



# **NAVAL POSTGRADUATE SCHOOL**

**MONTEREY, CALIFORNIA**

## **THESIS**

**TACTICAL WIRELESS NETWORKING IN  
COALITION ENVIRONMENTS: IMPLEMENTING  
AN IEEE 802.20 WIRELESS END-USER  
NETWORK UTILIZING FLASH-OFDM TO  
PROVIDE A SECURE MOBILE EXTENSION TO  
EXISTING WAN**

by

William J Parrish  
Daniel R Tovar

September 2005

Thesis Advisor:  
Second Reader:

Alex Bordetsky  
James Ehlert

**Approved for public release; distribution is unlimited.**

THIS PAGE INTENTIONALLY LEFT BLANK

<b>REPORT DOCUMENTATION PAGE</b>			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
<b>1. AGENCY USE ONLY (Leave blank)</b>		<b>2. REPORT DATE</b> September 2005	<b>3. REPORT TYPE AND DATES COVERED</b> Master's Thesis	
<b>4. TITLE AND SUBTITLE:</b> Tactical Wireless Networking In Coalition Environments: Implementing an IEEE 802.20 Wireless End-User Network utilizing FLASH-OFDM to Provide a Secure Mobile Extension to Existing WAN			<b>5. FUNDING NUMBERS</b>	
<b>6. AUTHOR(S)</b> William J. Parrish and Daniel R. Tovar				
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> Naval Postgraduate School Monterey, CA 93943-5000			<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>	
<b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> N/A			<b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>	
<b>11. SUPPLEMENTARY NOTES</b> 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.				
<b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b> Approved for public release; distribution is unlimited			<b>12b. DISTRIBUTION CODE</b> A	
<b>13. ABSTRACT (maximum 200 words)</b> <p>This thesis will focus on the area of 802.20 wireless networking as a feasible "last mile" solution to wireless access in a tactical coalition environment and will be implemented into a series of experiments. Implementation will primarily utilize Flarion's FLASH OFDM (Fast, Low-Latency Access with Seamless Handoff Orthogonal Frequency Division Multiplexing).</p> <p>Current and future military and homeland security forces, conducting operations in a tactical environment, require instant access to data. Wireless data requires a reliable air-link resource anchored to a viable service platform. Flarion's FLASH-OFDM wireless air-link mimics the performance of a high-speed wireline environment. Through Flarion's Radio Router base station and mobile data terminal, a Radio Access Network is created. It connects directly to a standard IP Packet Data Network forming a wireless data network.</p> <p>Utilizing this network environment, this thesis intends to document the implementation of a limited objective experiment (LOE) in support of homeland security and the War on Terrorism (WOT); specifically, the testing of an IEEE 802.20 network enabling US and key foreign partners to integrate mobile wireless local area network (WLAN) technologies into a surveillance and target acquisition network program.</p>				
<b>14. SUBJECT TERMS</b> 802.20, 802.16, OFDM, Fast Low Latency with Seamless Handoff (FLASH), Office of the Chief Technology Officer (OCTO), Military Operations in an Urban Terrain (MOUT), Mobile WAN, NLOS, Radio Router			<b>15. NUMBER OF PAGES</b> 139	
			<b>16. PRICE CODE</b>	
<b>17. SECURITY CLASSIFICATION OF REPORT</b> Unclassified	<b>18. SECURITY CLASSIFICATION OF THIS PAGE</b> Unclassified	<b>19. SECURITY CLASSIFICATION OF ABSTRACT</b> Unclassified	<b>20. LIMITATION OF ABSTRACT</b> UL	

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited.**

**TACTICAL WIRELESS NETWORKING IN COALITION  
ENVIRONMENTS: IMPLEMENTING AN IEEE 802.20 WIRELESS  
END-USER NETWORK UTILIZING FLASH-OFDM TO PROVIDE A  
SECURE MOBILE EXTENSION TO EXISTING WAN**

William J Parrish  
Lieutenant Commander, United States Navy  
B.S., Jacksonville University, 1993

Daniel R Tovar  
Lieutenant, United States Navy  
B.S., United States Naval Academy, 1997

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL  
September 2005**

Authors: William J Parrish

Daniel R Tovar

Approved by: Dr. Alex Bordetsky  
Thesis Advisor

James Ehlert  
Second Reader

Dan Boger, Chairman  
Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

This thesis will focus on the area of 802.20 wireless networking as a feasible “last mile” solution to wireless access in a tactical coalition environment and will be implemented into a series of experiments. Implementation will primarily utilize Flarion’s FLASH OFDM (Fast, Low-Latency Access with Seamless Handoff Orthogonal Frequency Division Multiplexing).

Current and future military and homeland security forces, conducting operations in a tactical environment, require instant access to data. Wireless data requires a reliable air-link resource anchored to a viable service platform. Flarion’s FLASH-OFDM wireless air-link mimics the performance of a high-speed wireline environment. Through Flarion’s Radio Router base station and mobile data terminal, a Radio Access Network is created. It connects directly to a standard IP Packet Data Network forming a wireless data network.

Utilizing this network environment, this thesis intends to document the implementation of a limited objective experiment (LOE) in support of homeland security and the War on Terrorism (WOT); specifically, the testing of an IEEE 802.20 network enabling US and key foreign partners to integrate mobile wireless local area network (WLAN) technologies into a surveillance and target acquisition network program.

In addition, this thesis will leverage previous experimental data from the Joint Information Operations Center (JIOC). This thesis will provide new analysis and data sets to supplement the JIOC’s efforts to catalogue baseline data across multiple networking protocols in order to further the JIOC’s ability to recommend specific wireless networking solutions to US Military Forces.

THIS PAGE INTENTIONALLY LEFT BLANK



# TABLE OF CONTENTS

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>1</b>
<b>A.</b>	<b>BACKGROUND .....</b>	<b>1</b>
<b>B.</b>	<b>OBJECTIVES .....</b>	<b>4</b>
<b>C.</b>	<b>RESEARCH QUESTIONS .....</b>	<b>5</b>
<b>D.</b>	<b>SCOPE .....</b>	<b>5</b>
<b>E.</b>	<b>METHODOLOGY .....</b>	<b>6</b>
<b>II.</b>	<b>WIRELESS NETWORKING.....</b>	<b>7</b>
<b>A.</b>	<b>WIRELESS NETWORKING.....</b>	<b>7</b>
1.	Multipath .....	7
2.	Time Dispersion .....	7
3.	Doppler Spread .....	8
4.	Rayleigh Fading .....	8
<b>B.</b>	<b>FLASH-OFDM VS. 802.16.....</b>	<b>8</b>
1.	FLASH-OFDM Physical Layer .....	9
a.	Downlink .....	10
b.	Uplink .....	12
2.	FLASH-OFDM MAC Layer vs. 802.16 MAC Layer.....	13
a.	802.20 MAC States.....	14
b.	802.16 MAC states.....	16
3.	FLASH-OFDM vs. 802.16 Quality of Service .....	17
a.	802.20 User Group Service Model QoS.....	17
b.	802.16 QoS .....	18
4.	FLASH-OFDM vs. 802.16 Security .....	19
a.	802.16 Security.....	21
b.	FLASH-OFDM Security.....	22
<b>III.</b>	<b>NETWORK CONFIGURATION .....</b>	<b>23</b>
<b>A.</b>	<b>PHYSICAL ARCHITECTURE OVERVIEW.....</b>	<b>23</b>
<b>B.</b>	<b>RADIOROUTER BASE STATION.....</b>	<b>24</b>
<b>C.</b>	<b>FLASHVIEW EMS SERVER .....</b>	<b>26</b>
1.	Flashview Server Installation.....	28
a.	FlashView Server Minimum Software/Hardware Requirements.....	29
<b>D.</b>	<b>MOBILE NETWORK SERVER.....</b>	<b>29</b>
<b>E.</b>	<b>AAA SERVER.....</b>	<b>30</b>
<b>F.</b>	<b>TERMINAL EQUIPMENT .....</b>	<b>31</b>
1.	PC Card .....	31
2.	Desktop Modem .....	32
<b>G.</b>	<b>THIRD PARTY ELEMENTS .....</b>	<b>33</b>
1.	Access Concentrator .....	33
2.	Aggregation Router .....	34

3.	Switching Infrastructure .....	34
4.	Home Agent .....	34
5.	Core Router .....	35
IV.	IMPLEMENTATION AND TESTING .....	37
A.	INTRODUCTION.....	37
B.	WASHINGTON, D.C. TESTING.....	37
1.	OCTO UL/DL Performance .....	37
2.	Setup and Power Consumption .....	39
3.	21 Mar Highlights .....	40
4.	22 Mar Highlights .....	44
5.	24-25 March Highlights.....	50
C.	MOUT FACILITY TESTING AT FORT ORD .....	56
1.	COLT and 802.16 to 802.20 Setup.....	57
3.	“Through Wall” and Urban Environment Testing .....	58
D.	CAMP ROBERTS TNT FIELD EXPERIMENTS.....	61
1.	802.20 Remote Sensor Support for TNT.....	62
2.	Additional NLOS and Mobility Testing at Camp Roberts .....	64
V.	NECESSARY ADAPTATIONS TO COTS.....	69
A.	INTRODUCTION.....	69
B.	NECESSARY ADAPTATIONS TO COTS EQUIPMENT .....	69
1.	Base Station Size .....	69
2.	Ability to MESH Network Cards .....	70
C.	STANDARDIZATION OF IEEE 802.20 TO LOWER COSTS.....	70
D.	SUMMARY .....	71
VI.	CONCLUSIONS.....	73
A.	FINDINGS .....	73
1.	Wireless Networking Requirements.....	73
2.	FLASH-OFDM.....	73
3.	Optimal 802.20 Configuration .....	74
4.	COLT Vehicle.....	74
5.	System Costs .....	75
6.	Recommendations and Lessons Learned.....	75
B.	FURTHER RESEARCH.....	76
1.	BS in an aerial asset .....	76
2.	Integrating 802.20 into Satellite Communications.....	77
3.	802.20 Vulnerability Testing.....	77
4.	Application to Collaborative Efforts for Coast Guard.....	77
5.	Utilizing 802.20 by a UAV .....	77
6.	FLEXBAND.....	77
C.	SUMMARY .....	79
APPENDIX A	OCTO TNT TEST SCENARIOS.....	81
1.	TESTING OVERVIEW AND EQUIPMENT.....	81
2.	SCENARIO 1 .....	82
3.	SCENARIO 2 .....	86

<b>APPENDIX B</b>	<b>MOUT FACILITY TNT TEST SCENARIOS.....</b>	<b>89</b>
<b>APPENDIX C</b>	<b>CAMP ROBERTS TNT TEST SCENARIOS.....</b>	<b>93</b>
1.	<b>SCENARIO 1 TNT FIELD DEMONSTRATION.....</b>	<b>93</b>
2.	<b>SCENARIO 2 ON THE MOVE NETWORK PERFORMANCE.....</b>	<b>94</b>
<b>APPENDIX D</b>	<b>FLASH-OFDM PRICE QUOTES TO NPS .....</b>	<b>99</b>
1.	<b>3 SECTOR SYSTEM.....</b>	<b>99</b>
2.	<b>OMNI SYSTEM.....</b>	<b>100</b>
3.	<b>ANTENNAS AND CABLING .....</b>	<b>101</b>
<b>APPENDIX E</b>	<b>RECOMMENDED EQUIPMENT AND SOFTWARE FOR FUTURE TESTING .....</b>	<b>103</b>
A.	<b>EQUIPMENT.....</b>	<b>103</b>
B.	<b>SOFTWARE.....</b>	<b>103</b>
<b>APPENDIX F</b>	<b>FMDM AND FMLP VARIABLES .....</b>	<b>105</b>
A.	<b>FMDM VARIABLES .....</b>	<b>105</b>
B.	<b>FMLP PROCESSED VARIABLES.....</b>	<b>107</b>
<b>APPENDIX G</b>	<b>OCTO TOWER SPECIFICATIONS .....</b>	<b>109</b>
<b>LIST OF REFERENCES .....</b>		<b>113</b>
<b>INITIAL DISTRIBUTION LIST .....</b>		<b>117</b>

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF FIGURES

Figure 1.	ARG ADNS Architecture with JTRS WNW [Ref 2] .....	2
Figure 2.	OMFTS Envisioned Architecture [Ref 2] .....	3
Figure 3.	Relationship of FLASH-OFDM to Traditional Layering [Ref 7] .....	9
Figure 4.	Example of Adjacent Cell Hopping Patterns [Ref 7] .....	11
Figure 5.	Uplink Dwell by dwell tone hopping sequence [Ref 7] .....	12
Figure 6.	MAC States and State Transitions [Ref 7] .....	14
Figure 7.	802.16 Network Entry Process [Ref 15] .....	15
Figure 8.	Redline Communications Man-Packable AN-50 (compare to Figure 15. below) .....	20
Figure 9.	Redline AN-50 Configuration .....	21
Figure 10.	802.16 MAC Data Unit [Ref 17] .....	22
Figure 11.	Indoor RadioRouter Base Station .....	25
Figure 12.	RadioRouter Supporting Equipment .....	26
Figure 13.	SNMP Model .....	27
Figure 14.	Flashview Configuration View [Ref 20] .....	28
Figure 15.	FLASH-OFDM Wireless PC Card .....	32
Figure 16.	Netgear Indoor Desktop Modem/Bridge (802.20/802.11) .....	33
Figure 17.	Inmotion Desktop Modem/Bridge (802.20/802.11/Ethernet/etc) .....	33
Figure 18.	WARN UL Performance [Ref 25] .....	38
Figure 19.	WARN DL Performance [Ref 25] .....	38
Figure 20.	HP iPAQ HX4700 with 802.20 NIC installed in expansion pack running FMM .....	39
Figure 21.	SA Server successful in DC .....	41
Figure 22.	OCTO Exterior and Sector Antenna Placement .....	42
Figure 23.	Pixilation and Artifacts at 512 Mbps .....	43
Figure 24.	QCheck Response Time Test .....	45
Figure 25.	NetPersec Results from 6 MB File DL .....	46
Figure 26.	Iperf DL Testing on 4 <sup>th</sup> District, OCTO 0241, Tower .....	47
Figure 27.	Concurrent UL/DL Testing on 4 <sup>th</sup> District, OCTO 0241, Tower .....	47
Figure 28.	DL Rate Compared with Velocity .....	48
Figure 29.	UL Test on 4 <sup>th</sup> District Tower (Kbps and MPH) .....	49
Figure 30.	Thematic Map Superimposed Over Satellite Street Level View for DL Test .....	50
Figure 31.	Individual and Group Sector Throughput Testing .....	51
Figure 32.	Walking Transit from US Capitol to OCTO Office .....	53
Figure 33.	Connection Status for Through Wall and NLOS Testing .....	53
Figure 34.	BSID Switching During Through Wall and NLOS Testing .....	54
Figure 35.	Highway Speed Testing .....	54
Figure 36.	NLOS Sibley Hospital Tower to Northwest Portion of GW HWY Run .....	55
Figure 37.	Scatter Plot of SNR vs. Velocity .....	56
Figure 38.	LOS 802.16 Relay Station, COLT and 802.16 Range 32 Tower .....	56

Figure 39.	Panoramic View of MOUT.....	57
Figure 40.	Interior and Exterior view of COLT .....	57
Figure 41.	MOUT Early Warning Using Full Duplex Audio and Video.....	58
Figure 42.	Connectivity in a 30” Metal Sewer Pipe Under Ground.....	59
Figure 43.	Early Warning, Identification and Remote Translation Test .....	59
Figure 44.	SNR with IDW Projection at MOUT.....	60
Figure 45.	COLT Next to TOC at Camp Roberts .....	61
Figure 46.	Camp Robert 802.20 and IP Camera Balloon Configuration .....	62
Figure 47.	Video Motion Detected by 802.20 Altitude Sensor.....	63
Figure 48.	Visual Identification by 802.20 Ground Sensor .....	63
Figure 49.	802.20 TNT Configuration with Elevation.....	64
Figure 50.	Camp Robert SNR Site Survey.....	65
Figure 51.	Screen Capture from Second Mobile User During Runway Testing.....	66
Figure 52.	SNR Received During Runway Trials.....	67
Figure 53.	D-DACT 802.20 Driver and Software Upload.....	68
Figure 54.	Current FLASH-OFDM Deployment [Ref 24].....	78
Figure 55.	FLEXBAND DEPLOYMENT [Ref 24].....	79

**LIST OF TABLES**

Table 1. FLASH OFDM Physical Layer Characteristics [Ref 7] .....10

Table 2. Uplink Modulation and Coding Class Peak Rates [Ref 7] .....13

Table 3. MS Portrait Settings Tested .....43

Table 4. Statistic for Individual and Group Sector Throughput Testing .....52

Table 5. OCTO Tower Sector Specifications .....111

THIS PAGE INTENTIONALLY LEFT BLANK



## LIST OF ACRONYMS

AAA	Authentication, Authorization and Accounting
ADNS	Automated Digital Network
AES	Advanced Encryption Standard
ARG	Amphibious Readiness Group
ARQ	Automatic Retransmission Request
ATM	Asynchronous Transfer Mode
BE	Best Effort
BS	Base Station
C/I	Carrier to Interface
C4ISR	Command, Control Communications, Computers, Intelligence, Surveillance and Reconnaissance
CE	Compact Edition
CENETIX	Center for Network Innovation and Experimentation
CLI	Command Line Interface
COLT	Cell on Light Truck
CT	Context Transfer
CTP	Context Transfer Protocol
dB	Decibel
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DNS	Domain Name System
DoD	Department of Defense
DSCP	Diffserv Code Point
DSL	Digital Subscriber Line
EMS	Element Management System
FCAPS	Fault Monitoring, Configuration, Accounting, Performance and Security
FDD	Frequency Division Duplexing
FLASH-OFDM	Fast Low Latency Seamless Handoff Orthogonal Frequency Division Multiplexing

GIG	Global Information Grid
GUI	Graphical User Interface
HA	Home Agent
HSRP	Hot Standby Router Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISI	Intersymbol Interference
ISNS	Integrated Shipboard Network System
JIOC	Joint Information Operations Center
JMCOMS	Joint Maritime Communications Strategy
JTA	Joint Technical Architecture
JTRS	Joint Tactical Radio System
LNA	Low Noise Amplifier
LOE	Limited Objective Experiment
MAC	Medium Access Control
MNS	Mobile Network Server
MOUT	Military Operations in an Urban Terrain
NCW	Network Centric Warfare
NLOS	Non-Line of Sight
NOC	Network Operations Center
NPS	Naval Postgraduate School
NRL	Naval Research Lab
nrtPS	Non-Real Time Polling Services
OCTO	Office of the Chief Technology Officer
OEF	Operation Enduring Freedom
OFDM	Orthogonal Frequency Division Multiplexing
OIF	Operation Iraqi Freedom
OMFTS	Operational Maneuver from the Sea
OSI	Open Systems Interconnect
OSPF	Open Shortest Path First

PAPR	Peak-to-Average Power Ratio
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications System
PDA	Personal Digital Assistant
PDU	Protocol Data Units
PHB	Per Hop Forwarding Behaviors
PHY	Physical Layer
PKM	Privacy Key Management
PPP	Point-to-Point Protocol
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RADIUS	Remote Authentication Dial-In Service
RDBMS	Relational Database Management System
RR	Radio Router
rtPS	Real-Time Polling Services
SDR	Session Data Record
SNMP	Simple Network Management Protocol
sNR	Signal-to-Noise Ratio
SS	Subscriber Station
STOM	Ship-to-Objective Maneuver
SUV	Sport Utility Vehicle
TDD	Time Division Duplexing
TNT	Tactical Network Topology
UAV	Unmanned Air Vehicle
UGS	Unsolicited Grant Services
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WNW	Wideband Networking Waveform

THIS PAGE INTENTIONALLY LEFT BLANK

## **ACKNOWLEDGMENTS**

There are several individuals that we would like to thank for their constant support during our thesis research. First and foremost, we'd like to extend our sincerest gratitude to the Office of the Chief Technology Officer of Washington, D.C for introducing us to this technology via their use of FLASH-OFDM. Specifically, Mr. Robert Vence, the Customer Operations Manager at OCTO and an NPS alum, for eagerly seeking approval for our visit and serving as our host for the entire week of testing. We'd also like to acknowledge George Hall, the Customer Operations Technical Support Engineer at OCTO for all of your help and guidance during our research. We are ever so grateful for the loan of your personal equipment, without which our testing would have been insignificant.

The OCTO office provided us the opportunity to test FLASH-OFDM which lead to our introduction to Dave Dukinfield of Flarion, Technologies. Dave, thank you so very much for your willingness to answer any and all questions we shot your way and for sacrificing your "family" time during the week of our visit. Without you, we may have never survived Georgia Avenue in Washington, D.C. Thanks for being a part of our research team and putting up with the heat and tarantulas of Camp Roberts. The presence of yourself and Fuad Abdeladiz at TNT testing helped us to extend our research beyond what we could have ever envisioned.

THIS PAGE INTENTIONALLY LEFT BLANK

# **I. INTRODUCTION**

## **A. BACKGROUND**

FORCEnet is the next generation of Network Centric Warfare (NCW) focused to provide the framework to integrate sensors, networks, decision aids, weapons, warriors, and supporting systems into a highly adaptive human-centric, comprehensive system that operates from seabed to space and from sea to land. [Ref 4] In addition, FORCEnets' mission is to support well-informed forces in their execution of military operations, using improved situational awareness and understanding of the adversary to dominate the information environment and dissuade, deter or decisively defeat any enemy.[Ref 4] The most powerful element of FORCEnet will be achieved with the real time connection of leading edge elements of the military to command and control by improving capabilities and increasing decentralization, to include initiative, adaptability and increased tempo. FORCEnet is an approach that will utilize network technologies to aid in command and control of future forces. [Ref 4]

FORCEnet must be able to provide a network infrastructure for both tactical evolutions and the more permanent rebuilding phases that are associated with post war activity while still adhering to the requirements of the Joint Tactical Radio System (JTRS) and the Wideband Networking Waveform (WNW). With the influx of commercial-off-the-shelf products into the fleet, it is possible to find a solution which can enhance command and control as well as execution at all echelons of warfighting. These enhancements should be possible through:

- Increased knowledge between decision and actor entities;
- Better connection between decision and actor entities;
- A much smaller footprint amongst all entities. [Ref 1]

Ongoing military operations in Iraq and Afghanistan have highlighted the challenges of supporting our maneuvering forces with network connectivity in support of NCW. The Navy's current networked communications strategy is the Joint Maritime Communications Strategy (JMCMS) which uses the Automated Digital Network System (ADNS) to connect the Integrated Shipboard Network System (ISNS) onboard

Naval vessels with other remotely located DoD networks via current RF communication systems already installed. ADNS is designed to enable end user systems to seamlessly exchange data when employing commercial standard interfaces and protocols (i.e. Internet Protocols). [Ref 2] A candidate Amphibious Readiness Group (ARG) ADNS deployment architecture including JTRS WNW capability is shown in Figure 1.

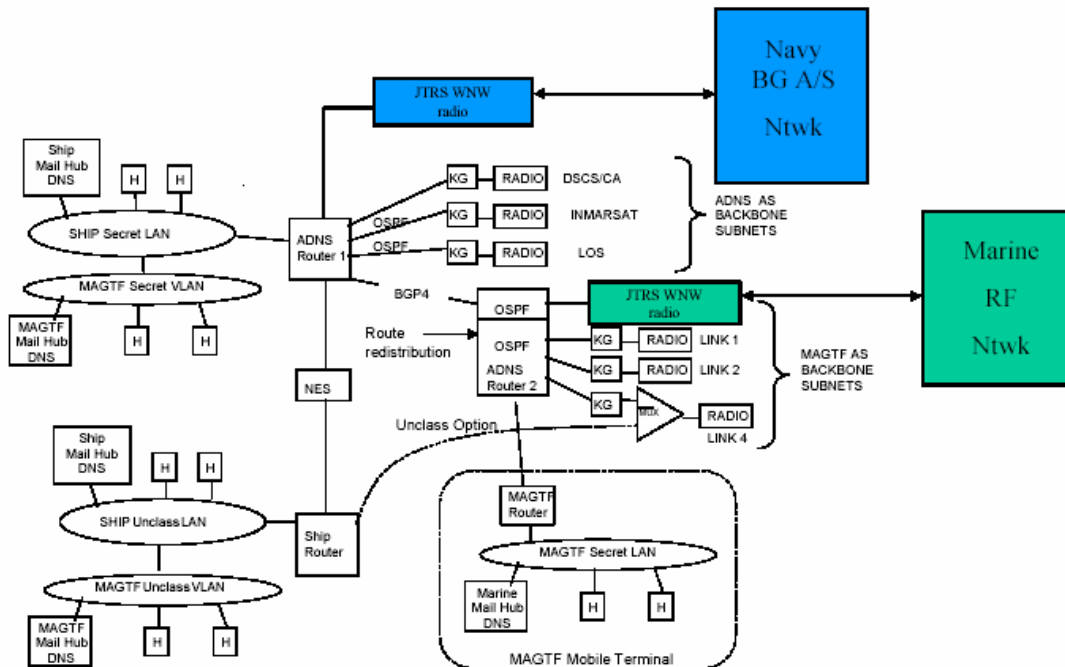


Figure 1. ARG ADNS Architecture with JTRS WNW [Ref 2]

The Navy JTRS WNW radio will eventually be interconnected to the Marine Corps RF Network to enable Ship-to-Objective Maneuver (STOM) in support of Operational Maneuver from the Sea (OMFTS). The objective of OMFTS is to reduce the footprint of military fighting forces needed ashore to obtain dominant maneuver, precision engagement, full-dimensional protection and focused logistics. [Ref 1] The desired end state of the JTRS WNW radio is to have a man-pack form device that can be employed to interconnected squad and reconnaissance size units with interlaced voice, video and data with relay capability. [Ref 2] The below diagram illustrates the Marine Corps vision of the C4ISR structure of OMFTS consisting of a large number of low-



power wireless local area networks (WLANs) interconnected by a self-organizing wide area network (WAN).

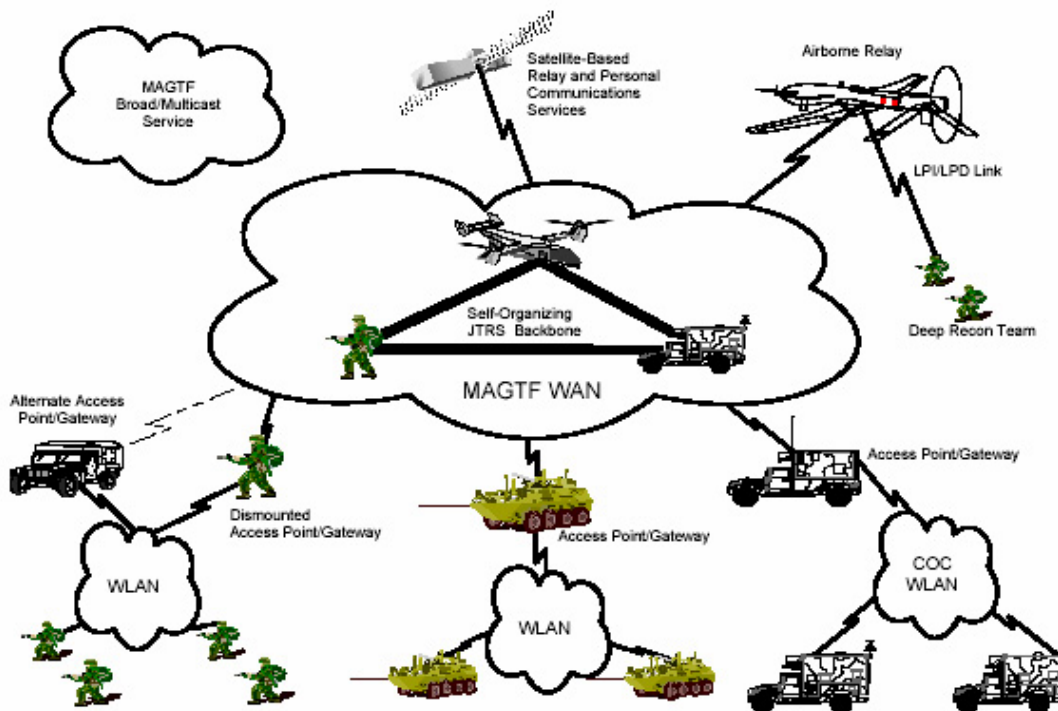


Figure 2. OMFTS Envisioned Architecture [Ref 2]

An emerging wireless technology exists within the private sector and is currently employed for both commercial and government purposes that may meet the requirements of FORCEnet and WNW. The Institute of Electrical and Electronics Engineers (IEEE) 802.20 pre-standard specifies an air interface for mobile broadband wireless access systems. This technology compliments and extends IEEE 802.16 fixed broadband research already completed by NPS as part of the Tactical Network Topology (TNT) test field.

The IEEE 802.20 pre-standard (henceforth just 802.20) utilizes a unique and proprietary adaptation to Orthogonal Frequency Division Multiplexing called Fast Low Latency Seamless Handoff (FLASH) OFDM. FLASH-OFDM uses fast hopping across all frequency tones in a pseudorandom predetermined pattern to create a complete spread

spectrum technology. It is a packet switched technology that is optimized across the physical, MAC, link and network layers to meet the following objectives:

- Spectrally efficient, high capacity physical layer
- Packet-switched air interface
- Contention free, QoS-aware MAC layer
- Support for interactive data application including voice
- Efficient operation using all existing Internet protocols (TCP/IP)
- Full vehicular mobility
- Low cost [Ref 3]

The MAC layer is capable of supporting 31 active users per cell and over 100 registered users per cell in either of the following states: On, Off, Hibernate, Sleep and Hold. The installed network for the Office of the Chief Technology Officer of the District of Columbia is currently utilizing an 802.20 network and has attained a range of up to 10 miles and the ability to transfer data, voice and video at shared data rates up to 3.2 Mbps downloaded and 900 kbps uploaded, each needing only 1.25 MHz of spectrum in the 750 MHz range.

There are numerous military “last mile” applications that can take advantage of this unique technology as a complement to JTRS or WNW as it applies to Network Centric Warfare. This research will explore the ability of 802.20 to provide a last mile solution and identify where current systems fall short in their attempt.

## **B. OBJECTIVES**

This research evaluates 802.20 standards and technologies currently under development to determine its potential near term application as a last mile solution in a tactical military environment.

## **C. RESEARCH QUESTIONS**

1. What is the military requirement for mobile wireless network technologies in a coalition environment?
2. What is FLASH-OFDM technology?
3. What is the optimal configuration of an 802.20 network in the given coalition environment?
4. How can an 802.20 end-user mobile network be implemented into a Limited Objective Experiment associated with an exercise such as TNT?
5. How will the 802.20 base station function when located in a mobile vehicle?
6. What are the costs associated with implementing an 802.20 end-user mobile network into a Limited Objective Experiment associated with an exercise such as TNT?
7. What are the recommendations and lessons learned for implementing an 802.20 end-user mobile network into a Limited Objective Experiment associated with an exercise such as TNT?

## **D. SCOPE**

This thesis will focus on incorporating an 802.20 end-user mobile network into coalition surveillance and targeting system. This network will be evaluated in a standardized manner in accordance with previous Joint Information Operations Center (JIOC/J53) experiments and incorporated into an LOE during an exercise such as Tactical Network Topology (TNT).

The technical side of the thesis will include experiments to compare/contrast implementation of a scalable FLASH-OFDM network, desensitized to allow collaboration with international partners. Field experiments will include collection of test data transfer rates, bandwidth utilization, and latency of multiple mobile systems actively using network resources.

The non-technical aspect of the thesis will be in developing, coordinating, and implementing a plan to integrate an LOE during an exercise such as TNT.

## **E. METHODOLOGY**

As an LOE in a coalition environment and in accordance with previous Naval Research Laboratory (NRL) and JIOC/J53 studies, packets of different sizes and types, accessed by users located in various environmental terrains with varying degrees of mobility will be used in a FLASH-OFDM network to provide a basis for comparison with 802.16, 802.11 and SecNet11 Plus devices utilized in previous NPS experiments.

Data from packet generators, text files, and streaming audio and video testing will be utilized in the testing of data transfer rates, bandwidth utilization, and latency of multiple nodes actively using network resources at varying distances and mobility. From this, the performance limitations of multiple nodes will be identified. Network capabilities will be ascertained through the measurement of received signal to noise (SNR) and observation of uplink/downlink throughputs for the mobile user. Testing will also identify the extent of usable network traffic on the system.

Throughout this research, the focus will revolve around testing equipment and network configurations in an IP network and integrating this into the coalition environment.

## **II. WIRELESS NETWORKING**

### **A. WIRELESS NETWORKING**

Previous experimentation at the Naval Postgraduate School utilizing the TNT test bed has verified the validity of OFDM technology as a viable wireless solution to military networking needs. OFDM is a multi-carrier approach that segments according to frequency and therefore divides spectrum into equally spaced tones. Each tone will contain a user's information and in conjunction with a multiple access scheme will allow many users to share the frequency. [Ref 6] The benefits of OFDM are realized in its ability to overcome the following problems often encountered in a wireless environment.

#### **1. Multipath**

When a user is transmitting to and from a base station his signal can be reflected by several objects including buildings, trees or even terrain. This reflection will create new "reflected" signals that will arrive at the receiver randomly offset in phase, creating signal fades. Each reflection is a copy of the original signal and will arrive at varying times and strength depending on the object from which it was reflected. A signal reflected off of a building or hill will arrive at the receiver stronger and faster than a signal reflected through trees. OFDM and 802.20's FLASH-OFDM use a cyclic prefix, or guard time, of sufficient length to account for the anticipated multipath delay spread experienced by the system. [Ref 7]

#### **2. Time Dispersion**

Time dispersion is a distorted signal that is caused by the time spread of the modulated symbols. This phenomenon leads to Intersymbol Interference (ISI) and is caused when one symbol overlaps with another. ISI is a source of noise which will decrease the Signal to Noise Ratio (SNR) of the communication system. OFDM and FLASH-OFDM overcome this phenomenon by having multiple parallel data streams instead of one high rate data stream. [Ref 7]

### **3. Doppler Spread**

Doppler Spread is the random changes in a channel as a direct result of user mobility. Signal fading degradation occurs as a result of the random frequency modulation of the subcarriers. Signal fading is directly tied to the user's level of mobility. A rapid moving user will see fast fading, where the rate of change of the channel is higher than the modulated symbol rate and a slow moving user will experience slow fading, where the channel changes are slower than the symbol rate. [Ref 5] FLASH-OFDM counters this phenomenon by instituting enough tone spacing to allow Doppler toleration of 200 Hz with negligible loss. By contrast, a velocity of 60 mph will result in Doppler of about 200 Hz at PCS frequencies, while at cellular frequencies the shift will be about 100 Hz. 802.16 does not have this tolerance built into it and thus does not currently work for mobile use. [Ref 9]

### **4. Rayleigh Fading**

Mobile users often have a non line of sight (NLOS) component to their network traffic as a mobile user can be in a building or around other obstructions. This will create Rayleigh fading, which is a probability distribution describing the fading signal amplitude.

## **B. FLASH-OFDM VS. 802.16**

FLASH-OFDM as it applies to the 802.20 standard is a direct competitor to the yet to arrive 802.16e mobile broadband standard. FLASH-OFDM differs from 802.16 OFDM applications, in that it is vertically layered across the network, link and physical layers of the OSI model. Figure 3 illustrates this difference. This implementation is possible because in an IP network, only the layers above the network layer need to be layered horizontally to ensure interoperability across multiple link layer technologies. [Ref 7] The 802.16 standard utilizes multiple MACs for multiple Physical layers and has run into design challenges because of the large amount of internetworking needed between the 802.16 MAC and PHY layers [Ref 8]. 802.20 on the other hand utilizes a non-contention MAC together with OFDM which allows for the support of many low bit rate dedicated control channels.

The use of dedicated signaling enables the system to distinguish the request priority of each active user and schedule the appropriate uplink and downlink resources. The system can rapidly schedule the active users between MAC states. This is critical to efficiently using the scarce wireless resource, particularly for burst data users, and is responsible for the system's ability to provide low latency and QoS to a large number of users. [Ref 7]

FLASH-OFDM incorporates the necessary changes to account for user degree of mobility, required data rates, services to be supported, number of users to be supported, and the environment the system will be used in.

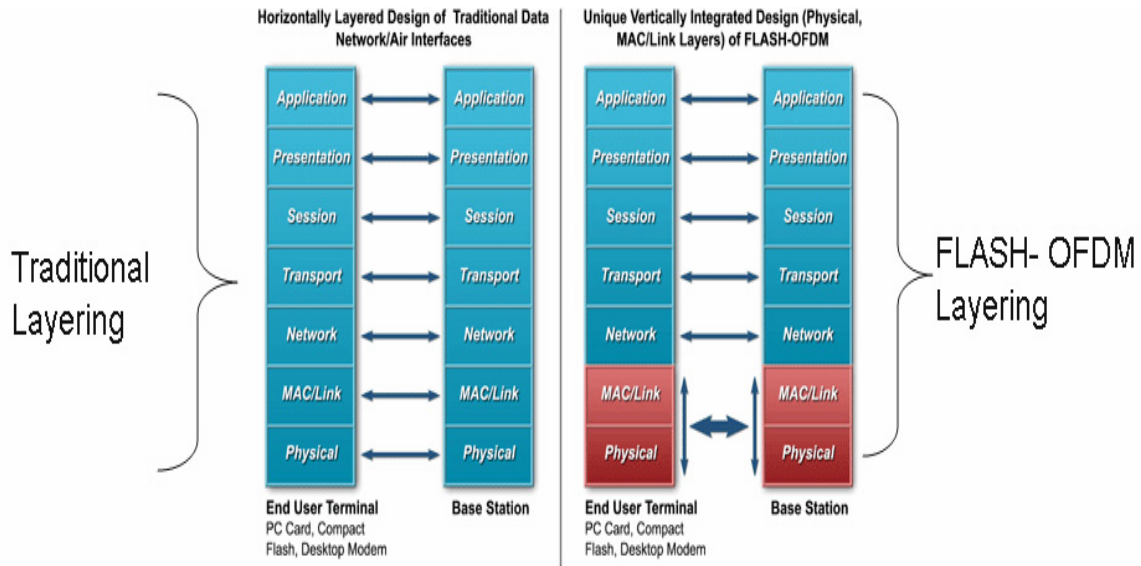


Figure 3. Relationship of FLASH-OFDM to Traditional Layering [Ref 7]

### 1. FLASH-OFDM Physical Layer

FLASH-OFDM operates on paired Frequency Division Duplexing (FDD) and supports a spectrum allocation of 1.25 MHz. Conversely, 802.16 operates primarily in bandwidths of 10 MHz or 20 MHz and optionally at 5 MHz. [Ref 10] The OFDM scheme used in 802.16 operates on Time Division Duplexing. Flarion's FDD network uses separate antennas for receiving and transmitting. TDD is a slightly newer technology which uses only one antenna and uses time to divide between receiving and transmitting. A TDD system can adapt to requirements of the network to allow either more or less time for the uploading or downloading of traffic. The 802.20 network is more permanent in its ability to allocate bandwidth, and counters this limitation via its QoS capabilities to be discussed in a subsequent section of this thesis.

Carrier frequency	Up to 3.5 GHz
Channel Size	1.25 MHz uplink, 1.25 MHz downlink
Number of tones	113
Tone spacing	11.25 kHz
Symbol duration	100 us
Max delay spread	~10 us*
Max Doppler spread	~200 Hz*

*\*Graceful degradation if more delay or Doppler occurs*

Table 1. FLASH OFDM Physical Layer Characteristics [Ref 7]

FLASH-OFDM is a spread spectrum, multiple access technology with frequency tone hopping and like 802.16, employs both Quadrature Phase Shift Keying (QPSK), 16-point Quadrature Amplitude Modulation (16QAM), and 64-point Quadrature Amplitude Modulation (64QAM) to place two, four, or six bits of information on a tone. [Ref 7] Multiple users can be assigned different tones and time and when paired with tone hopping which enables a frequency reuse of 1 ( $N=1$ ) due to the improved frequency diversity and low intercell interference. No intracell interference is created due to tone orthogonality. The FLASH-OFDM tone hopping system was designed with the following characteristics:

- Any two tone hopping sequences in the same cell never collide (no intracell interference),
- The maximum collision between any two-tone hopping sequences in different cells is minimized (averaged intercell interference). [Ref 7]

The tone hopping frequencies actually create the physical uplink and downlink channels that perform interface functionalities such as traffic, pilot, assignments, acknowledgements, paging and power and timing controls. [Ref 7]

#### **a. Downlink**

The FLASH-OFDM downlink utilizes 96 traffic tones and 17 control tones in addition to a 4 tone pilot signal. The pilot signal is used for mobile access/recognition to the base station/s accessible to the user. Each base station has a distinct pilot slope which identifies the random frequency hopping of the pilot signal. A



pilot hopping algorithm is utilized to avoid collisions from base stations in adjacent cells. The pilot slope is also used to determine the data tone frequency hopping sequence. The following Figure illustrates the possible data tone hopping sequence of adjacent base stations.

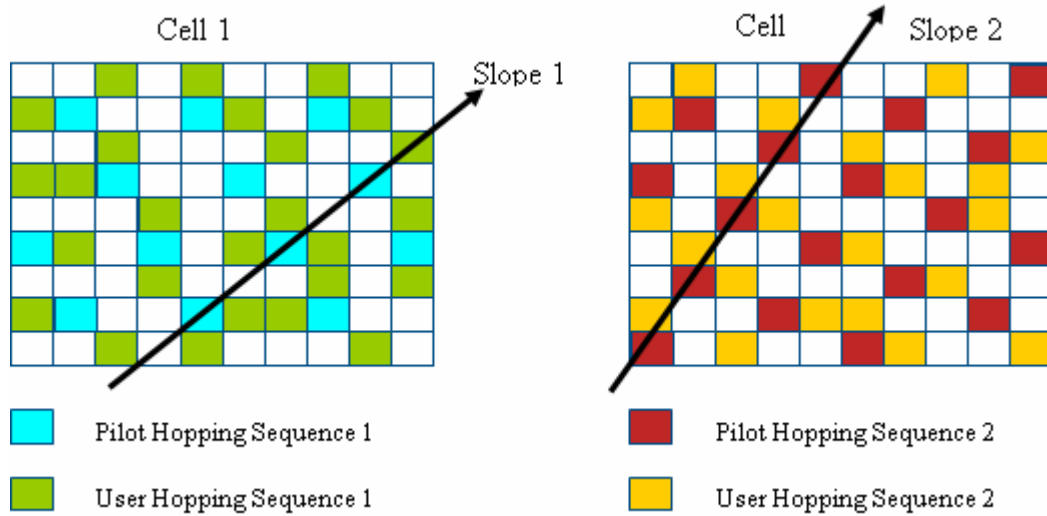


Figure 4. Example of Adjacent Cell Hopping Patterns [Ref 7]

FLASH-OFDM has the capabilities to leverage orthogonality to allow approximately 25dB of power discrimination between tones in order to allocate resources according to power, bandwidth and time. The network thus has the ability to maximize capacity according to channel conditions and users throughput and latency needs. [Ref 7] FLASH-OFDM enables some unique capabilities that may apply to specific military applications. One of those capabilities is described below:

This allows the system to allocate most of the power to a single user who needs it, while allocating more of the bandwidth (tones) to a user that needs relatively little power. For example, the user at the edge of the cell, or in poor channel conditions, can be allocated a disproportionate amount of the overall power over a small number of tones, resulting in a high power density per tone. This translates directly into link budget gains. The base station, which manages the traffic channel resources locally, through its scheduler, is responsible for segment-by-segment allocation of power, bandwidth, and code rate. [Ref 7]

### b. Uplink

The uplink in the FLASH-OFDM system does not utilize a pilot and therefore requires significantly less power than the downlink. Without a pilot, the system resembles a non-coherent detection system. The OFDM application in 802.16 is coherent in nature and will see approximately a 3dB gain in SNR compared to differential techniques but requires channel state information at the receiver and yet still suffers from non-coherent performance loss. [Ref 11] This loss is identified in the 802.16 system by its high transmit peak-to-average power ratio (PAPR). [Ref 12] Flarion has created a technique called turbo equalization to aid in overcoming any performance loss in the uplink that would be associated with non-coherent detection. The loss would generally be about 4dB but with the turbo equalization, FLASH-OFDM realizes a gain that is typically between 2 to 2.5dB without the need for channel state information at the receiver. [Ref 7] The uplink also incorporates 2 path receive diversity which allows for varying degrees of gain depending on channel fading characteristics.

The frequency tone hopping sequence in FLASH-OFDM occurs once every 7 symbols.

The interval where a user's tones remain at the same frequency is called a dwell. Figure 5 shows the dwell based uplink tone hopping. In a dwell, the middle symbol is used to transmit a known symbol, which can be used as a training symbol for channel estimation or as a reference symbol for differential modulation. [Ref 7]

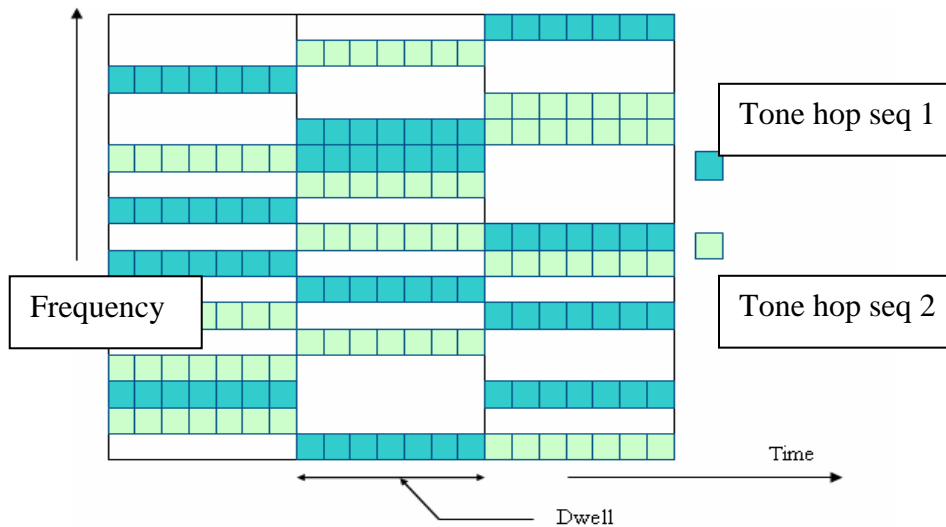


Figure 5. Uplink Dwell by dwell tone hopping sequence [Ref 7]

The scheduler assigned code rate and the number of tones assigned to a mobile user aid in determining the uplink burst rates for a particular user. The base station will recognize and determine the uplink signal quality of the mobile user and will then assign the appropriate code rate. The peak physical layer rates associated with different code selections are shown below. [Ref 7]

Approximate Code Rate	Modulation	Tones			
		7	14	28	77
1/6	QPSK	17	35	69	191
1/3	QPSK	33	67	134	368
1/2	QPSK	50	99	198	545
2/3	QPSK	66	131	263	722
5/6	QPSK	82	164	327	899

Table 2. Uplink Modulation and Coding Class Peak Rates [Ref 7]

## 2. FLASH-OFDM MAC Layer vs. 802.16 MAC Layer

The greatest difference between 802.20 and 802.16 exists in the implementation of their MAC layers and how they Link users to each MAC state. The FLASH-OFDM MAC layer structure includes several MAC states. Each mobile device will have an associated traffic profile and activity associated with it and will therefore have a corresponding assigned MAC state. User traffic will then be labeled and mapped to one of the MAC streams by the link layer. 802.16 MAC layer is capable of supporting Asynchronous Transfer Mode (ATM) while 802.20 currently does not. ATM is a switching technology that utilizes a dedicated connection to organize digital data into 53-byte cell units and transmits them over a physical medium using digital signal technology. What 802.16 currently lacks is Automatic Repeat Request (ARQ) capabilities. [Ref 13] 802.20 Link Layer includes ARQ capabilities used to recover from frame errors and improve link reliability without causing incremental latency. This capability is essential for any system to be able to provide quality of service and superior end user experience to a large group of mobile users. [Ref 7] ATM on the other hand is easily scalable, meaning that the amount of bandwidth can be tailored to the needs of

each user without impacting the performance of other applications and hosts on the network. [Ref 14]

*a. 802.20 MAC States*

A mobile user can be in one of several MAC states in the FLASH-OFDM system. Those states are depicted in the below Figure. A user will be in the Null state

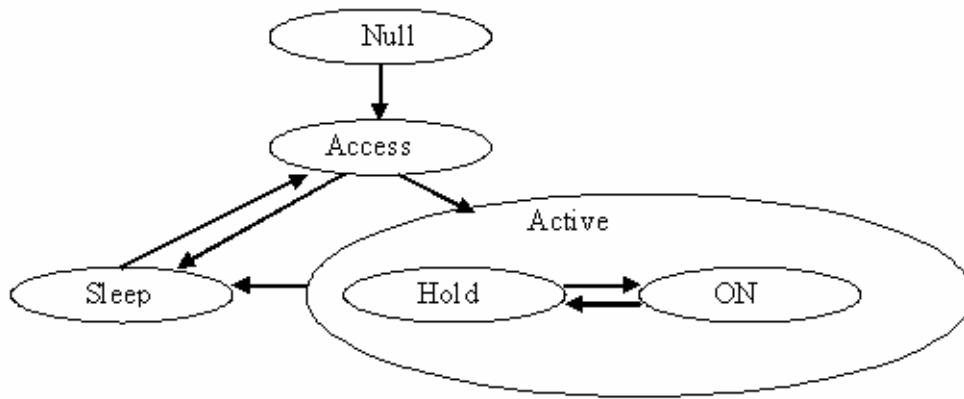


Figure 6. MAC States and State Transitions [Ref 7]

when powered off. The user will attempt to access the network immediately after being powered on and will acquire the system information through the downlink pilot and broadcast control channels of the nearest base station. The mobile will use a random access scheme designed not to interfere with other active mobiles in the sector. Without interference, the accessing mobiles are able to ramp their transmission power in order to be seen and recognized by the base station. Once on the network, the mobile device will either be placed in Sleep or Active mode depending on its requirements for network access. [Ref 7] It is important to note that the mobile user can access any basestation operating on the same frequency.

Network entry on an 802.16 network is established when the Subscriber Station (SS) completes the following processes:

The network entry process is divided into Downlink (DL) channel synchronization, initial ranging, capabilities negotiation, authentication message exchange, registration, and IP connectivity stages. The network entry state machine moves to reset if it fails to succeed from a state. Upon completion of the network entry process, the SS creates one or more service flows to send data to the Basestation (BS). [Ref 15]

When using a licensed frequency in 802.16, a SS is normally configured to use a specific BS. If using an unlicensed frequency, the SS can join any active BS when configured correctly. The following Figure illustrates the complicated process of entry and registration onto an 802.16 network in licensed or unlicensed frequencies.

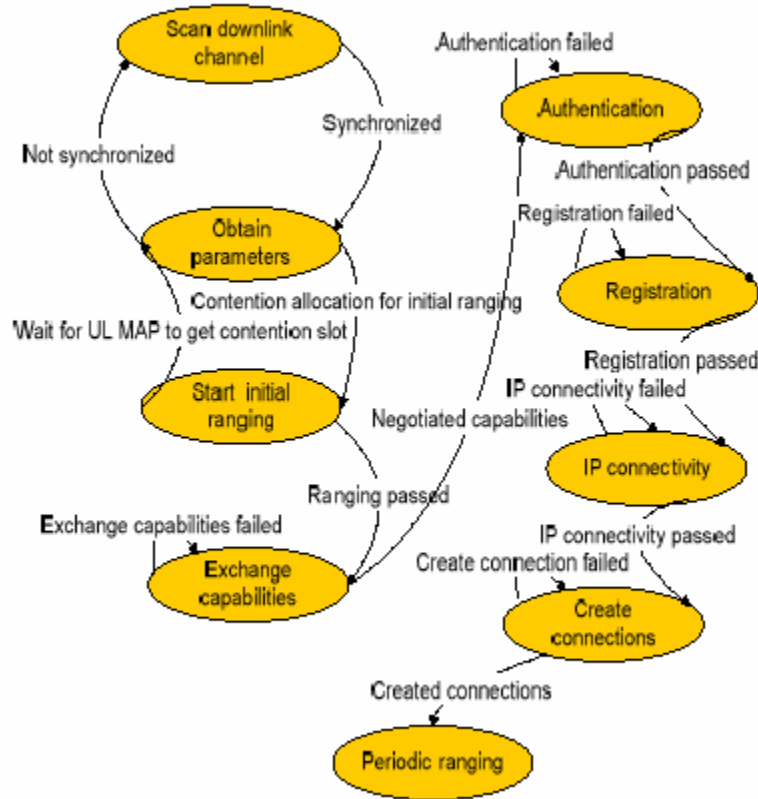


Figure 7. 802.16 Network Entry Process [Ref 15]

The FLASH-OFDM active state has two substates: ON and HOLD. A mobile in the ON state has a dedicated uplink control channel that is power and timing controlled. On this channel, the mobile will also periodically send downlink channel quality information, such as signal-to-noise-ratio (SNR) and carrier to interference (C/I) ratios and a report of its traffic queue status. The BS will use the traffic queue status to determine which mobiles to schedule in the uplink. The BS also controls all downlink control channels for the mobile users and determines the power and transmit rates to be used.

A mobile in the Hold state has a very small dedicated uplink channel that is used to indicate the mobiles intention to either migrate to the ON or SLEEP state. These

dedicated control channels enable state transitions to take place rapidly and contention free and therefore transparent to the upper layers of the OSI model. This is an extremely important aspect of providing a mobile IP solution as TCP/IP is not delay tolerant. All mobiles in a HOLD state share a fast paging channel in which the BS signals to an individual mobile to transition from the HOLD state. The HOLD state enables mobiles to conserve power since they do not need full transmission power for the few airlink resources they are utilizing. [Ref 7]

FLASH-OFDM users can also be placed into a SLEEP State. The SLEEP State mobile uses no airlink resources but will frequently wake to receive paging messages. The SLEEP state mobile is in the greatest state for power saving. In order to use airlink resources, a mobile in sleep state must complete the Access process from the BS.

***b. 802.16 MAC States***

In 802.16, once a user (non-mobile) is authenticated on the system, it will receive a service class assignment. Each service class has an assigned QoS level and is based on the application in use at the time of authentication. Below are the 802.16 service classes:

- i. Unsolicited Grant Services (UGS)- is designed to support Constant Bit Rate (CBR) services such as T1/E1 emulation, and Voice Over IP (VoIP) without silence suppression.
- ii. Real-Time Polling Services (rtPS)- is designed to support real-time services that generate variable size data packets on a periodic basis, such as MPEG video or VoIP with silence suppression.
- iii. Non-Real-Time Polling Services (nrtPS)- is designed to support non real-time services that require variable size data grant burst types on a regular bases.
- iv. Best Effort (BE) Services- is designed to provide best effort services as currently provided by the internet today for web surfing. [Ref 15]

A user will be polled as to its intentions. 802.16 uses two polling methods:

- 1) Unicast- each SS is polled individually and allocated bandwidth accordingly
- 2) Contention based- each SS must contend with other SS's for bandwidth.

This method is used during multicast, or when bandwidth is insufficient to poll multiple users. [Ref 15]

It is important to note that the 802.16 MAC does not yet support full mobility for the users accessing the network. The 802.20 MAC together with Flarion's RadioRouter Base Station enable the network administrator to change mobile user's access privileges in real time. For example, if there were an incident of military interest in an area of Baghdad in which there were several mobile users accessing the network, the network administrator could immediately change privileges and grant access to only those users at the immediate scene, or those who were involved in the operation. User privileges could be changed at the RadioRouter and pushed down to each of the network access cards without requiring the user to return the cards to the NOC. This capability will be explained further in the below section.

### **3. FLASH-OFDM vs. 802.16 Quality of Service**

As per the requirements of the WNW, FLASH-OFDM supports DiffServ RFC 2474 for providing Quality of Service (QoS) to end users.

The differentiated services framework enables quality-of-service provisioning within a network domain by applying rules at the edges to create traffic aggregates and coupling each of these with a specific forwarding path treatment in the domain through use of a codepoint in the IP header. The diffserv workgroup has defined the general architecture for differentiated services and has focused on the forwarding path behavior required in routers, known as "per-hop forwarding behaviors" (or PHBs). [Ref 16]

FLASH-OFDM uses the Diffserv Code Point (DSCP) identifier of each packet to determine its QoS treatment when forwarding through the routers and currently utilizes a User Class Service Group to differentiate. Future implementation in FLASH-OFDM calls for the use of a Class-Based Model.

#### ***a. 802.20 User Group Service Model QoS***

FLASH-OFDM can incorporate up to eight different User Groups with predefined QoS attributes assigned to them on the RadioRouter BS. As a mobile user is

authenticated onto the network via the Authentication, Authorizing and Accounting (AAA) server, a user profile with the designated User Group is downloaded to the BS for traffic assignment. Each User Group has the following pre-assigned attributes:

- Rate caps: A set of parameters that dictate maximum downlink and uplink data rates for traffic to and from a user associated with the User Group.
- Link-sharing weights: A set of parameters that dictate the scheduling of air-link resources during periods of congestion (i.e., when queue backlogs exists).
- Classifier rules: An ordered list of packet filtering rules applied on the FLASH-OFDM interface for both egress (downlink) and ingress (uplink) traffic to/from users associated with the User Group. [Ref 7]

Future implementation of QoS will involve a Class-Based Model where service classes based on the traffic will be utilized to differentiate between traffic priorities. The Class-Based Model is representative of the current QoS system utilized in the 802.16 architecture and differentiates based on Traffic Profile, Delivery Objective and Handling Specification.

- Traffic Profile: Defines the expected temporal characteristics of corresponding traffic flows, typically in statistical terms such as: average rate and burst size.
- Delivery Objective: Defines the target end-to-end service metrics for corresponding traffic flows that remain ‘in profile’, e.g., mean delay, 99th percentile delay or minimum rate.
- Handling Specification: Defines the required treatment of corresponding traffic flows, e.g., metering, marking, policing, shaping, or queuing and scheduling. [Ref 7]

In a military operation, the User Group Model should prove more useful in assuring that the right people have the capability to send and receive data no matter which application or device is used for that transmission. The NOC should be able to easily assign users to a predefined group with a predetermined level of accessibility prior to an operation, in addition to being able to operate “on the fly” as the situation and needs change due to the fog of war.

#### ***b. 802.16 QoS***

802.16 assigns a QoS based on the aforementioned Service classes (UGS, rtPS, nrtPS, and BE) together with either a unicast or contention-based polling method. These levels are determined at the establishment of the data flow connection. Below are the QoS parameters as identified in the 802.16 standard:



- QoS parameter set type - specifies the proper application of the QoS parameter set to either a provisioned, admitted or active set.
- Traffic priority - used to assign a priority to a service flow's traffic.
- Maximum sustained traffic rate - expressed in bits per second.
- Maximum traffic burst - calculated from the byte following the MAC header to the end of the MAC PDU.
- Minimum reserved traffic rate - specifies the minimum rate reserved for a service flow.
- Vendor specific QoS parameters - can be used by vendors to encode their own QoS parameters.
- Service flow scheduling type - specifies the uplink scheduling service being used for the service flow.
- Request / transmission policy - used to specify various scheduling service rules and restrictive policies on uplink requests and transmissions.
- Tolerated jitter - specifies the maximum delay variation (jitter) for a connection.
- Maximum latency - specifies maximum latency between receipt of packet on the network interface and forwarding to the RF interface.
- Fixed length versus variable length SDU indicator - indicates whether data packets must be fixed length or may be variable length. [Ref 17]

802.16 QoS is provided primarily through a contention-based access scheme and are therefore subject to various performance variations and inefficiencies when dealing with mobile users. FLASH-OFDM does away with the contention-based scheme by providing a fully scheduled uplink and downlink air resource to the user. [Ref 7]

#### **4. FLASH-OFDM vs. 802.16 Security**

FLASH-OFDM and 802.16 both provide sufficient levels of security in their systems. It is important to understand that 802.16 security is performed between a BS and Subscriber Station (SS), not involving an individual user. A viable 802.16 PC card for an individual mobile user does not yet exist and a rudimentary man-packable device has been created by Redline Communications to best simulate a “mobile” SS. The current 802.16 security architecture is implemented across two AN-50 stations with one acting as the BS and the other as the SS.



Figure 8. Redline Communications Man-Packable AN-50 (compare to Figure 15. below)

**AN-50**

General Information  
System Status  
System Logs

► Configure System  
Upload Software  
Product Options  
System Password

Ethernet Configuration	
System Name:	NPS NOC_Root Hall
System Details:	PTP_NPS Roo/Spa
IP Address:	192.168.100.10
IP Subnet Mask:	255.255.0.0
Default Gateway Address:	192.168.1.1
Flow Control Enable:	<input type="checkbox"/>
Ethernet Mode:	Auto
HTTP Enable:	<input checked="" type="checkbox"/>
Telnet Enable:	<input checked="" type="checkbox"/>
Telnet Port:	23
SNMP Enable:	<input checked="" type="checkbox"/> [Configure SNMP]

Wireless Configuration	
RF Freq. [MHz]:	5815 <span style="float: right;">Auto scan: <input type="checkbox"/></span>
DFS Action:	None
DFS Antena Gain:	90
Tx Power[dBm]:	20
ATPC Enable:	<input type="checkbox"/>
Adaptive Modulation:	<input checked="" type="checkbox"/>
Modulation Reduction Level:	0
Uncoded Burst Rate [Mb/s]:	54 Mb/s
Master Mode:	<input checked="" type="checkbox"/>
Software Version:	1.32.013
Encryption Enable:	<input checked="" type="checkbox"/>
Encryption Key:	000902003EE9
Link Length Mode:	Auto
Link Measurements Units:	Km
Link Length:	0
General Antenna Alignment:	<input checked="" type="checkbox"/>
Radio Enable:	<input checked="" type="checkbox"/>

Ability to place the AN-50 unit in Master Mode to become BS vice SS.

→

Figure 9. Redline AN-50 Configuration

**a. 802.16 Security**

802.16 has a privacy sublayer that provides security by encrypting the link and service flows between the BS and SS. The security sublayer employs an

authenticated client/server key management protocol. The BS will control key distribution via two component protocols. The first protocol is encapsulation and the second protocol is the Privacy Key Management Protocol (PKM) using the RSA public key algorithm. [Ref 17] In the 802.16 protocol, all MAC management messages and encrypted data packet headers are sent in the clear. These clear messages contain information specific to the encryption such as encryption control field, key sequence field and corresponding CID. [Ref 17]

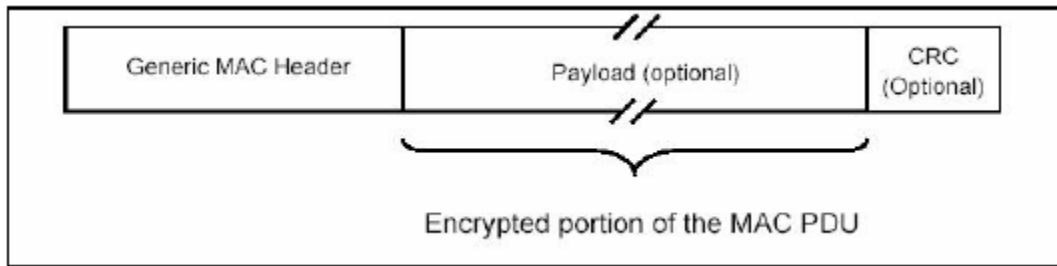


Figure 10. 802.16 MAC Data Unit [Ref 17]

Upon network entry, a SS will establish a Security Association with the appropriate BS. A SS can only associate with one BS at a time and must break its connection before being able to connect to another BS.

#### ***b. FLASH-OFDM Security***

Flarion has developed a wireless technology that provides end-to-end security. End-to-end security consists of protecting the communication path between the applications or network stacks at the two communicating end nodes. [Ref 21] The main element of network security is achieved through the Authentication architecture to access the network. Future planned capability calls for adding an air link encryption capability based on the Rijndael block cipher, a basis of AES encryption. [Ref 7] Additionally, network layer protocols can be added to the air interface when necessary. Network layer protocols include Internet Protocol Security (IPSEC) and Virtual Private Networks (VPN). [Ref 21]

### **III. NETWORK CONFIGURATION**

#### **A. PHYSICAL ARCHITECTURE OVERVIEW**

The IEEE 802.20 system is IP based and designed to be deployed over multiple technologies to ease transition into existing network architecture. The equipment necessary in implementing the FLASH-OFDM system makes this seamless deployment possible. The system architecture is designed to provide the following benefits:

- Ease of manageability due to the use of a single, highly redundant, cost effective IP environment
- Future proofing due to immediate deployment of an IP backbone for the transport of converged voice and data applications, without the need to do costly intrusive upgrades at some later point
- Maximal scalability and efficiency of transport methods
- Standards compatibility using IP technology for the transport and distribution of information throughout the network. [Ref 7]

The required equipment to deploy a FLASH-OFDM system is as follows and will be explained in depth below:

##### Flarion Equipment

- RadioRouter base station
- Terminal equipment
- EMS server
- Mobile Network Server
- AAA server [Ref 7]

##### Necessary Third Party Elements

- Access concentrator
- Aggregation router
- Switching infrastructure
- Home Agent
- Core router
- DNS server [Ref 7]

## **B. RADIOROUTER BASE STATION**

The RadioRouter BS is both a wireless base station and an IP access router providing all network connectivity for mobile users. In a mobile IP infrastructure, the BS manages all IP links between the mobile user and the infrastructure that the Router is tied into. The RadioRouter also manages all air link processing of the Physical, MAC and Network layers, and provides all scheduling and QoS management based on the user's downloaded profiles and user service groups. From an accounting standpoint, the Router is also capable of tracking and reporting user traffic statistics. To ease transition into existing networks, the BS can be tied into network backbones using T1/E1 or Ethernet. During TNT testing, the 802.20 and 802.16 networks were successfully connected by simply utilizing a switch.

The RadioRouter (RR) is currently available in both an indoor and outdoor configuration for deployment in either a three sector or omni arrangement using COTS antenna systems. The RR is made up of four subsystems:

- RadioRouter chassis where the core FLASH-OFDM waveform processing, routing, and control occur
- Power Amplifier shelf
- Filter shelf, which includes the Low Noise Amplifier (LNA) duplexer
- Power subsystem [Ref 7]

The indoor RR measures 71"H X 24" W X 26.5"D and weighs just under 650 pounds. The outdoor RR measures 62.5"H X 49.2"W X 42.6"D and weighs 1150 pounds and includes the weight of a 2 hour backup battery. [Ref 18] The power requirements for the RR are as follows:

- +24VDC, -48VDC, 110/220AC, 50-60Hz, Max power consumption- 1800W Outdoor/ 1400W Indoor [Ref 18]

The RR, both indoor and outdoor, can be stored in temperatures ranging from-40°F to 158°F. During operation, the outdoor RR is more weather tolerant and can operate in a range from -40°F to 114°F compared to the -40°F to 104°F max operating temperatures of the indoor RR. [Ref 18]

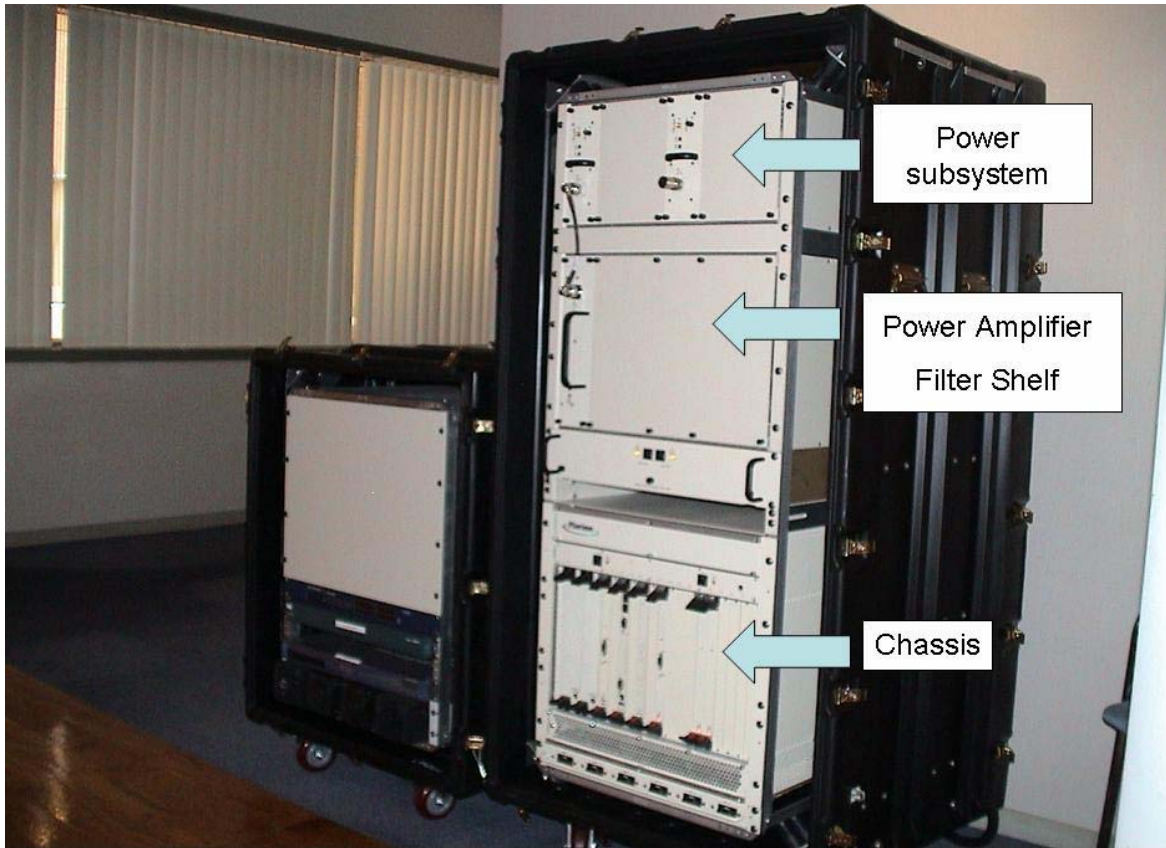


Figure 11. Indoor RadioRouter Base Station



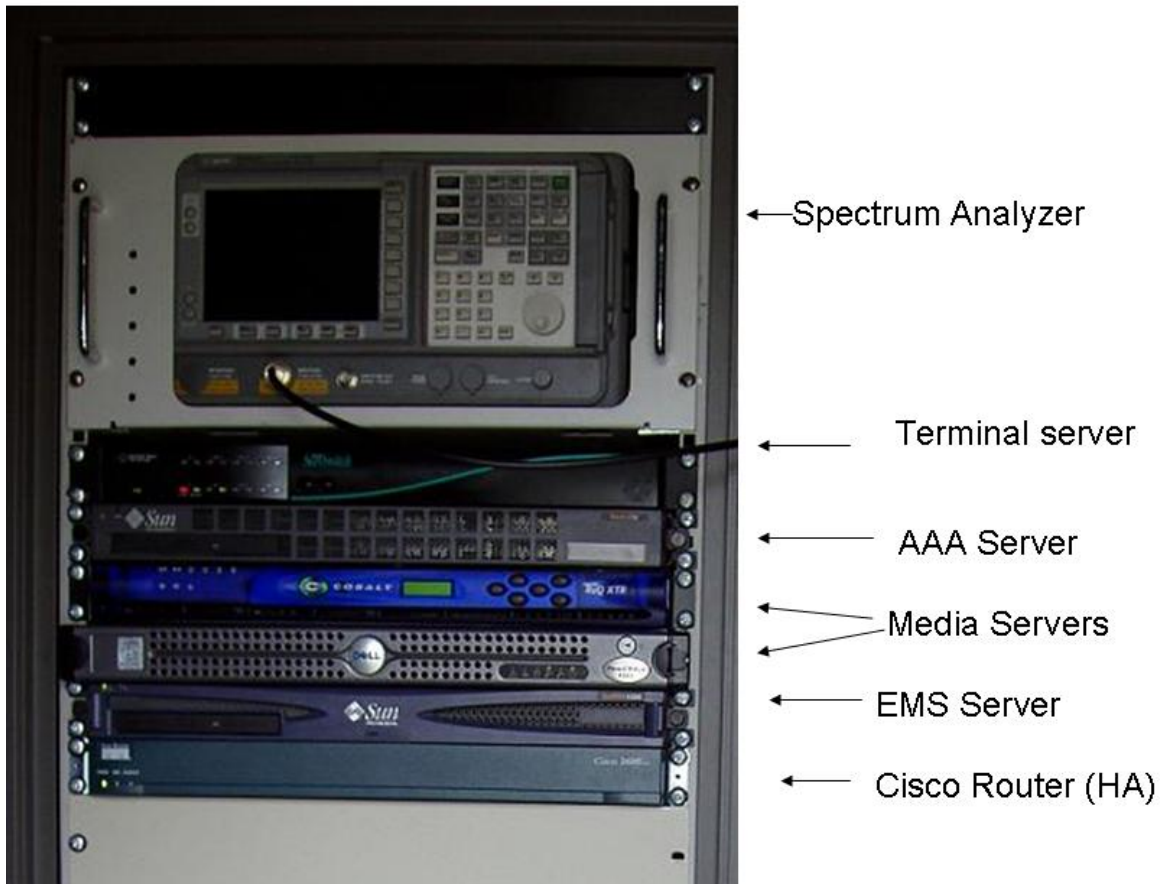


Figure 12. RadioRouter Supporting Equipment

### C. FLASHVIEW EMS SERVER

The Flashview Element Management System Server (EMS) is a radio access network management system that provides event handling, network discovery and provisioning capabilities as well as network monitoring, troubleshooting, BS remote control, Fault monitoring configuration, accounting, performance and security (FCAPS), and network capacity planning. [Ref 20] The Remote Monitoring feature of Flashview enables off site RR maintenance. It is based off of the HP-Open View platform and performs the following tasks while supporting a large number of client devices:

It performs the transaction processing required to effectively provision network elements and easily integrate with existing database servers and OSS applications. [Ref 7]



The EMS server and the RR communicate and exchange user information via SNMP.

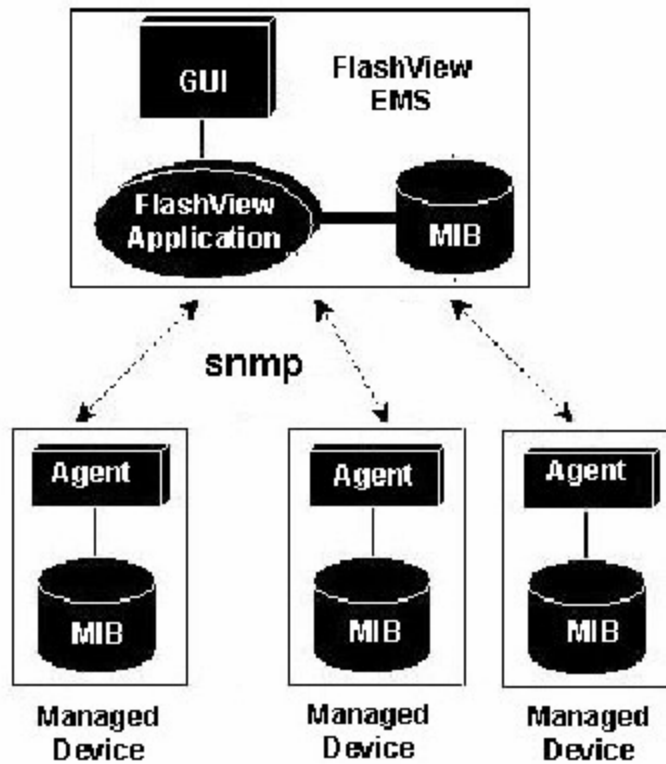


Figure 13. SNMP Model

The server itself has four main parts:

- Solaris™ 9.0 Operating Environment
- Oracle 9i™ Relational Database Management System (RDBMS)
- HP OpenView™ Network Node Manager (version 7.01 or later)
- FlashView RadioRouter Manager [Ref 20]

Flashview provides the network administrator with direct access to the FLASH-OFDM MIB and can be accessed via either a Command Line Interface (CLI) or Graphical User Interface (GUI). The Flashview program itself is very similar to the Solarwinds program currently in use at NPS in both appearance and performance with additional incorporated management robustness.

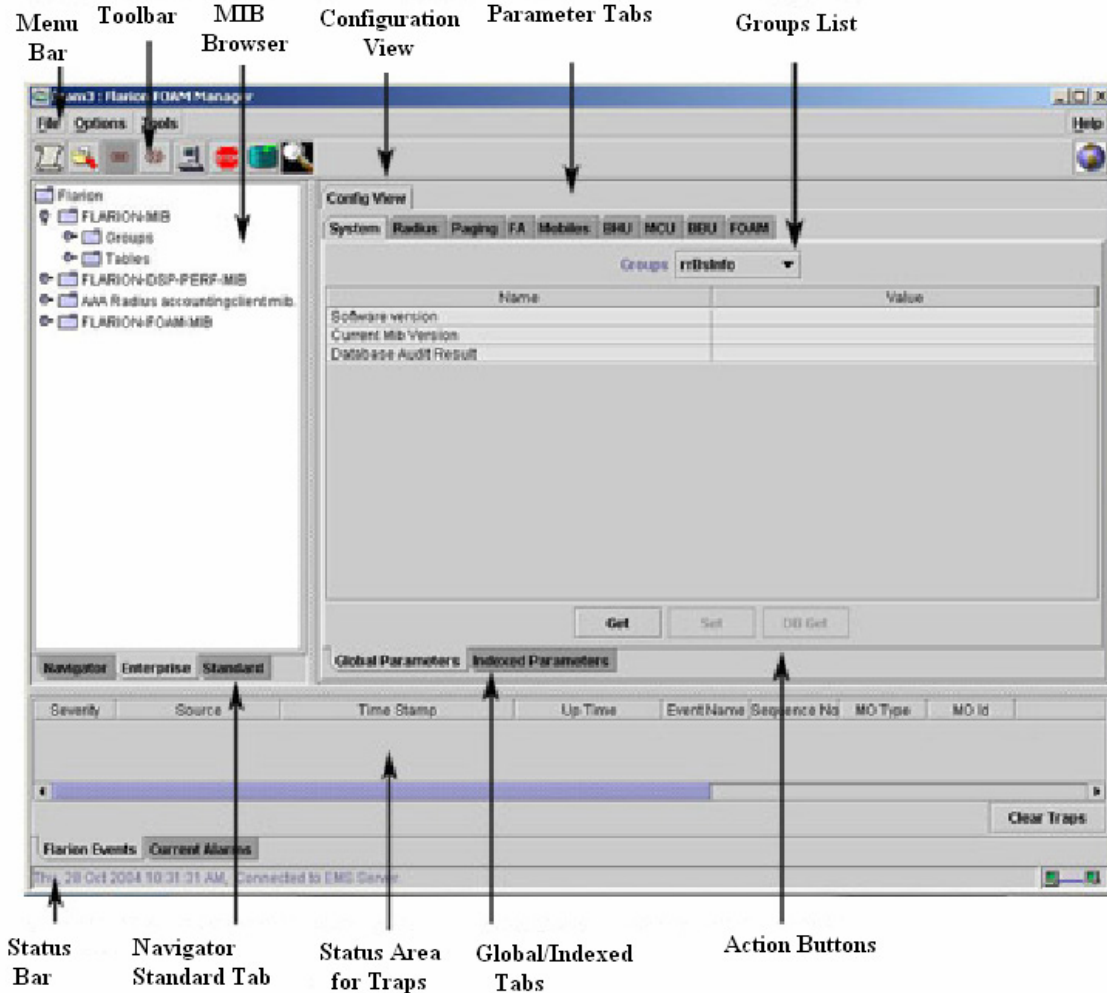


Figure 14. Flashview Configuration View [Ref 20]

## 1. Flashview Server Installation

Installing FlashView server requires completing five main tasks and it is highly recommended that the installer/user have experience in both Sun Solaris systems and HP OpenView:

- Setting up the Sun hardware, and making sure that it meets minimum requirements
- Installation of the Solaris operating system
- Installation of HP OpenView Network Node Manager
- Installation of the Oracle database
- Installation of FlashView RadioRouter Manager [Ref 20]

**a. *FlashView Server Minimum Software/Hardware Requirements***

Minimum software requirements for installation are:

- Sun Solaris operating system, version 9.0
- HP OpenView Network Node Manager, version 6.4 or later (250 nodes)
- Oracle 9i Standard RDBMS [Ref 20]

Minimum hardware requirements for installation are:

- Sun hardware (for example, SunBlade, SunFire, Ultra Sparc)
- Memory (RAM) 1024 MB
- Hard disk 40 GB
- Internal CD drive
- Sun monitor, or a remote terminal [Ref 20]

**D. MOBILE NETWORK SERVER**

The Mobile Network Server (MNS) assists the RadioRouter base stations with maintaining mobile connectivity, and performs context transfer. Context Transfer (CT) is the process that involves maintaining an accurate picture of a mobile's state within the MNS and is a key piece of the architecture which enables mobility in the 802.20 network in addition to aiding in the process of seamless handoffs between base stations. [Ref 7] The MNS operates as a CT server using a pre-standard Context Transfer Protocol (CTP) currently being reviewed by the IETF Working Group.

As a user moves through the footprint of an area BS, a new dynamic mobile state profile is repeatedly created in the BS. As this state changes, an updated version is pushed to the CT server utilizing the CTP. The CTP operates at handoff speed in and between all RadioRouter BS's. As a mobile user approaches the furthest region of its current BS and the leading edge of the nearest BS, a subset of its state profile is re-established at the new BS. This procedure is done in a Make-Before-Break process meaning that successful registration and access is granted to the new BS before the connection with the current BS is broken. The CTP protocol eliminates the need for the transfer of a Master Session Key state on a new link which most IP protocols currently maintain in static IP environments. [Ref 7]

## **E. AAA SERVER**

FLASH-OFDM uses Remote Authentication Dial-In Service (RADIUS) as the Authentication, Authorization and Accounting (AAA) protocol on the AAA server. RADIUS (RFC 2138, RFC 2139, and RFC 1321) are used for the main AAA functions. RADIUS is defined as:

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. [Ref 19]

The AAA server allows the operator to control which statistics are collected and how often collection occurs. The accounting function of the AAA server generates per mobile-terminal Session Data Records (SDRs) that form the basis of usage-based-charging mechanisms. [Ref 7]

Some Flarion specific RADIUS extensions are also used by the AAA server, they are:

- RFC 2865 RADIUS
- RFC 2866 RADIUS Accounting
- RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC 2868 RADIUS Attributes for Tunnel Protocol Support
- RFC 2869 RADIUS Extensions
- RFC 2619 RADIUS Authentication Server MIB
- RFC 2621 RADIUS Accounting Server MIB
- RFC 2251 LDAP v3
- Flarion Vendor-Specific Extensions [Ref 7]

A typical reliable configuration of AAA servers is characterized as follows:

- Two or more RADIUS servers installed depending on the number of base stations deployed
- Load balancing between the servers such that a primary and secondary server is available to each base station
- Fail over to an available RADIUS server in the event of a failure [Ref 7]

The AAA server is able to log accounting information to a log file or SQL server and process more than 400 RADIUS transactions per second per 400 MHz processor. [Ref 7] All accounting information is then logged to the master AAA server for the region of deployment.

## **F. TERMINAL EQUIPMENT**

Flarion has designed a FLASH-OFDM modem engine that resembles an Ethernet NIC card that performs all digital baseband and RF processing. It is available for all frequencies that Flarion supports, but will only work for the assigned BS frequency. [Ref 7] For example, the BS's in use for the Office of the Chief Technology Officer (OCTO) in Washington, D.C. are 700 MHz. Each OCTO card will only work in the 700 MHz range and would not operate in Raleigh, North Carolina where there is currently a 2.4 GHz FLASH-OFDM network in use. The modem engine will work in any IP enabled device such as laptops, tablets, or PDA's.

### **1. PC Card**

The FLASH-OFDM PC Card is a Type II PCMCIA card that is currently compatible with Microsoft Windows Operating Systems, including CE editions and will operate with any Pentium-class processor. The host device does not need to be mobility-aware as the connection will appear as a fixed Local Area Connection. A laptop device will require the following resources:

- Card Slots: 1 Type II PCMCIA Card Slot
- Memory: 32 MB
- Hard Disk Space: 5 MB
- Disk Drive: CD-ROM
- I/O Resources: 1 IRQ, 256 bytes I/O space
- Operating Systems: Microsoft Windows 2000, XP
- Typical peak current draw through PCMCIA slot: 850 mA @ 5VDC
- Typical current draw depends on usage [Ref 7]

The PC Card can also be placed into a PDA given that the PDA is capable of supplying 1 watt of power to the card via its PCMCIA slot. Field tested PDA's were able to supply this power level for approximately 30 minutes without a battery pack, and for an hour and a half with a battery pack.



Figure 15. FLASH-OFDM Wireless PC Card

## 2. Desktop Modem

The FLASH-OFDM Desktop Modem provides connectivity to users who may intend to be stationary within the footprint of a BS. It is primarily designed for residential or small office users. The modem operates as an Ethernet modem having both a RJ 45 port and a USB port and acts as a DHCP server to the connected device. Although it was designed for an office user, the device can easily be deployed in an outdoor setting as it is easily powered by a properly configured battery pack. Development of the Desktop Modems has been passed on to industry partners to create a modem that is capable of combining 802.11 a/b/g and FLASH-OFDM in one device. Inmotion Inc makes a ruggedized desktop modem while Netgear Inc has an indoor unit available.



Figure 16. Netgear Indoor Desktop Modem/Bridge (802.20/802.11)



Figure 17. Inmotion Desktop Modem/Bridge (802.20/802.11/Ethernet/etc)

## G. THIRD PARTY ELEMENTS

To complete the network, several third party elements are needed in order to provide the remainder of the functions that make the FLASH-OFDM scalable and highly adaptable to any pre-existing network.

### 1. Access Concentrator

The access concentrator is the device that enables the RadioRouter BS to be connected to the backhaul technology. Current BS's are equipped with T1 and E1



interfaces. Future implementations of the BS will support Gigabit Ethernet, Sonet, ATM and DSL among others. [Ref 7]

## **2. Aggregation Router**

The aggregation router is the point at which the BS's internal backhaul is terminated at the IP layer and supports standard routing protocols such as OSPF.

Given a T1-type backhaul, it terminates a large number of PPP connections on accordance with the number of associated base stations.  
[Ref 7]

## **3. Switching Infrastructure**

Due to the demands of the network, an IP QoS-aware, Gigabit Ethernet switched network is highly recommended and should have the following options:

- Redundant supervisor engines
- Redundant, load-sharing power supplies (AC and DC)
- Redundant sharing fans
- Redundant system clocks
- Redundant uplinks
- Redundant switch fabrics [Ref 7]

## **4. Home Agent**

The Home Agents (HA) in the FLASH-OFDM system share the load of registrations and traffic forwarding. They are directly connected to the switching infrastructure over high-speed links and must be extensible and redundant. A recommended configuration for deployment is via Cisco's Hot Standby Router Protocol (HSRP) method. [Ref 7] In this setup, the active HA sends binding updates to the backup HA every time a new registration is entered into the binding table for synchronization. At a minimum, the HAs should also support the following features:

- Mobile IP Home Agent specification, RFC 3344
- Static private or public IP addresses and address assignment
- Dynamic private or public IP addresses and address assignment
- MN-HA Authentication
- IP-in-IP encapsulation, RFC 2003
- NAI Extension [Ref 7]



## **5. Core Router**

The purpose of the Core Router is to interconnect the zone with the core infrastructure of the operator and should support all standard routing protocols. [Ref 7]

THIS PAGE INTENTIONALLY LEFT BLANK

## **IV. IMPLEMENTATION AND TESTING**

### **A. INTRODUCTION**

The purpose of this chapter is to detail the results of our field testing for TNT. The experiments spanned three weeks of testing. The first week of experimentation began in Washington D.C. and utilized the 802.20 network established for the Office of The Chief Technology Officer (OCTO). The second week of testing was conducted at the Military Operations in an Urban Terrain (MOUT) facility located at Fort Ord and utilized Flarion's COLT vehicle for network connectivity. The third and final week of testing was conducted at Camp Roberts and again utilized the COLT for connectivity.

### **B. WASHINGTON, D.C. TESTING**

The city government of the District of Columbia, Office of the Chief Technology Officer (OCTO) is located at Judiciary Square in downtown Washington, DC. OCTO has successfully implemented a Wireless Accelerated Responder Network (WARN), a Flarion prototype 802.20 network used for public safety. A VLAN was created for testing on the wireless network utilizing a single broadcast domain on one subnet. The first part of testing was conducted for 802.20 familiarization of the equipment and software being utilized for logging and testing in the DC area. Events conducted and details of all experiment parameters have been provided in appendix A. The following section will expound on the details of the OCTO network, data observed, value of experiment and applicability to military use.

#### **1. OCTO UL/DL Performance**

At the time of experimentation, the OCTO network utilized 10 base stations to cover the portion of the District of Columbia in the licensed spectrum of 700 MHz. The below figures are area maps of OCTO's uplink (UL) and downlink (DL) coverage, generated from site drive surveys. This data is not all inclusive as not all of the coverage area had been mapped as of our visit. Plans to add two additional base stations were progressing. Appendix G provides a complete description of all parameters of the OCTO towers.

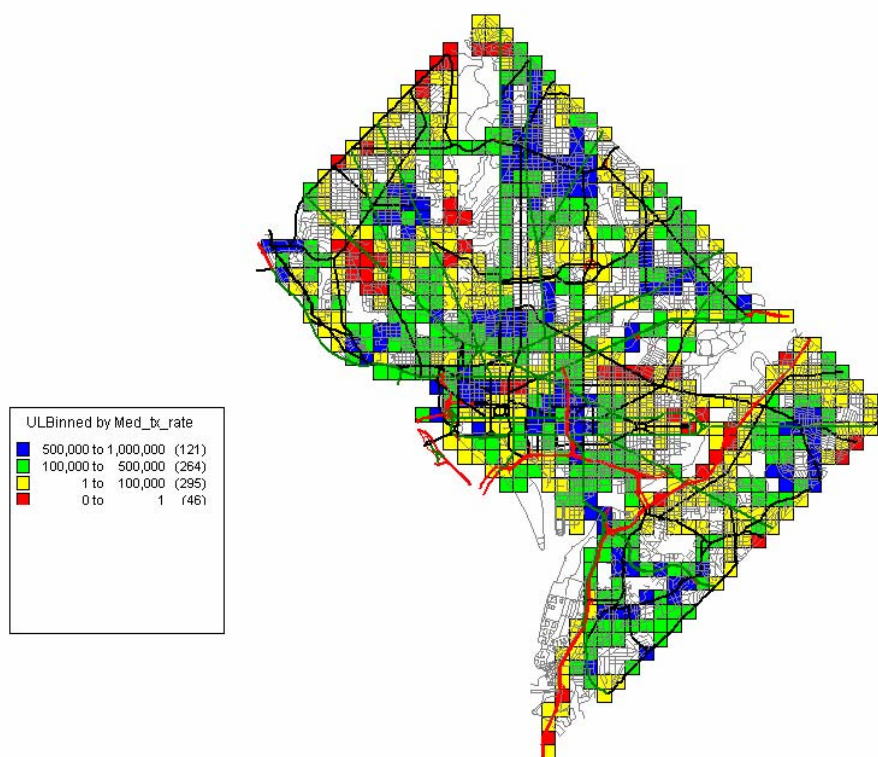


Figure 18. WARN UL Performance [Ref 25]

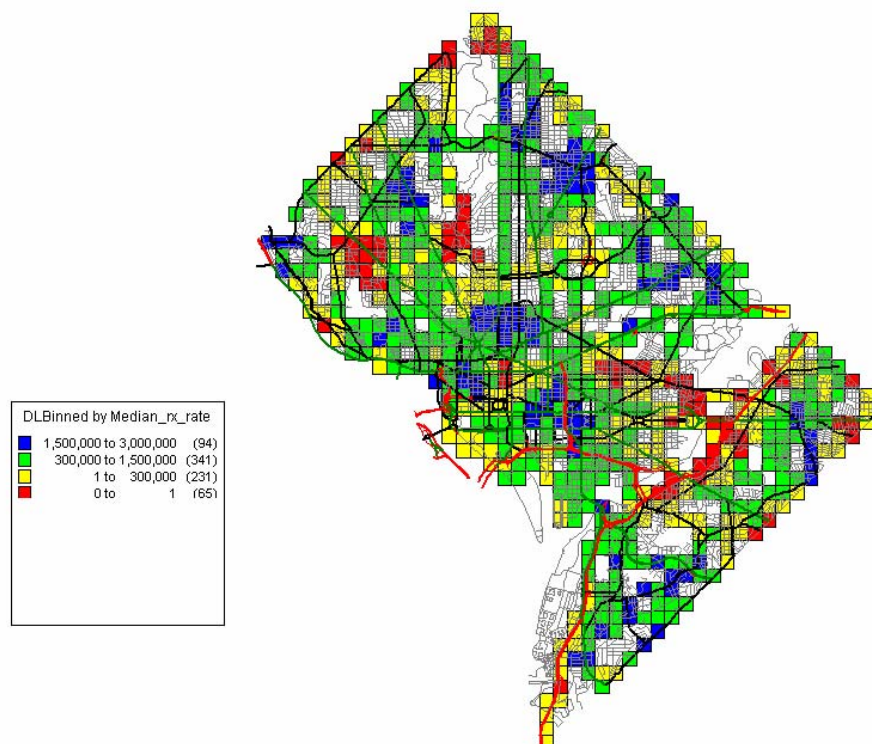


Figure 19. WARN DL Performance [Ref 25]

## 2. Setup and Power Consumption

802.20 NIC cards (Fig 14) were installed into the laptops (Panasonic Tough Book TF-73) and the PDAs (Hewlett Packard iPAQ 4700). The PDAs required Microsoft Windows Mobile 2003 Second Edition NIC drivers and were equipped with a HP Photosmart mobile SD camera. Battery expansion jackets with a PCMCIA interface were required for the PDAs, as the NIC cards were PCMCIA and the HP iPAQ HX4700 had only external SD and CF connections. An attempt to use a CF to PCMCIA adapter failed; the power requirement of 1 watt for the NIC was not met by the CF slot. The NIC has two receivers and two transmitters which are required to perform the “make before break” connection when switching from one mobile sector to the next. Figure 20 provides a photo of PDA after a complete install.



Figure 20. HP iPAQ HX4700 with 802.20 NIC installed in expansion pack running FMM

The installation required 5-10 minutes per device to include installation of Flarion Mobility Manager (FMM), Flarion Mobility Diagnostic Monitor program (FMDM) and Windows drivers. The FMM program configures and monitors the network connection and provides a GUI interface to depict status of network. FMDM is licensed software

developed by Flarion and used to capture data pertaining to a nodes network status. A Garmin GPS V was connected to each TF-73 to provide GPS data to FMDM (WinCE version of FMDM was not available).

Power consumption comparisons between 802.11 and 802.20 were conducted. The HP4700's used a rechargeable 1800 mAh Lithium-ion internal battery and the expansion jacket with 1840 mAh Lithium-ion internal rechargeable battery. The HP4700 has integrated WLAN 802.11b, Bluetooth®, Fast Infrared, IrDA, USB & Serial. With the expansion pack fully charged and attached, the HP4700 operated for 2 hours 20 minutes while constantly using the 802.11 connection. While attached to the 802.20 networked, the battery life was noticeably shorter; it yielded only 1 hour 10 minutes of operation. Similar testing was performed on the Panasonic Tough Book TF-73 laptops which also had an integrated WLAN 802.11b. On average, the 802.20 power requirements drained the battery 15% faster, approximately 20 minutes faster. The 1 watt power requirement for the two receivers and two transceivers on each NIC card is the likely reason for the rapid battery power depletion while on the 802.20 network.

### **3. 21 Mar Highlights**

All events for the day were conducted successfully. The Situational Awareness (SA) server was setup in a conference room on the 8<sup>th</sup> floor of the OCTO building. SA is a Flash based software and has a server application supporting multiple clients. SA was developed by NPS Research Assistant, Eugene Bourakav, to facilitate Tactical Network Topology user communications and situational awareness. The Server was connected to the network via an 802.20 NIC. Fig 21 is a screen capture from the server with a raster map of DC for graphical depiction of mobile user.

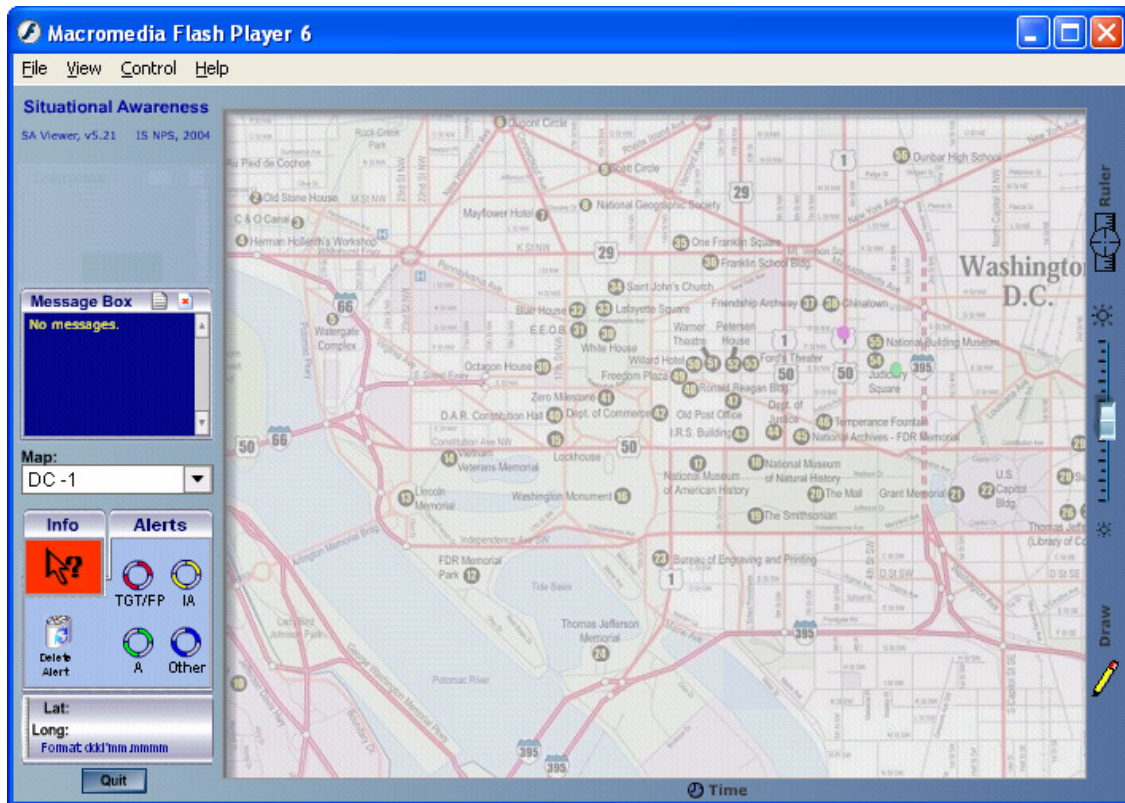


Figure 21. SA Server successful in DC

The server was able to register full signal and quality strength in FMM even though it was centrally located in the null of the roof mounted antennas. Fig 22 depicts the OCTO grounds, building exterior and external sector antenna placement.



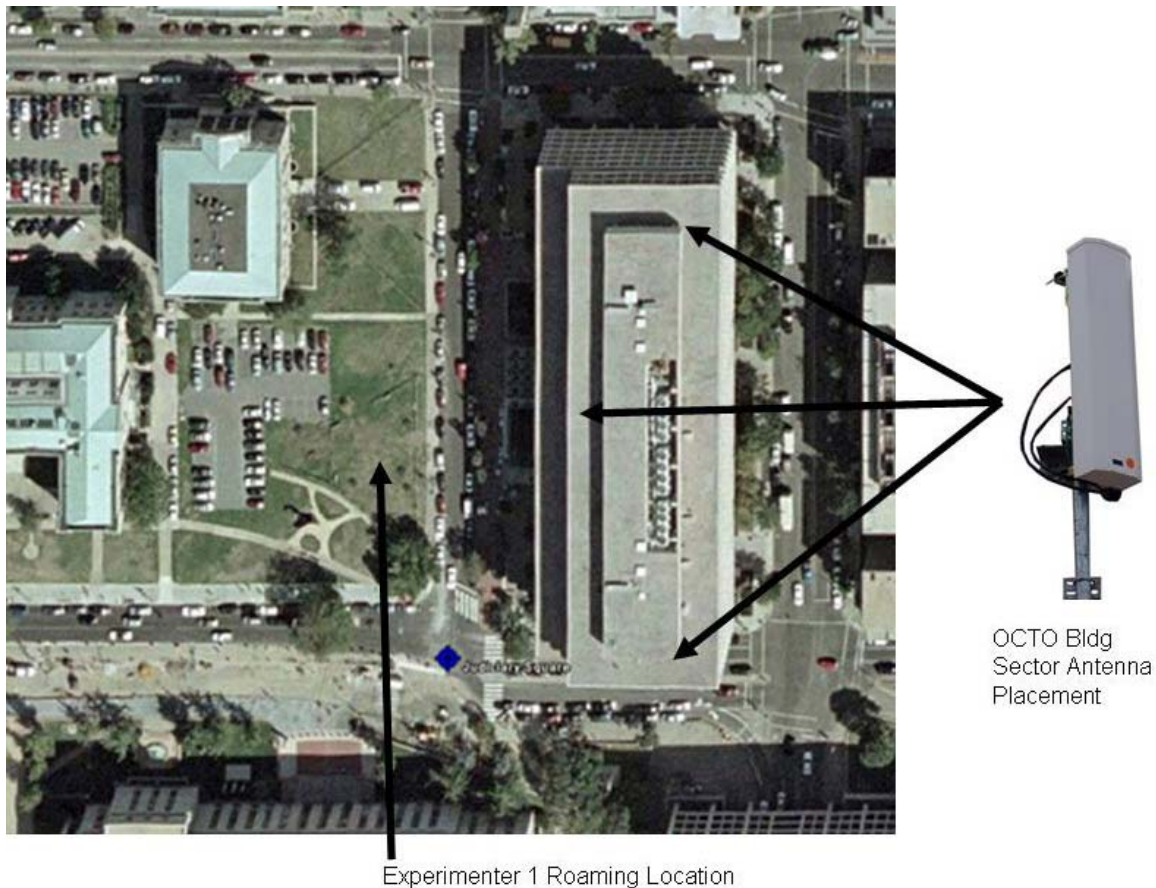


Figure 22. OCTO Exterior and Sector Antenna Placement

Mobile communications were conducted successfully using Microsoft Portrait installed on each experimenter's laptop and PDA.

Microsoft Portrait is a research prototype for mobile video communication. It supports .NET Messenger Service, Session Initiation Protocol and Internet Locator Service on PCs, Pocket PCs, Handheld PCs and Smartphone. It runs on local area networks, dialup networks and even wireless networks with bandwidths as low as 9.6 kilobits/second. Microsoft Portrait delivers portrait-like video if users are in low bandwidths and displays full-color video if users are in broadband. In low bandwidths, portrait video possesses clearer shape, smoother motion, shorter latency and much cheaper computational cost than do conventional video technologies. Microsoft Portrait pursues providing presence notification, chat/voice/video functions anytime, anywhere, on any device. Ref [26]



Demonstration consisted of stepping through the available capture settings for image size and frame rate, as well as various compression settings for keyframe interval and video bandwidth. Table 3 shows all settings tested.

Capture Settings		Compression Setting	
Image Size	Frame Rate	Keyframe Interval	Video Bandwidth
128x96	1 fps	1 sec	14.4 Kbps
<b>160x120</b>	3 fps	2 sec	28.8 Kbps
320x240	5 fps	3 sec	28.8 Kbps
652x288	10 fps	<b>5 sec</b>	33.3 Kbps
	<b>15 fps</b>	10 sec	56 Kbps
	25 fps		<b>128 Kbps</b>
	30 fps		256 Kbps
			512 Kbs
<b>Bold</b> are Optimal setting for two user full duplex audio and video in the same sector.			

Table 3. MS Portrait Settings Tested

As a mobile user with a .25 Watt transmitter, the UL is limited to 900kps. With OCTO network operating in an N=1 configuration and both users located in that same sector, user selections requiring greater than 300kbs demand resulted in one, or both, users experiencing frame stutter and audio gaps or lag. During the testing, bandwidth selections above capabilities of the network were selected. In Fig 23, the pixilation and artifacts are visible when both the mobile users were simultaneously attempting UL/DL of 512 Mbps bandwidth.

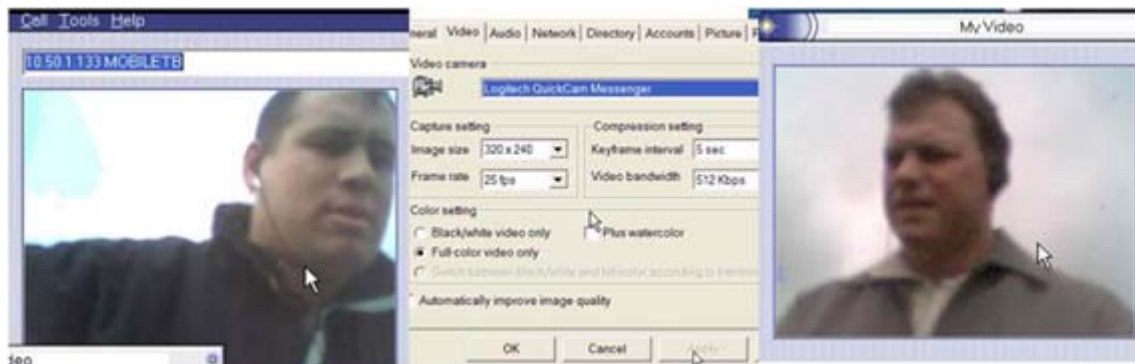


Figure 23. Pixilation and Artifacts at 512 Mbps

Flarion's Flexband, discussed later in the thesis, addresses the N=1 limitation for each sector. The new technology increases UL capability to 1.8 Mbps.

#### **4. 22 Mar Highlights**

The events conducted on this day were designed to best simulate an environment with a single BS. Forward deployed military implementations of 802.20 may have only one BS rack mounted in a HMMWV/HumVee. The experimenters used the LRV and four mobile nodes consisting of two laptops and two PDAs. UL/DL tests were conducted at various intervals throughout the scenarios. Appendix F contains a table of all variables collected by FMDM and computed statistics of FMLP.

Low latency is an important factor in ensuring that real-time and time sensitive communications are achieved. The testing demonstrated an excellent ping response with a median response time of just 65 ms. Below are the overall ping statistics for all combined events on 22 Mar, calculated from a total of 10043 pings.

- The number of ping drops was 485 (4.83%)  
Taking 100% of the data (not including ping drops):
- The number of pings was 9558
- The max ping delay (rtt) was 3731.0 ms
- The mean ping delay (rtt) was 99.7 ms
- The median ping delay (rtt) was 65.0 ms
- The min ping delay (rtt) was 37.0 ms
- The standard deviation was 178.7 ms  
Taking the best 90% by ping delay (rtt):
- The number of pings was 8602
- The max ping delay (rtt) was 136.0 ms
- The mean ping delay (rtt) was 68.6 ms
- The median ping delay (rtt) was 63.0 ms
- The min ping delay (rtt) was 37.0 ms
- The standard deviation was 17.3 ms

QCheck was installed on all mobile nodes. Free software from XIAIA, QCheck can be used for testing response time, throughput, streaming and traceroute. Below is a

screen capture supporting the overall ping data. QCheck ping response test resulted in a minimum 80 ms, average 94 ms and maximum 103 ms.

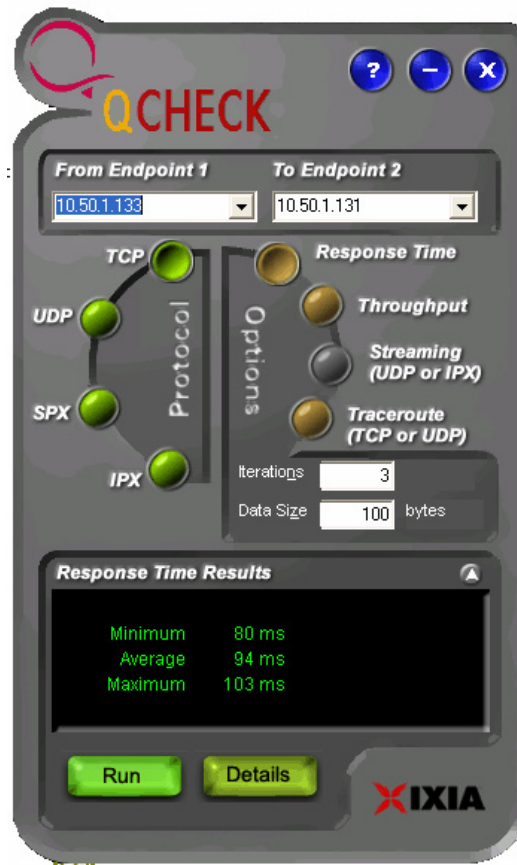


Figure 24. QCheck Response Time Test

NetPerSec was used to measure the real-time speed of the network connection. A graph of the communication speed of TCP/IP activity to and from the network was displayed in a GUI. During mobile testing at speeds up to 40mph (legal road limit), a 6 MB file was downloaded from NASA. A sustained rate of 1.7 Mbps with a maximum of 2.5 Mbps was observed.

Developed by associates at the National Laboratory for Applied Network Research (NLNR), Iperf was used to measure maximum TCP bandwidth. Iperf reports bandwidth, delay jitter, and datagram loss. IPerf was used to test UL and DL capabilities. These tests were done both independently and simultaneously with other activities. Mobile Iperf testing on the Georgia Avenue tower, Site ID (sector for a tower) OCTO 0241 and site name 4<sup>th</sup> District, yielded average DL of 742.4 kbps and a maximum of 789.2 kbps. An UL average rate of 635.9 kbps and maximum of 800.9 kps, and a DL

average rate of 567.9 kbs and maximum of 757.5 kbps, were generated while running the Iperf UL test and concurrently downloading from the web. Figures 24-26 are screen captures from the LRV during mobile testing.

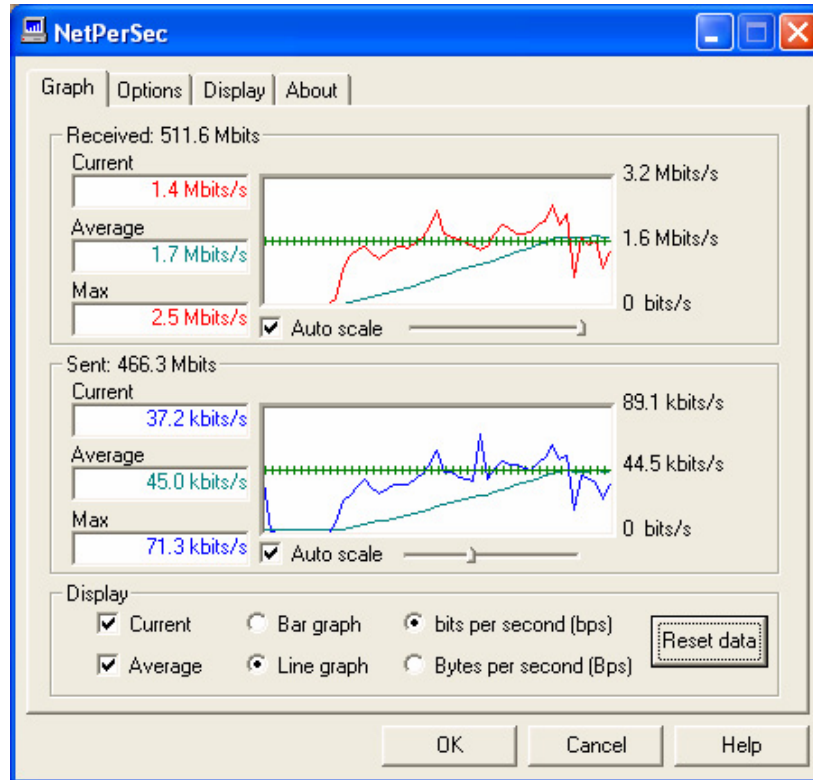


Figure 25. NetPersec Results from 6 MB File DL

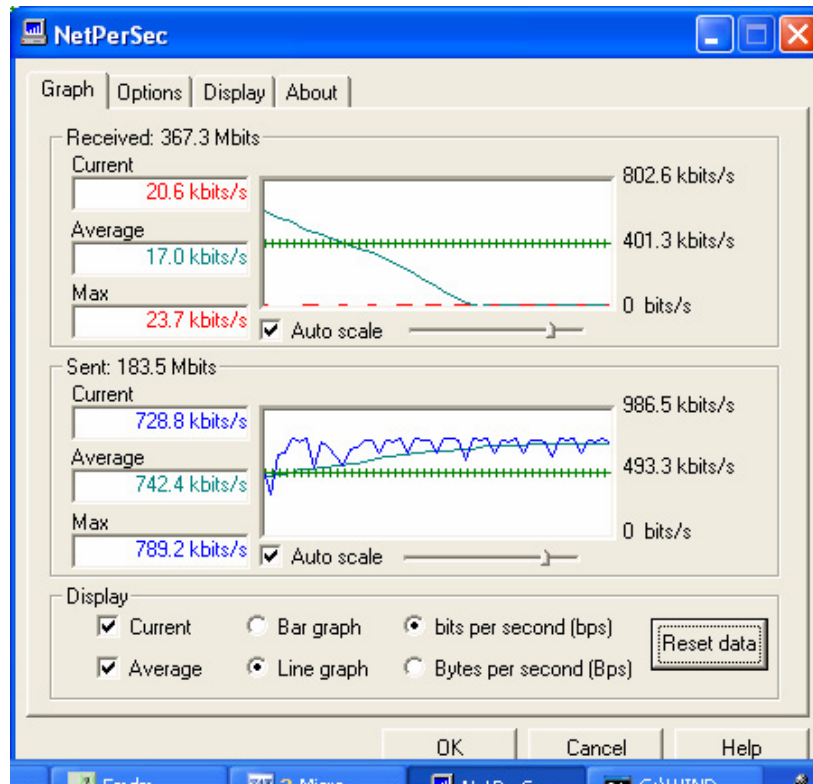


Figure 26. Iperf DL Testing on 4<sup>th</sup> District, OCTO 0241, Tower

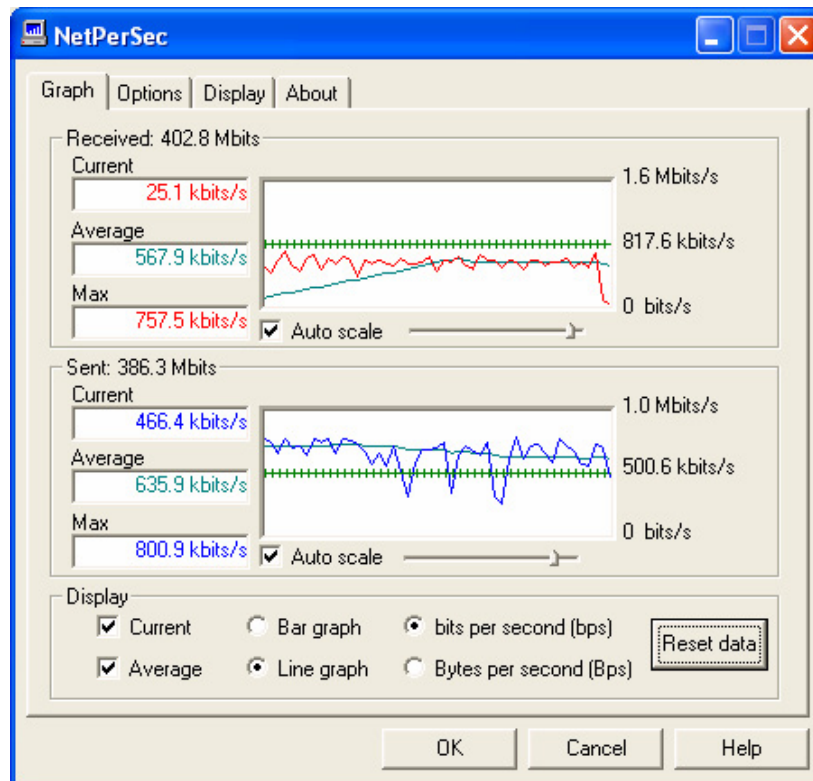


Figure 27. Concurrent UL/DL Testing on 4<sup>th</sup> District, OCTO 0241, Tower

A requirement of the experiment was to demonstrate connectivity while on the move and recording speed. The portions of Georgia Ave where the LRV transited consisted of two and four lane city street driving, with numerous traffic signals. Testing was done during regular city traffic and therefore achieved speeds were limited to traffic volume and traffic lights. Experimenters were able to successfully demonstrate single tower usage on both OCTO 0241 and OCTO 0031. Fig 28 is a composite of two DL trials of 6 MB file from the NASA website. Instant rate is the number of bits per second that were transmitted corresponding to that data sample. This is adjusted for the time interval between subsequent samples, which gives a number in bits per second for the data rate. [Ref 28] Experimenters were the only users on the Reeves and 4<sup>th</sup> District towers at the time of testing. However, experiment was not able to control parameters external to the 802.20 gateway.

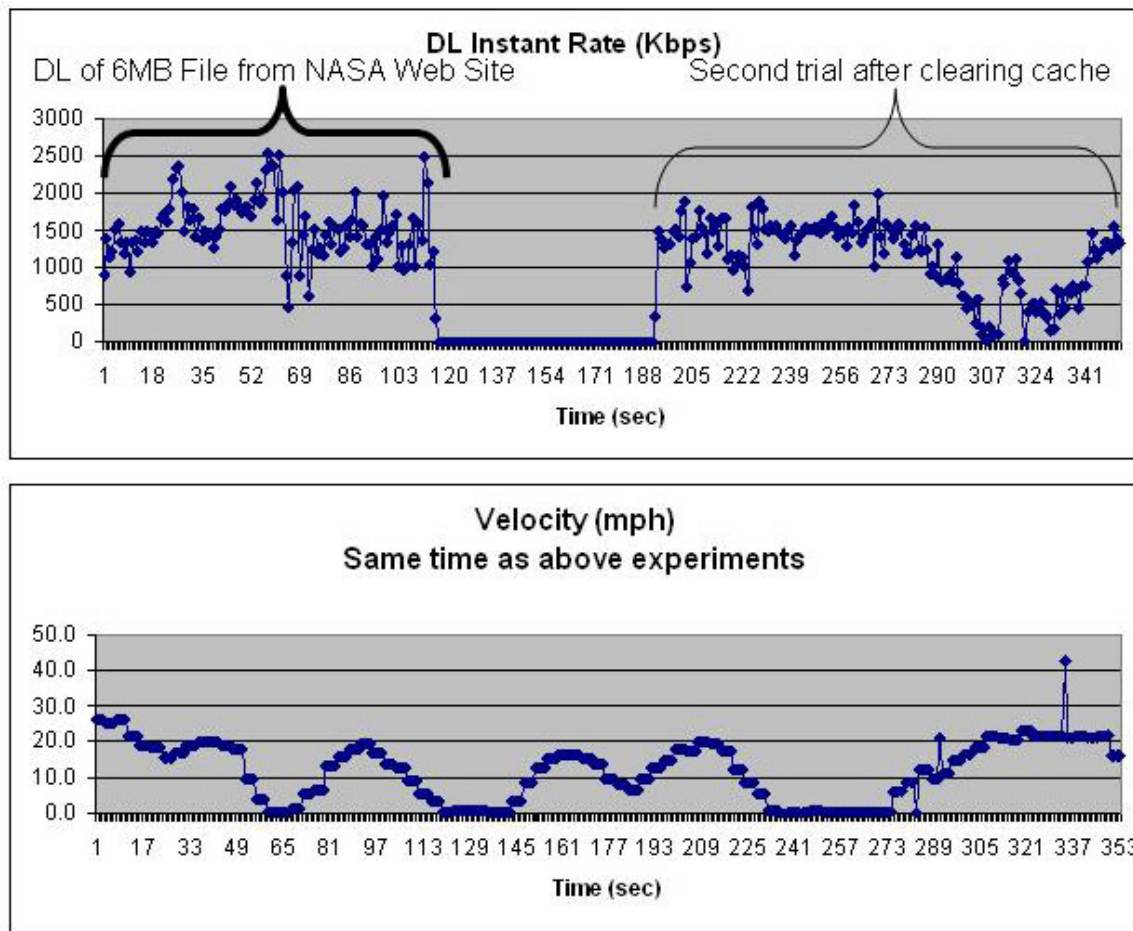


Figure 28. DL Rate Compared with Velocity

The UL test was conducted on the 4<sup>th</sup> District tower. As previously mentioned, the maximum UL capability was 900 Kbps. The UL test was able to sustain rates greater than 600 Kbps for the majority of the test. Traffic was lighter and LRV was able to maintain 30 MPH for approximately 5 minutes. Fig 29 shows the graph of UL rates against LRV velocity.

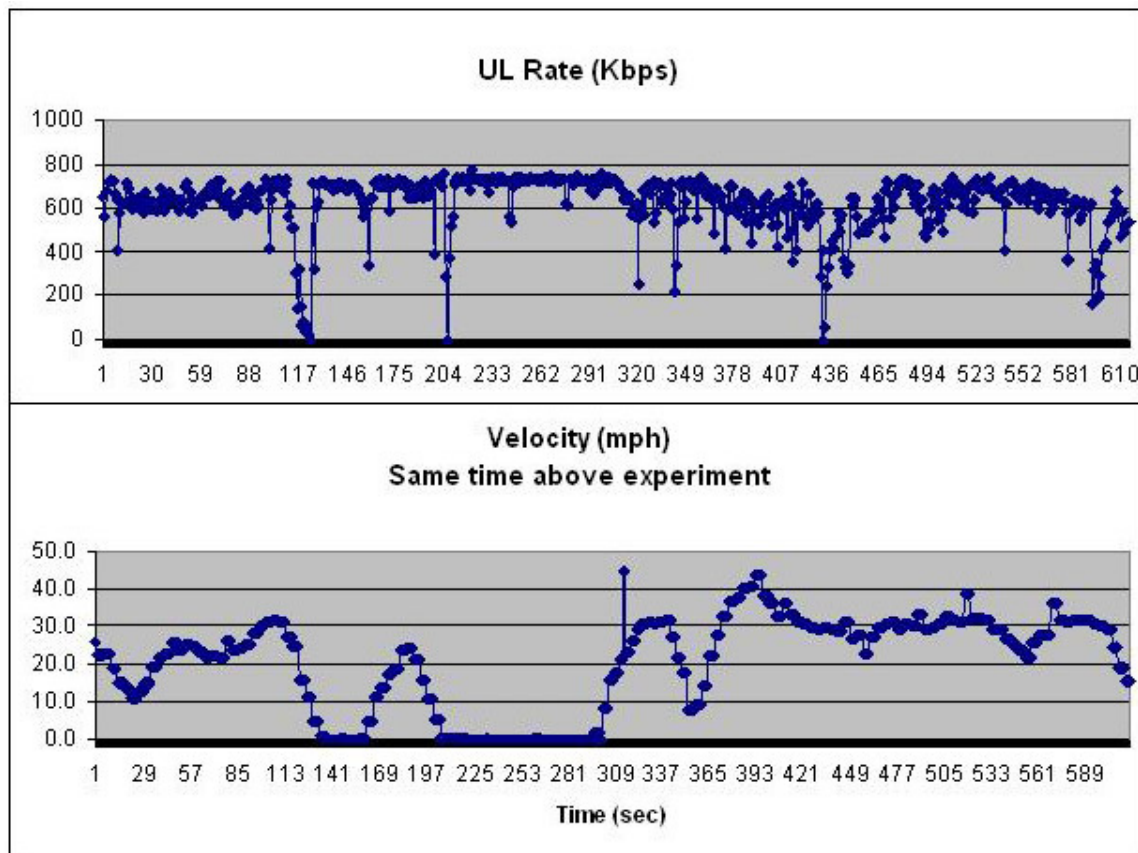


Figure 29. UL Test on 4<sup>th</sup> District Tower (Kbps and MPH)

FMDM program logged received SNR from both transmitters and receivers on the NIC. When the data was processed using FMLP, a variable for the active received SNR was created. As a rule of thumb from the experiments, an SNR of 9 dB or greater was required to maintain solid connectivity.

For post-processing of track and digital data, the following programs and services were used:

- Global Mapper: used to download US Geological Survey (USGS) Digital Ortho-Quadrangle (Grayscale Aerial Imagery).



- MapInfo: used to overlay track with USGS imagery, create thematic representation of data collected and provide overlay of street level mapping.
- National Geospatial-Intelligence Agency Digital Terrain Elevation Data (DTED) Level 2 Coverage 1:25,000: used to provide layer of terrain on graphs against plotted tracks and thematic tracks.
- Google Earth Pro Demo: provide digital satellite imagery combined with street and building information.

The SNR values from the DL test depicted in Fig 30 have been superimposed over the digital satellite imagery. Each point was mapped to create a thematic view. Fig 29 supports the consistent DL rate against the mapped SNR.

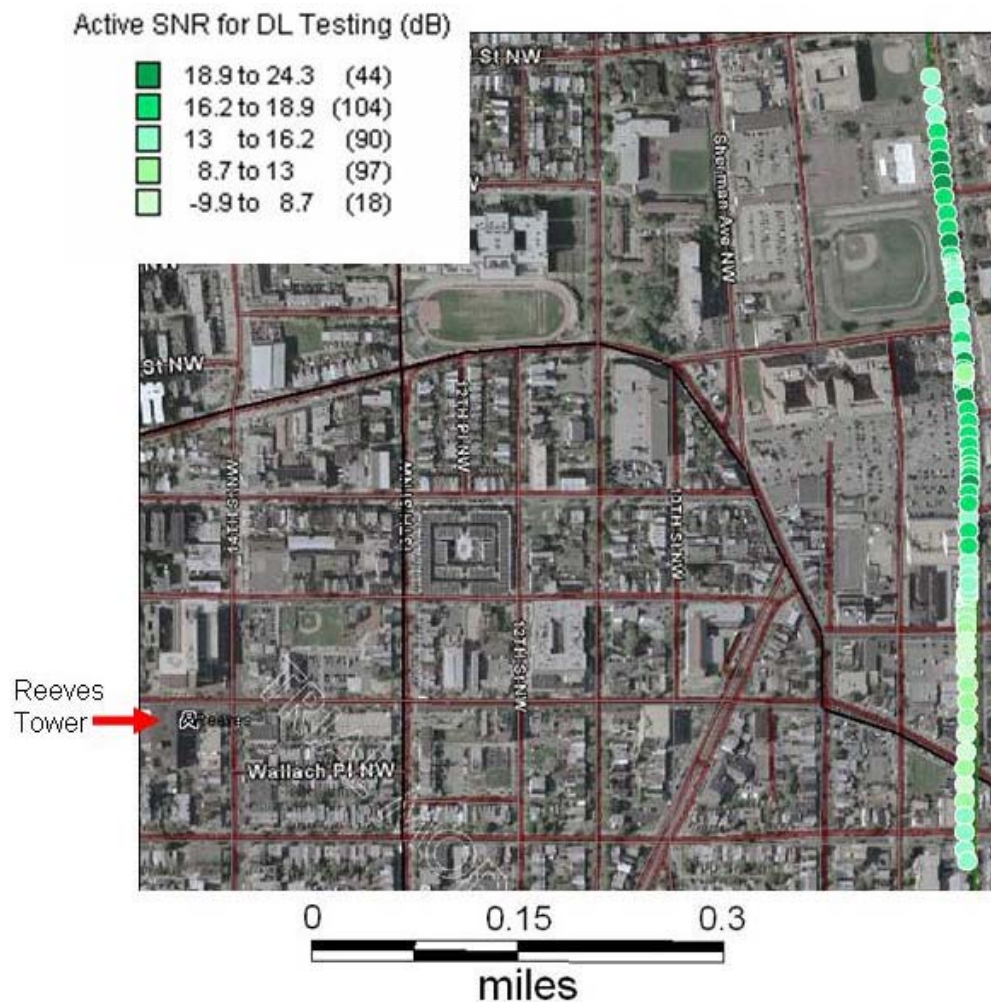


Figure 30. Thematic Map Superimposed Over Satellite Street Level View for DL Test  
**5. 24-25 March Highlights**

Three key aspects of the 802.20 network capabilities were evaluated in this round of testing; sector sustained throughput, “through wall”, NLOS, user access in an urban



environment and mobile access at highway speeds. Event 1 supports Flarion's claim of sustainable sector throughput DL of 1-1.5Mbps and sustainable sector throughput UL of 300-500 Kbps. The published maximum sustained DL is 3.2 Mbps (200 Kbps at cell edge) and maximum sustained UL is 900 Kbps (50 Kbps at cell edge). Event 2 effectively established "through wall", NLOS, mobile to mobile user communications in an Urban environment. Event 3 provided positive results for highway speed testing and sustained connectivity with adverse environmental conditions.

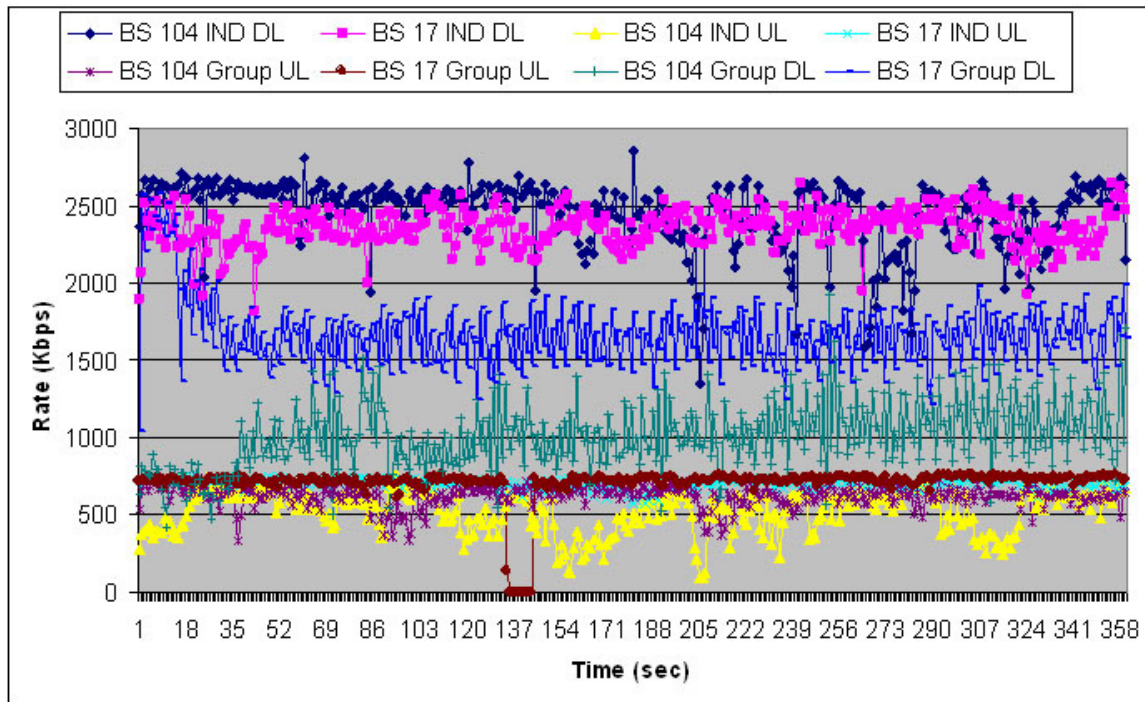


Figure 31. Individual and Group Sector Throughput Testing

The testing for Event 1 was performed by a team of six experimenters conducting a prearranged sequence of activities. Each experimenter performed an individual UL and DL on single sector. Following the individual testing, the group performed a simultaneous UL and DL test on the same sector. The Judiciary Square tower, OCTO0001, sectors 7, 17, and 104 were selected. Appendix G provides a complete description of all parameters of the OCTO towers. One mobile user was in the OCTO building on the 8<sup>th</sup> floor connected to sector 104 with another mobile user outside the building attached to the same sector. One of the two experimenters connected to sector 17 was located at the Capitol Building. Fig 31 graphically depicts the ability of both mobile users to sustain the published capabilities. Operating from within the OCTO

Building, the sector 104 user was in the antenna null and slight performance degradation was noted.

When the group and individual DL tests were compared, rates for the UL remained relatively consistent for all tests. However, as expected, the group download test demonstrated a decrease in individual available bandwidth for all users in each sector. Even with the decrease, the BS was able to allocate available bandwidth to ensure that mobile users were able to sustain published rates. The below table shows the statistics for the two users from Fig 31. Although only two users were graphed, it is important to note all test subjects were able to maintain sustained connections in both individual and group tests.

	BS 104 IND DL	BS 17 IND DL	BS 104 Group DL	BS 17 Group DL	BS 104 IND UL	BS 17 IND UL	BS 104 Group UL	BS 17 Group UL
<b>Mean</b>	2450	2356	1011	1671	529	706	624	703
<b>Median</b>	2528	2367	985	1669	564	713	640	725
<b>Std Dev</b>	215	124	222	224	134	33	67	119
<b>Maximum</b>	2528	2367	1011	1671	564	713	640	725
<b>Minimum</b>	215	124	222	224	134	33	67	119

Table 4. Statistic for Individual and Group Sector Throughput Testing

The testing for Event 2 was done both NLOS and “through wall” as a mobile experimenter walked through the accessible interior areas of the US Capitol Building, then headed northwest toward the OCTO office down the city streets and returning to the 8<sup>th</sup> floor of the OCTO building using the elevator. Experimenter was able to sustain connectivity, with the results below:

- The median value of active received SNR was:
  - 14.00 over all data (100% data)
  - 14.70 over good data (90% best data by metric)
  - min= -13.10, max= 23.60, std= 5.81 for all data samples
- Data points with at least 1 connection: 1742
  - Drop percentage =  $19/1761 = 1.07893\%$
  - Data points with 2 connections (MBB): 372
  - MBB percentage =  $372/1742 = 21.1244\%$

Fig 32 shows the route the experimenter used to transit from the US Capitol Building to the OCTO building. Numerous times during the transit, NLOS connectivity was demonstrated. At a pedestrian level, the buildings would block LOS to all sectors of the Judiciary Square tower.

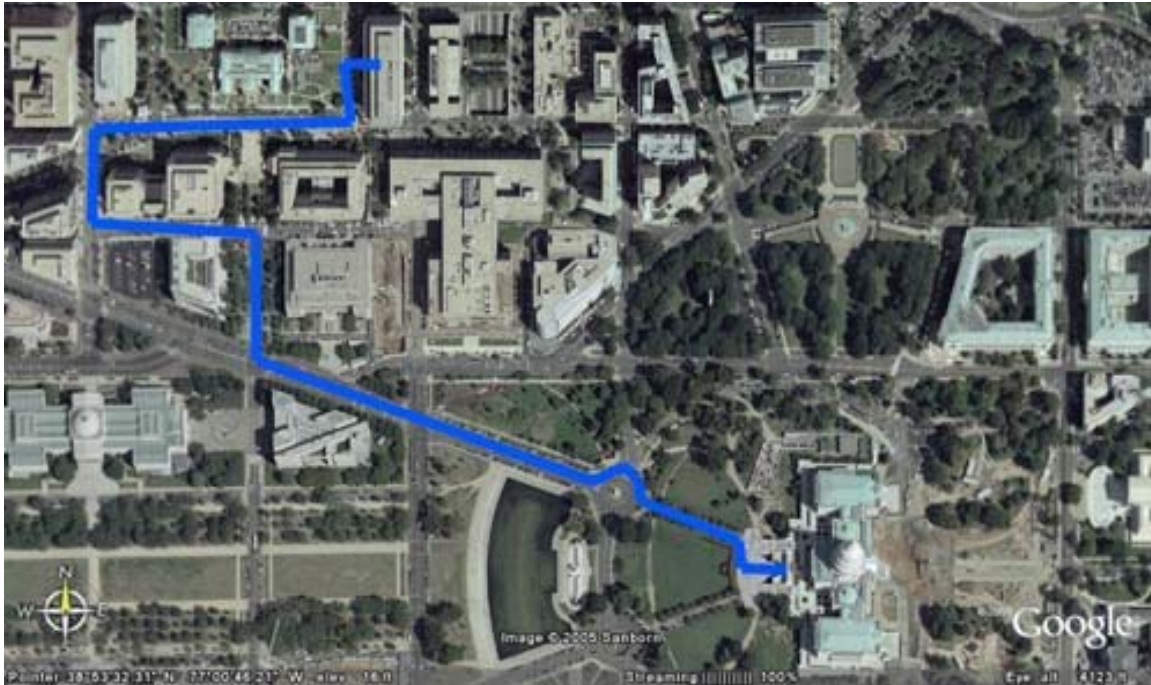


Figure 32. Walking Transit from US Capitol to OCTO Office

The next two graphs demonstrate that the mobile user was able to maintain connectivity throughout the transit. Each graph was done over the same time sequence from 1761 data points. Fig 33 supports the 1.08 drop percentage. The mobile unit sustained a connection while in the elevator from the 1<sup>st</sup> to 8<sup>th</sup> floor.

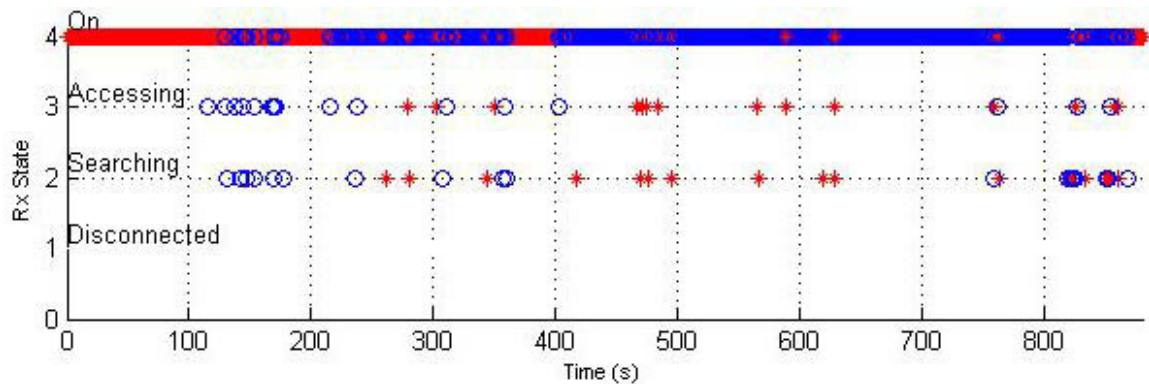


Figure 33. Connection Status for Through Wall and NLOS Testing



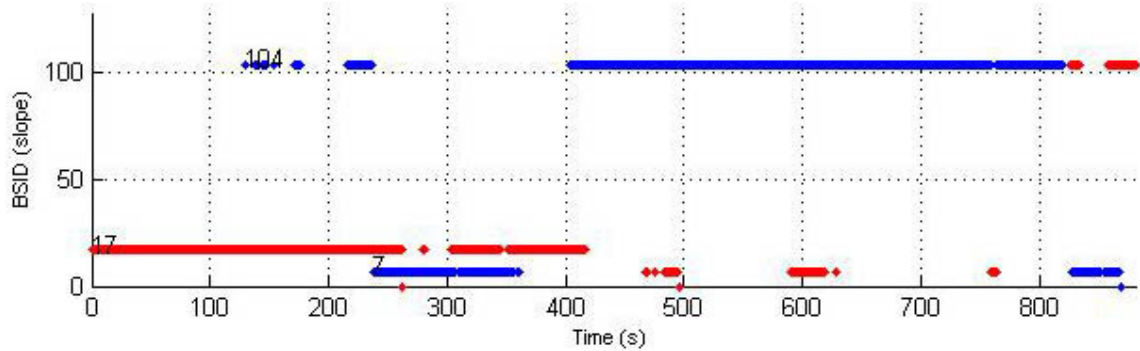


Figure 34. BSID Switching During Through Wall and NLOS Testing

On 25 March, scattered but heavy thunderstorms were present during the entire day of testing. After acquiring the 802.20 network, the LRV departed the OCTO basement parking garage and traveled south for one leg of mobile testing followed by a high speed leg of testing on the George Washington Highway. Iperf, QCheck and FMDM were used to test and track results of each run. Fig 35 combines the sNR of both events superimposed over Terra Server maps and DTED elevation data.

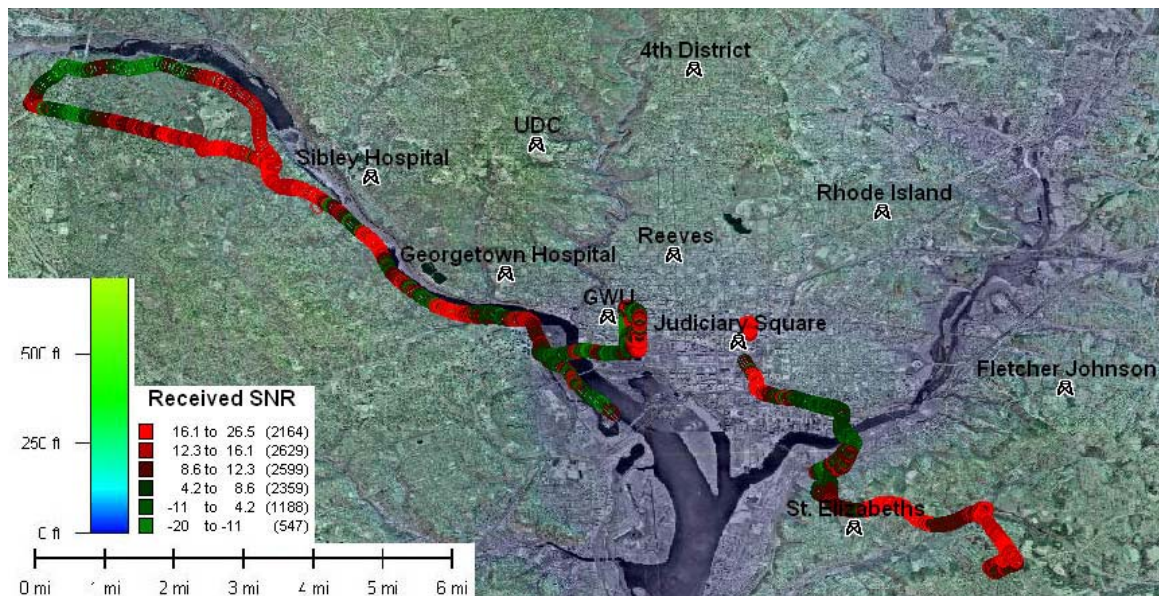


Figure 35. Highway Speed Testing

Sector interference can be seen as the route trace nears the cell's edge. As mentioned earlier, Flarion's Flexband was developed to address this concern. Speeds greater than 70mph were obtained while observed SNR received was at the highest levels. The north-to-south and south-to-north highway speed runs past Sibley Hospital tower were some of the strongest sustained signals received during all testing. The drop

percentage observed was 4.3%. This was due mostly to the portion of the trial completed in the hilly terrain northwest of Sibley tower. The elevation difference and NLOS conditions experienced have been graphed in Fig 36.

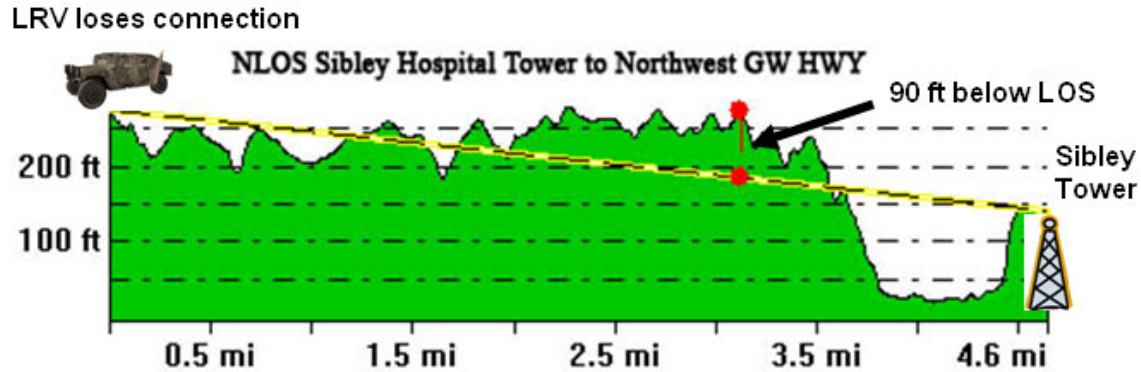


Figure 36. NLOS Sibley Hospital Tower to Northwest Portion of GW HWY Run

The GPS altitude recorded 200-250 feet. The total statistics for the combined SNR for both trials was:

- Total data points: 11486
- Time: 1 hour, 35 minutes, 43 seconds (assuming 0.5 seconds per point)
- Data points with at least 1 connection: 10983
  - Drop percentage =  $503/11486 = 4.37924\%$
  - Data points with 2 connections (MBB): 1237
  - MBB percentage =  $1237/10983 = 10.7696\%$
- The median value of active received SNR was:
  - 11.30 over all data (100% data)
  - 11.40 over good data (90% best data by metric)
  - min= -20.00, max= 26.50, std= 5.87 for all data samples

When SNR received was plotted against LRV velocity, no noticeable effect was observed. There were a few errant outlying data points for velocity, which mostly likely occurred due to an erroneous GPS data point. The polling was performed every .5sec. The SNR was evenly spread across the range of LRV velocity.

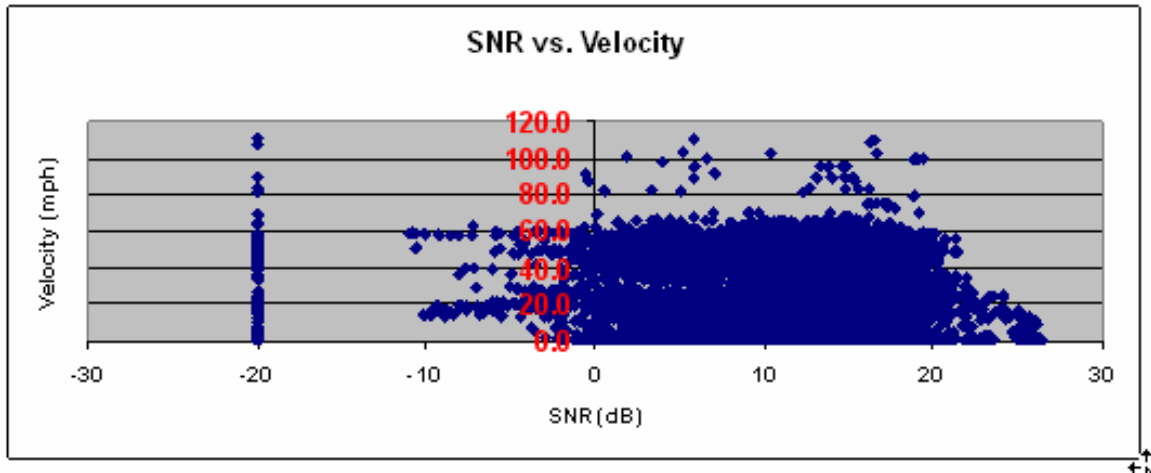


Figure 37. Scatter Plot of SNR vs. Velocity

### C. MOUT FACILITY TESTING AT FORT ORD

The testing conducted at the Military Operations in an Urban Terrain (MOUT) facility from 16-18 March was designed to see if an 802.20 mobile BS could address the last mile solution in an urban environment. SOF and frontline troops require a highly mobile solution which must function in the demanding environment of highly populated areas. The events completed during the week supported further testing of 802.20 as a last mile alternative.

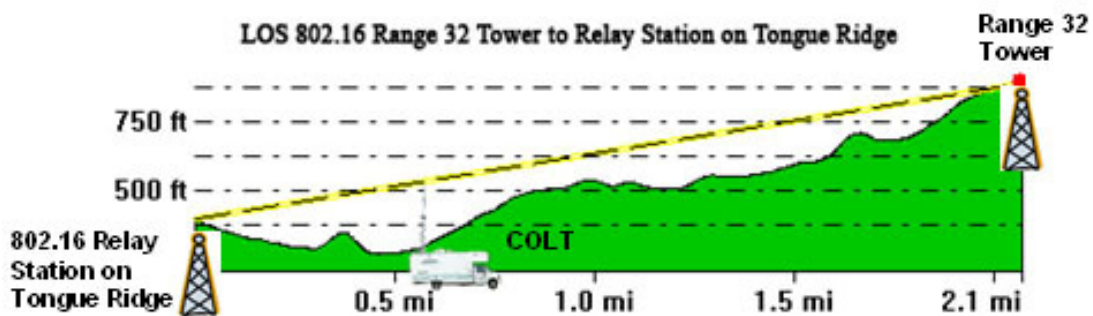


Figure 38. LOS 802.16 Relay Station, COLT and 802.16 Range 32 Tower

The MOUT facility, located on Fort Ord in Marina, CA, contained numerous 2-3 story cinder block buildings designed to simulate concrete urban construction. MOUT was positioned in a valley between two ridgelines, Impossible Canyon and Tongue Ridge, which did not facilitate LOS connection to NPS's 802.16 backbone R32 tower. A relay station on the ridge opposite R32 was required to connect the two networks. Fig 39



is a panorama stitching of photos taken from the roof of a two story building with the COLT vehicle located adjacent to the building.



Figure 39. Panoramic View of MOUT

#### 1. COLT and 802.16 to 802.20 Setup

The 802.20 network was provided by the Cell On Light Truck (COLT), which was designed as a self-sufficient network Tactical Operation Center (TOC). COLT was equipped with a 38 ft retractable antenna mast deploying a 20W omni antenna. All required hardware to support an 802.20 network: Radio Router, AAA, Home Agent, Router, Web Server (not required, but utilized in testing), Power Sub System and Low Noise Amplifier was located inside the vehicle.

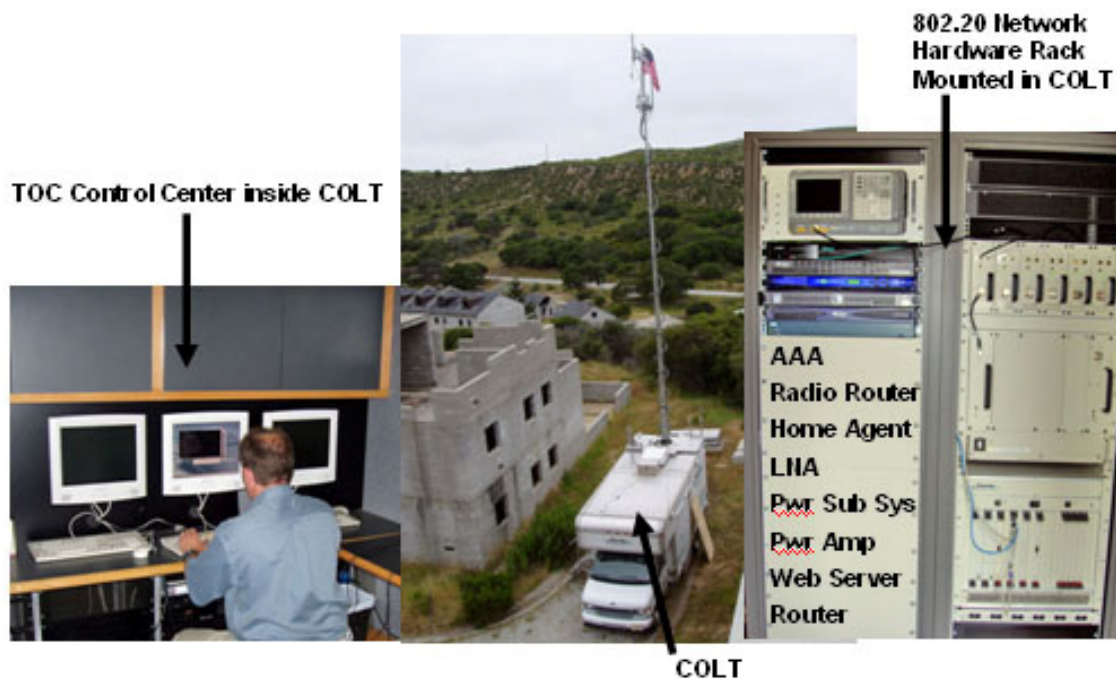


Figure 40. Interior and Exterior view of COLT

Fig 40 depicts the COLT, TOC control center inside COLT and rack mounted 802.20 network hardware. A Cisco switch established the connection between the WAN (for experiments 802.16 was used as a WAN) and 802.20 networks. Event 1 was successful in connecting the two, however, Solar Winds monitoring was not possible. Experimenters did not have access privileges to the NPS TOC router to update the static routing table. The TOC was able to ping the COLT as a node in Solar Winds, but the router blocked all other traffic. VOIP communications between TOC at NPS and the COLT were successful. Solar Winds network monitoring software does not contain the Management Information Base (MIB) for 802.20 in its database. 802.20 MIB supported some of the Simple Network Monitoring Protocol (SNMP) MIB, and if monitoring were possible, these would have been visible monitoring parameters in Solar Winds.

### 3. “Through Wall” and Urban Environment Testing



Figure 41. MOUT Early Warning Using Full Duplex Audio and Video

Representatives from United States Special Operations Command (SOCOM) were present to observe Event 3. With the same PDA configuration as OCTO events, mobile to mobile testing was conducted. MS Portrait was utilized for full duplex audio and video transmission. One experimenter lead a group to a position in the MOUT’s mock prison and another experimenter took a group to a basement of a building



positioned at the other end of the facility. In Fig 41, the experimenter in the prison located a bullet on the floor of the building, took a photo of it with his PDA and transmitted the file to the operator in the COLT. Experimenter also sent a live video feed of the bullet to the other group. Two additional “through wall” demonstrations were conducted. The first (Figure 42) demonstrated connectivity in a 30 inch diameter sewer pipe of corrugated steel, tunneling between two buildings. The second test (Figure 43) was used to demonstrate capability to send data back to TOC for dissemination to a subject matter expert for aid in translation. A simulated advance party entered the building and noted Arabic writing. A video feed of the sign was sent to the other group as well as the TOC. No translators were involved in this set of events (area for expansion in future trials).

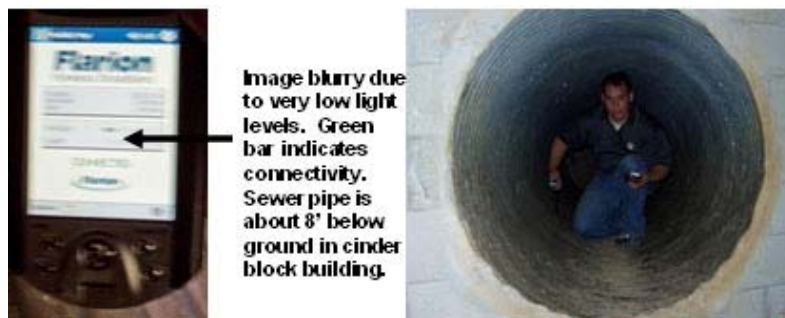


Figure 42. Connectivity in a 30” Metal Sewer Pipe Under Ground



Figure 43. Early Warning, Identification and Remote Translation Test

SOCOM observers and Mark Meoni of the Naval Special Warfare Command, were given the opportunity to perform live testing with the PDAs as well as laptops connected to the network. While transiting the MOUT and surrounding vicinity, they were able to view pages hosted on the COLT's web server, perform MS Portrait calls from laptop to PDA, and PDA to PDA, and control an IP camera located on the roof of the COLT. The camera was connected wirelessly utilizing a Personal Access Device (PAD). The PAD was developed to be an IP bridging device with an internal 802.20 NIC and battery. External connections available were a DC power input and RJ-45 connection for IP devices.

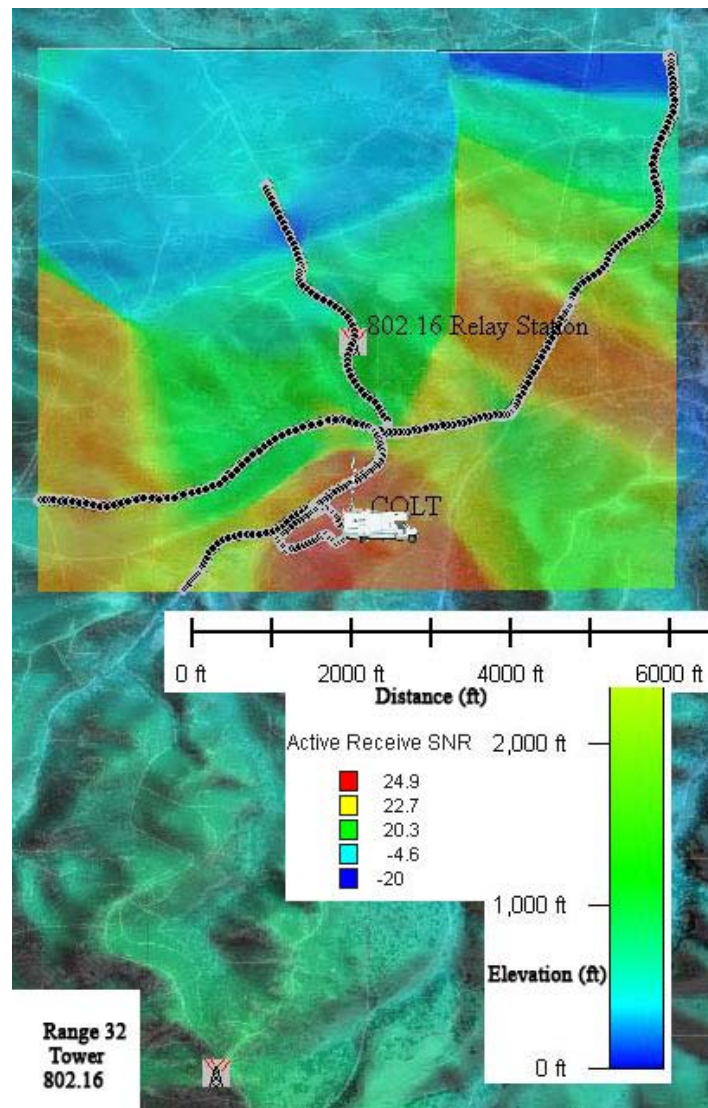


Figure 44. SNR with IDW Projection at MOUT

From the data captured during the MOUT and vicinity drive, a graph using Inverse Distance Weighting was created. IDW interpolation uses a distance weighted average of data points to calculate grid cell values. Tower/COLT locations, DTED data and Terra Maps were layered onto the IDW to create Fig 44. This graphic along with Fig 37 demonstrates again the NLOS capabilities of 802.20.

#### **D. CAMP ROBERTS TNT FIELD EXPERIMENTS**

Testing developed for 802.20 at Camp Roberts was two fold. The first objective was to play a role in the collaborative effort between numerous activities and thesis groups all working to further TNT. The principal focus was to simulate a coalition environment with sensors from various wired and wireless network technologies all reporting to, and being monitored by, the TOC. The second area of focus of the testing was to duplicate NLOS and mobility type testing as performed in DC and MOUT to further support implementation of 802.20 as a last mile solution.



Figure 45. COLT Next to TOC at Camp Roberts

All of the equipment used in the prior experiments was delivered to Camp Roberts for use in the scheduled events. As with the MOUT, the 802.20 network was supplied by the COLT which was located adjacent to the TOC (Fig 45). A CAT 5 cable was used to connect the Cisco switch in the COLT to the Cisco router in the TOC. As access privileges to the static routing table had been acquired for trials, TOC monitors

were able to see and capture TCP/IP traffic from the 802.20 network on the NPS backbone.

### 1. 802.20 Remote Sensor Support for TNT

The first sensor requirement for 802.20 was to provide high altitude early warning motion detection. The configured sensor consisted of a PAD and DLink IP camera combination connected to a high capacity battery, and raising it to altitude, approximately 1000 ft, from a tethered weather balloon. Fig 46 shows the completed configuration and its implementation.



Figure 46. Camp Robert 802.20 and IP Camera Balloon Configuration

The camera was adequate for motion detection, however, the optics were not intended for this type of use. The video from the IP camera was sent over the 802.20 network to the TOC via the COLT. The video was displayed on a plasma screen in the TOC. Microsoft Encoder was used to capture the streaming IP video feed. Due to the intense processor requirements for displaying and capturing video simultaneously, the video captured appears more pixilated than what was actually observed in the TOC. Fig 47 shows the video motion detection as well as the degree of balloon spinning. Top left



frame time was 04:19:02 to last frame on bottom right with a time of 04:19:21. The total detection time acquired was 27 seconds (not all frames shown).



Figure 47. Video Motion Detected by 802.20 Altitude Sensor

The second remote sensor called for ground level visual identification. Sensor consisted of an IP based Sony PTZ camera on a tripod, AC/DC inverter, 12-volt auto battery, Netgear 802.20 to 802.11 bridge (Fig 15) and a PAD for 802.20 access. The ground based IP camera was set up 2.5 miles South of the balloon position on Boy Scout and E. Perimeter Rd. From Figure 48, it is possible to successfully identify vehicle type, make and model was not easily discerned from the photos. The resolution of the images was set to 320 x 240 to ensure ten frames per second could be captured and transmitted. There was a ridgeline between the camera and COLT which limited connectivity. The SNR received fluctuated between 9-10 dB. This was adequate to complete the exercise.



Figure 48. Visual Identification by 802.20 Ground Sensor

The terrain provided challenges for completion of the tasked events. The below graph indicates the contouring issues which were overcome to conduct the exercises. If the balloon was lowered below, 500 feet, connectivity was not possible. 1,000 feet was utilized to eliminate a disconnection due to wind. In the later part of the day, the winds increased and pushed the balloon in one direction lowering its altitude. The balloon was positioned just on the other side of the 1000 ft ridge from the COLT's perspective.

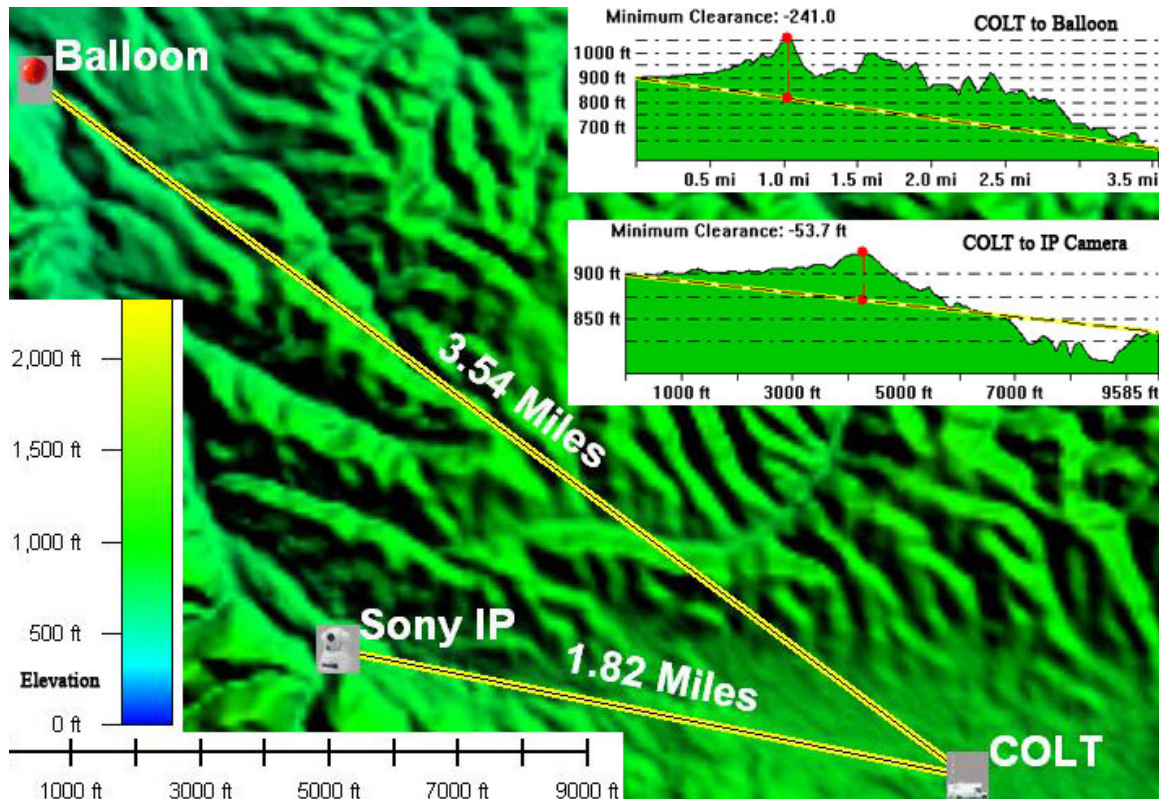


Figure 49. 802.20 TNT Configuration with Elevation

## 2. Additional NLOS and Mobility Testing at Camp Roberts

The next test focused on conducting similar NLOS and mobility testing as was performed in DC and MOUT to further support implementation of 802.20 as a last mile solution. To accomplish this, an area site survey and high speed runs were conducted.

There was limited road access to and from the TOC, as such; the area drive test was also limited. Fig 50 shows how the connectivity was lost as the LRV dropped behind ridge lines. Only one area survey was conducted due to time limitation.



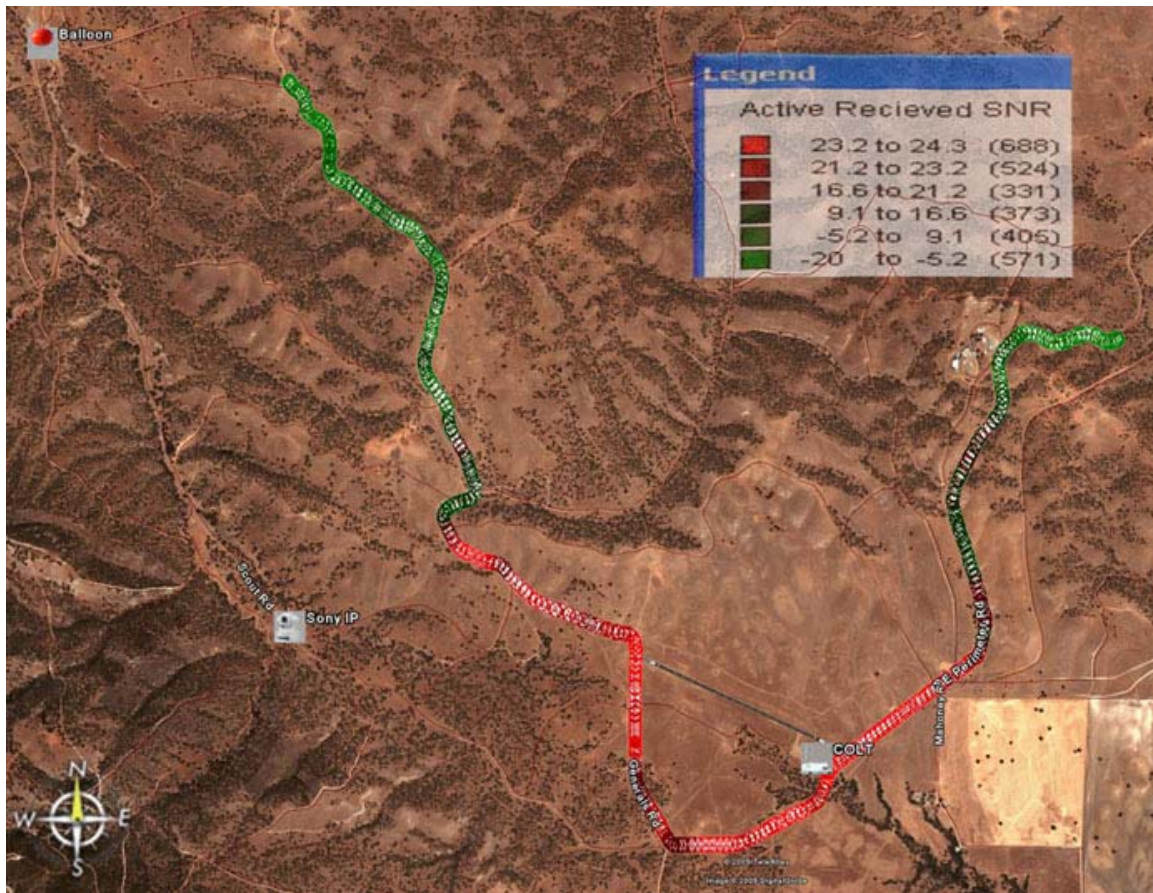


Figure 50. Camp Robert SNR Site Survey

The tarmac at Camp Roberts was used for the high velocity experiments. The Sony IP camera was positioned at the northwest end of the runway and the LRV at the opposite end. The LRV made multiple trips to both ends of the runway. While traveling the runway legs, the mobile user in the LRV was downloading from COLT's web server, conducting MS Portrait call with mobile user in COLT, and streaming the video feed from the IP camera. Fig 51 is a good example of how many frames are dropped by MS encoder when a full screen capture of video was attempted. This was the desktop of the second user talking to the Sony IP Web cam and to the Mobile user in the auto via MS Portrait. The mobile user in the LRV had identical settings.

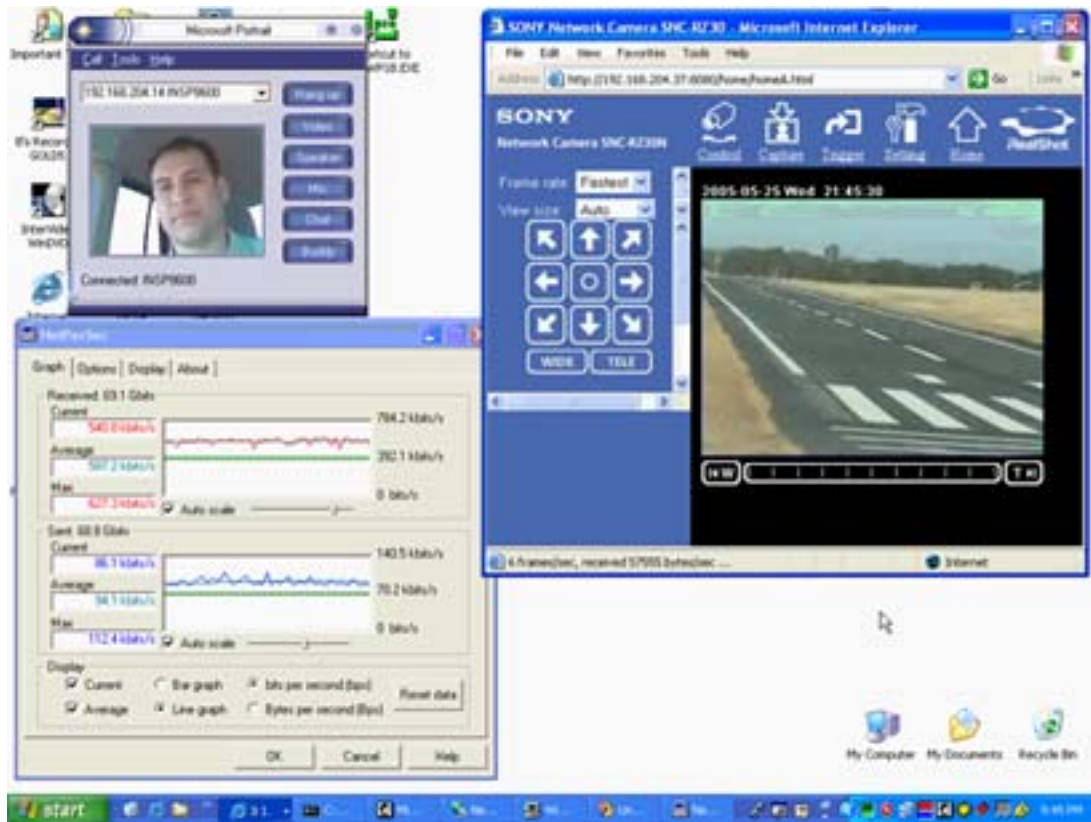


Figure 51. Screen Capture from Second Mobile User During Runway Testing

The temperature throughout the week was in the high 90's, and equipment only malfunctioned twice due to the heat. The Netgear bridge (Fig 15) overheated on the first day as it was placed alongside the road exposed to direct sunlight. Overheating was prevented in subsequent tests by placing the portable inverter, battery and bridge in a covered plastic container with the lid cracked open for natural ventilation. The second malfunction occurred during the runway testing. The Low Noise Amplifier (LNA) started to fail in the first two recorded runway trials and had completely failed by the third. The problem was isolated and a backup card for the RR was used. The remaining trials on the runway were done without incident.

During the runway trials, the LRV was able to reach speeds in excess of 90 mph; speed was limited by the length of the runway and safety concerns. The tests showed LRV velocity had no effect on received SNR. As shown in Fig 52, during the first two trials, the max SNR received was between 15-16 dB. During the third trial (failed LNA),



the LRV experienced sporadic SNR received. After the LNA was repaired, all of the remaining runs, 4 through 7, experienced a received SNR of approximately 23-24.5 dB.

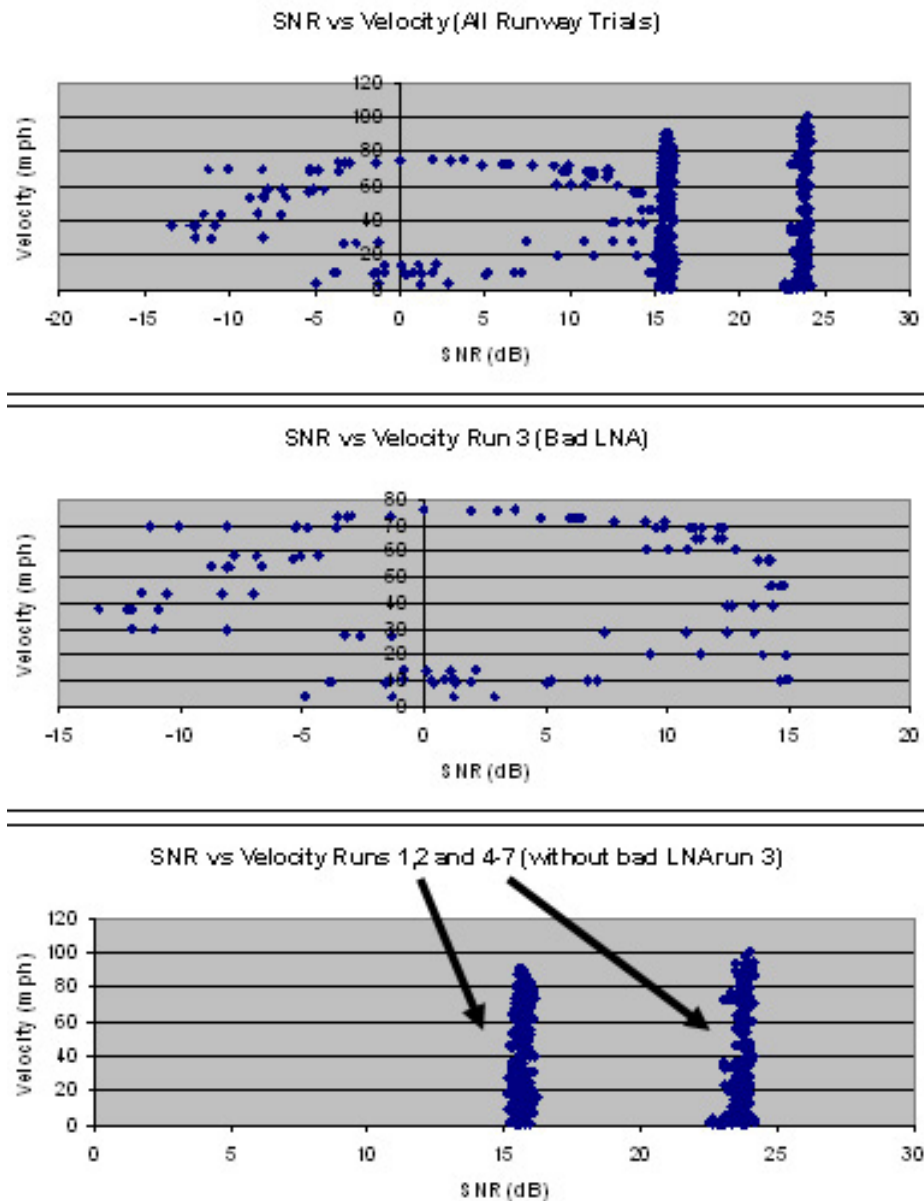


Figure 52. SNR Received During Runway Trials

During the same week at Camp Roberts, Marine Corps Captain Francisco Caceres was conducting TNT thesis research with the Dismounted Data Automatic Communications Terminal (D-DACT). D-DACT is a ruggedized PDA with an extended battery life and PCMCIA Type II slot. Cpt Caceres's testing was directed at utilizing a PCMCIA SECNET 11 NIC to access the wireless medium.

In 15 minutes, experimenters loaded the 802.20 Windows Mobile Edition drivers, installed MS Portrait and placed the D-DACT on the 802.20 network (Fig 53). Experimenters conducted MS Portrait calls from the D-DACT to another iPAQ and a laptop. However, the SD camera could not be installed as it required an SD slot extender which the group did not have.



Figure 53. D-DACT 802.20 Driver and Software Upload

## **V. NECESSARY ADAPTATIONS TO COTS**

### **A. INTRODUCTION**

This chapter will outline the necessary steps that must be taken in order to make this technology a viable solution for leading edge military communications.

### **B. NECESSARY ADAPTATIONS TO COTS EQUIPMENT**

Unlike 802.16, the IEEE 802.20 standard does not require changes to its use of frequency and encryption, nor does it require an antenna pointing mechanism. These problems with 802.16 have been noted in previous NPS testing and were highlighted specifically in the thesis by Captain Munoz, USMC and Captain Guice, USMC. [Ref 17] The technology and current equipment setup may be viable as-is for installation onboard a Navy vessel or military installation. There are a few changes to the physical setup of the network that should be pursued in order to easily integrate this technology with military field deployment.

#### **1. Base Station Size**

Although the current size of the indoor and outdoor BS's are well within the size and weight limitations of a military Humvee or other field vehicle, it is infeasible for deployment in the field of operations. The size of the unit should be reduced as much as possible to facilitate its portability and ability to blend into the array of military equipment present, so as not to identify itself as the leading communication target. A vehicle the size of the COLT could be successfully implemented only after a given area has been secured.

Flarion Technologies has stated that the company is currently pursuing the creation of a PICO cell to provide a solution to the size problem. It is expected that the PICO cell will be the size of a large briefcase and could provide BS functionality, albeit at a much smaller, and yet unknown geographical footprint and weight. This smaller size BS should be more practical for deployment into a Humvee and may be of sufficient weight to be man-portable in the field.

## **2. Ability to MESH Network Cards**

As per the mandate of the Center for Network Innovation and Experimentation (CENETIX), NPS has been tasked by school sponsors to provide interdisciplinary studies of multiplatform tactical networks, Global Information Grid connectivity, collaborative technologies, situational awareness systems, multi-agent architectures, and management of sensor-unmanned vehicle-decision maker self-organizing environments, to include MESH networks. [Ref 22]

Military entities foresee a need for network cards to provide the ability to communicate with one another in the event that the BS were eliminated by enemy fire, especially given its' high-value-asset target rating. NPS is currently in the early stages of conducting research with ITT Mesh to validate their ability to provide this function. The current 802.20 system is a pure hub-and-spoke system meaning all network communications from the mobile user must first travel through the corresponding BS. If the BS were to succumb to enemy fire, all network connectivity in that area would be lost. The system would be much more valuable to a mobile unit if the cards were also able to communicate with one another at a given distance in the event of BS failure. The MESH functionality is achieved when enough network cards are able to "see" each other and then self create a virtual "chain" linking members of the unit for communication. At issue is whether or not the cards could be coded to default to the BS in normal network usage and then automatically switch to MESH functionality during BS failure.

## **C. STANDARDIZATION OF IEEE 802.20 TO LOWER COSTS**

The DoD is bound by the restraints of the Joint Technical Architecture (JTA) for integrating information technology solutions for network communications. One of the metrics for the JTA requires that solutions be standards based. Progress may be realized in this aspect by the recent acquisition of Flarion Technologies by QUALCOMM Incorporated on 11 August, 2005. [Ref 23] QUALCOMM is the current chair of the IEEE 802.20 Working Group and had been the lone dissenter in approving the technology for standardization. It is expected that with the acquisition, QUALCOMM will be able to produce the equipment necessary to implement FLASH-OFDM technology at a much lower cost than previously quoted and will push for standardization. The current cost

structure of FLASH-OFDM equipment is as follows on a per unit basis and is further delineated in Appendix D.

- Indoor Base Station- \$135,000
- Outdoor Base Station- \$155,000
- PC Card- \$375
- Desktop Modem- \$475
- AAA w/Oracle Database- \$25,000
- EMS w/HPOpenView- \$30,000

The OCTO office in Washington, D.C. has a network of 10 RadioRouter BS's that cover the entire metropolitan area of the city at a contracted cost of just over \$3 Million which includes all equipment, setup, licenses and maintenance.

#### **D. SUMMARY**

Our research has shown that this solution can serve many applications with the added robustness of user mobility at DSL speeds. The adaptations described above would further enhance the utility of 802.20 by allowing it to be easily integrated with highly mobile units at the leading edge of military force projection. Once the WG approves standardization, it is expected that the cost of the system implementation will lower dramatically to a level much more affordable for individual military commands, including NPS.

THIS PAGE INTENTIONALLY LEFT BLANK

## **VI. CONCLUSIONS**

### **A. FINDINGS**

Our research on IEEE 802.20 was focused on the networks' ability to provide network connectivity to mobile users at a level comparable to DSL in order to satisfy the requirements of JTRS as it applies to the specifications of the WNW. Mobile service is a feature that has yet to be accomplished via any other wireless technology currently on the market. The intent of this thesis was to investigate the viability of 802.20's network performance when applied as a "last mile" solution in a tactical coalition environment as modeled by a series of TNT experiments.

#### **1. Wireless Networking Requirements**

The requirements of the WNW as mandated by the JTA are successfully met by 802.20 according to our investigation in this thesis. The JTA mandates that future DoD C4I systems operate in accordance with the following metrics: interoperability, maturity, implementability, publicly available, non-proprietary and network centric. Our testing highlighted the interoperability, network centricity and implementability of this publicly available technology. QUALCOMM Incorporated's recent purchase of Flarion Technologies should aid in the emergence of FLASH-OFDM's maturity and eliminate its' appearance as solely a proprietary solution. The ability for 802.20 to provide DSL capable connectivity to highly mobile users at a frequency ideal for through-wall penetration is superior compared to WNW and other tactical data networking waveforms. The size of the BS equipment needs to be reduced dramatically in order to make this a more viable solution for field operations.

#### **2. FLASH-OFDM**

FLASH-OFDM is vertically layered across the network, link and physical layers of the OSI model, an implementation that utilizes a non-contention MAC together with OFDM. This differs greatly from 802.16's contention based MAC where multiple MACs are used to control multiple Physical layers, creating a large internetworking problem that has yet to be overcome to enable mobility in 802.16 deployed networks. FLASH-OFDM allows for the support of many low bit rate dedicated control channels, the use of which enables the system to distinguish request priorities of each active user. This system can

rapidly schedule the active users between all MAC states. FLASH-OFDM incorporates the necessary changes to account for user degree of mobility, required data rates, services to be supported, number of users to be supported, and the environment the system will be used in. FLASH-OFDM is ideal for leading edge military connectivity because of its ability to provide exceptional low latency data rates with an added capability to seamlessly handoff between network sectors.

### **3. Optimal 802.20 Configuration**

Flarion Technologies currently employs their networks in any licensed bandwidth up to 3.5 GHz needing only 1.25 MHz of paired radio spectrum. 802.16 equipment is currently available in the license-exempt band of 5.8 GHz. Previous TNT experimentation has advanced the hypothesis that the 700 MHz frequency band is an ideal frequency for military communications due to its unique ability to provide through-wall signal penetration. Our testing solidified this hypothesis as network connectivity and successful voice, video and data transmission were successfully sent when mobile users were located in various structures in Washington, D.C. and MOUT city at Fort Ord. These structures included the marble Rotunda of the U.S. Capitol building, an elevator located in the null region of the antenna, a galvanized-steel sewer pipe, and a mock prison cell located four levels into the building. Additionally, this frequency was able to provide NLOS capabilities in the very challenging terrain of Camp Roberts at a distance of over 2 miles. During this testing, the BS was located in the COLT vehicle with a deployed antenna height of 42 feet. It is important to note that our testing distances were comparable to the distances successfully tested by previous 802.16 TNT experiments. The main difference between the two sets of tests is that the 802.20 testing was collected while traversing the terrain in a mobile vehicle. The 802.16 links at 2 miles were completed once fixed antenna sites were set up and linked back toward the Camp Roberts NOC, a feat which took approximately 45 minutes to complete.

### **4. COLT Vehicle**

All field testing was completed with the COLT vehicle firmly established at the MOUT facility and Camp Roberts. The vehicle had a retractable antenna, BS and necessary power supply integrated into its design in order to establish a mobile network at any location. It is not feasible to test the COLT while in motion in its current physical



setup. Mobile vehicle testing may be conducted once the size of the BS is condensed into a more manageable size for military ground vehicles. Flarion testing has been done with the BS located in an aerial asset providing a downward network footprint. We were unable to conduct this test again due to the size of the equipment given the current payload capacities of NPS UAVs.

## **5. System Costs**

The cost to integrate 802.20 into an LOE or field deployment may appear steep at first glance when compared to current costs of an 802.16 BS. It is important that the purchaser realize that there is a vast difference between the capabilities of an 802.20 BS and that of an 802.16 BS and these capabilities are what make up the cost differential. Current company price quotes to NPS have been listed in the previous chapter. A more detailed description of actual costs is supplied in Appendix D.

Unlike 802.16, an 802.20 BS is capable of controlling all mobile users associated with the BS in a 3-sector configuration. The network operator would need three 802.16 AN-50's in order to accomplish this same design at a cost of approximately \$15,000 per AN-50. Each 802.16 user also needs an AN-50 in order to join the network, whereas a "mobile" user in 802.20 needs only the \$375 PC card.

## **6. Recommendations and Lessons Learned**

The 802.20 standard is an excellent solution for future development toward the wideband networking standard for military data communication needs. The two areas in need of revamping in order to provide a truly robust "militarized" solution are a reduction in equipment size and an added capability for "MESHING" network cards. These recommended adaptations would greatly enhance the capability of 802.20 to be integrated into a more hostile and mobile environment as per military needs.

The OCTO office in Washington, DC has indicated a willingness and strong desire to continue working with NPS students to test and stress their 700 MHz network. This is a unique and relatively cost effective way for NPS to continue to obtain necessary data for 802.20 network integration. If NPS pursues this opportunity, it would behoove them to send a minimum, six-man team for data collection. Mobility testing with just two individuals was difficult given that one person was always necessary for driving, thus

making him incapable of participating in the data collection process. A six-man team would be better suited to take two cars of testers throughout the city to properly emulate mobile-user to mobile-user or mobile-user to NOC communications as is done with the TNT testbed. Each team should be granted the capability of renting an SUV in order to meet space and power requirements for the testers. Our testing was accomplished with a Fullsize car which was incapable of powering the three laptops that we utilized for testing, needing constant replacement of the vehicles cigarette lighter fuses. A properly equipped modern SUV should have integrated power outlets located throughout the vehicle. The six-man team should arrive on a Monday morning in order to meet the OCTO officials who will oversee NPS testing. The OCTO personnel will then distribute necessary network cards and brief the members on network locations and broadcast limitations. Testing can then be done throughout the week with the final day designated for returning all OCTO equipment. Recommended test equipment and programs are listed below in Appendix E.

## **B. FURTHER RESEARCH**

The following section provides a brief description of follow-on research possibilities and their associated research questions.

### **1. BS in an Aerial Asset**

Company testing has included placing a BS in an aerial asset and providing a downward footprint for network connectivity, but no testing of this nature has yet been done for military specific applications or scenarios. This area of research can apply specifically to the “last mile” solution of network connectivity as an aerial asset may be best suited for extending network reachability to hostile areas. The current size of the BS equipment would require an aerial asset of sufficient size and payload capacity to be employed in the testbed. At issue would be the size of the network footprint at various aircraft altitudes and speeds to measure latency, throughput and effects on through-wall capabilities. Additionally, network operators should then investigate the ability to extend the BS network from a ground BS to the aerial BS and measure handoff capabilities between assets utilizing the two available sectors.

## **2. Integrating 802.20 into Satellite Communications**

Flarion Technologies has stated that this technology is capable of being utilized for satellite backhaul connectivity but has not yet pursued this from a physical standpoint. It is hypothesized that network latency will be improved by using this technology in conjunction with satellite systems. At issue will be the actual capabilities and latency improvements seen in this implementation.

## **3. 802.20 Vulnerability Testing**

The greatest concern with a full implementation of wireless technology into military communications rests with information assurance. This thesis has ascertained that the technology is capable of providing the airlink to leading edge operations but further research is necessary to determine all security and vulnerability issues related to military applications.

## **4. Application to Collaborative Efforts for Coast Guard**

NPS has conducted various research on collaborative wireless technologies as they apply to aiding the U.S. Coast Guard in missions in support of Homeland Defense. The most recent series of TNT experiments tested the validity of 802.16 as a sea-to-shore network solution with varying degrees of success. Further research of 802.20 capabilities at the 700MHz frequency in this scenario is warranted in order to compare more succinctly to 802.16.

## **5. Utilizing 802.20 by a UAV**

A wireless camera on the 802.20 network was attached to an aerial balloon at an altitude of 400ft during research conducted for this thesis; however no testing was done in conjunction with UAVs. The “last mile” of military operations is frequently extended by a UAVs’ flight-distance capabilities. It is imperative that research between 802.20 and UAVs be conducted in order to ascertain the proper antenna-network configurations in order to achieve maximum “last mile” reachability.

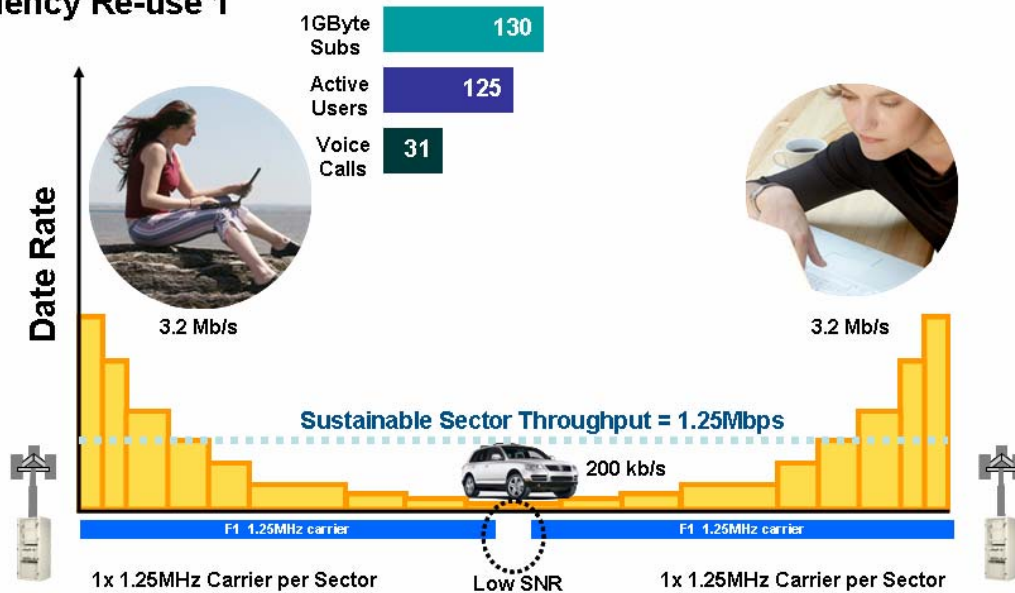
## **6. FLEXBAND**

Flarion Technologies was due to unveil their new FLEXBAND technology this fall, an event which ultimately led to Qualcomm’s acquisition of the company. Flexband is configured as an N=3 solution as opposed to the N=1 setup currently deployed by the company. This change allows more “active” mobile users per sector and decreases the

relevant sNR of each signal. In a fully supported 5MHz multi-carrier system, voice calls increase to 186 per sector and data rates increase to 15.9Mbps peak and 6Mbps sustainable. A single 1.25MHz Flexband carrier sector will be able to deliver peak downlink rates of 5.3Mbps (2.5Mbps sustainable) and an uplink rate of 1.8Mbps (800kbps sustainable at the cell edge). [Ref 24] Flarion Technologies, prior to Qualcomm's acquisition, had stated that NPS could receive the Flexband enabled RadioRouter BS's when funding became available. The equipment has not yet been released and therefore testing on it has not yet been completed. The capabilities comparison between Flexband and the current setup is illustrated in the two figures below.

## FLASH-OFDM® Today

### FLASH-OFDM 1.25MHz Frequency Re-use 1 N=1



\* Copyright Flarion Technologies

Figure 54. Current FLASH-OFDM Deployment [Ref 24]

# FLASH-OFDM® Flexband™

**Flexband 5MHz  
Frequency Re-use 1  
N=1**

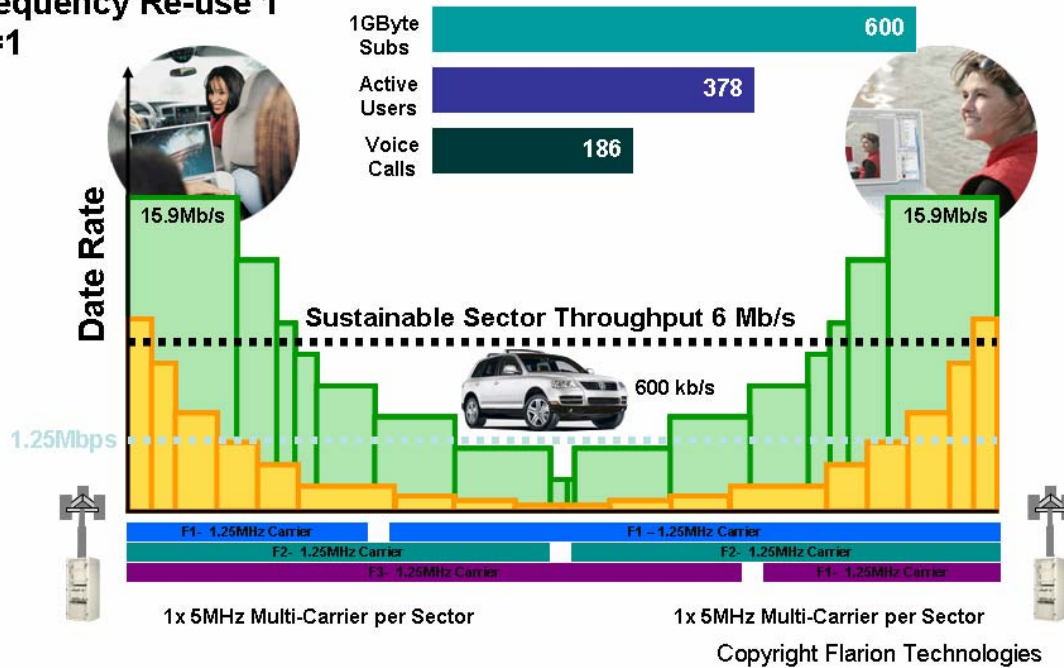


Figure 55. FLEXBAND DEPLOYMENT [Ref 24]

## C. SUMMARY

Our research found that FLASH-OFDM, implemented specifically at the 700 MHz frequency, provides a highly data-capable airlink with unique through-wall penetration capabilities robust enough for military “last mile” network connectivity needs. The few adaptations listed in the previous chapter would permit this technology to be more easily implemented into military applications to address current gaps in tactical radio systems while meeting the requirements of FORCEnet and WNW. This technology compliments and extends fixed broadband research already completed by NPS as part of TNT and when applied in conjunction with 802.16 provides a high bandwidth solution capable of extending a military network by many miles in the most challenging environments.

THIS PAGE INTENTIONALLY LEFT BLANK

## **APPENDIX A    OCTO TNT TEST SCENARIOS**

### **1.    TESTING OVERVIEW AND EQUIPMENT**

#### **Naval Postgraduate School Field Experiment TNT 05-02 (802.20)**

LCDR Bill Parrish and LT Dan Tovar will be traveling to Washington DC to conduct experiments on the 802.20 OFDM network established for the Office of the Chief Technology Officer (OCTO) by Flarion Technologies in support of their thesis:

Tactical Wireless Networking In Coalition Environments:  
Implementing an IEEE 802.20 Wireless End-User Network utilizing  
FLASH-OFDM to Provide a Secure Mobile Extension to Existing WAN.

Date of travel will be from 19 March 2005 to 26 March 2005. All research will involve field experiments similar to NPS's TNT experiments of 05-02.

#### **Pre Experiment Setup:**

##### **20 MAR**

Experimenters will join an 802.11 network provided by the hotel in Washington DC and will determine baseline battery drainage for all equipment on the .11 network for comparison with the .20 network.

All equipment will be tested prior to arrival in Washington DC

Upon arrival in DC, experimenters will determine appropriate locations for testing based on accessibility, environmental exposure and safety.

#### **EQUIPMENT CHECKLIST**

- Panasonic Toughbooks Model TF-73
- 2 battery expansion packs with PCMCIA slots
- 2 PDA's IPAQ HP4700
- 2 cradles
- 2 chargers

- 2 HP IPAQ Bluetooth GPS Receivers
- 2 Tacticomps
- 2 chargers
- 2 IP Remote Cameras (remote pan-tilt-zoom)
- 1 Video Camera
- Wireless Cisco/Linksys 802.11B/G Router

## **2. SCENARIO 1**

### **Experiment 1. Component Performance for Force Connectivity**

#### **Assumption:**

SOF lack critical capabilities to effectively conduct network-centric operations in urban and near-urban environments. Shortfalls include availability of shared situational awareness, high bandwidth and persistent communications at tactical level, ability to identify and track enemy personnel and equipment, collaborative tools and visualization to more effectively conduct highly coordinated combined U.S. and coalition activities. Secure communications at the tactical level are needed.

#### **Basic Requirements:**

- Maintain local C3I and global C3I for experiment team.
- GC3I connectivity required from experimenters to TOC.
- Experiment/Demonstration Technologies
- Mobile vehicle(MV) that has both LC3I and GC3I; e.g. reliable and wideband reach to experimenter and TOC/Command Post.
- Effective intra-team communications with reachback to TOC (PDA and Laptops with access to 802.20 network)
- Short haul wireless network: 802.20



Note: Through-wall performance characteristics will be evaluated in Scenario #2

**Capabilities and Network Building Blocks:**

- MV equipped with 802.20 laptop with SA, GPS and Solar Winds Engineering trial edition, and 802.20 enabled PDA. Cell phones utilized for backup coordination.
- Experimenter equipped with 802.20 Laptop with SA and Solar Winds Engineering trial edition, FMDM, and Netpersec
- Experimenter may be non-line-of-sight with LRV and LRV may be non-line-of-sight with TOC.
- OCTO 700 MHz network in Washington DC.
- FLARION Network Cards in Tacticoms, PDA's and Laptops.
- IP camera located in remote location and controlled by MV .
- OCTO TOC/Command Post with short-haul 802.20/OFDM connectivity to experimenters, sector antennas for connectivity.

**Experiment Variables:**

State Variables

- Distance between experimenter and MV
- “Visibility” between experimenter and MV (LOS, OLOS, NLOS)
- Distance between MV and OCTO TOC/Command Post
- “Visibility” between MV and OCTO TOC/Command Post
- Distances between remote sensors and MV (LOS)
- Proximity and distance to closest sectional antennas.

**Environmental Variables:**

- Weather
- Background wireless traffic

- Measures of Performance
- 802.20/OFDM networks performance (throughput, packet loss, latency) as function of distance and “visibility”.
- Network system performance (multiple criteria evaluation)

### **Experiments:**

**21 Mar.** (TOC will be located at OCTO)

**0900** Meet at OCTO for initiation, load/troubleshoot laptop, and PDA. Verify all connections between mobile nodes.

### **1A. Short-Range LOS Performance – 802.20**

**1200** Testers will evaluate short range connection from within OCTO in sight of each other

#### **EVENT 1**

Experimenter 1 will leave OCTO building and proceed to Judicial square to initiate Communication with Experimenter 2 via Microsoft Portrait. Once connection is complete, experimenters will transfer files and will run FMDM, Qcheck, and Netpersec to test/record network performance.

#### **EVENT 2**

Experimenter 1 will initialize SA client to demonstrate 802.20’s ability to deliver SA traffic. Experimenter 2 located in OCTO will run SA server.

**22 Mar.**

**1B. Operations with LOS between Experimenters in MV**

**EVENT 1**

MV and experimenters deploy to northernmost Base station isolated from other sectors of the OCTO network. Drive tests will be performed on a run from southernmost footprint of the antenna to the northernmost footprint. Drive test will utilize two 802.20 laptops, and two 802.20 PDA's. Connectivity drops will be noted by distance from tower for each device. The two laptops will be both be mobile within the same sector and will communicate to each other via file downloads initiated from one and transferred to the other. FMDM, Qcheck, and Netpersec will be utilized to collect/record network data. Additionally, one laptop will access streaming video from NASA website as a visual demo of connectivity. Vehicle speed will also be annotated.

**1C. 802.20 (NLOS) Throughput vs. Range**

(Note: through-wall capability and LPD characteristics are in scenario 2)

**EVENT 1**

Experimenters will embark in MV and will maneuver through inner city Washington DC in a NLOS condition to network towers being accessed. FMDM, Qcheck, and Netpersec will be utilized to collect/record network data. Additionally, experimenters will utilize the client test of Miperf to flood the network for maximum data statistical collection. During drive, experimenters will access a web-enabled DLink camera (located in OCTO office). Microsoft Encoder will be used to record the desktop view of this test.

**EVENT 2**

Experimenters will embark in MV and will redo Event 1 of section 1B. On this run, experimenters will utilize Miperf to flood the northernmost base station without acquiring a signal from an additional station. Runs will be made on both north and south runs utilizing Miperf, FMDM and Netpersec to record data.

### **EVENT 3**

Experimenters will do a high speed highway test traversing a minimum of 3 base stations in order to force seamless handoffs between the stations at highway speed in the southeastern side of Washington DC. FMDM, Miperf and Netpersec will be utilized to collect and generate traffic.

### **3. SCENARIO 2**

#### **ON-THE-MOVE NETWORK PERFORMANCE**

##### **Assumption**

Future SOF and Marine Corp operations will require the use of an on-the-move network between multiple, dissimilar manned and unmanned assets to include air to provide situational awareness and enhanced warfighting capabilities. These assets could include UAVs (micro, small, tactical, strategic), manned and unmanned aircraft, and squad personnel with advanced video/audio capabilities. Some assets might be permanent while others may rapidly join and leave the area. Network mobility is a necessity driven by target mobility. An integrated network for all assets and the TOC is essential for providing situational awareness, a common operational picture, and collaborative behavior. In the near future this will also permit autonomous, collaborative behavior of large numbers of UAVs and other assets utilizing a minimum number of operating personnel.

##### **Basic Requirements**

- Local C3I using multiple assets with rapidly changing participants and network node locations
- Network that permits control of multiple assets as well as rapid insertion of new assets
- Situational awareness and common operational picture

### **Experiment/Demonstration Technologies**

- “On-the-move” network.
- Local and remote location SA from multiple assets

### **Capabilities/Assets**

- All 802.20 tactical equipment connected to 802.20/OFDM network
- TOC and MV and experimenter with SA

### **Experiment Variables**

#### **State Variables**

- Time and space variations of network node locations
- Distance of nodes beyond FOV of TOC

#### **Environmental Variables**

- Weather
- Wireless traffic (non 802.20)

### **Measures of Performance**

- Ability of network to rapidly adapt to number of nodes, location of nodes, and rate-of-change of location
- Quality and effectiveness of operating team communications and information flow
- Reliability and quality of asset video
- Reliability and “usability” of SA at local TOC and MV

### **Scenario**

**24-25 MAR**

To be tested is the networks ability to provide “through-wall” user access in an urban area and mobile access at highway speeds.

### **EVENT 1**

Network availability will be initially tested at the OCTO facility in Washington DC, a physical location of one of the base stations. It is noted that the building itself is located in the null region of the antennas, however user access has been achieved

Experimenters will take part in network sector capacity testing. Experimenters will utilize Miperf both as the server and client to flood segments of the DC network. Comparisons of rates received and transmitted for both individual and group will be recorded. Experiment requires at least six members, two per sector.

### **EVENT 2**

Through-wall testing will be conducted during a downtown walk from the Capitol building toward the OCTO building. Experimenter will enter the Capitol building, the Department of State building and then the OCTO building while on the 802.20 network and will download large files for testing.

### **EVENT 3**

Experimenters will conduct connectivity and DL/UL testing while traveling at highway speeds. LRV will traverse the George Washington HWY will mobile users conduct Iperf testing and log SNR.

## **APPENDIX B      MOUT FACILITY TNT TEST SCENARIOS**

### **Scenario   ON-THE-MOVE   NETWORK   PERFORMANCE   AT   MOUT FACILITY**

#### **Assumption**

Future SOF and Marine Corp operations will require the use of an on-the-move network between multiple, dissimilar manned and unmanned assets to include air to provide situational awareness and enhanced warfighting capabilities. These assets could include UAVs (micro, small, tactical, strategic), manned and unmanned aircraft, and squad personnel with advanced video/audio capabilities. Some assets might be permanent while others may rapidly join and leave the area. Network mobility is a necessity driven by target mobility. An integrated network for all assets and the TOC is essential for providing situational awareness, a common operational picture, and collaborative behavior. In the near future this will also permit autonomous, collaborative behavior of large numbers of UAVs and other assets utilizing a minimum number of operating personnel.

#### **Basic Requirements**

- Local C3I using multiple assets with rapidly changing participants and network node locations
- Network that permits control of multiple assets as well as rapid insertion of new assets
- Situational awareness and common operational picture

#### **Experiment/Demonstration Technologies**

- “On-the-move” network.
- Local and remote location SA from multiple assets

### **Capabilities/Assets**

- All 802.20 tactical equipment connected to 802.20/OFDM network
- TOC and MV and experimenter with SA

### **Experiment Variables**

#### **State Variables**

- Time and space variations of network node locations
- Distance of nodes beyond FOV of TOC

#### **Environmental Variables**

- Weather
- Wireless traffic (UWB, non 802.20)

#### **Measures of Performance**

- Ability of network to rapidly adapt to number of nodes, location of nodes, and rate-of-change of location
- Quality and effectiveness of operating team communications and information flow
- Reliability and quality of asset video
- Reliability and “usability” of SA at local TOC and MV

### **Scenario**

#### **16-18 May**

To be tested is the networks ability to provide “through-wall” user access in an urban area utilizing the Military Operations in an Urban Terrain (MOUT) facility located at Fort Ord.

Network availability will be provided by the Cell on Light Truck (COLT) vehicle provided by Flarion Technologies. The vehicle is a highly mobile network provider which contains all elements necessary for a wireless 802.20 network to include: omni-directional antenna, basestation, AAA server and a connection to the backhaul network.



Network availability and capability will then be tested throughout the MOUT facility beginning at the buildings closest to the COLT vehicle and moving outward.

Network availability will be tested in a highly mobile environment throughout the facility. Experimenters will rapidly enter and exit the MOUT buildings utilizing a vehicle to traverse the facility and will determine connectivity as a result of speed and distance from the base station. The COLT location will be stationary while the area of coverage and NLOS capabilities are determined.

### **EVENT 1**

Experimenters will establish a working 802.16 link into the MOUT facility, connecting to a pre-existing antenna on R32. This link will require a line of sight shot from R32 to a ridgeline above the MOUT facility. At the ridgeline, experimenters will need two AN-50s, a generator, one sectional antenna pointed at R32 and an omni antenna to connect to the MOUT facility. The link will be completed by placing an Omni antenna at the building nearest the 802.20 COLT vehicle. This Omni will be connected to an AN-50 placed inside the COLT vehicle. Once connected, experimenters will ensure “plug and play” connectivity between 802.16 and 802.20. From the 802.20 side of the network, experimenters will ping servers located at NPS and will utilize VOIP to communicate on the NPS infrastructure.

### **EVENT 2**

Experimenters will utilize a Sony Pan-Tilt-Zoom camera located in the MOUT facility and will continue to access and move the camera using the 802.20 network from a mobile laptop. Testing will be done throughout the facility and again via vehicular travel in and around the MOUT facility until connectivity is lost. Network capability will be demonstrated by the ability to view the video stream from the internet camera at given distances with varying terrain.

### **EVENT 3**

Experimenters will traverse the MOUT facility utilizing handheld PDA's connected to the 802.20 network. They will use Microsoft Portrait to communicate with each other in and around the buildings. Network capability will be demonstrated by the

ability for the experimenters to communicate effectively. Testing will specifically be done at two points of interest as identified by SOCOM. The first location will be inside a basement and the second will be inside a “mock” prison cell well within a windowless MOUT building.

#### **EVENT 4**

Experimenters will drive rapidly through the facility and surrounding terrain utilizing a laptop connected to the 802.20 network. Measures of performance will be measured using FMDM, Netpersec and Miperf. Network connectivity will be measured in relation to distance and speed.

## **APPENDIX C      CAMP ROBERTS TNT TEST SCENARIOS**

### **1.      SCENARIO 1 TNT FIELD DEMONSTRATION**

#### **Assumption**

SOF lack critical capabilities to effectively conduct network-centric operations in urban and near-urban environments. Shortfalls include availability of shared situational awareness, high bandwidth and persistent communications at tactical level, ability to identify and track enemy personnel and equipment, collaborative tools and visualization to more effectively conduct highly coordinated combined U.S. and coalition activities. Secure communications at the tactical level are needed.

#### **Basic Requirements**

- Maintain local C3I and global C3I for experiment team.
- GC3I connectivity required from experimenters to TOC.

#### **Experiment/Demonstration Technologies**

- Web enabled camera attached to 802.20 network.
- Effective video transmission with reachback to TOC
- Short haul wireless network: 802.20

#### **Capabilities and Network Building Blocks**

A web enabled camera attached to the 802.20 network will be installed and launched via an aerial balloon. Connectivity will be established and maintained throughout demonstration to include sending suitable footage of the demonstration back to the TOC. Balloon will be located at a distance of 4 miles from the TOC at an elevation of 1000ft.

Flarion 700 MHz network via COLT

FLARION Network Card in the pad and a 3db gain omni-antenna.

#### **Experiment Variables**

### **State Variables**

- Distance between COLT and camera
- “Visibility” between COLT and camera (LOS, OLOS, NLOS)
- Distance between camera and TOC/Command Post
- “Visibility” between camera and TOC/Command Post

### **Environmental Variables**

- Weather
- Background wireless traffic

### **Measures of Performance**

- 802.20/OFDM mesh networks performance (throughput, packet loss, latency) as function of distance and “visibility”.

### **Experiments**

#### **25 May.**

**0900** Re-establish camera connectivity from setup of the prior day. Camera is to be connected constantly throughout the demonstration with picture stability and quality used as a visual measure of effectiveness of the experiment given the terrain of the area, cameras optical capabilities and distance between network components.

## **2. SCENARIO 2 ON THE MOVE NETWORK PERFORMANCE**

### **Assumption**

Future SOF and Marine Corp operations will require the use of an on-the-move network between multiple, dissimilar manned and unmanned assets to include air to provide situational awareness and enhanced warfighting capabilities. These assets could include UAVs (micro, small, tactical, strategic), manned and unmanned aircraft, and squad personnel with advanced video/audio capabilities. Some assets might be permanent while others may rapidly join and leave the area. Network mobility is a

necessity driven by target mobility. An integrated network for all assets and the TOC is essential for providing situational awareness, a common operational picture, and collaborative behavior. In the near future this will also permit autonomous, collaborative behavior of large numbers of UAVs and other assets utilizing a minimum number of operating personnel.

### **Basic Requirements**

- Local C3I using multiple assets with rapidly changing participants and network node locations
- Network that permits control of multiple assets as well as rapid insertion of new assets
- Situational awareness and common operational picture

### **Experiment/Demonstration Technologies**

- “On-the-move” network.
- Local and remote location SA from multiple assets

### **Capabilities/Assets**

- All 802.20 tactical equipment connected to 802.20/OFDM network
- TOC and MV and experimenter with SA

### **Experiment Variables**

#### **State Variables**

- Time and space variations of network node locations
- Distance of nodes beyond FOV of TOC

#### **Environmental Variables**

- Weather
- Wireless traffic (UWB, non 802.20)

## **Measures of Performance**

- Ability of network to rapidly adapt to number of nodes, location of nodes, and rate-of-change of location
- Quality and effectiveness of operating team communications and information flow
- Reliability and quality of asset video

## **Scenario**

### **26 May**

To be tested is the networks “range” ability to provide user access in an area of varying geography and vegetation utilizing Camp Roberts.

Network availability will be provided by the Cell on Light Truck (COLT) vehicle provided by Flarion Technologies. The vehicle is a highly mobile network provider which contains all elements necessary for a wireless 802.20 network to include: omni-directional antenna, BS, AAA server and a connection to the backhaul network.

Network availability and capability will then be tested throughout Camp Roberts starting at the COLT vehicle and moving outward until connectivity is lost.

Network availability will be tested in a highly mobile environment throughout the base. Experimenters will rapidly enter and exit the network utilizing a vehicle to traverse the facility and will determine connectivity as a result of speed and distance from the base station. The COLT location will be stationary while the area of coverage and NLOS capabilities are determined.

### **EVENT 1**

Experimenter will enter the network by placing a network card into his laptop and proceed to utilize Miperf to flood the network and receive packet throughput information. Testing and recording will be done utilizing Flarion’s Mobile Diagnostic Monitor to record all pertinent information to include; SNR, throughput, GPS data, etc. Experimenter will then proceed around Camp Roberts via vehicle to ascertain geographical limits of the COLT 802.20 network.

## **EVENT 2**

Experimenter will enter the network via network card and proceed to utilize a Sony Pan-tilt-zoom camera attached to the network via a Personal Access Device (PAD). Network capability will be determined via the ability to receive quality video and audio while traversing the camp. The physical limits from Event 1 will be used to determine vehicular path.

## **EVENT 3**

Experimenters will traverse Camp Roberts utilizing handheld PDA's connected to the 802.20 network. They will use Microsoft Portrait to communicate with each other in and around the facility. Network capability will be demonstrated by the ability of the experimenters to communicate effectively. Physical limits from Event 1 will be used to determine experimenter's locations. The experimenters should be at the two furthest locations possible for transmission.

## **EVENT 4**

Experimenters will drive rapidly through the facility utilizing a laptop connected to the 802.20 network. Measures of performance will be measured using FMDM, Netpersec and Miperf. Network connectivity will be measured in relation to distance and speed. Experimenters will simulate a rapid military movement utilizing solely the 802.20 network for communications. Experimenters will utilize Camp Roberts airfield to make a high speed run and demonstrate networks ability to stream video and voice without any apparent degradation in quality at speeds in excess of 90mph (90mph is the claimed speed threshold of the forthcoming 802.16e standard, 802.20 has been successfully tested at speeds of up to 300mph).

## **EVENT 5**


Experimenters will demonstrate the ease of denying user access. Experimenters will have three laptops accessing the network. They will randomly pick one network card to have been compromised and will notify the COLT at which point network access will be denied. All three laptops will be downloading information. To be noted is the networks ability (time) to end the transmission.

**The above experiments will not highlight the capability of the technology to seamlessly handoff between two base stations. Once more than one base station has been acquired, this can be demonstrated.**



## APPENDIX D FLASH-OFDM PRICE QUOTES TO NPS

### 1. 3 SECTOR SYSTEM

Price Quotation			
Ship To:			
Date 06-3-05			
Attn:		Bedminster One	
Office:		135 Route 202/206 South	
		Bedminster, NJ 07921	
Bill to:			
Terms	This Quote is Valid For:	FOB	Lead Time ARO
Net 30	30 Days	Origin	
Part #	Description	Price	Qty
101-0170-004	Radio Router Base Station Chassis 19" - 3 sector - indoor	\$135,000.00	1
RRSS-1	Flarion Radio Router Software -per Radio Router (included)	\$7,500.00	1
RRSM-1	Flarion RadioRouter Software Maintenance-per Radio Router ( Annual) ( Included for the first year)	\$7,500.00	1
		Total	\$135,000.00
NOTE: <b>RRSS-1 RTU for year one - included in Radio Router price</b> <b>RRSM-1 - for year one - included in Radio Router price</b> <b>Radio Router comes with a one-year warranty.</b> <b>For outdoor enclosure add \$20,000 per Radio Router to the base station price</b>			
Mobiles			
100-145-001	Flash OFDM PC Card	\$375.00	1
100-145-002	Flash OFDM - Desktop Modem	\$475.00	1
		Total	\$850.00
NOTE: <b>Terminal pricing does not include custom branding and packaging</b>			
3rd party software			
RRAAA-1	FUNK Steel-Belted RADIUS AAA server, with Flarion EAP optimization for FLASH-OFDM network, including Oracle Database licence (only one is needed per network)	\$25,000.00	1
		Total	\$25,000.00
NOTE: <b>RRAA -1 pricing does not include h/w platform</b>			
Element Management system			
RREMS-1	Flarion EMS, including Oracle Database licence and HP Openview licence (only one is needed per network)	\$30,000.00	1
		Total	\$30,000.00
NOTE: <b>RREMS-1 pricing does not include h/w platform</b>			
SERVICES			
RRINST-1	Installation and Commissioning (per Radio Router) ( does not include Cell site Antenna mounting and cabling)	\$12,000.00	1
RROPT-1	Network Optimization (per Radio Router)	\$6,000.00	1
		Total	\$18,000.00

<h1 style="margin: 0;">Price Quotation</h1> <p style="margin: 10px 0;">Ship To:</p> <p style="margin: 10px 0;">Date 06-3-05</p> <p style="margin: 10px 0;">Attn:</p> <p style="margin: 10px 0;">Office:</p> <p style="margin: 10px 0;">Bill to:</p>		<p style="margin: 10px 0;"><b>Bedminster One</b></p> <p style="margin: 10px 0;"><b>135 Route 202/206 South</b></p> <p style="margin: 10px 0;"><b>Bedminster, NJ 07921</b></p>
---	--	---

Terms	This Quote is Valid For:	FOB	Lead Time ARO
Net 30	30 Days	Origin	

Part #	Description	Price	Qty	Ext List	Total Price
101-0170-001	Radio Router Base Station Chassis 19" - Omni - indoor	\$90,000.00	1	\$90,000.00	\$90,000.00
RRSS-1	Flarion Radio Router Software -per Radio Router (included)	\$7,500.00	1	\$7,500.00	\$0.00
RRSM-1	Flarion RadioRouter Software Maintenance-per Radio Router ( Annual) ( Included for the first year)	\$7,500.00	1	\$7,500.00	\$0.00
				<b>Total</b>	<b>\$90,000.00</b>
<b>NOTE: RRSS-1 RTU for year one - included in Radio Router price</b> <b>RRSM-1 - for year one - included in Radio Router price</b> <b>Radio Router comes with a one-year warranty.</b> <b>For outdoor enclosure add \$20,000 per Radio Router to the base station price</b>					
<b>Mobiles</b>					
100-145-001	Flash OFDM PC Card	\$375.00	1	\$375.00	\$375.00
100-145-002	Flash OFDM - Desktop Modem	\$475.00	1	\$475.00	\$475.00
				<b>Total</b>	<b>\$850.00</b>
<b>NOTE: Terminal pricing does not include custom branding and packaging</b>					
<b>3rd party software</b>					
RRAAA-1	FUNK Steel-Belted RADIUS AAA server, with Flarion EAP optimization for FLASH-OFDM network, including Oracle Database licence (only one is needed per network)	\$25,000.00	1	\$25,000.00	\$25,000.00
				<b>Total</b>	<b>\$25,000.00</b>
<b>NOTE: RRAA -1 pricing does not include h/w platform</b>					
<b>Element Management system</b>					
RREMS-1	Flarion EMS, including Oracle Database licence and HP Openview licence (only one is needed per network)	\$30,000.00	1	\$30,000.00	\$30,000.00
				<b>Total</b>	<b>\$30,000.00</b>
<b>NOTE: RREMS-1 pricing does not include h/w platform</b>					
<b>SERVICES</b>					
RRINST-1	Installation and Commissioning (per Radio Router) ( does not include Cell site Antenna mounting and cabling)	\$12,000.00	1	\$12,000.00	\$12,000.00
RROPT-1	Network Optimization (per Radio Router)	\$6,000.00	1	\$6,000.00	\$6,000.00
				<b>Total</b>	<b>\$18,000.00</b>

### 3. ANTENNAS AND CABLING

Part #	Description	List Price	Qty	Ext List	%	Total Price
FR65-12-05-DAL2-SP	EMS antenna ( Each one covers one sector)	\$1,500.00	1	\$1,500.00	0%	\$1,500.00
MTG-DXX-20	EMS antenna mounting kit 0, 5, 10 degree ( Each one covers one sector)	\$0.00	1	\$0.00	0%	\$0.00
Total						\$1,500.00
Note: Omni Radio Router in simulcast configuration requires three antenna per tower						

Recommended Antenna Feeder line sizes for length of runs (in feet) and frequency.

Assumed Line Loss: 3 dB

Recommended Antenna Feeder line sizes for length of runs (in feet) and frequency.

Cable Diameter	700 MHz	800 MHz	900 MHz	1.9 GHz	2.1 GHz	3 GHz
1/2"	164	152	138	95	90	73
7/8"	291	270	254	166	156	127
1 1/4"	410	380	355	229	216	173
1 5/8"	498	462	430	274	258	n/a

Recommended Antenna Feeder line sizes for length of runs (in meters) and frequency.

Cable Diameter	700 MHz	800 MHz	900 MHz	1.9 GHz	2.1 GHz	3 GHz
1/2"	50	46	42	29	27	22
7/8"	89	82	77	51	48	39
1 1/4"	125	116	108	70	66	53
1 5/8"	152	141	131	83	78	n/a

dB/100 feet	700 MHz	800 MHz	900 MHz	1.9 GHz	2.1 GHz	3 GHz
1/2"	1.83	1.97	2.17	3.159	3.34	4.09
7/8"	1.03	1.11	1.18	1.809	1.92	2.37
1 1/4"	0.732	0.789	0.84	1.309	1.39	1.73
1 5/8"	0.602	0.65	0.7	1.095	1.165	MAX 2.5 GHz

dB/100 meters	700 MHz	800 MHz	900 MHz	1.9 GHz	2.1 GHz	3 GHz
1/2"	6.01	6.46	7.12	10.365	10.958	13.418
7/8"	3.379	3.642	3.88	5.934	6.299	7.775
1 1/4"	2.402	2.589	2.77	4.295	4.56	5.676
1 5/8"	1.975	2.133	2.29	3.593	3.824	MAX 2.5 GHz

THIS PAGE INTENTIONALLY LEFT BLANK

## **APPENDIX E      RECOMMENDED EQUIPMENT AND SOFTWARE FOR FUTURE TESTING**

The below list contains recommended equipment and software for future testing of 802.20 when utilizing the Washington, D.C. network

### **A.      EQUIPMENT**

Two laptops with available PCMCIA II slot per user

One PDA with battery jacket and PCMCIA II slot per user

One PDA cradle

Two wireless web enabled cameras

One sD camera for PDA per user

Power inverters for rental car to power equipment

Necessary Cat5 cable

Minimum two power strips

One Garmin V GPS per user

Minimum one 3db gain magmount omni antenna per user

### **B.      SOFTWARE**

Flarion Mobile Diagnostic Monitor (fmdm.exe)

Flarion laptop and PDA drivers

Miperf.exe

Microsoft Portrait

Microsoft Encoder

Netpersec

Qcheck

THIS PAGE INTENTIONALLY LEFT BLANK

## APPENDIX F FMDM AND FMLP VARIABLES

The Flarion Mobile Device Manager (FMDM) is a Windows based software tool used for gathering data during drive testing. It is typically loaded on a laptop PC equipped with both a mobile PC card (for communicating with base stations) and a Global Positioning System (GPS) device (for capturing positional information). [Ref 27]

The Flarion Mobile Log Processor (FMLP) is a Windows based software tool for post processing log files generated from the Flarion Mobile Diagnostic Monitor (FMDM). [Ref 28]

### A. FMDM VARIABLES

All names and description sited from Ref 27.

- gpsTime 16:55:46 Format (UTC connected for local time)
- gpsLat Decimal latitude
- gpsLong Decimal longitude
- gpsAlt Altitude (meters)
- networkDate 11/8/2003 Format
- networkTime 16:55:47:174 (HH:MM:SS:Thousandths)
- rx\_pwr Total RSSI in band (dBm)
- tx\_pwr Total Mobile Transmit (dBm)
- bsid0 Receiver 0- Base Station I D(test)
- rx0\_pilot\_pwr Receiver 0 pilot power (dBm)
- rx0\_snr Receiver 0 SNR (dB)
- tx0\_dcch\_backoff Transmitter 0 digital control channel backoff (dB)
- tx0\_sample\_off Transmitter 0 digital sample offset (dB)
- bsid1 Receiver 1- Base Station ID (text)
- rx1\_pilot\_pwr Receiver 1 pilot power (dBm)
- rx1\_snr Receiver 1 SNR (dB)
- tx1\_dcch\_backoff Transmitter1 digital control channel backoff (dB)
- tx1\_sample\_off Transmitter 1 digital sample offset (dB)
- rx\_rate\_arq (Down Link) Post ARQ Receive data rate (bps)
- tx\_rate\_arq (Up Link) Post ARQ Transmit data rate (bps)

- `active_rx`                      Either RX 0 or 1 active indicator
- `active_tx`                      Either TX 0 or 1 active indicator
- `rx_frame_counter`            Total Received Frames (since last connection was made)
- `rx_frame_error`            Total Rx Frames Dropped post-ARQ (since last connection)
- `tx_frame_counter`            Total Transmitted Frames (since last connection)
- `tx_frame_error`            Total Tx Frames Dropped (since last connection)
- `rx_SNR_avg`                  Give consistent smoothing for the SNR. The averaging is done as follows:  $\text{new average} = c * \text{old\_average} + (1-c) * \text{sample}$  The constant for this snr is  $c=255/256$
- `rx_frames_avg`              Average number of frames per segment, which is a measure of the rate option that is used (only updated for segments that are assigned to the mobile)
- `rx_tones_avg`              Average number of tones that are used in slots where the mobile is receiving
- `rx_idle`                      Proportion of the slots such that the mobile is not receiving  
`tx_frames_avg` Average number of frames per segment, which is a measure of the rate option that is used (only updated for segments that are assigned to the mobile)
- `tx_tones_avg`              Average number of tones that are used in slots where the mobile is transmitting
- `tx_idle`                      Proportion of the slots such that the mobile is not transmitting
- `bsip0`                      The IP address of base station sector that rx0 is connected to. In particular, this is the IP address of the baseband unit (BBU)
- `bsip1`                      The IP address of base station sector that rx1 is connected to
- `son_id0`                      The Session-On ID that has been assigned by the base station to receiver rx0 when it is in the "On" state. This value ranges from 1 to 31.
- `son_id1`                      The Session-On ID that has been assigned by the base station to receiver rx1 when it is in the "On" state. This value ranges from 1 to 31.
- `act_id0`                      The Active ID that has been assigned by the base station to the receiver rx0 when it is in the "On" or "Hold" states. This value ranges from 1 to 125.



- `act_id1`                      The Active ID that has been assigned by the base station to receiver rx1 when it is in the "On" or "Hold" states. This value ranges from 1 to 125.
- `rx_0_state`                      The state (e.g., Disconnected, Searching, Access, On, Hold Sleep) of transceiver 0.
- `rx1_state`                      The state (e.g., Disconnected, Searching, Access, On, Hold Sleep) of transceiver 1.
- `mgsm_state`                      The state (e.g., idle, searching, active) of the Mobile Global State Machine, reflecting the Layer 3 connection.
- `mip_state`                      The state (e.g., idle, registered) of the Mobile IP connection.

Note: The Session-On ID and the Active ID are independent of each other. A mobile in the "On" state will have both a Session-On ID and an Active ID, and these are not necessarily the same. A mobile in the "Hold" state, however, only has an Active ID.

## **B. FMLP PROCESSED VARIABLES**

For the computation of the overall statistics, the averaging of quantities that are measured in dB is done using the median function, while the averaging for linear quantities is done using the mean function.

The median Rx SNR and median Rx Pilot Pwr are computed for the log file, corresponding to `active_rx_snr` and `active_rx_pilot_pwr`, which are chosen for each point based on the active receiver.

The median Tx DCCH Backoff is computed for each log file, corresponding to `active_tx_dcch_backoff`, which are chosen for each point based on the active transmitter.

The mean Rx Data Rate and Tx Data Rate are computed for the log file, based on the mean of `rx_rate_arq` and `tx_rate_arq`.

The counters `tx_frame_counter`, `rx_frame_counter` and `tx_frame_error` all increase monotonically. They only decrease if a new connection is made and an internal counter is reset. Note that there are two sets of internal counters, one for each receiver (i.e., `rx0_frame_counter` and `rx1_frame_counter`). Whenever the connection is lost, the counters for the receiver are reset, possibly causing a decrease in the frame counters.

Note that due to the DL frame retransmission algorithm, it is not possible for the mobile to determine whether a frame will be retransmitted again. Hence, if a frame is in a segment that is in error, it gets counted within `rx_frame_error`. But if the frame subsequently shows up, it gets removed from the counter, so that `rx_frame_error` can go up and down in value over time.

Several new columns are created by the process of transforming the collected log file: tx\_frame\_counter\_diff, rx\_frame\_counter\_diff, tx\_frame\_error\_diff, rx\_frame\_error\_diff. These represent the increments to these counters based on the difference in the counter between subsequent data samples in time. These values are zeroed out when an inappropriate value appears.

Note that from tx\_frame\_counter\_diff and rx\_frame\_counter\_diff, it is possible to compute an “instantaneous” rate. This is the number of bits per second that were transmitted corresponding to that data sample. This is adjusted for the time interval between subsequent samples, which gives a number in bits per second for the data rate. The resulting variables are rx\_rate\_instant and tx\_rate\_instant, which are given in the transformed\_collected file. These are more accurate representations of the throughput as they do not include the effects of smoothing that are present in rx\_rate\_arq and tx\_rate\_arq.

The post-ARQ frame error rate is computed over the whole file, so as to remove the effect of these local variations. For example, the Rx Post-ARQ FER is computed by taking the total sum of rx\_frame\_error\_diff over the file and dividing by the total sum of rx\_frame\_counter\_diff.

The MBB percentage is the percentage of samples in which the mobile is connected to two base stations.

The drop percentage is the percentage of samples in which the mobile is connected to no base stations. [Ref 28]

## APPENDIX G      OCTO TOWER SPECIFICATIONS

Below table contains the tower list and parameters for OCTO WARN network at time of testing. Each tower has three sectors. Two additional towers have been added to increase coverage.

SiteID	Site Name	Sector ID	Sector Name	Latitude	Longitude	Slope	PlotID	GE (ft)
OCTO241	4th District	OCTO2411	Alpha	38.9637	-77.0273	34	4D1	298
OCTO241	4th District	OCTO2412	Beta	38.9637	-77.0273	102	4D2	298
OCTO241	4th District	OCTO2413	Gamma	38.9637	-77.0273	6	4D3	298
OCTO074	Fletcher Johnson	OCTO0741	Alpha	38.8834	-76.9341	5	FJ1	134
OCTO074	Fletcher Johnson	OCTO0742	Beta	38.8834	-76.9341	74	FJ2	134
OCTO074	Fletcher Johnson	OCTO0743	Gamma	38.8834	-76.9341	18	FJ3	134
OCTO271	Georgetown Hospital	OCTO2711	Alpha	38.9121	-77.0747	95	GT1	157
OCTO271	Georgetown Hospital	OCTO2712	Beta	38.9121	-77.0747	103	GT2	157
OCTO271	Georgetown Hospital	OCTO2713	Gamma	38.9121	-77.0747	19	GT3	157
OCTO393	GWU	OCTO03931	Alpha	38.9012	-77.0491	36	GW1	59
OCTO393	GWU	OCTO03932	Beta	38.9012	-77.0491	46	GW2	59
OCTO393	GWU	OCTO03933	Gamma	38.9012	-77.0491	106	GW3	59
OCTO001	Judiciary Square	OCTO0011	Alpha	38.8948	-77.0162	7	OJ1	36
OCTO001	Judiciary Square	OCTO0012	Beta	38.8948	-77.0162	17	OJ2	36
OCTO001	Judiciary Square	OCTO0013	Gamma	38.8948	-77.0162	104	OJ3	36
OCTO003	Reeves	OCTO0031	Alpha	38.9168	-77.0325	94	RV1	95
OCTO003	Reeves	OCTO0032	Beta	38.9168	-77.0325	9	RV2	95
OCTO003	Reeves	OCTO0033	Gamma	38.9168	-77.0325	105	RV3	95
OCTO256	Rhode Island	OCTO02561	Alpha	38.9276	-76.9801	39	RI1	150
OCTO256	Rhode Island	OCTO02562	Beta	38.9276	-76.9801	40	RI2	150
OCTO256	Rhode Island	OCTO02563	Gamma	38.9276	-76.9801	91	RI3	150
OCTO275	Sibley Hospital	OCTO02751	Alpha	38.9365	-77.1084	77	SB1	226
OCTO275	Sibley Hospital	OCTO02752	Beta	38.9365	-77.1084	35	SB2	226
OCTO275	Sibley Hospital	OCTO02753	Gamma	38.9365	-77.1084	73	SB3	226
OCTO260	St. Elizabeths	OCTO02601	Alpha	38.8483	-76.9872	93	SE1	173
OCTO260	St. Elizabeths	OCTO02602	Beta	38.8483	-76.9872	10	SE2	173
OCTO260	St. Elizabeths	OCTO06603	Gamma	38.8483	-76.9872	67	SE3	173
OCTO319	UDC	OCTO03191	Alpha	38.9446	-77.0669	92	UD1	291
OCTO319	UDC	OCTO03192	Beta	38.9446	-77.0669	8	UD2	291
OCTO319	UDC	OCTO03193	Gamma	38.9446	-77.0669	11	UD3	291

SiteID	Antenna Model (EMS Technologies)	Antenna Gain (dBi)	Radiation BW	Mechanical Tilt (ft)	Electrical Tilt (deg)	Azimuth	Cable Size (inch)	Cable Length (ft)	Line Loss (dB)	Power Antenna (dBm)	
OCTO241	FR65-12-05-DAL2-SP-752-806-MHz	11	65	125	330	0	5	1 5/8 Andrew	350	2.205	37.4456
OCTO241	FR65-12-10-DAL2-SP-752-806-MHz	11	65	125	100	0	10	1 5/8 Andrew	350	2.205	37.4456
OCTO241	FR65-12-10-DAL2-SP-752-806-MHz	11	65	125	195	2	10	1 5/8 Andrew	350	2.205	37.4456
OCTO074	FR65-12-05-DAL2-SP-752-806-MHz	11	65	50	345	7	5	7/8 Andrew	100	1.08	39.4
OCTO074	FR65-12-05-DAL2-SP-752-806-MHz	11	65	50	95	0	5	7/8 Andrew	94	1.0152	39.4648
OCTO074	FR65-12-05-DAL2-SP-752-806-MHz	11	65	50	245	0	5	1 5/8 Andrew	198	1.2474	39.2326
OCTO271	FR65-12-10-DAL2-SP-752-806-MHz	11	65	80	0	0	10	7/8 Andrew	60	0.648	40.2148
OCTO271	FR65-12-10-DAL2-SP-752-806-MHz	11	65	80	150	0	10	7/8 Andrew	60	0.648	40.2148
OCTO271	FR65-12-05-DAL2-SP-752-806-MHz	11	65	80	240	0	5	7/8 Andrew	20	0.216	40.6468
OCTO393	FR65-12-10-DAL2-SP-752-806-MHz	11	65	120	155	3	10	1 5/8 Andrew	450	2.835	37.311
OCTO393	FR65-12-05-DAL2-SP-752-806-MHz	11	65	120	200	0	5	1 1/4 Andrew	450	3.555	36.591
OCTO393	FR65-12-05-DAL2-SP-752-806-MHz	11	65	122	345	0	5	1 5/8 Andrew	450	2.835	37.311
OCTO001	FR65-12-10-DAL2-SP-752-806-MHz	11	65	130	20	0	10	1 5/8 Andrew	363	2.2869	38.0655
OCTO001	FR65-12-05-DAL2-SP-752-806-MHz	11	65	130	120	0	5	7/8 Andrew	36	0.3888	39.9636
OCTO001	FR65-12-10-DAL2-SP-752-806-MHz	11	65	130	250	2	10	7/8 Andrew	36	0.3888	39.9636
OCTO003	FR65-12-05-DAL2-SP-752-806-MHz	11	65	100	60	0	5	1 5/8 Andrew	275	1.7325	38.7475
OCTO003	FR65-12-10-DAL2-SP-752-806-MHz	11	65	100	160	4	10	7/8 Andrew	57	0.6156	39.8644
OCTO003	FR65-12-10-DAL2-SP-752-806-MHz	11	65	100	280	4	10	7/8 Andrew	15	0.162	40.318
OCTO256	FR65-12-05-DAL2-SP-752-806-MHz	11	65	85	345	0	5	7/8 Andrew	90	0.972	39.1571
OCTO256	FR65-12-10-DAL2-SP-752-806-MHz	11	65	85	115	2	10	7/8 Andrew	90	0.972	39.1571
OCTO256	FR65-12-05-DAL2-SP-752-806-MHz	11	65	85	220	3	5	7/8 Andrew	90	0.972	39.1571
OCTO275	FR65-12-05-DAL2-SP-752-806-MHz	11	65	90	30	0	5	7/8 Andrew	50	0.54	39.7486
OCTO275	FR65-12-05-DAL2-SP-752-806-MHz	11	65	90	140	0	5	7/8 Andrew	50	0.54	39.7486
OCTO275	FR65-12-05-DAL2-SP-752-806-MHz	11	65	90	270	0	5	7/8 Andrew	150	1.62	38.6686
OCTO260	FR65-12-05-DAL2-SP-752-806-MHz	11	65	160	305	3	10	1 1/4 Andrew	160	1.264	38.8651
OCTO260	FR65-12-05-DAL2-SP-752-806-MHz	11	65	160	70	0	5	1 1/4 Andrew	160	1.264	38.8651
OCTO260	FR65-12-10-DAL2-SP-752-806-MHz	11	65	160	215	0	10	1 1/4 Andrew	160	1.264	38.8651
OCTO319	FR65-12-05-DAL2-SP-752-806-MHz	11	65	95	0	0	5	7/8 Andrew	110	1.188	39.3877
OCTO319	FR65-12-10-DAL2-SP-752-806-MHz	11	65	95	160	4	10	7/8 Andrew	160	1.728	38.8477
OCTO319	FR65-12-10-DAL2-SP-752-806-MHz	11	65	95	260	2	10	7/8 Andrew	160	1.728	38.8477

SiteID	Power Antenna (W)	Lower Jumper Length (ft)	Upper Jumper Length (ft)	Jumper Losses (dB)	VLANX	VLANY	BBU
OCTO241	5.55341	48	6	1.6	10.50.247.89	10.50.247.209	10.50.240.28
OCTO241	5.55341	48	6	1.6	10.50.247.89	10.50.247.209	10.50.240.29
OCTO241	5.55341	48	6	1.6	10.50.247.89	10.50.247.209	10.50.240.30
OCTO074	8.70964	22	6	0.8	10.50.247.17	10.50.247.137	10.50.240.1
OCTO074	8.84056	22	6	0.8	10.50.247.17	10.50.247.137	10.50.240.2
OCTO074	8.38031	22	6	0.8	10.50.247.17	10.50.247.137	10.50.240.3
OCTO271	10.507	10	6	0.4	10.50.247.73	10.50.247.193	10.50.240.22
OCTO271	10.507	10	6	0.4	10.50.247.73	10.50.247.193	10.50.240.23
OCTO271	11.6059	10	6	0.4	10.50.247.73	10.50.247.193	10.50.240.24
OCTO393	5.38394	30	10	1.2	10.50.247.41	10.50.247.161	10.50.240.10
OCTO393	4.56142	30	10	1.2	10.50.247.41	10.50.247.161	10.50.240.11
OCTO393	5.38394	30	10	1.2	10.50.247.41	10.50.247.161	10.50.240.12
OCTO001	6.40546	26	6	0.9	10.50.247.33	10.50.247.153	10.50.240.7
OCTO001	9.91654	26	6	0.9	10.50.247.33	10.50.247.153	10.50.240.8
OCTO001	9.91654	26	6	0.9	10.50.247.33	10.50.247.153	10.50.240.9
OCTO003	7.49463	22	6	0.8	10.50.247.49	10.50.247.169	10.50.240.13
OCTO003	9.69259	22	6	0.8	10.50.247.49	10.50.247.169	10.50.240.14
OCTO003	10.7597	22	6	0.8	10.50.247.49	10.50.247.169	10.50.240.15
OCTO256	8.23588	33	6	1.2	10.50.247.65	10.50.247.185	10.50.240.19
OCTO256	8.23588	33	6	1.2	10.50.247.65	10.50.247.185	10.50.240.20
OCTO256	8.23588	33	6	1.2	10.50.247.65	10.50.247.185	10.50.240.21
OCTO275	9.43757	28	6	1	10.50.247.81	10.50.247.201	10.50.240.25
OCTO275	9.43757	28	6	1	10.50.247.81	10.50.247.201	10.50.240.26
OCTO275	7.3597	28	6	1	10.50.247.81	10.50.247.201	10.50.240.27
OCTO260	7.70034	33	6	1.2	10.50.247.25	10.50.247.145	10.50.240.4
OCTO260	7.70034	33	6	1.2	10.50.247.25	10.50.247.145	10.50.240.5
OCTO260	7.70034	33	6	1.2	10.50.247.25	10.50.247.145	10.50.240.6
OCTO319	8.685	19	6	0.7	10.50.247.57	10.50.247.177	10.50.240.16
OCTO319	7.66955	19	6	0.7	10.50.247.57	10.50.247.177	10.50.240.17
OCTO319	7.66955	19	6	0.7	10.50.247.57	10.50.247.177	10.50.240.18

Table 5. OCTO Tower Sector Specifications

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF REFERENCES

1. Alberts, David et al, *Network Centric Warfare: Developing and Leveraging Information Superiority*, CCRP Publication Series February 2000.
2. JTRS, Joint Program Office, *Joint Tactical Radio System (JTRS) Wideband Networking Waveform (WNW) Functional Description Document (FDD) Version 2.21*, November 29, 2001.
3. Flarion. OFDM for Mobile Data Communications White Paper [online] [http://www.flarion.com/viewpoint/whitepapers/OFDM\\_Mobile\\_Data\\_Communications.pdf](http://www.flarion.com/viewpoint/whitepapers/OFDM_Mobile_Data_Communications.pdf) Last accessed on July 13, 2005.
4. Naval Network Warfare Command. FORCENet a Functional Concept for the 21<sup>st</sup> Century [online] <http://forcenet.navy.mil/News/Articles/cno-concept.pdf> Last accessed on July 13, 2005.
5. Lawrey, Eric, Adaptive Techniques for Multiuser OFDM, PhD thesis, James Cook University, Townesville, Australia, December 2001.
6. Flarion Technologies, Inc. Secure Mobile Broadband for State and Local Government Agencies: Connecting Legacy Networks with a Secure Mobile IP WAN. February 2004.
7. Flarion Technologies, Inc. FLASH-OFDM System Description. Version 1.3. March 15, 2005.
8. Freescale Semiconductor, Inc. Using the PowerQUICC II Pro MPC8360E to Build a Line Card in 802.16 (WiMAX) Wireless Equipment. Rev. 0. March, 2005.[online][http://www.freescale.com/files/32bit/doc/white\\_paper/WIMAX8360EWP.pdf](http://www.freescale.com/files/32bit/doc/white_paper/WIMAX8360EWP.pdf) Last accessed on June 20, 2005.
9. Tanglao, Roland. The End of Wireless as We Know It. February 2004. [online] [http:// www.telepocalypse.net/archives/000239.html](http://www.telepocalypse.net/archives/000239.html) Last accessed on July 18, 2005.
10. IEEE 802.16.4 PHY Strawman-01/12r1 [online] [http://wirelessman.org/tg4/docs/802164-01\\_12r1.pdf](http://wirelessman.org/tg4/docs/802164-01_12r1.pdf) Last accessed on July 18, 2005.
11. Matz, Gerald and Schafhuber, Dieter MMSE and Adaptive Prediction of Time-Varying Channels for OFDM Systems. IEEE Transactions on Wireless Communications, Vol. 4, No.2, March 2005 [online] [http://www.nt.tuwien.ac.at/Dspgroup/dschafhu/Schafhuber\\_wc\\_03.pdf](http://www.nt.tuwien.ac.at/Dspgroup/dschafhu/Schafhuber_wc_03.pdf)

12. Andrews, Jeffrey. Predistortion Techniques and Peak-to-Average Ratio Reduction for OFDM. [online] <http://www.ece.utexas.edu/~jandrews/research.html> Last accessed on July 20, 2005.
13. OFDM Tutorial. [online] <http://www.wave-report.com/tutorials/OFDM.htm> Last accessed on July 21, 2005.
14. Davis, Charles PhD and Cadogan, Rochelle PhD. The Many Faces of Asynchronous Transfer Mode. [online] <http://www.stthom.edu/bschool/pdf/ATM%20Paper%20for%20IRMA%202004.pdf> Last accessed on July 22, 2005.
15. Nair, Govindan and Chou, Joey Intel Communications Group, Intel Corporation. IEEE 802.16 Medium Access Control and Service Provisioning. [online] [http://developer.intel.com/technology/itj/2004/volume08issue03/art04\\_ieee80216mac/vol8\\_art04.pdf](http://developer.intel.com/technology/itj/2004/volume08issue03/art04_ieee80216mac/vol8_art04.pdf) Last accessed on July 25, 2005.
16. Nichols, K. and Carpenter B. RFC 3086 Definition of Differentiated Services Per Domain Behaviors and Rules for Their Specification. [online] <http://www.ietf.org/rfc/rfc3086.txt> Last accessed on July 27, 2005.
17. Guice, Robert J., Munoz, Ramon J., IEEE 802.16 Commercial Off the Shelf (COTS) Technologies as a Compliment to Ship to Objective Maneuver (STOM) Communications, Master's Thesis, Naval Postgraduate School, Monterey, California, September 2004.
18. Flarion. Whitepaper: RadioRouter Base Station. [online] [http://www.flarion.com/products/overviews/RadioRouter\\_Product\\_Overview.pdf](http://www.flarion.com/products/overviews/RadioRouter_Product_Overview.pdf) Last accessed on July 29, 2005.
19. Network World. Definition of RADIUS. [online] <http://www.networkworld.com/details/534.html> Last accessed on June 18, 2005.
20. Flarion Technologies, Inc. Flashview Element Management System (EMS) Reference Manual v1.5 November 2, 2004.
21. Flarion Technologies, Inc. Whitepaper. End-to-End Security Across a Mobile Broadband Network. [online] [http://www.flarion.com/viewpoint/whitepapers/wireless\\_security.pdf](http://www.flarion.com/viewpoint/whitepapers/wireless_security.pdf) Last accessed on July 30, 2005.
22. Naval Postgraduate School. Research Center Proposal. Center for Network Innovation and Experimentation (CENETIX).



23. QUALCOMM, Inc. QUALCOMM to Acquire Flarion Technologies. [online] [http://www.qualcomm.com/press/releases/2005/050811\\_flarion\\_acquisition.html](http://www.qualcomm.com/press/releases/2005/050811_flarion_acquisition.html)  
Last accessed on August 11, 2005.
24. Flarion, Technologies, Inc. Whitepaper. Gigabyte Performance in a Mobile Broadband Network [online] <http://www.flarion.com/products/whitepapers/Gigabyte%20Performance.pdf>
25. District of Columbia, Office of Chief Technology Officer, WARN Coverage 2-15-05.ppt.
26. Microsoft Research. Microsoft Portrait. [online] <http://research.microsoft.com/~jiangli/portrait/> Last accessed on August 30, 2005.
27. Flarion Technologies, Inc. Flarion Mobile Diagnostic Monitor (FMDM) Users Guide. Version 1.7. August 6, 2004.
28. Flarion Technologies, Inc. Flarion Mobile Log Processor (FMLP) Users Guide. Version 1.0. December 15, 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Dan Boger  
Information Sciences, Naval Postgraduate School  
Monterey, California
4. Alex Bordetsky  
Naval Postgraduate School  
Monterey, California
5. Kyle Longcrier  
JSOC J-6  
FT Bragg, North Carolina
6. Roger Merk  
SPAWAR  
San Diego, California