort Hunter Liggett					
Date: 18-Jan-07	**ES520 throughput/light vegetation/Temp: 55 F/dry conditions**				
Distance	**Run 1**	**Run 2**	**Run 3**	**Run 4**	**Run 5**
1 mile	MAX: 32 Mbps MIN: 21 Mbps **AVG: 28 Mbps**	MAX: 32 Mbps MIN: 20 Mbps **AVG: 28 Mbps**	MAX: 31 Mbps MIN: 21 Mbps **AVG: 28 Mbps**	MAX: 31 Mbps MIN: 21 Mbps **AVG: 28 Mbps**	MAX: 31 Mbps MIN: 21 Mbps **AVG: 28 Mbps**

Table V-1. ES520 2007 Fixed Ground Network Throughput Data.

b. Conclusion

Operationally, the ES520s met all test requirements for the Fort Hunter Liggett field test. The ES520s provided flawless network support for all attached peripherals and network degradation during the full scenario run was not detected. The multicasting feature limited the work load of the single root AP that brought all of the data and video traffic to the TOC for dissemination out to the operators and the achievement of 28Mbps was a considerable network throughput accomplishment.

The ES520 network performance at Fort Hunter Liggett was outstanding with encryption disabled. The next step was to compare the throughput achieved at Fort Hunter Liggett with the results in Thailand with the encryption activated.

c. Recommendations

The ES520 network performance was outstanding at Fort Hunter Liggett. Problems with configuration and deployment have been consistent with the ES520 because each ES520 has to be configured individually by one console (laptop). The lack of a user friendly GUI made troubleshooting and AP configuration time consuming. At Fort Hunter Liggett only four APs were used so, configuration and deployment time was between 45 minutes to a 1.5 hours. Unfortunately, with missions that require more than five ES520s, deployment times could reach 2 hours or more which would be unsatisfactory for tactical use. Therefore it is highly recommended that a GUI network viewer be implemented to lesson the burden of configuration and monitoring deployed APs. This GUI should also implement the standard SNMP protocol which would allow the AP to be managed from any SNMP console.

d. Lessons Learned

(1) Graphical User Interface. Time can be saved by configuring all APs prior to deployment due to remote management problems**.**

The lack of an ES520 consolidated AP management capability made it very time consuming to troubleshoot and configure the ES520 APs for the deployment.

4. ES520 and Mesh Dynamics Ground Network Comparison

Both Mesh Dynamics and the ES520 networks supported the Fort Hunter Liggett 2006 and 2007 field test objectives. The main scenario objective was to be able to pass video through the 802.11 network (Mesh and ES520) back to the TOC. The Mesh Modules network throughput averaged 11Mbps and the ES520 network throughput averaged 28Mbps which were more than enough throughput to support the network peripheral requirements for tactical operations.

a. Network Performance

Mesh Dynamics and the ES520 network performance for the Fort Hunter Liggett 2006 and 2007 network test and evaluation was very excellent. All Mesh Dynamics and Fortress ground APs and aerial APs were deployed along the dirt runway at Fort Hunter Liggett. All peripheral devices were attached to the specified nodes and connectivity tested. After a successful network operation test, the COASTS scenarios were run to evaluate the networks (Mesh Dynamics and ES520) ability to provide command and control situational awareness of the AOR with multiple surveillance devices attached. The scenario consisted of a red force infiltrating the AOR through covert methods for instance, they tried to utilize the terrain i.e., hills, trees and low brush to covertly pass the deployed surveillance devices. Mesh Dynamics and Fortress effectively provided situational awareness for the scenario at Fort Hunter Liggett and denied the red forces access to the AOR. No security attacks were carried out for this field test. The Red Team main objective was to covertly pass the surveillance not attack the network.

b. Network Problems

Although the ES520 satisfied all network requirements, network management via the ES520 GUI remained an issue. When network troubleshooting was required for the ES520, each AP had to be individually troubleshot in order to ascertain the network issue. On the other hand, Mesh Dynamics did not have any problems with network management because it has a network manager that feeds all of the deployed APs health information back to the user onto one console. In regards to AP deployment, it was noted that careful set-up of the Mesh Dynamics APs had to be taking due to the multiple antennas alignment requirements.

c. Test Limitations

The objectives that were not tested at the Fort Hunter Liggett field test included security, availability, network performance and ability to support video streaming in a full tactical scenario these objectives were examined in the Thailand field test.

D. THAILAND I

The main 2007 COASTS objective for the test experiments conducted 19-30 Mar 2007 was to deploy and conduct operational tests on the IEEE 802.11 and IEEE 802.16 networks and peripheral devices to assess network readiness for final demonstration in Thailand. Due to time constraints and the fact that the ES520 incorporates the IEEE 802.11 technology utilized for COATS 2007, Mesh Dynamics was not deployed in this field experiment. As a result, 2006 Mesh Dynamics network performance data were used to compare to the ES520's network performance in the Thailand II section.

The Thailand IEEE 802.11 main objectives were to; 1) determine the number of ES520 required to provide IEEE 802.11 wireless coverage over the dam area of operations, 2) determining antenna configuration requirements and deployment requirements, and 3) evaluate ES520 operations in high temperature environment.

1. Test Conditions

This section will describe the terrain, weather and topology conditions during the ES520 network deployment in Thailand.

a. Terrain

Mae Ngat Dam located north of Chiang Mai, Thailand was the ideal location to conduct the Maritime Interdiction Operations, Aerial Surveillance, Ground Sensors and Video scenarios. The dam face is approximately 1.3 miles long with a 60ft drop to the lake and the light poles that run along the dam face are 30ft high. The light poles height enabled the ES520s to be deployed at a height of eye that limited RF

interferences from the surrounding vegetation. The environmental surroundings of the AOR at the dam face consisted of heavy vegetation, hills, water and rocks. The dam face area of operation is depicted in Figure V-6.

Figure V-6. Mae Ngat Dam (from Google Earth 2007)

b. Weather

The Thailand I experiment was conducted from 19-30 MAR 2007. The weather was hot (70F to 100F) and humid (70F to 90F) with sporadic thunderstorms. Therefore weather data was recorded for evaluation purposes. Appendix G details the weather conditions at the dam face.

c. Topology

The environmental surroundings did not provide the ideal conditions for RF propagation in that the RF energy could bounce off the lake, rocks and be absorbed by the vegetation. With all of these possible influences on RF, throughput could be affected. Therefore it was very important to determine the number of ES520s that would

be required to overcome the above affects on the network and promote enough throughput to support the attached peripherals that would be needed for surveillance of the AOR.

The 2007 802.11 network layout with the ES520s was similar to the 2006 802.11 network layout. For the 2006 Mesh Dynamics deployment, as many as nine Mesh Dynamics Mesh Modules were deployed as ground APs in order to support the integration of unattended sensors (Russo, p 90). However, eleven ES520s were needed and deployed in the Thailand I field test to achieve the same capability as Mesh Dynamics. The eleven ES520 APs were deployed in order to provide satisfactory support for UAV video, ground cameras, balloon camera, maritime camera, ground sensors and biometric devices. The same 8dbi omni-directional antenna configuration used at Fort Hunter Liggett was used for all deployed APs in Thailand I tests. Power was provided by the light-poles, instead of a car battery and inverter and the APs were mounted at a height of 30ft instead of 10ft. Figure V-7 depicts the 2007 ES520 topology and Figure V-8 depicts how all ES520 APs were deployed in this field test.

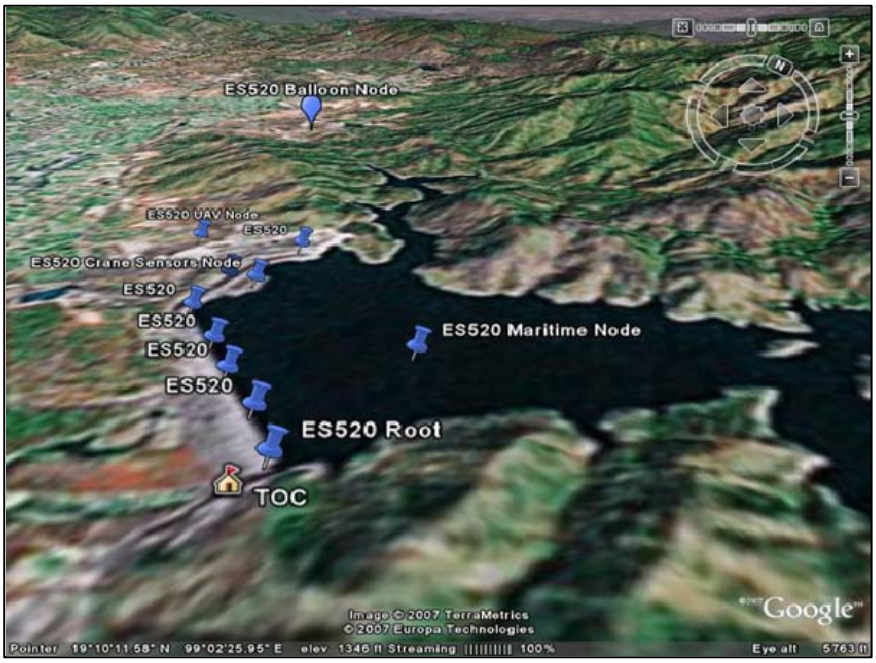


Figure V-7. ES520 Network Mae Ngat Dam 802.11 Topology 2007 (from Google Earth 2007).

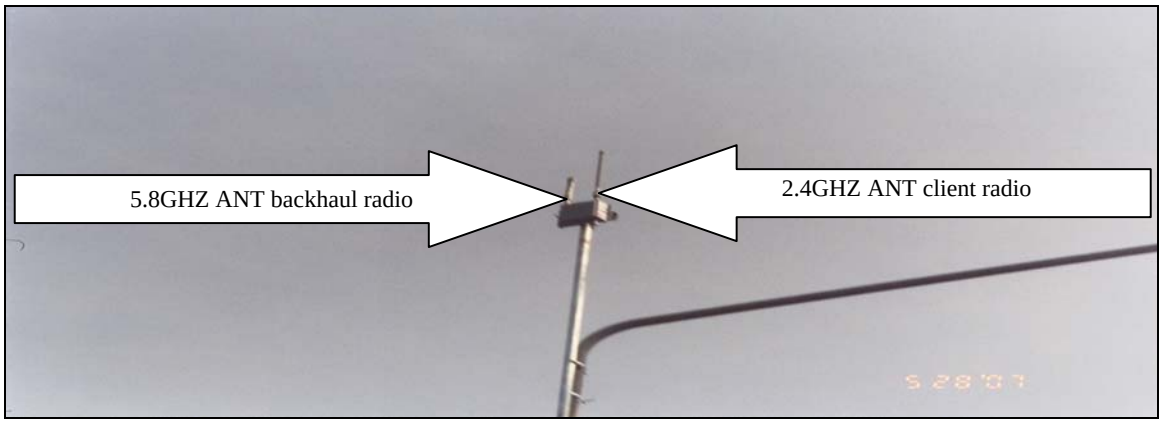


Figure V-8. ES520 root/non-root AP configuration/deployment at Mae Ngat Dam, Thailand 2007.

2. Fortress ES520 Test Results

This section will present the test results, of Fortress ES520 network performance in a fixed ground configuration during Thailand I tests.

a. Results and Discussion

(1) Network performance in high temperature environment. The ES520s are rated for ambient temperature of 122(F) and based on the temperatures in Appendix G; 122(F) was never reached. So temperature should not have caused the network degradation problems that were observed in week two. The ES520s performed superbly in the first week at Mae Ngat Dam. Operationally, the ES520s supported all peripherals used in the scenario. All eleven ES520s were shut down and restarted each morning and all APs stayed operational throughout the testing phase. However, during the mid to late afternoons when the sun was at its hottest, the network did seem to degrade because feeds from the attached devices started to drop off line sporadically; but it was not noticeable enough to disrupt network operations. In the second week the above degradation seemed to be escalated resulting in delay in executing the planned scenarios on time.

The cause of the network degradation in the second week remained unclear. While the scenario was in run during the second week, attached cameras sporadically dropped offline and no video data could be retrieved from the UAV AP due to connectivity issues and the maritime AP video was sporadic. In order to eliminate all physical connection and configuration issues, the ES520s were isolated to their on switch and operation tests were performed utilizing ping. The results were the same, sporadic video and link connection issues.

(2) Network Availability. Operationally, the ES520s provided excellent backhaul for all peripherals attached to the network; Figure V-9 is an axis camera snapshot which shows excellent video quality while conducting surveillance of the ground sensor area. Each day after day two of the first week, the ES520s was shutdown over night and restarted in the mornings. Each day of the first week, the ES520s restarted with no issues and network operation was satisfactory all day. Therefore Ao for the first week was 100 percent.

$$Ao = \frac{(40\ hours - 0)}{40\ hours} \times 100\,\% = 100\%$$

In contrast, on Monday morning of the second week all ES520s were started up and connectivity tests conducted. Each AP was logged into in order to check throughput from AP to AP and connectivity signal strength (This method of troubleshooting took over 40 minutes everyday because of the lack of a GUI that consolidates deployed AP information). The ES520s averaged 5.5Mbps with connectivity strength between -66dbm to -82dbm which were good enough throughput and signal strength to pass video and maintain a usable network link in both weeks. The daily troubleshooting connectivity issues that occurred in the second week resulted in low a lower network availability of 50%.

$$Ao \frac{40\,hours - 20\,hours}{40 hours} \times 100\,\% = 50\%$$

An Ao of 50% is a significant drop from the 100% Ao experienced in the first week and is considered militarily unsuitable. Possible causes for this significant drop in availability are addressed in the conclusion section.

Figure V-9. ES520 AP backhauling video surveillance of ground sensor area at Mae Ngnat Dam, Thailand 2007.

(3) Antenna Configuration. The 8dbi omni-directional antenna was attached to all of the ES520s backhaul radios. The 8dbi omni-directional antenna was used because the 360degree coverage that it offered along with the 10 degree vertical beam width provided the best network connectivity at Fort Hunter Liggett and Fort Ord. In Thailand, this configuration was also used but due to the network degradation issues that occurred in the second week, a new antenna configuration strategy had to be utilized. The lesson learned section describes the new configuration strategy.

(4) Number of ES520s required for 802.11 coverage and support for attached devices. Eleven ES520s were configured and ready for deployment in less than 3.5 hours. All ES520s were deployed at a height of 30ft and attached to light poles along the dam face. By the second day all attached devices (cameras, ground sensors) were attached to the ES520s and a test run scenario was successfully conducted. The ES520s provided backhaul to the TOC for five ground cameras, a UAV providing camera feed, Crane Ground sensors providing ground detection feeds and a Mobile

Maritime AP that provided connectivity for a biometric device and camera backhaul to the TOC. All attached sensors were able to provide satisfactory tactical data utilizing the ES520s in the first week despite of a network throughput limit of 5.5Mbps. However, the network degradation that occurred in the second week indicated that eleven APs in combination with utilizing omni-directional antennas were not enough APs to sufficiently provide data and video backhaul for the AOR.

(5) The current web based user interface became quite difficult to use and manage in a dense AP configuration. The operator had to open thirteen tabs using Internet Explore 7. One for the FC-1500, one for an ES520 in AP only mode for wireless access at the TOC, and eleven more tabs, one for each deployed ES520. The network manager then had to create a manual spreadsheet of each ES520's MAC address for VAP2. Then each ES520 had to be logged into to check the AP associations to monitor the RF link quality and draw lines between APs to understand how each ES520 was linked to any other AP in order to keep track of hop count and debug the network for example when mobile APs became relays for stationary ground APs. The auto logout feature of the Web interface proved to be quite burdensome as it required frequent re-authenticate against each AP and re-select the AP association option.

b. Conclusion

The ES520 only partially met the COASTS 802.11 network requirements for the Thailand I test. The availability issues that occurred in the second week raised concerns about the ES520's network suitability for COASTS 2007 scenario and military applications. All APs were configured with omni-direction antennas for the client and backhaul radios. The omni-directional antennas provided RF coverage throughout the AOR but it was assumed that the high heat and humidity that occurred in the second week affected the RF coverage and ultimately the ES520s performance. The exact cause of the network degradation experienced in the second week could not be ascertained. Therefore more ES520s along with directional antennas were deployed to provide maximum RF coverage over the operation area. The network configuration with

directional antennas helped to lessen the affect of the heat and humidity on the network for the Thailand II deployment because it provided more efficient use of the RF energy from the deployed APs. The current web based user interface is difficult to use and is not suitable for military operations.

It also appeared that the ES520 was limited to software based cryptography at this time. The maximum network throughput achieved was 5.5Mbps of usable data bandwidth when crypto was enabled. This limited how and where the APs could be deployed for testing. This caused the network to be set up in a dense configuration and was not optimal throughput capacity for operations requiring real time video feeds.

c. Recommendations

(1) Product Prototype. There are a few mechanical, software, management and configuration issues with the ES520. Considering the infancy of the product, these issues should be resolved over time. Although all of the below ES520 issues should be addressed at some point; the 5.5Mbps throughput limitation, control over AP association, and antenna configuration should be solved before the Thailand II deployment. Inability to establish network availability, redundancy and the lack AP association control, could limit the 2007 COASTS team's ability to provide full situational awareness of the AOR

(2) Network Manager. An investment in implementing a Simply Network Management Protocol (SNMP) would simplify the management of multiple APs and provide the required data collection capability utilizing Management Information Base (MIB) to monitor network health. A network management application can be built utilizing SNMP and MIB that present an administrator with several ways to view and analyze network data (Dean, p 797). This capability will also allow monitoring of the network from more than one location because SNMP is part of TCP/IP.

d. Lessons Learned

The ES520 is capable of providing network support for the COASTS 2007 scenario, but the network management remains an issue as the number of deployed APs increases.

(1) Unit status. The face plate had to be removed each and every time to verify that the unit was functioning correctly. Countless man hours were lost during operations asking the deployed personnel to remove the face plate and verify the LED activity and then replace the faceplate to maintain a full weatherized package. In some cases due to having the unit mounted on light poles and other locations to clear the Fresnel zone, personnel were completely unable to verify any status of the device short of bringing a laptop into the field and looking for the 802.11g radio SSID. This is less than ideal as in some cases personnel had to walk out to individual APs and wirelessly log into the AP to observe AP status. The vendor should invest in developing a network management capability that assists with monitoring deployed AP statuses.

E. THAILAND II FINAL DEMONSTRATION

Thailand II demonstration marked the culmination of COASTS 2007 operations in Thailand. The main objective was to fully integrate all peripherals into the 802.11 and 802.16 networks in order to provide real-time situation awareness of the AOR in support of a Maritime, Humanitarian relief and SAR scenarios. This section will contrast and compare Mesh Dynamics 2006 network performance to the ES520's network performance in the COASTS 2006 and 2007 scenarios.

1. Test Conditions

This section will describe the terrain, weather and topology conditions during the 2007 ES520 network deployment in Thailand.

a. Terrain

March is the burning season in Thailand and most of the heavy vegetation around the deployed network was burned down. By the May field test, the vegetation around the Dam had grown back. The vegetation was not an issue for the 802.11 network because it was more or less around the lake outside of the 802.11 coverage.

b. Weather

The Thailand II experiment was conducted from May-Jun 2007. The weather during the May deployment was not much different from the weather during the March deployment. On the other hand during the Mesh Dynamics deployment in 2006, the temperature reached 100 plus a few times, which is a concern for AP CPU cooling. See Appendix H for details on the 2006 and 2007 weather conditions at the Dam face.

c. Topology

Thirteen ES520 APs had to be deployed to provide the required network support to the deployed UAVs, ground cameras, balloon camera, maritime camera, ground sensors and biometric devices for 2007 Thailand II exercise.

The same 8dbi omni-directional antenna configuration used in the Fort Hunter Liggett field tests were used for 7 ground APs in the Thailand II network see Figure V-10. The root–AP along with 6 other non-root APs were configured with directional antennas, see Figure V-11. Power was provided by light-poles for the ES520s and UBI batteries powered the Mesh Dynamics APs. Figure V-12 depicts the revised topology for Thailand II.

The topology was revised for Thailand II which included the use of more APs and directional antennas in order to provide the best availability and reliability throughout the network. As for the set-up, APs NR 1, 4, 6, balloon root, UAV APs, and, second TOC root-AP were configured with directional antennas to provide increased reliability for video traffic from the UAV site and balloon AP camera back to the TOC. The directional antennas were also used to help improve network availability with the

maritime AP, (which was configured with the prefer root AP deselected as to allow it to hop to the nearest non-root ground AP), by providing a more direct RF propagation to the TOC. See Figure V-13 for a graphic of the prefer root upgrade.

As mentioned in the previous test evaluations, the Fortress ES520s configured in non-root mode do not have the ability to associate with the non-root with the strongest RF signal. The Fortress engineers developed the 2.63 firmware update to rectify the association issues. The 2.63 upgrade allows the network administer to configure the non-root AP to prefer root AP only or closet non-root for traffic data flow. The ES520 user manual states:

> Prefer Root allows you to configure whether a non-root Bridge in a point-to-multipoint network will default to communicating with the root Bridge whenever it is available (Enabled) or will always communicate with the closest network node (i.e., the Bridge from which the received signal is strongest, Disabled). You can enable Prefer Root to limit the number of hops a non-root Bridge in a point-to-multipoint network must make in order to access a LAN through the root Bridge. If the root Bridge is not available, a network Bridge on which Prefer Root is Enabled will then establish communication with the closest Bridge (ES520 Bridge Guide, p 1).

The 2.63 upgrade should increase network availability and redundancy in that the AP that is configured to shift to the closet AP.

Figure V-10. ES520 and Mesh Dynamics non-root APs at Mae Ngat Dam, Thailand 2007.

Figure V-11. ES520 and Mesh Dynamics root APs configuration at Mae Ngat Dam, Thailand 2007.

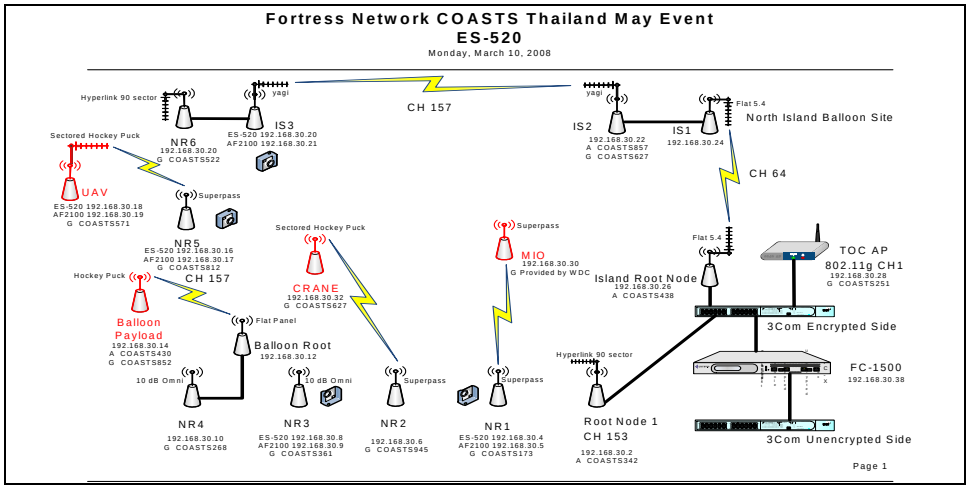


Figure V-12. Topology for Thailand II at Mae Ngat Dam, Thailand 2007.

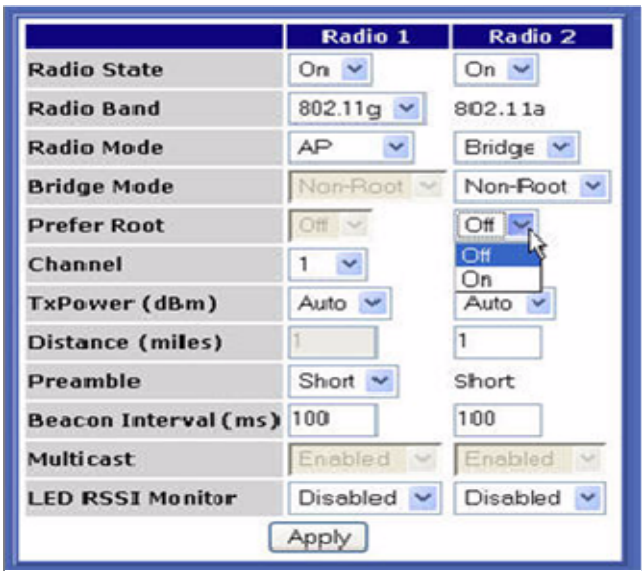


Figure V-13. ES520 GUI presenting the new prefer root configuration option. (from ES520 user guide, p 25).

2. Mesh Dynamics Test Results

Mesh Dynamics was also deployed at Thailand II in order to test the automatic frequency management protocol. The same network link instability that occurred during the Fort Hunter Liggett mobile field test occurred again during operation tests with the Mesh Dynamics APs in Thailand. After consulting with ITAC employee at NPS, network technicians and Mesh Dynamics engineers, it was determined that the RF space for COASTS 2007 was to saturated which contributed to Mesh Dynamics link degradations. Due to the inability to establish a usable link during Thailand 2007 deployment, Mesh Dynamics Thailand II 2006 network performance data was used to compare to the ES520 2007 network performance.

The below objectives for Mesh Dynamics network performance was explained in the Russo thesis, 2007 after action report and the Red Team's report on Mesh Dynamics 2006 network security performance.

a. Results and Discussion

(1) Transportability. The Mesh APs are highly transportable. One large shoulder mounted book bag can carry four Mesh APs, three UBI batteries, eight omni antennas and connectors. Two pelican cases were utilized to pack all Mesh Dynamics APs and accessories for the 2007 Thailand II field test. The weight limit for the Thailand field experiment could not exceed 70 pounds per case. All Mesh Dynamics APs and accessories for the field test weighed less than 140 pounds total. The case used for transport is displayed in Figure V-14. Another aspect of the Mesh Dynamics APs that made it very transportable was its lower power requirements. One UBI battery could power one Mesh AP for eight hours. The light weight of the battery and the ease of configuring the AP made the deployment of the Mesh Dynamics APs very user friendly. Tactically this enabled the 802.11 network, when using Mesh Dynamics APs, to be deployed in within an hour. See Figure V-15 for a picture of the UBI battery.

Figure V-14. Storage case utilized for transport of 802.11 devices (from www.pelicancase.com, DEC 2007).

Figure V-15. Ultralife UBI-2590 Battery (from www.batteryproducts.com SEPT 2007)

(2) Network throughput in high temperature environment.

As explained in Russo's 2006 thesis, the COASTS 2006 team successfully established a full 802.11 wireless mesh network and was able to provide wireless support for the scenario. Both directional and omni-directional antennas were used to maintain usable wireless coverage of the dam face. As indicated by the throughput data in Table V-2, Mesh Dynamics provided good quality throughput for data and video traffic for the 2006 COASTS scenario in Thailand. The 2006 Mesh Dynamics network also was able to provide network support for, real-time video surveillance of the entire area of operations through the use of up to six separate Axis 213 PZT cameras, all operating on the network at one time (one aerial-deployed camera, five ground-deployed cameras)(Russo, p 98).

As indicated by the throughput data collected below, Mesh Dynamics Mesh Modules were capable of surviving the harsh weather conditions of Thailand and provide usable throughput for the 2006 COASTS operations.

Mesh throughput/hevy vegetation/Temp: 98 F/wet/humid conditions			
13dBi to 13dBi 802.11a at Thailand			
Date:May 2006	**Direct to Direct AVG Throughput**		
Miles	**Min(Mbps)**	**Max(Mbps)**	**Final AVG(Mbps)**
0.2	18	22	20
0.3	2.4	19	14
0.4	2	19	14
0.5	0.755	18.6	12.9
0.6	2.2	18	14.8
0.7	1.22	18.6	14.7
0.8	3.04	17.77	14.88
13dBi to 5dBi 802.11a at Thailand			
Date: May 2006	**Direct to Omni AVG Throughput**		
Miles	**Min(Mbps)**	**Max(Mbps)**	**Final AVG(Mbps)**
0.3	2.87	18.6	13.68
0.4	0.406	18.6	11.57
0.5	3.9	9.19	7.3
0.6	0.708	6.6	5
0.7	3.63	8.4	4.7
0.8	17	21.6	19.4
0.9	15.8	22.8	19.9
1	16	21.05	18.3

Table V-2. Mesh Dynamics 2006 throughput data from Lounsbury 2006 thesis

(3) Network security capability and limitations against Red Team's network security attacks. Having usable throughput was very important to the COASTS 2006 team, but having usable throughput and securing the throughput traffic was even more important. The fully wireless meshed network created by the 2006 COASTS team was quickly degraded once the Information Warfare Red Team began its network attacks. The IWRT main objective was to cause a denial of service utilizing open source hacking methods found on the internet. The below excerpt from the IWRT 2006 AAR report details the Mesh Dynamics Mesh Modules vulnerability to DOS attacks.

The IWRT was able to easily degrade the Mesh access points utilizing denial of service (DOS) tactics. "The DoS attack resulted in the entire network going offline for the duration of the DoS. IWRT performed the DoS attack using one notebook computer, the Linux OS, and the TCPReplay utility configured to use small

UDP packets with the intention of degrading, but not significantly interrupting network availability. The attack was directed at a single Mesh Dynamics access point while network availability was monitored using Kismet (Coast 2006 Network Assessment, p 19). During the DoS, the Mesh Dynamics APs recycled based on their response to the network load, however, some APs required manual resets and power cycling to recover." (Coast 2006 Network Assessment, p 25)

The Mesh Dynamics APs are constantly broadcasting updates to other Mesh APs in order to stay in a Mesh link. Broadcasting allows the Mesh Dynamics APs to adjust frequencies and know which AP or APs are available for traffic. The IRWT was able to use the Mesh Dynamics' automatic frequency management protocol against itself by capturing the broadcasting sessions and replaying them, which overwhelmed the APs CPUs and effectively resulted in major network degradation. By spoofing the broadcast sessions and replaying them, the Mesh APs assumed that broadcast packets were legitimate and tried to process them which resulted in a DOS because the legitimate broadcast packets could not efficiently be processed.

The IRWT made the following observations during the DoS attacks. The entire network could be halted in six to ten seconds by capturing traffic and retransmitting the same traffic to all of the mesh APs:

1. Mesh devices would continually recycle, and several did not recover.

2. During the DoS attack manual resets of hardware were required for one AP and the attached Camera.

3. Each packet type used by the IWRT successfully denied service with no noticeable variations.

4. Both DoS tools, TCP Replay and Netcat, were equally affective.

5. Only one attack system was required to halt 802.11a traffic.

6. No usable data was identified on the network during the DoS attacks (Coast 2006 Network Assessment, p 26)

The Mesh Dynamics network protocol that creates the meshed links between APs is faulty and that is how the IWRT were able to exploit the 2006 802.11 network. Mesh Dynamics completely failed at establishing network access security for the network traffic for the 2006 COASTS Thailand exercise. Therefore the network access security capability of Mesh Dynamics was very limiting.

The attacks conducted by the Red Team affected network availability but did not result in data compromise. For the tactical users, data compromise would affect tactical operations more than availability; but availability would affect operation efficiency because of the information delays caused by DOS.

(4) Availability. The Mesh Dynamics APs were deployed for eight hours per day for ten days during the COASTS 2006 deployment. The 2006 Mesh network seemed to be robust enough to support the COASTS 2006 scenario based on the COASTS 2006 network Mesh network accomplishments mentioned above. Availability for Mesh Dynamics in the AOR was 100%. All mesh modules successfully provided suitable throughput for the scenarios. On the other hand, as indicated by the 2006 Red Team's report, the mesh modules failed in the availability category when network security was tested. The IWRT successfully halted network traffic during the live scenario which resulted in 100% network degradation.

> Two successful DoS attacks were conducted on the COASTS system at Mae Ngat Dam, Thailand. The first DoS attack resulted in confusion, as a lack of verifiable network problems on the COASTS network prevented the COASTS team from successfully mitigating the attack during the assessment exercise. On a second DoS attempt, the IWRT completely halted 802.11a traffic while decreasing 802.11g transmissions to minimal packet traffic, causing a manual re-start for several mesh devices. The final Objective consisting of a man-in-the-middle deception was only demonstrated and never attempted as the network never fully recovered from previous attacks. In its current configuration, the security posture of the COASTS mesh network is poor (Coast 2006 Network Assessment, p 28)

IEEE 802.11 wireless network availability is very important in both military and civilian applications. Due to the nature of their work, local police and fire departments always need 100 percent availability in their line of work because of the possible life and death factors. The military operations also have the need for high availability in their wireless networks because relaying video or data back to commanders for situation awareness can significantly affect the decision making process of the commanders. Mesh Dynamics network availability was at a 100% when it was not under security attacks on the other hand network availability was very poor during the DOS attacks, which resulted in a complete network failure for the 2006 COASTS team's scenario. Therefore Mesh Dynamics would not be satisfactory for environments that require robust wireless security and high availability.

(5) Military Suitability. The flaws with the automatic frequency management protocol and security vulnerabilities make Mesh Dynamics unusable for military applications. Mesh Dynamics modules are very easily configured, can be deployed in less than five minutes, have a network viewer that can management all connected APs, and have multiple radios that are dedicated to receive and send transmissions. All of these features would help make military deployments more rapid and efficient, but the protocol that provides Mesh Dynamics its ability to self heal, self form, and manage bandwidth can be exploited, therefore making this product not suitable for military applications.

b. Conclusion

Mesh Dynamics network performance in the Thailand II 2006 and 2007 deployment was unsatisfactory. Mesh Dynamics does have promising network features but the protocol that runs the features seems to be flawed.

The Mesh Dynamics APs in 2006 deployment provided satisfactory unsecured throughput for the COASTS team scenario. The multiple radio implementations that are unique to Mesh Dynamics APs allowed the 2006 COASTS team to create a fully meshed network that supported all deployed peripheral devices.

Although the accomplishment of a fully meshed network was great for the 2006 team, the security set-backs that occurred nullified this accomplishment.

The Mesh Dynamics Mesh Module AP does implement all of the IEEE security standards but these standards have not been evaluated by any third party i.e., WiFi Alliance or NSA. Therefore in the operational test of the Mesh Dynamics AP's security capability, it was found that the protocol that produces the mesh architecture made the Mesh Dynamics APs susceptible to DOS attacks.

While utilizing free hacking tools, the IWRT were able to easily degrade the Mesh Dynamics APs. See Appendix I for more details on the tools utilized. In one case they were able to capture video and replay it back through the network without network manager's knowledge. The security mechanism of the Mesh Dynamics Modules must be reexamined before this product can be used in military applications.

c. Recommendation

(1) Protocol update. The Mesh Dynamics AP needs an update to its proprietary mesh protocol. Updates in this category should make this product more capable of providing a more stable 802.11 network.

(2) Network security**.** Due to flaws in its network protocol, and a lack of a good defense against basic network attacks i.e., replay and DOS, the Mesh Dynamics APs need an alternative security mechanism to protect network data from network replay attacks. For example, third party security products such as authentication devices and end to end encrypters could be used to encrypt the data before it is passed through the network and authenticate users before network access is allowed. It is highly recommended that when using Mesh Dynamics for military operations, a third party security devices be used to eliminate the security duties from the Mesh Dynamics APs.

3. Fortress ES520 Test Results

This section will detail the test results, of Fortress ES520 network performance in a fixed ground configuration during the Thailand II testing.

a. Results and Discussion

(1) Transportability. The face plate on the ES520 seems to be a vulnerable component that was subject to extensive damage in shipping and operational accidents. There were numerous bent and damage faceplates that render the entire ES520 unusable for any outdoor deployments. The ES520's WAN Ethernet weatherization kit construction is flawed. Once the kit is configured with a CAT 5 cable, it can not be disassembled without destroying the kit.

The power supply was not been a problem for the deployment of the ES520, but it was not a seamless process. The ES520 requires 48volts for operation and this was generated by a car battery and power inverter for the Fort Hunter Liggett and Fort Ord field tests. In Thailand, the light poles that were used to power the ES520s supplied a 120volts (specially rigged by Thai's) but it required that extra Ethernet cables and Power Over Ethernet (POE) devices be purchased. It was understandable that IEEE 802.11 devices deployed in the field require power but in the case of rapid deployment for tactical reasons, this power supply has to be pre-deployed if the ES520 is to be used. Finally shipping the ES520s over to Thailand took up a lot of space. Over four Pelican cases, see Figure V-15, were used to carry thirteen ES520s and its accessories to Thailand since the airline weight limit was 70 pounds per case. Since this weight limit is for commercial carriers only and it would not be much of a limiting factor for military deployments. However, compared to Mesh Dynamics, the ES520 required more resources for deployment.

(2) Determine usable throughput in high temperature environment. The ES520 engineers did not fix the previously identified 5.5Mbps throughput limitation while in encryption mode for the Thailand II field test. Therefore the average throughput remained at 5.5Mbps and the directional antennas did not help at

all with improving throughput. The ES520 did not meet the COASTS 2007 fixed ground network throughput requirement of 11Mbps. On the other hand adding a second root AP along with a dedicated backhaul AP for the UAV site coupled with the 2.63 firmware upgrade, the ES520 did do an outstanding job backhauling video and data for the scenario. The second root AP added network redundancy so when the first root AP became unreachable, the non-root APs configured with the prefer root AP feature off were able to backhaul traffic to the second root-AP via connected non-root APs. Table V-3 details the IxChariot throughput readings from a directional antenna to an omni-directional antenna and from a directional to directional antenna. The directional to directional antenna had a 1Mbps increase in throughput over the omni to directional antennas which was not a significant improvement to network operations. Another highlight of the ES520 providing usable throughput is depicted in Figure V-17 which is a PTZ AXIS 213 camera attached to a ground AP zoomed out to provide surveillance of the Maritime Interdiction Operations that took place on the dam face lake.

The ES520 did not meet the established minimum network throughput requirement of 11Mbps, but operationally the actual network throughput was usable while deployed in the harsh environment of Thailand.

Figure V-16. Ground ES520 backhauling video from Axis 213 camera back to TOC of the MIO scenario. (Thailand 2007)

ES520 throughput/hevy vegetation/Temp: 98 F/wet/humid conditions				
13dBi to 13dBi 802.11a at Thailand				
Date:May 2007		**Direct to Direct AVG Throughput**		
Miles	**Test Runs**	**Min(Mbps)**	**Max(Mbps)**	**Final AVG(Mbps)**
1.2	1	5.7	7	6.8
	2	1.2	7	6.4
	3	5.9	7	6.7
	4	5.9	7	6.8
	5	6	7	6
	6	5.9	7	6.8
	7	5.7	7	6.8
	8	5.6	7	6.8
	9	5.5	7	6.8
	10	5.9	7	6.8
13dBi to 8dBi 802.11a at Thailand				
Date:May 2007		**Direct to Omni AVG Throughput**		
Miles	**Test Runs**	**Min(Mbps)**	**Max(Mbps)**	**Final AVG(Mbps)**
1	1	4.8	5.7	5.6
	2	4.8	5.7	5.6
	3	3.8	5.7	5.4
	4	3.7	5.7	5.1
	5	3.7	5.7	5.1
	6	4.8	5.7	5.6
	7	4.8	5.7	5.6
	8	4.9	5.7	5.7
	9	4.6	5.7	5.5
	10	4.3	5.7	5.3

Table V-3. (ES520 2007 throughput data Thailand II field test)

(3) Network security capability and limitations against Red Team's network security attacks. Fortress security mechanisms were very affective against the Red Team's network attacks. Fortress secure client software was used coupled with FC1500 to provide encryption at the Media Access Control (MAC) layer of the OSI model. This security implementation required that all wireless devices be authenticated to the network before access would be allowed. The above security configuration joined with the redundant topology set-up made it very difficult for the Red Team to find a weak point in the network to attack. Here are some comments made by the Red Team in their situation report on 27 May 2007.

a. Achievements:

1. The JIOWIC, in coordination with the COASTS Red Team Coordinator, re-accomplished the wireless 802.11a/g attacks used in COASTS 2006 to include the following:

• Single attack box denial of service: used to degrade the network to not allow critical data transmission while allowing network control packets.

• Targeted nodes: used to disable a specific node with critical assets (video, sensors, UAS controls, etc.)

• Complete denial of service: accomplished by attacking multiple points of the wireless network.

2. The attacks in COASTS 2006 exercise were all successful, but the same attacks used against COASTS 2007 were minimally effective, only increasing network traffic 5% to 15%, and not affecting COASTS 2007 operations (Thailand II SITREP 27 May 2007).

As shown in the above excerpt, the ES520s successfully provided robust security in the Thailand II scenarios by protecting all video and data traffic.

(4) Availability. The ES520 maintained a 100 percent operational availability in network performance with all APs deployed for the Thailand II scenarios. While under attack by the Red Team and deployed in a harsh environment, the ES520s successfully provided full usability of all attached assets to the TOC which resulted in a successful COASTS demonstration for the Royal Thai Air Force.

The success of the ES520 in this Thailand iteration was due to the addition of extra ES520 APs joined with the 2.63 firmware upgrade and the inclusion of directional antennas which helped marginally increase the availability of the network. Therefore availability was 100% for the Thailand II deployment.

(5) Military Suitability. The ES520 network performance test results in availability, network security and usable throughput, indicated that the ES520s can be used in military applications for providing base surveillance, maritime operations from shore to sea, aerial video surveillance and ground mobile operations.

The ES520's 5.5Mbps throughput limitation while in encryption mode was not the optimal throughput capability according to the 802.11a standard but this data rate was deemed to be adequate to support over eleven attached peripheral devices during the operations in Thailand.

b. Conclusion

The ES520 network performance was outstanding in the Thailand II operations. All network requirements were completed effortlessly and the only network deployment set-backs occurred due to faulty Thai equipment. The cherry picker used to lift the APs to 30 feet constantly had mechanical failures in the first few days of deployment.

All thirteen deployed ES520s stayed operational throughout the two week deployment in Thailand and the high heat and humidity (see Appendix H for weather data) did not affect the network performance. The ES520s performance against the Red Team's network attacks was the highlight of the operation. All of the Red Team's network attack objectives were incomplete when it came to applying them to the ES520 network. The Fortress security suite provided the proper wireless defense against the same attacks that degraded the 2006 Mesh Dynamics network. As a result of its network security performance, the ES520 was designated to be the 802.11 wireless network for the 2008 COASTS deployments.

Overall the ES520 performance in COASTS 2007 Thailand II scenarios surpassed the previous COASTS 802.11 network performances. As a result of the ES520's network performance, military use of the product is feasible.

c. Recommendation

(1) Encryption and GUI. The ES520s needs a throughput greater than 5.5mbps while in encryption mode. This would help with AP requirements for operations. A GUI should be developed that consolidates all AP information for monitoring and updating. This would decrease the network administrator's tasking when

more than four APs are deployed. Providing updates for these two features would add immediate user benefits in the tactical arena.

(2) Data encryption processing. Utilizing the AF2100 or similar product that will encrypt the data before it is sent through the ES520 is recommended for future deployments. This would optimize the ES520s performance by eliminating the encryption processing job.

d. Lessons Learned

(1) Accessories for Network Deployment. Providing the accessories required to attach the APs to the light pole was not a vendor problem but rather a network manager's problem. Extra poles approximately four feet in length were procured with hose clamps to properly attach the APs to the light poles. The Network Managers must identify the additional equipment needed for successful deployment beyond what is already included with the standard ES520 package.

4. ES520 and Mesh Dynamics Ground Network Comparison

a. Network Performance

The Mesh Dynamics APs have many usable features which allow easy configuration and deployment. The features include, self configuring, self healing, remote management and easy transportability, which makes the mesh modules attractive devices for military applications. All of the above benefits of the Mesh Dynamics APs could make military deployments more efficient and conserve operational man-hours. Unfortunately, Mesh Dynamics network performance during the Red Team's network attacks was unsatisfactory and resulted in a total network failure for the 2006 COASTS demonstration in Thailand. The products inability to support COASTS 2006 demonstrations and RF auto management protocol problems that occurred in the 2007 deployment makes Mesh Dynamics unsuitable for military applications.

On the other hand in the COASTS 2007 Thailand demonstration, the ES520s network performance was excellent. The same Red Team network attacks that

successfully degraded the Mesh Dynamics network deployed in 2006 did not have the same success with the ES520s. The robust security suite coupled with a firmware update that allowed all non-root APs to connect to the nearest available AP help make it extremely difficult for the Red Team to conduct a successful network attack. The 5.5Mbps throughput limitation while in encryption mode did not significantly hinder network availability in the scenarios. Although the ES520's ability to provide a secure, continuous available and redundant network is limited, it could be used for some military applications such as pier surveillance, base security, and maritime interdiction operations.

b. Overall Conclusion

Both products required at least eleven APs to be deployed in order to provide wireless coverage over a 1.5 mile area. For Mesh Dynamics, having more than thirteen APs in such close proximity would cause problems for its automatic RF manager and probably affect throughput because each AP would try to connect to all active APs within its RF space which could take up bandwidth. As for Fortress, the limit of 5.5 Mbps throughput while encryption is activated would be easily consumed if more than thirteen peripheral devices were deployed.

Although both Mesh Dynamics and the ES520s have network strengths and weaknesses, the ES520 outperformed Mesh Dynamics in the network requirements that contributed to the success of the COASTS demonstrations in Thailand.

5. Other Network Problems not Specific to ES520 and Mesh Dynamics

IEEE 802.11 wireless devices are vulnerable to wireless attacks because RF energy has to be propagated in order to establish a WiFi connection. The Red Team network attack objectives included, degrade network, conduct a successful DOS and hijack network session for deception operations. All of the techniques used to complete their objectives were open source techniques and can be found on the internet. See Appendix I for a list and description of the tools used by the Red Team to attack the network. The average home AP would probably be susceptible to exploitation by some

of the tools listed in Appendix I but with proprietary products such as Mesh Dynamics and Fortress a proprietary solution is usually devised to counter these threats.

The Thai 220vac electrical system has only two wires and there is no grounding option. Most lines were connected using a standard 20 amp circuit breaker, but GFCI outlets are not available. This presented a hazardous condition for the operators, in particular during the rainy season.

The two products used for the IEEE 802.11 network did not have all of the required accessories needed to attach the APs to the light poles in Thailand. When deploying wireless devices, the antenna configuration (i.e., utilizing directional antennas versus using omni-direction antennas) can affect the required accessories needed to properly deploy the AP. The management of the accessories that were required to attach the APs to the light pole was not a vendor problem but rather a network manager's problem. Extra poles approximately four feet in length with hose clamps were needed to properly attach the APs to the light poles.

VI. CONCLUSIONS AND RECOMMENDATIONS

A. OVERVIEW

The COASTS team during the past field experiments conducted in California and Thailand proved that COTS wireless technologies can be applied to real world scenarios i.e., disaster relief, mobile communications, base security and maritime operations in both the civilian and military environments. The COASTS field experiments with COTS technologies have captured the attention of all U.S. military branches and some foreign militaries as well. The main objective of the COASTS team is to demonstrate that COTS technologies that are readily available, easily manageable, secure, structurally hardened, and easily transportable for military operations can be used to create a full command and control architecture in support of real world threat scenarios.

The purpose of this thesis was to evaluate the military suitability of Fortress ES520 802.11 wireless technology and Mesh Dynamic's 4000 series 802.11 wireless technology by conducting a comparative analysis of the technologies network performance while deployed in a tactical ground, maritime and mobile configuration in support of COASTS 2007 field experiments. Several specific field tests were conducted in California and Thailand in order to evaluate the network performance of both the Mesh Dynamics and Fortress ES520s.

B. GENERAL CONCLUSION

The COASTS 2007 team was successful in using COTS technologies in the Search and Rescue, Maritime Interdiction and Humanitarian Assistant scenarios conducted in Thailand. This should benefit United States and coalition militaries in their efforts to provide base security, port security, nation security and disaster relief teams in providing humanitarian assistance through out the world. In particular, the U.S. Navy is currently in a transitional phase that involves a shifting from conducting naval operations in blue water to the littorals areas. In the civilian sector, disasters caused by terrorists attack of 9-11 and hurricane Katrina in New Orleans, have created organizational

changes in how the federal and local forces coordinate and share information in order to prevent and survive major disasters in the United States. COTS technologies can and will assist the military and civilian entities in their transition to a more network centric plug and play ideology which will affectively establish a seamless transfer of information.

The Mesh Dynamics and Fortress access points evaluated in this thesis are not very different from the basic commercial access points marketed by Linksys, Cisco, and Netgear. However, they do have specified proprietary implementations that are not implemented in their counterpart products. The specific proprietary implementations include algorithms that create mesh capability, advance network managers, network security beyond the basic WPA/WPA2 requirement, ruggedness for outside use and the capability to be deployed in a mobile application as an access point. Because both Mesh Dynamics and Fortress devices are proprietary, their special features were only tested during operational experiments.

1. Major Findings

During the evaluations, both the ES520 and Mesh Modules had periods when their product was unable to maintain a 100 percent reliable network. In their current configurations, neither the Fortress nor Mesh Dynamics APs are fully satisfactory for military operations. Both products need improvement to be militarily suitable.

2. ES520

The ES520 outperformed the Mesh Dynamics Mesh Modules in the Thailand scenarios. The 2007 COASTS team was able to configure and maintain a fully integrated 802.11 network that effectively secured all network traffic, provided sustain availability and usable throughput in concert with network attacks conducted by the Red Team with the ES520s. The ES520s successfully supported the scenarios demonstrated in Thailand and appear to be sufficient for use by law enforcement agencies and natural disaster recovery teams.

During mobile testing the ES520 network was significantly degraded. It appeared that the ES520s protocol was not capable of supporting a mobile network from an AP to

AP application. As a result Fortress engineers developed a 2.63 firmware update that provided improved AP to AP mobility. In the Maritime scenario, the ES520s were able to pass data and video from the ES520 attached to the boat back to the TOC. However, during encryption the throughput was limited to 5.5Mbps which is not satisfactory for military operations requiring heavy bandwidth.

The ES520 needs improvement in overall network data throughput while in encryption mode, remote management, transportability, and network security, to be fully suitable for military use.

3. Mesh Dynamics

Mesh Dynamics multiple radio configurations, network management capability, mobile capability and ease of transport are features that can make military operations requiring wireless coverage very efficient. The proprietary protocol that allows the Mesh Dynamics AP to self heal, and self form could make it a very advantageous IEEE 802.11 product. For example in disaster relief scenarios, having a wireless device that can automatically connect and de-conflict radio frequency channels allows more time to be focused on relief efforts rather than network set-up. The advance network capabilities that the Mesh Dynamics' APs offer, although highly beneficial to the network administer, seemed to be flawed while testing the product for COASTS 2007 deployments

The advance mesh protocol that gives the Mesh Dynamics APs their ability to automatically change RF channels and connect to multiple APs is flawed. These APs were easily exploited in their network security test trials and network degradation in the mobile and ground deployments were experienced. It appeared that the Mesh Module protocol that gives the APs the capability to self heal, self form and automatically shift frequency was faulty and that this fault caused the unreliable network problems in both the 2007 and 2006 deployment.

C SPECIFIC CONCLUSIONS FOR FORTRESS ES520

1. Mobile Tests

The specific conclusions of the ES520 network performance mobile tests at Fort Hunter Liggett (flat terrain) and Fort Ord (hilly terrain) are as follows:

a. Graphical User Interface

The ES520s network manager does not provided adequate management when more than four APs are deployed. The ES520 needs a configuration manager that is easy and scaleable. Each AP had to be configured independently of each other, which required configuring each AP by plugging directly into the unit was time consuming and resulted in deployment delays. Once the APs were deployed, each AP required individual wireless logging into or local connection in order to troubleshoot the AP.

b. Network Connectivity in a Mobile Configuration While Deployed on Flat Terrain

The ES520s networking protocol does not associate and re-associate automatically. Therefore, once the mobile configured AP connected to the root AP at the TOC, it stayed connected until line of sight was lost. Network connectivity was limited because the mobile AP was limited to only connecting to the root AP, which was a single point of failure for the network.

c. Network Link Stability While Traversing the Area of Operation

The ES520 software during the FHL tests did not support non-root AP to non-root AP associations in a mobile application. Therefore the link stability from the mobile AP to the stationary ground APs was not achieved. After making a network architecture change, the network link was stable between the mobile AP and ground APs during the Fort Ord operational tests.

d. Mobile AP to Ground AP Handoff Capability

The ES520 network protocol does not support AP hopping. Therefore, as the mobile AP traverses the Area of Operation at FHL, it did not connect to the AP with the strongest RF signal. At Fort Ord, the mobile AP was configured as the root AP, and all non-root ground APs immediately connected while the mobile AP passed through the terrain. However, network mobility was also lost because the ground APs did not connect to each other after the root AP was out of line of sight. Because of this lack of connection, the entire ES520 network would have failed if the root AP had suffered a casualty. As a result, the ES520 AP handoff capability is not suitable for mobile military operations.

e. Usable Throughput in a Mobile Environment

The minimum acceptable operational throughput needed for the mobility test was 3Mbps out to 1.5 miles from the root AP to maintain a useable network connection. At Fort Ord, the throughput data collected for the ES520 averaged 5Mbps. Although the throughput was usable, throughput is considered not military suitable because of the inability of the mobile AP to hop to the closer ground AP when the root AP is out of the line of sight of the root AP.

f. Mobile AP to Ground AP Handoff Capability

The ES520 with an attached Mesh Dynamics AP was able to meet the minimum requirement of one mile with one non-root AP (mobile AP) and the root AP during the flat terrain FHL tests. The maximum usable network distance achieved at Fort Ord was one mile because the Fresnel zone blockage that was brought on by the hilly terrain limited RF propagation. Although the minimum connectivity was achieved, it was not satisfactory for the Thailand deployment which required the other non-root ground APs be connected to the mobile AP as well in order to establish a stable and redundant mobile network out to 1.5 miles.

2. Fixed Ground Tests

The specific conclusions of the ES520 network performance for the Fort Hunter Liggett fixed ground network tests are as follows

a. NetworkAability to Support Peripherals for Scenario, i.e., Cameras, Sensors and UAV Video

The ES520 satisfactorily supported all attached peripheral devices for the 2007 Fort Hunter Liggett fix ground field test.

b. Throughput Capacity in Unencrypted Mode

The ES520 averaged a total network throughput of 28Mbps while in unencrypted mode. This exceeded the requirement of 11Mbps.

3. Thailand Tests

The specific conclusions of the ES520 network performance for the Thailand I and II trials are as follows:

a. Network Performance in High Temperature Environment

The 5.5Mbps throughput limitation while in encryption mode continued to be a problem for the Thailand II field test. Therefore the average network throughput while in encryption mode remained at 5.5Mbps. The ES520 did not meet the established network throughput requirement of 11Mbps, but operationally the network throughput was usable while deployed in the harsh environment of Thailand.

b. Availability

In the Thailand I deployment, the Ao for the first week of operations was 100%. The availability in the second week was 50% and was not militarily suitable. It was suspected that the high heat and humidity that occurred in the second week affected the RF coverage and ultimately degraded the ES520s' network performance. However, this was not proven

The ES520 maintained 100% availability in network performance with all APs in Thailand II scenarios. While under attack by the Red Team and deployed in a harsh environment, the ES520s successfully provided full usability of all attached assets to the TOC which resulted in a successful COASTS demonstration for the Royal Thai Air Force.

c. Antenna Configuration

Due to the network degradation issues that occurred in the second week, a new antenna configuration strategy was utilized which consisted of omni-directional and directional antennas for the Thailand II deployment. The combination of directional and omni-directional antennas created network redundancy in the Thailand II deployment and increased throughput by 1Mbps. (See V-4) The directional antennas also made it very difficult for the Red Team to degrade the entire network because the directional antennas provided concentrated RF energy at a higher gain.

d. ES520s Required for 802.11 Coverage and to Support Peripheral Devices

The network degradation that occurred in the second week led to conclusion that eleven APs in combination with utilizing omni-directional antennas were not enough APs to sufficiently provide data and video backhaul for the AOR. Therefore, the ES520 network covering capability is not militarily suitable.

e. Network Security Capability and Limitations Against Red Team's Network Security Attacks

Fortress security mechanisms were very affective against various Red Team denial of service network attacks. Fortress secure client software was used coupled with FC1500 to provide encryption at the Media Access Control (MAC) layer of the OSI model and successfully provided robust security by protecting all video and data traffic. This was a major improvement over COAST 2006 results.

f. Military Suitability

The ES520 network performance test results in availability, network security and usable throughput, indicated that the ES520s can be used in military applications such as providing base surveillance, maritime operations from shore to sea, aerial video surveillance and ground mobile operations. On the other hand, military operations such as mechanized force support, and tactical situations that require more than five ES520s could not be supported. The ES520's current limitations with throughput while in encryption mode and the limited GUI capability would affect network availability

D. SPECIFIC CONCLUSIONS FOR MESH DYNAMICS

1. Mobile Tests

The specific conclusions of Mesh Dynamics network performance for the Fort Hunter Liggett (flat terrain) and Fort Ord (hilly terrain) mobile network trials are as follows:

a. Remote Management

The Mesh Dynamics' remote manager is a proprietary implementation that creates a network interface that combines all deployed AP information onto a single console. The all in one display and reporting of deployed AP's network information made network management very efficient for AP deployment for the Fort Hunter Liggett mobile test trial.

b. Mesh AP Frequency Shifting Capability

The Mesh APs have a proprietary protocol implemented in hardware that gives all APs the ability to shift to the least busy RF channel when frequency conflicts are detected. This feature was activated as recommended by a Mesh Dynamics engineer, the

connectivity between the APs failed and resulted in the inability to conduct tests involving network connectivity, network stability, throughput, and mobile node handoff capability at FHL.

c. Usable Throughput in a Mobile Environment Conducted on Hilly Terrain

All ten successful throughput runs were fully completed as the mobile AP transverse the area of operation. The Mesh Modules maintained a maximum throughput of 13Mbps throughout the test runs which was more than required to support data and video transfer for COAST 2007 mobile applications.

d. Network Link Stability while Traversing the Area of Operation

The Mesh Dynamics APs successfully maintained a stable network link throughout the test period.

e. Maximum Distance with an Attached Wireless ES520/Mesh Dynamics AP Attached to a Mobile Unit

At Fort Ord, one mile from the first ground AP was the minimum distance needed to meet the stable network criteria. When the mobile AP dipped into the valley, the link connectivity began to degrade. The maximum usable network distance achieved with an attached Mesh Dynamics AP in this hilly environment was one mile.

f. Mobile AP to Ground AP Handoff Capability while Deployed on HillyTterrain

The Mesh Dynamics ground APs connected to both the mobile root-AP and surrounding ground APs at the same time, which created a full meshed network throughout the AOR. As the mobile AP passed the ground APs, it successfully re-associated to the nearest ground AP with no network interruptions.

g. Mesh Dynamics Frequency Management Protocol in a Low RF Environment

Network link problems observed at Fort Hunter Liggett with the auto RF management feature activated were not experienced at the Fort Ord test site. This fact suggests that the RF saturation could have overtaxed the auto frequency management protocol of Mesh Dynamics during the Fort Hunter Liggett mobile test trials.

2. Fixed Ground Tests

The specific conclusions of the Mesh Dynamics network performance for the Fort Hunter Liggett fixed ground network trials are as follows:

a. Network Ability to Support Peripherals for Scenario, i.e., Cameras, Sensors and UAV Video

As reported by Russo, the Mesh Dynamics network was able to pass live video from multiple cameras which demonstrated the Mesh Dynamics 802.11 video management capability. The Mesh Dynamics network also provided full AOR situational awareness by utilizing a balloon deployed at 1,500 feet with an attached Mesh Dynamics AP and Axis 213 PTZ camera.

b. Evaluate Throughput Capacity in Unencrypted Mode –

Mesh Dynamics achieved an average throughput of 11Mbps at Fort Hunter Liggett, which was minimal usable throughput established for the 2007 COASTS 802.11 network.

3. Thailand Tests

The specific conclusions of the Mesh Dynamics network performance for the Thailand II tests are as follows:

a. Transportability

The Mesh APs are highly transportable. One large shoulder mounted book bag can carry four Mesh APs, three UBI batteries, eight omni antennas and connectors. Tactically this enabled the 802.11 network, when using Mesh Dynamics APs, to be deployed in within an hour.

b. Network Throughput in High Temperature Environment

The Mesh Dynamics Mesh Modules were capable of surviving the harsh weather conditions of Thailand and provide usable throughput for the 2006 COASTS operations.

c. Network Security Capability and Limitations Against Red Team's Network Security Attacks

The IWRT easily degraded the Mesh access points utilizing denial of service (DOS) tactics.

d. Availability

Availability for Mesh Dynamics in the AOR was 100%. All mesh modules successfully provided suitable throughput for the scenarios. On the other hand, as indicated by the 2006 Red Team's report, the mesh modules failed in the availability category when network security was tested.

e. Military Suitability

The flaws with the automatic frequency management protocol and security vulnerabilities make Mesh Dynamics unusable for military applications. Mesh Dynamics APs are very easily configured, can be deployed in less than five minutes, have a network viewer that can management all connected APs, and have multiple radios that are dedicated to receive and send transmissions. All of these features would help make military deployments more rapid and efficient, but the protocol that provides Mesh

Dynamics its ability to self heal, self form, and manage bandwidth can be exploited, therefore making this product unsuitable for military applications.

E. RECOMMENDATIONS

Fortress ES520 and Mesh Dynamics Mesh Module ™ APs have usable features that can benefit military applications. The following are recommendations for improvements that are needed to achieve better military suitability for the ES520 and Mesh Dynamics modules:

1. Fortress should improve the ES520' overall network data throughput while in encryption mode, remote management, transportability, and network security.

2. The current ES520 GUI implementation should be improved for more efficient management of deployed ES520 assets.

3. The ES520's weatherization kit should be reconstructed to allow viewing of LED lights for visual diagnosis.

4. The ES520's CAT 5 cable kit should be reconstructed to allow disassembly in order to change out bad cables.

5. The Mesh Dynamics APs should be certified by the WiFi alliance.

6. The advance mesh protocol that gives the Mesh Dynamics AP its ability to automatically change RF channels and connect to multiple APs should be improved to prevent network security exploitation for both mobile and ground operations.

7. A simple network protocol should be implemented in both Mesh Dynamics' and Fortress' APs protocol to allow for network management over the Internet.

F. FURTHER RESEARCH AND STUDY

The following are recommendations for further research and study:

1. The COASTS team should explore more integration with the IEEE 802.16 and IEEE 802.11 networks in future deployments since IEEE 802.16 networks are capable of providing network capabilities at longer distances with better mobile and security capabilities than the 802.11 networks.

2. The COASTS team should develop a local area network that has redundancy while utilizing IEEE 802.11 and IEEE 802.16 technologies.

3. An application layer security capability should be a part of the COASTS 2008 security implementation.

4. More at sea testing should be conducted with wireless devices before conducting Maritime Scenarios in order to ascertain optimal antenna configuration for operations.

5. Voice over IP should be incorporated as a part of the wireless network attachment support requirement for the 2008 deployment.

6. Unmanned Aerial Vehicles (UAV) video should be passed through the 802.16 links for the 2008 deployment.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Akin, Devin "Certified Wireless Network Administrator." Berkeley: McGrewHill/Osbourne, February 18, 2003.

Buddenberg, Rex, Dr. Network analog: "Amateurs talk about bits per second; Professionals discuss availability." April 95.

Burke, Karen. CS4680: "Introduction to Certification and Accreditation." September 2007.

Dean, Tamara. "Network Guide to Networks." Thomson: Course Technology, 2005.

ES520 Bridge Guide. Fortress Technologies. Retrieved September 2007 from http://www.fortresstechnologies.com.

Fresnel zone calculator Retrieved August 2007 from http://www.terabeam.com/support/calculations/fresnel-zone.php.

Hyperlink Technologies. Hyperlink Technologies Antenna Specifications. Retrieved August 2007 from http://www.hyperlinktech.com.

Joint Electronic Warfare Center Assessment and Testing Division (COASTS) Network Assessment (August 2006) report produced by the Naval Postgraduate School (NPS) and the Deputy Under Secretary of Defense for Advanced Systems and Concepts (DUSD/AS&C).

Lee, Christopher R. "Aerial Command and Control Utilizing Wireless Meshed Networks in Support of Joint Tactical Coalition Operations." September 2005. Master's Thesis, Naval Postgraduate School, Monterey, CA.

Lounsbury, Robert. "Optimum Antenna Configuration for Maximizing Access Point Range of an IEEE 802.11 Wireless Mesh Network in Support of Multi-Mission Operations Relative to Hastily Formed Scalable Deployments." June 2007. Master's Thesis. Naval Postgraduate School, Monterey, CA.

Multicast Conformance and Performance Testing. IXIA. Retrieved September 2007 from http://www.ixiacom.com/.

Russo, Anthony Joseph. "Test and Evaluation of Mesh Dynamics 802.11 Multi-Radio Mesh Modules in Support of Coalition Riverine operations." June 2006. Master's Thesis, Naval Postgraduate School, Monterey, CA.

Why Structured Mesh. Mesh Dynamics. Retrieved August 2007 from http://www.meshdynamics.com/WhyStructured Mesh.html.

APPENDIX A. WEATHER DATA FORT HUNTER LIGGETT MOBILE TEST TRIALS

2007 Weather Conditions during ES520/Mesh Deployment at Fort Hunter Liggett.						
Date		Temperature (F)	Wind Speed	Precipitation	Dew Point(F)	Humidity(F)
16-JAN-07	High Average Low	52 51.1 50.2	11.9 knots	0 inches	13	68
17-JAN-07	High Average Low	51.4 49.6 46.6	16.7 knots	0 inches	26	85
18-JAN-07	High Average Low	53.2 52.3 50.7	10.4 knots	0 inches	19	84
19-JAN-07	High Average Low	54 52.8 51.4	14.9 knots	0 inches	19	81
20-JAN-07	High Average Low	53.1 52.5 51.8	23.6 knots	0 inches	21	81
21-JAN-07	High Average Low	54.1 53.3 52.7	21.9 knots	0 inches	21	81

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. MESH DYNAMICS AND FORTRESS NODE CONFIGURATIONS FOR FORT HUNTER LIGGETT MOBILE TEST TRIAL

The Mesh Dynamics mobile configuration was as follows:

- Root Node (Mesh Dynamics box 4452) Equipped with one 2.4GHz service radio and three 5.8Ghz backhaul radios
- Two 8dbi Omni-directional antennas connected to the uplink and downlink radios.
- One 8dbi Omni-directional antenna connected to the service radio.
- Powered by POE connected to generator.

Mesh non-root nodes were configured as follows:

- First non-root Node (Mesh Dynamics box 4350) Equipped with one 2.4GHz service radio and two 5.8Ghz backhaul radios
- Two 8dbi Omni-directional antennas connected to the uplink and downlink radios.
- One 8dbi Omni-directional antenna connected to the service radio.
- Tripod with Mounting Pole, mounting brackets and screws.
- One UBI battery with cable.

- Second non-root Node (Mesh Dynamics box 4350) Equipped with one 2.4GHz service radio and two 5.8Ghz backhaul radios
- Two 8dbi Omni-directional antennas connected to the uplink and downlink radios.
- One 8dbi Omni-directional antenna connected to the service radio.
- Tripod with Mounting Pole, mounting brackets and screws.
- One UBI battery with cable.

- Mobile non-root Node (Mesh Dynamics box 4425)
  Equipped with three 2.4GHZ backhaul radios and one 2.4GHZ scanner radio.
- Two 8dbi Omni-directional antennas connected to the uplink and downlink radios.
- One 8dbi Omni-directional antenna connected to the scanner radio.
- Tripod with Mounting Pole, mounting brackets and screws.
- One UBI battery with cable.

The Fortress mobile configuration was as follows:

- Root Node (ES520 box) Equipped with one 2.4GHz service radio and one 5.8GHz backhaul radio.
- One 8dbi Omni-directional antennae connected to the 5.8GHz backhaul port.
- One 8dbi GHz Omni-directional antennae connected to the 2.4GHz access port.
- Powered by POE connected to generator.

- First non-root Node (ES520) Equipped with one 2.4GHz service radio and one 5.8GHz backhaul radio.
- One 8dbi Omni-directional antennae connected to the 5.8GHz backhaul port.
- One 8dbi GHz Omni-directional antennae connected to the 2.4GHz access port.
- Powered by car battery.
- Tripod with Mounting Pole, mounting brackets and screws.

- Second non-root Node (ES520) Equipped with one 2.4GHz service radio and one 5.8GHz backhaul radio
- One 8dbi Omni-directional antennae connected to the 5.8GHz backhaul port.
- One 8dbi GHz Omni-directional antennae connected to the 2.4GHz access port.
- Powered by car battery.
- Tripod with Mounting Pole, mounting brackets and screws.
- Mobile non-root Node (ES520) Equipped with one 2.4GHz service radio and one 5.8GHz backhaul radio.
- One 8dbi Omni-directional antennae connected to the 5.8GHz backhaul port.
- One 8dbi GHz Omni-directional antennae connected to the 2.4GHz access port.
- Powered by car battery.
- Tripod with Mounting Pole, mounting brackets and screws.

APPENDIX C. WEATHER DATA FORT ORD MOBILE TEST TRIALS

2007 Weather Conditions during ES520/Mesh Deployment at Fort Ord.						
Date		Temperature (F)	Wind Speed	Precipitation	Dew Point(F)	Humidity(F)
30-Jan-07	High Average Low	55.4 49.4 42.8	4 knots	0 inches	43.3	78
2-Feb-07	High Average Low	57.2 49.1 39.2	4 knots	0 inches	38.8	89

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. MESH DYNAMICS AND FORTRESS NETWORK THROUGHPUT DATA FROM FORT ORD MOBILE TEST TRIALS

Run #	MD Mobile at Fort ORD, CA	Throughput	Weather/Temperature	Date	Terrain Type
0	at 30 Mph out to a mile	MAX: 12 Mbps MIN: 1 Mbps AVG: 10 Mbps	Clear/55.4	30-Jan-07	Hills, very light vegetation and paved ground
1	at 30 Mph out to a mile	MAX: 6 Mbps MIN: 3 Mbps AVG: 4 Mbps	Clear/55.4	30-Jan-07	Hills, very light vegetation and paved ground
2	at 30 Mph out to a mile	MAX: 11 Mbps MIN: .7 Mbps AVG: 8 Mbps	Clear/55.4	30-Jan-07	Hills, very light vegetation and paved ground
3	at 30 Mph out to a mile	MAX: 9 Mbps MIN: 3 Mbps AVG: 8 Mbps	Clear/55.4	30-Jan-07	Hills, very light vegetation and paved ground
4	at 30 Mph out to a mile	MAX: 10 Mbps MIN: 2 Mbps AVG: 8 Mbps	Clear/55.4	30-Jan-07	Hills, very light vegetation and paved ground
5	at 30 Mph out to a mile	MAX: 13 Mbps MIN: 5 Mbps AVG: 11 Mbps	Clear/55.4	30-Jan-07	Hills, very light vegetation and paved ground
6	at 30 Mph out to a mile	MAX: 13 Mbps MIN: 2 Mbps AVG: 7 Mbps	Clear/55.4	30-Jan-07	Hills, very light vegetation and paved ground
7	at 30 Mph out to a mile	MAX: 13 Mbps MIN: .8 Mbps AVG: 10 Mbps	Clear/55.4	30-Jan-07	Hills, very light vegetation and paved ground
8	at 30 Mph out to a mile	MAX: 13 Mbps MIN: .2 Mbps AVG: 6 Mbps	Clear/55.4	30-Jan-07	Hills, very light vegetation and paved ground
9	at 30 Mph out to a mile	MAX: 13 Mbps MIN: 2 Mbps AVG: 10 Mbps	Clear/55.4	30-Jan-07	Hills, very light vegetation and paved ground
10	at 30 Mph out to a mile	MAX: 6 Mbps MIN: 1 Mbps AVG: 5 Mbps	Clear/55.4	30-Jan-07	Hills, very light vegetation and paved ground

Run #	ES520 Mobile at Fort ORD, CA	Throughput	Weather/Temperature	Date	Terrain Type
0	at 30 Mph out to a mile	MAX: 5 Mbps MIN: 4 Mbps AVG: 5 Mbps	Clear/57	2-Feb-07	Hills, very light vegetation and paved ground
1	at 30 Mph out to a mile	MAX: 5 Mbps MIN: .9 Mbps AVG: 4 Mbps	Clear/57	2-Feb-07	Hills, very light vegetation and paved ground
2	at 30 Mph out to a mile	MAX: 5 Mbps MIN: 3 Mbps AVG: 5 Mbps	Clear/57	2-Feb-07	Hills, very light vegetation and paved ground
3	at 30 Mph out to a mile	MAX: 5 Mbps MIN: .7 Mbps AVG: 4 Mbps	Clear/57	2-Feb-07	Hills, very light vegetation and paved ground
4	at 30 Mph out to a mile	MAX: 6 Mbps MIN: .9 Mbps AVG: 5 Mbps	Clear/57	2-Feb-07	Hills, very light vegetation and paved ground
5	at 30 Mph out to a mile	MAX: 6 Mbps MIN: .7 Mbps AVG: 4 Mbps	Clear/57	2-Feb-07	Hills, very light vegetation and paved ground
6	at 30 Mph out to a mile	MAX: 6 Mbps MIN: 2 Mbps AVG: 4 Mbps	Clear/57	2-Feb-07	Hills, very light vegetation and paved ground
7	at 30 Mph out to a mile	MAX: 6 Mbps MIN: 1 Mbps AVG: 4 Mbps	Clear/57	2-Feb-07	Hills, very light vegetation and paved ground
8	at 30 Mph out to a mile	MAX: 6 Mbps MIN: .6 Mbps AVG: 4 Mbps	Clear/57	2-Feb-07	Hills, very light vegetation and paved ground
9	at 30 Mph out to a mile	MAX: 5 Mbps MIN: 4 Mbps AVG: 5 Mbps	Clear/57	2-Feb-07	Hills, very light vegetation and paved ground
10	at 30 Mph out to a mile	MAX: 5 Mbps MIN: .01Mbps AVG: 1 Mbps	Clear/57	2-Feb-07	Hills, very light vegetation and paved ground

APPENDIX E. WEATHER DATA FORT HUNTER LIGGETT FIXED GROUND TEST TRIALS FOR MESH DYNAMICS AND FORTRESS

2007 Weather Conditions during ES520 Deployment at Fort Hunter Liggett.						
Date		Temperature (F)	Wind Speed	Precipitation	Dew Point(F)	Humidity(F)
26-Feb-07	High Average Low	55 52.6 50.2	8 knots	.12 inches	38	92
27-Feb-07	High Average Low	54.7 51.4 49.6	14.4 knots	.09 inches	40	85
28-Feb-07	High Average Low	50.2 49.3 47.3	18.5 knots	0 inches	34	96
1-Mar-07	High Average Low	59 41.3 30	5.5 knots	0 inches	30	92
2-Mar-07	High Average Low	62.6 44.6 32	5.4 knots	0 inches	33	96
2006 Weather Conditions during Mesh Deployment at Fort Hunter Liggett.						
10-Feb-06	High Average Low	59.7 53.9 49.6	7.4 knots	0 inches	33	96
11-Feb-06	High Average Low	54.9 52.8 50.4	13.9 knots	0 inches	39	86
12-Feb-06	High Average Low	55 54 52	16 knots	0 inches	38	89
13-Feb-06	High Average Low	58.8 56.7 55.8	8.2 knots	0 inches	39	92
14-Feb-06	High Average Low	58.1 55 54	18 knots	0 inches	39	92

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F. FORT HUNTER LIGGETT TOPOLOGY FOR THE FIXED GROUND TEST TRIALS FOR MESH DYNAMICS AND FORTRESS

- ES520 Topology: Root AP (ES520 box) Equipped with one 2.4GHz service radio and one 5.8GHz backhaul radio. Frequency channel is 153 will for 5.8 backhaul.

  a. One 8dbi Omni-directional antennae connected to the 5.8GHz backhaul port.

  b. One 8dbi GHz Omni-directional antennae connected to the 2.4GHz access port.

  c. Powered by POE connected to generator.

  d. Cat 5 cable to connect to switch from Laptop.

- First non-root AP (ES520) Equipped with one 2.4GHz service radio and one 5.8GHz backhaul radio.

  a. One 8dbi Omni-directional antennae connected to the 5.8GHz backhaul port.

  b. One 8dbi GHz Omni-directional antennae connected to the 2.4GHz access port.

  c. Powered by Car battery utilizing an inverter with DC adapter or POE.

  d. Tripod with Mounting Pole, mounting brackets and screws.

- Second non-root AP (ES520) Equipped with one 2.4GHz service radio and one 5.8GHz backhaul radio.

  a. One 8dbi Omni-directional antennae connected to the 5.8GHz backhaul port.

  b. One 8dbi GHz Omni-directional antennae connected to the 2.4GHz access port.

  c. Powered by Car battery utilizing an inverter with DC adapter or POE.

  d. Tripod with Mounting Pole, mounting brackets and screws

- Third non-root AP (ES520) Equipped with one 2.4GHz service radio and one 5.8GHz backhaul radio.

    a. One 8dbi Omni-directional antennae connected to the 5.8GHz backhaul port.

    b. One 8dbi GHz Omni-directional antennae connected to the 2.4GHz access port.

    c. Powered by Car battery utilizing an inverter with DC adapter or POE.

    d. Tripod with Mounting Pole, mounting brackets and screws.

- Fourth non-root AP (ES520) Equipped with one 2.4GHz service radio and one 5.8GHz backhaul radio.

    a. One 8dbi Omni-directional antennae connected to the 5.8GHz backhaul port.

    b. One 8dbi GHz Omni-directional antennae connected to the 2.4GHz access port.

    c. Powered by Car battery utilizing an inverter with DC adapter or POE.

    d. Tripod with Mounting Pole, mounting brackets and screws

The details for the 2006 Mesh Dynamics ground set-up are as follows:

- Mesh Topology: Root AP (Mesh Dynamics box 4452) Equipped with one 2.4GHz service radio and three 5.8Ghz backhaul radios (Russo, pg 82)

    a. Two 8dbi Omni-directional antennas connected to the uplink and downlink radios.

    b. One 8dbi Omni-directional antenna connected to the service radio.

    c. Powered by POE connected to the TOC switch.

    d. Cat 5 cable to connect to switch from Laptop.

- First non-root AP (Mesh Dynamics box 4350) Equipped with one 2.4GHz service radio and two 5.8Ghz backhaul radios (Russo, pg 82)

    a. Two 8dbi Omni-directional antennas connected to the uplink and downlink radios.

    b. One 8dbi Omni-directional antenna connected to the service radio.

    c. Tripod with Mounting Pole, mounting brackets and screws.

    d. One UBI battery with cable.

- Second non-root Node (Mesh Dynamics box 4350) Equipped with one 2.4GHz service radio and two 5.8Ghz backhaul radios (Russo, pg 82)

    a. Two 8dbi Omni-directional antennas connected to the uplink and downlink radios.

    b. One 8dbi Omni-directional antenna connected to the service radio.

    c. Tripod with Mounting Pole, mounting brackets and screws.

    d. One UBI battery with cable.

- Third non-root AP (Mesh Dynamics box 4350) Equipped with one 2.4GHz service radio and two 5.8Ghz backhaul radios (Russo, pg 82)

    a. Two 8dbi Omni-directional antennas connected to the uplink and downlink radios.

    b. One 8dbi Omni-directional antenna connected to the service radio.

    c. Tripod with Mounting Pole, mounting brackets and screws.

    d. One UBI battery with cable.

- Fourth non-root AP (Mesh Dynamics box 4350) Equipped with one 2.4GHz service radio and two 5.8Ghz backhaul radios.

a. Two 8dbi Omni-directional antennas connected to the uplink and downlink radios.

b. One 8dbi Omni-directional antenna connected to the service radio.

c. Tripod with Mounting Pole, mounting brackets and screws.

d. One UBI battery with cable.

APPENDIX G. WEATHER CONDITIONS AT MAE NGAT DAM, THAILAND I

19 MAR to 1 APR 2007 Weather Conditions MAE NGAT DAM, Thailand						
Date		Temperature (F)	Wind Speed	Precipitation	Dew Point(F)	Humidity(F)
19-Mar-07	High Average Low	94 82 67	9 knots	0 inches	54	73
20-Mar-07	High Average Low	97 84 72	12 knots	0 inches	66	78
21-Mar-07	High Average Low	95 82 67	20 knots	0 inches	65	88
22-Mar-07	High Average Low	95 82 68	10 knots	0 inches	64	83
23-Mar-07	High Average Low	95 82 68	10 knots	0 inches	66	83
24-Mar-07	High Average Low	95 82 68	8 knots	0 inches	58	78
25-Mar-07	High Average Low	99 85 68	7 knots	0 inches	61	78
26-Mar-07	High Average Low	99 84 70	12 knots	0 inches	63	78
27-Mar-07	High Average Low	101 87 69	8 knots	0 inches	64	78
28-Mar-07	High Average Low	100 84 69	8 knots	0 inches	61	78
29-Mar-07	High Average Low	101 86 70	13 knots	0 inches	62	82
30-Mar-07	High Average Low	99 88 77	18 knots	0 inches	71	78

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX H. WEATHER CONDITIONS AT MAE NGAT DAM, THAILAND II

21-May to 3-Jun 2007 Weather Conditions MAE NGAT DAM, Thailand						
Date		Temperature (F)	Wind Speed	Precipitation	Dew Point(F)	Humidity (F)
21-May-07	High Average Low	86 80 74	13 knots	0 inches	73	94
22-May-07	High Average Low	88 82 75	15 knots	0 inches	73	94
23-May-07	High Average Low	90 82 73	13 knots	0 inches	72	94
24-May-07	High Average Low	94 84 73	13 knots	0 inches	73	94
25-May-07	High Average Low	93 84 75	15 knots	0 inches	73	94
26-May-07	High Average Low	93 84 75	14 knots	0 inches	74	94
27-May-07	High Average Low	96 86 75	10 knots	0 inches	75	100
28-May-07	High Average Low	93 84 76	12 knots	0 inches	76	92
29-May-07	High Average Low	94 84 75	16 knots	0 inches	74	95
30-May-07	High Average Low	92 82 73	18 knots	0 inches	73	100
31-May-07	High Average Low	92 82 73	19 knots	0 inches	73	100
1-Jun-07	High Average Low	89 82 74	8 knots	0 inches	73	100
2-Jun-07	High Average Low	91 83 75	12 knots	0 inches	76	100

21-29 Mar 2006 Weather Conditions MAE NGAT DAM, Thailand						
21-Mar-06	High Average Low	101 91 79	8 knots	0 inches	68	88
22-Mar-06	High Average Low	107 89 73	16 knot	0 inches	61	78
23-Mar-06	High Average Low	100 90 67	7 knots	0 inches	58	73
27-Mar-06	High Average Low	109 96 72	7 knots	0 inches	61	73
28-Mar-06	High Average Low	96 80 64	14 knots	0 inches	59	73
29-Mar-06	High Average Low	96 80 63	18 knots	0 inches	65	87

APPENDIX I. TOOLS USED BY THE RED TEAM

Itronix GoBook Model IX260+ (Commercial Off-the-Shelf (COTS)): GoBook is a registered trademark of Itronix, a General Dynamics company. It is designed as a fully-rugged notebook computer that includes an Intel® Mobile Pentium® 1.8 GHz Processor, removable shock-mounted encased hard drive, simultaneous support of up to three RF modems, and touch screen display.

For COASTS, the IWRT configured the GoBook computers to use a dual-boot configuration that included standard installations of Fedora Core 3 and Microsoft Windows XP with Service Pack 2. The CB9-GP-EXT 802.11a/b/g Card bus Card uses the Atheros Super AG chipset. In 802.11b mode, the output power is 18 dBm. In 802.11g mode, the output power is 18 dBm at 6 Mbps and 15 dBm at 54 Mbps. In 802.11a mode, the output power is 17 dBm at 6 Mbps and 13 dBm at 54 Mbps. In addition to the internal antenna, the CB9-GP-EXT has a Hirose MS-147-C connector that supports the use of external antennas.

D-Link ANT24-1801 Directional Antenna (COTS): The D-Link ANT24-1801 18 dBi Directional Yagi Antenna is weatherproof and made of corrosion-resistant material to withstand harsh outdoor conditions and wind speeds up to 120 miles/hr. It has a maximum range of 5 miles; however, in Thailand it had a range of 2 miles.

2.4 GHz Flat Antenna Model HG2414P-NF (COTS): HyperLink Technologies' 2.4 GHz 14 dBi Flat Patch Wireless LAN Antenna Model: HG2414P-NF is a high performance directional antenna that is suitable for indoor and outdoor applications. It can sustain winds up to 150 miles/hour.

5.8 GHz ISM / UNII Antenna Model HG5808P (COTS): The HyperLink Technologies' 5.8 GHz ISM / UNII Band Wireless LAN Flat Patch Antenna 8 dBi Model: HG5808P offers all-weather operation and can sustain winds up to 150 miles/hour.

Fedora Core 3 (Open-Source): Red Hat Linux is a distribution of the Linux OS assembled by Red Hat. Version 9 was released on March 31, 2003 and has since been replaced by Red Hat Enterprise Linux, which is available commercially, and the open source alternative; Fedora.

Kismet 2006-04-R1 (Open-Source): Kismet is a passive 802.11 wireless network detector, packet sniffer, and intrusion detection system. Kismet's passive capability means it can scan networks without sending any detectable packets. The IWRT uses Kismet to enumerate 802.11 wireless networks.

Ethereal 10.9 (Open-Source): Ethereal, now known as Wireshark, is developed by Gerald Combs. It is a protocol analyzer used to identify and enumerate network communications. It similar in functionality to TCPDump; however, it has a graphical user interface and runs on multiple OSs to include Microsoft Windows, various distributions of Linux, Sun Solaris, FreeBSD and Mac OS X.

TCPDump 3.9.4 (Open-Source): TCPDump is designed to intercept and display the communications of another user or computer on a network. TCPDump is developed by the Network Research Group at the Lawrence Berkeley National Laboratory in Berkeley, California.

TCPReplay (Open-Source): TCPReplay allows users to replay captured network traffic for testing the robustness of network devices. TCPReplay can run on most UNIX systems and is maintained as an open-source project by SourceForge.net.

Nessus 2.2.5 (Open-Source): Nessus is an open source vulnerability scanner that begins with a port scan to determine which ports are open on the target computer and then runs various exploits on the target system. Nessus is developed by Tenable Security.

Nmap 3.93 (Open-Source): Nmap is a freeware Linux-based port scanner written by Fyodor. It is used to evaluate the level of security of one or more target computers, determine the OSs and identify potentially vulnerable network services or server applications.

NetCat 0.7.1 (Open-Source): Netcat is a network utility that can read and write data to and from TCP and UDP network connections. The IWRT used Netcat at COASTS to write large amounts of data to specific network resources on the wireless mesh network.

Windows XP (COTS) (Open-Source): Windows XP is Microsoft's latest desktop OS, which is built on the Windows NT kernel. The IWRT attack computers had all of the latest hot fixes, updates, and service packs installed.

UDPFlood version 2.0 (Open-Source): UDPFlood is a Windows-based stress test utility that sends UDP packets to a specific IP and port at a predetermined rate. The packets can be generated by a typed text string, a given size of random bytes or data from a file. This tool is a free download from Foundstone's website at http://www.foundstone.com.

AirMagnet Laptop Analyzer (COTS): AirMagnet's Laptop Analyzer is a commercial wireless network detector, packet sniffer, and intrusion detection system developed by AirMagnet, Incorporated. Its passive capability makes it capable of scanning without being detected. The IWRT uses AirMagnet to enumerate 802.11 wireless networks and corroborate the results from comparable open source utilities.

NetStumbler (Open-Source): Jelsoft Industries, Limited built NetStumbler, a freeware Windows-based utility, to identify wireless network access points. In addition to the SSID, NetStumbler is capable of displaying the signal strength, signal-to-noise ratio, and whether or not the access point is encrypted.

YellowJacket (COTS): The YellowJack by Berkeley Varitronics is a hand-held wireless receiver that interfaces with Hewlett-Packard's iPAQ® PocketPC® in sweeping, analyzing and optimizing 2.4 GHz wireless networks. The receiver measures all 14 802.11b/g channels allowing the user to determine the access point's MAC address, SSID and received signal strength indication signal levels for all nearby access points.

Anritsu Model 2721A Spectrum Master (COTS): The Spectrum Master MS2721A by Anritsu is a fully-functional handheld spectrum analyzer designed to for next generation wireless LAN and cellular signals, including 802.11a, 3G, ultra-wideband, WiMAX, wireless monitoring systems and measurement capability for applications up to 7.1 GHz.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX J. MESH DYNAMICS NETWORK RESULTS FORT HUNTER LIGGETT 2006

a) Results and Discussion

(1) Network ability to support peripherals for scenario i.e., cameras, sensors and UAV video

As reported by Russo, the Mesh Dynamics network was able to pass live video from multiple cameras which demonstrated the Mesh Dynamics 802.11 video management capability. The Mesh Dynamics network also provided full AOR situational awareness by utilizing a balloon deployed at 1,500 feet with an attached Mesh Dynamics AP and Axis 213 PTZ camera. No report was provided for UAV nor ground sensor support.

(2) Evaluate throughput capacity in unencrypted mode –

The IEEE 802.11a implementation of the OFDM technology claims to boost network data rates to 54Mbps (Akins, p 314). 54Mbps is the optimal data rate for 802.11a but data rates from 5Mbps and greater should be usable for data and video transfer. In the 2006 deployment, Mesh Dynamics achieved an average throughput of 11Mbps at Fort Hunter Liggett, which was minimal usable throughput established for the 2007 COASTS 802.11 network. See the table below for more throughput details.

Mesh throughput/light vegetation/Temp: 58 F/dry conditions			
8dBi to 8dBi 802.11a at FORT HUNTER LIGGETT			
Date:12 FEB 2006	**AVG Throughput**		
Miles	**1st Run**	**2nd Run**	**Final AVG**
0	21.896	21.724	21.81
0.1	20.533	21.245	20.889
0.2	20.622	20.189	20.406
0.3	20.939	16.134	18.537
0.4	17.747	12.851	15.299
0.5	2.137	14.567	8.352
0.6	9.064	15.936	12.5
0.7	12.691	13.238	12.965
0.8	12.468	11.918	12.193
0.9	11.475	13.614	12.545
0.98	**10.241**	**12.137**	**11.189**

In summary it appeared the Mesh Dynamics 802.11 network performed well for the 2006 COASTS deployment. The mesh modules passed live video from ground APs and aerial APs providing full situational awareness of the AOR. This achievement qualified the Mesh Dynamics network as a usable asset for the 2006 Thailand deployment. The interconnectivity that the patent Mesh Dynamics protocol provided resulted in the achievement of 11Mbps network throughput which was an excellent accomplishment according to the 2006 network managers.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Tom Hoivik
   Naval Postgraduate School
   Monterey, California

4. Professor Rex Buddenberg
   Naval Postgraduate School
   Monterey, California

5. LtCol Karl Pfeiffer
   Naval Postgraduate School
   Monterey, California

6. Mr. James Ehlert
   Naval Postgraduate School
   Monterey, California