



**NAVAL  
POSTGRADUATE  
SCHOOL**

**MONTEREY, CALIFORNIA**

**THESIS**

**IEEE 802.16 COMMERCIAL OFF THE SHELF (COTS)  
TECHNOLOGIES AS A COMPLIMENT TO SHIP TO  
OBJECTIVE MANEUVER (STOM) COMMUNICATIONS**

by

Robert J Guice  
Ramon J Munoz

September 2004

Thesis Advisor:  
Second Reader:

Rex Buddenberg  
Dan Boger

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

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE September 2004	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: IEEE 802.16 Commercial Off the Shelf (COTS) Technologies as a Compliment to Ship to Objective Maneuver (STOM) Communications			5. FUNDING NUMBERS	
6. AUTHOR(S) Robert J Guice and Ramon J Munoz				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			12b. DISTRIBUTION CODE A	
<p><b>13. ABSTRACT (maximum 200 words)</b></p> <p>This research evaluates the IEEE 802.16 standards and technologies that are currently being developed in the commercial sector. The robust capability of this standard lends itself potentially to numerous military applications. This research explores how this technology might address the shortcomings of existing military radio and data systems; specifically, with respect to the issues surrounding the Ship to Objective Maneuver (STOM) communications. The intent of this research is to provide recommendations on the necessary 'adapt from COTS' changes for this technology to address STOM networking requirements.</p> <p>This research includes discussions on the military requirements for an IEEE 802.16 adapted waveform. The requirements are for the IEEE 802.16 'adapt from COTS' are derived from researched on the Concept of Employment for STOM operations and the specification of the Joint Tactical Radio Systems (JTRS) Wideband Networking Waveform (WNW). These discussions offer an illustration of the complex networking demands the COTS adapted systems would need to address. Through detailed exploration of the current IEEE 802.16 standards and implementation testing with pre-standard IEEE 802.16a equipment, we were able to make recommendations on the COTS adaptations necessary to make IEEE 802.16 suitable as a complimentary technology within the STOM scenario.</p>				
14. SUBJECT TERMS 802.16, OFDM, STOM, OTM, NLOS, COTS, 802.11, MANET, MESH, JTRS, WNW, Wideband Networking Waveform			15. NUMBER OF PAGES 140	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

THIS PAGE INTENTIONALLY LEFT BLANK

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

**IEEE 802.16 COMMERCIAL OFF THE SHELF (COTS) TECHNOLOGIES AS A  
COMPLIMENT TO SHIP TO OBJECTIVE MANEUVER (STOM)  
COMMUNICATIONS**

Robert J. Guice  
Captain, United States Marine Corps  
B.S., University of Maryland, 1996

Ramon J. Munoz  
Captain, United States Marine Corps  
B.S., Northeastern University, 1996

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN  
INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL  
September 2004**

Author: Robert J Guice

Ramon J Munoz

Approved by: Rex Buddenberg, Thesis Advisor

Dan Boger, Second Reader

Dan Boger, Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

This research evaluates the IEEE 802.16 standards and technologies that are currently being developed in the commercial sector. The robust capability of this standard lends itself potentially to numerous military applications. This research explores how this technology might address the shortcomings of existing military radio and data systems; specifically, with respect to the issues surrounding the Ship to Objective Maneuver (STOM) communications. The intent of this research is to provide recommendations on the necessary 'adapt from COTS' changes for this technology to address STOM networking requirements.

This research includes discussions on the military requirements for an IEEE 802.16 adapted waveform. The requirements are for the IEEE 802.16 'adapt from COTS' are derived from researched on the Concept of Employment for STOM operations and the specification of the Joint Tactical Radio Systems (JTRS) Wideband Networking Waveform (WNW). These discussions offer an illustration of the complex networking demands the COTS adapted systems would need to address. Through detailed exploration of the current IEEE 802.16 standards and implementation testing with pre-standard IEEE 802.16a equipment, we were able to make recommendations on the COTS adaptations necessary to make IEEE 802.16 suitable as a complimentary technology within the STOM scenario.

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>4</b>
<b>D.</b>	<b>SCOPE .....</b>	<b>5</b>
<b>E.</b>	<b>METHODOLOGY .....</b>	<b>5</b>
<b>F.</b>	<b>ORGANIZATION OF THESIS .....</b>	<b>5</b>
<b>II.</b>	<b>IDENTIFYING SHIP TO OBJECTIVE MANEUVER NETWORKING REQUIREMENTS.....</b>	<b>7</b>
<b>A.</b>	<b>INTRODUCTION.....</b>	<b>7</b>
<b>B.</b>	<b>OVERVIEW .....</b>	<b>7</b>
<b>C.</b>	<b>STOM NETWORK REQUIREMENTS.....</b>	<b>9</b>
<b>1.</b>	<b>Self-Organization .....</b>	<b>9</b>
<b>2.</b>	<b>Ubiquitous Communications Relays .....</b>	<b>9</b>
<b>3.</b>	<b>Common Operational Picture (COP).....</b>	<b>10</b>
<b>4.</b>	<b>Cooperative Engagement .....</b>	<b>10</b>
<b>5.</b>	<b>Consolidated Networks.....</b>	<b>10</b>
<b>D.</b>	<b>SUMMARY .....</b>	<b>10</b>
<b>III.</b>	<b>JTRS WIDEBAND NETWORKING WAVEFORM OVERVIEW .....</b>	<b>13</b>
<b>A.</b>	<b>INTRODUCTION.....</b>	<b>13</b>
<b>B.</b>	<b>JOINT TACTICAL RADIO SYSTEM OVERVIEW.....</b>	<b>13</b>
<b>1.</b>	<b>Overview .....</b>	<b>13</b>
<b>2.</b>	<b>JTRS Wideband Networking Waveform .....</b>	<b>16</b>
<b>3.</b>	<b>WNW Employment within STOM.....</b>	<b>17</b>
<b>C.</b>	<b>WNW PLANNED OPERATING REQUIREMENTS .....</b>	<b>18</b>
<b>1.</b>	<b>Performance Characteristics .....</b>	<b>18</b>
<b>2.</b>	<b>Networking Requirements .....</b>	<b>19</b>
<b>3.</b>	<b>Network Services.....</b>	<b>21</b>
<b>5.</b>	<b>Information Assurance and Security .....</b>	<b>23</b>
<b>6.</b>	<b>Program Status.....</b>	<b>25</b>
<b>D.</b>	<b>SUMMARY .....</b>	<b>26</b>
<b>IV.</b>	<b>IEEE 802.16 STANDARD OVERVIEW .....</b>	<b>27</b>
<b>A.</b>	<b>INTRODUCTION.....</b>	<b>27</b>
<b>B.</b>	<b>WHAT IS IEEE 802.16?.....</b>	<b>27</b>
<b>1.</b>	<b>Comparison of IEEE 802.11 and IEEE 802.16.....</b>	<b>28</b>
<b>2.</b>	<b>WiMax and Interoperability .....</b>	<b>31</b>
<b>C.</b>	<b>THE IEEE 802.16 STANDARDS .....</b>	<b>31</b>
<b>D.</b>	<b>DEPLOYMENT ARCHITECTURES .....</b>	<b>32</b>
<b>E.</b>	<b>THE PHYSICAL LAYER (PHY) .....</b>	<b>33</b>
<b>1.</b>	<b>10-66 GHz Systems .....</b>	<b>33</b>

2.	2-11 GHz Systems .....	34
3.	Error Control .....	35
	<i>a. Forward Error Correction</i> .....	35
	<i>b. Automatic Retransmission Request</i> .....	35
4.	Framing.....	35
	<i>a. Downlink Subframe</i> .....	36
	<i>b. Uplink Subframe</i> .....	39
5.	Transmission Convergence (TC) Sublayer.....	40
F.	<b>MEDIUM ACCESS CONTROLLER LAYER (MAC)</b> .....	40
1.	Connection Orientation .....	41
2.	The MAC PDU .....	41
	<i>a. PDU Description</i> .....	41
	<i>b. Construction of the MAC PDU</i> .....	42
3.	Sub-layers .....	44
	<i>a. Convergence Sublayer</i> .....	44
	<i>b. Privacy Sublayer</i> .....	46
	<i>c. Payload Header Suppression</i> .....	46
4.	Radio Link Control.....	46
5.	Network Entry and Initialization .....	46
	<i>a. Scanning and Synchronization to the Downlink</i> .....	47
	<i>b. Obtaining Transmit Parameters</i> .....	47
	<i>c. Ranging and Power Adjustment</i> .....	48
	<i>d. Negotiation of Basic Capabilities</i> .....	48
	<i>e. Authorize SS to Perform Key Exchange</i> .....	49
	<i>f. Registration</i> .....	49
	<i>g. Establish IP Connectivity</i> .....	49
	<i>h. Establish Time of Day</i> .....	49
	<i>i. Transfer Operational Parameters</i> .....	49
	<i>j. Set Up Connections</i> .....	49
6.	Bandwidth Requests and Grants.....	50
	<i>a. GPC</i> .....	50
	<i>b. GPSS</i> .....	50
7.	Bandwidth Requests .....	51
	<i>a. Request Periods</i> .....	51
	<i>b. Bandwidth Request Header</i> .....	51
	<i>c. Piggyback Request</i> .....	52
8.	Polling.....	52
	<i>a. Unicast polling</i> .....	52
	<i>b. Multicast and Broadcast Polling</i> .....	53
	<i>c. Poll-Me Bit</i> .....	54
9.	Uplink Scheduling Services.....	54
	<i>a. Unsolicited Grant Service</i> .....	54
	<i>b. Real Time Polling Service</i> .....	55
	<i>c. Non Real Time Polling Service</i> .....	56
	<i>d. Best Effort Service</i> .....	56

10.	Quality of Service .....	56
11.	Security .....	58
	<i>a. Packet Data Encryption</i> .....	58
	<i>b. Key Management Protocol</i> .....	59
	<i>c. Security Associations</i> .....	59
G.	SUMMARY .....	59
V.	COMPARISON OF IEEE 802.16 TO THE WNW AND STOM REQUIREMENTS.....	61
A.	INTRODUCTION.....	61
B.	REQUIREMENTS FOR RADIO WAN .....	61
	1. Routable Networks.....	61
	2. Ability to Support Multicast Traffic .....	62
	3. QoS Control.....	62
	4. Layer 2 Security .....	62
	5. Manageability.....	63
C.	COMPARISON OF IEEE 802.16 AND THE JTRS WNW .....	63
	1. Performance Characteristics .....	63
	<i>b. Supported Data Rates</i> .....	63
	<i>c. Automatic Power Control</i> .....	64
	<i>d. Range</i> .....	64
	<i>e. Propagation Environment Support</i> .....	64
	<i>f. Frequency Spectrum</i> .....	64
	<i>g. Noise Environments</i> .....	65
	<i>f. Anti-jamming capabilities</i> .....	65
	2. Networking capabilities .....	65
	<i>a. Network size</i> .....	65
	<i>b. Topology</i> .....	65
	<i>c. Mobility management (Layer 1)</i> .....	66
	3. Network services .....	66
	<i>a. Traffic Support</i> .....	66
	<i>b. QoS control</i> .....	66
	<i>c. Packet Delivery</i> .....	66
	<i>d. Channel Access</i> .....	67
	4. Information Assurance and Security .....	67
	<i>a. Confidentiality</i> .....	67
	<i>b. Availability</i> .....	67
	<i>c. Integrity</i> .....	67
	<i>d. Identification and Authentication</i> .....	68
	<i>e. Waveform cryptographic functions</i> .....	68
	5. Program status and Standard maturity.....	68
D.	COMPARISON OF IEEE 802.16 AND STOM REQUIREMENTS .....	69
	1. Self-Organization .....	69
	2. Ubiquitous Communications Relays .....	69
	3. Common Operational Picture (COP).....	70
	4. Cooperative Engagement .....	70

5.	Consolidated Networks.....	70
E.	CONCLUSIONS .....	71
VI.	IMPLEMENTATION AND TESTING .....	73
A.	INTRODUCTION.....	73
B.	METHODOLOGY .....	73
C.	PMP TESTING (AUG 2004).....	74
1.	Introduction.....	74
a.	<i>Redline Communications</i> .....	75
b.	<i>Antennas</i> .....	76
3.	Testing Terrain.....	77
4.	Network Description.....	78
a.	<i>Hardware devices</i> .....	78
b.	<i>Software Tools</i> .....	79
5.	Test Results.....	80
a.	<i>Test #1 LOS Baseline Testing</i> .....	80
b.	<i>Test # 2 NLOS testing in a PMP deployment</i> .....	82
c.	<i>Test #3 Multicast Traffic Test</i> .....	85
d.	<i>Test #4. QoS Test</i> .....	87
D.	OBSERVATIONS FROM TEST RESULTS .....	88
E.	SUMMARY .....	89
VII.	ADAPT FROM COTS RECOMMENDATIONS.....	91
A.	INTRODUCTION.....	91
B.	ADAPT-FROM-COTS ITEMS .....	91
1.	Frequency .....	91
2.	Encryption .....	92
3.	Antenna Pointing Mechanism.....	92
C.	SUMMARY .....	92
VIII.	CONCLUSIONS .....	95
A.	FINDINGS .....	95
1.	Addressing the Networking Requirements.....	95
2.	Adapt From COTS .....	95
B.	FURTHER RESEARCH.....	95
1.	The IEEE 802.16e Standard.....	95
2.	MANET in STOM Operation .....	96
3.	Mobility Management .....	96
4.	IEEE 802.16 Vulnerability Testing .....	97
5.	IEEE PHY Level Independence .....	97
6.	Application to Satellite Communications .....	97
C.	SUMMARY .....	97
APPENDIX A	REDLINE COMMUNICATIONS AN-50 SPECIFICATIONS ...	99
APPENDIX B	802.16 AND OFDM VENDORS .....	101
LIST OF REFERENCES	.....	103

<b>GLOSSARY.....</b>	<b>107</b>
<b>INITIAL DISTRIBUTION LIST .....</b>	<b>111</b>

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF FIGURES

Figure 1.	STOM Scheme of Maneuver (From: Ref 6) .....	8
Figure 2.	JTRS within the Global Information Grid (From: Ref 11) .....	15
Figure 3.	JTRS Interconnected Network (From: Ref 12) .....	16
Figure 4.	JTRS Concept of Employment (From: Ref 12) .....	17
Figure 5.	Dismounted Mobile WLAN (From: Ref 12) .....	18
Figure 6.	TDD Downlink Subframe Structure (From: Ref 21) .....	36
Figure 7.	The downlink subframe structure (From: Ref 20) .....	38
Figure 8.	The uplink subframe structure (From: Ref 20) .....	39
Figure 9.	The TC PDU format (From: Ref 21) .....	40
Figure 10.	PDU and SDU in a Protocol Stack (From: Ref 21) .....	42
Figure 11.	Construction of the MAC PDU (From: Ref 21) .....	43
Figure 12.	IEEE 802.16 Protocol Layering (From: Ref 21) .....	44
Figure 13.	Classification and CID mapping (From: Ref 21) .....	45
Figure 14.	SS Initialization Overview (From: Ref 21) .....	47
Figure 15.	The Unicast Polling process (From: Ref 21) .....	53
Figure 16.	Poll-me bit usage (From: Ref 25) .....	55
Figure 17.	MAC PDU Encryption (From: Ref 6) .....	59
Figure 18.	Redline Communications AN-50 System with Antenna and 5.8 GHz Transceiver Radio (From: Ref 35) .....	76
Figure 19.	Overhead View of Testing Area .....	77
Figure 20.	Network Diagram .....	78
Figure 21.	Example of an IPerf® Multicast Test Output .....	80
Figure 22.	Base Station Sector Antenna Overlooking Runway .....	80
Figure 23.	Baseline PMP LOS Throughput Test Results .....	82
Figure 24.	Photo of Capt Munoz Deploying a 1ft 9 degree antenna at Hill #1 .....	83
Figure 25.	Photo of SS Antenna Deployed at FP 13 .....	84
Figure 26.	NLOS Throughput Test Results .....	85
Figure 27.	Example of IPerf® Multicast Client Test Output .....	86
Figure 28.	Multicast Server Output of Link from FP13 to NOC .....	86

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

Table 1.	Throughput Comparisons for MAGTF Communication Systems (From Ref 8) .....	19
Table 2.	WNW Performance Characteristics (After Ref 12).....	20
Table 3.	WNW Networking Requirements (After: Ref 12).....	21
Table 4.	WNW Requirements for Network Services (after Ref 12).....	22
Table 5.	WNW Requirements for Network Layer Addressing (After: Ref 12).....	23
Table 6.	WNW Requirements for Information Assurance and Waveform Security (After: Ref 12).....	25
Table 7.	Comparison of 802.11 vs. 802.16 (After: Ref 18) .....	30
Table 8.	The DL-MAP message format (From: Ref 21).....	37
Table 9.	The UL-MAP message format (From: Ref 21).....	38
Table 10.	Sample Uplink Map with multicast and broadcast IE (From: Ref 21) .....	54
Table 11.	Request Transmission Policy Example (From: Ref 25) .....	57
Table 12.	Antenna Specifications .....	76
Table 13.	Test 1. LOS PMP Data Sheet (Baseline) .....	81
Table 14.	NLOS PMP Throughput Test .....	84
Table 15.	Tests #1 and #2 Consolidated Results .....	85
Table 16.	NOC to FP 13 QoS Test Results.....	87
Table 17.	NOC to Hill #1 QoS Test Results .....	88
Table 18.	NOC to Runway QoS Test Results.....	88
Table 19.	AN 50 Specifications (From: Ref 35).....	99
Table 20.	WMAN Vendors (From: Ref 30).....	101

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF ACRONYMS

AAAV	Advanced Amphibious Assault Vehicle
AES	Advanced Encryption Standard
AP	Access Point
API	Application Programming Interface
ARG	Amphibious Readiness Group
ARQ	Automatic Retransmission Request
ATM	Asynchronous Transfer Mode
BS	Base Station
CAS	Close Air Support
CBR	Constant Bit Rate
CID	Connection Identifier
COC	Combat Operations Centers
COP	Common Operational Picture
CRC	Cyclic Redundancy Check
CPS	Common Part Sublayer
CS	Convergence Sublayer
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
DAMA	Demand Assigned Multiple Access
DCD	Downlink Channel Descriptor
DHCP	Dynamic Host Configuration Protocol
DL-MAP	Downlink Map
DoD	Department of Defense
DoN	Department of the Navy
EPLARS	Enhance Position Location Systems
FDD	Functional Description Document
FDD	Frequency Division Duplexing
FEC	Forward Error Correction
GFR	Guaranteed Frame Rate
GIG	Global Information Grid
GPC	Grant Per Connection
GPS	Global Positioning System
GPSS	Grant Per Subscriber Station
HF	High Frequency
HMMWV	High-Mobility Multipurpose Wheeled Vehicle
IE	Information Element
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
JTRS	Joint Tactical Radio System

LAN	Local Area Network
LPD	Low Probability of Detection
LPI	Low Probability of Intercept
MAC	Medium Access Control
MAGTF	Marine Air-Ground Task Force
MAN	Metropolitan Area Network
MEF	Marine Expeditionary Force
MEU	Marine Expeditionary Unit
MSC	Major Subordinate Commands
NCW	Network Centric Warfare
NLOS	Non-Line of Sight
OEF	Operation Enduring Freedom
OFDM	Orthogonal frequency-division multiplexing
OIF	Operation Iraqi Freedom
OMFTS	Operational Maneuver from the Sea
OSI	Open Systems Interconnect
OTH	Over-the-Horizon
OTM	On-the-Move
PDU	Protocol Data Units
PHY	Physical Layer
PKM	Privacy Key Management
PMP	Point-to-Multipoint
PTCM	Point-to-Consecutive Point
PTP	Point-to-Point
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift Keying
QoS	Quality of Service
REG-REQ	Registration Request
REG-RSP	Registration Response
RF	Radio Frequency
RLC	Radio Link Controller
RNG-REQ	Ranging Request
RNG-RSP	Ranging Response
SA	Security Association
SATCOM	Satellite Communications
SCA	Software Communications Architecture
SBC-REQ	SS Basic Capability Request
SBC-RSP	SS Basic Capability Response
SDU	Service Data Unit
SINGARS	Single Channel Ground Air Radio System
SOHO	Small Office / Home Office
SS	Subscriber Station
STOM	Ship-to-Objective Maneuver
TC	Transmission Convergence
TDMA	Time Division Multiple Access

TDD	Time Division Duplexing
TDM	Time Division Multiplexing
TI	Tactical Internet
TOC	Tactical Operations Center
TRANSEC	Transmission Security
UAV	Unmanned Air Vehicle
UCD	Uplink Channel Descriptor
UDP	User Datagram Protocol
UGS	Unsolicited Grant Uplink Scheduling Service
UHF	Ultra High Frequency
UIUC	Uplink Interval Usage Code
UL-MAP	Uplink Map
VLAN	Virtual Local Area Network
VTUAV	Vertical Takeoff Unmanned Aerial Vehicle
WAN	Wide Area Network
WEP	Wireless Equivalent Privacy
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WNW	Wideband Networking Waveform
WPA	WIFI Protected Access

THIS PAGE INTENTIONALLY LEFT BLANK

## **ACKNOWLEDGMENTS**

We would like to thank Rex Buddenberg and Dan Boger specifically for their tremendous support and guidance throughout this process. We would also like to extend our appreciation to Brain Steckler for his equipment support and advice during the past year. We also extend a special thanks to both our families whom have supported each of us throughout our careers. Specifically, Ray would like to thank his loving wife Sonia for her constant support and understanding during the research and development of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

## EXECUTIVE SUMMARY

Operations Desert Storm, Enduring Freedom (OEF) and Iraqi Freedom (OIF) all demonstrated the challenges with data connectivity to our maneuvering forces in support of Network Centric Warfare (NCW). During these conflicts, the “Digital Divide” between the Major Subordinate Commands (MSC) and the maneuvering forces was more pronounced when units were dispersed over large distances in Afghanistan and Iraq (i.e. beyond the reach of the wired tactical network). The DoD saw firsthand the limitations of current radio frequency (RF) based tactical networks in terms of bandwidth, on-the-move (OTM), and non line-of-sight (NLOS) capabilities. Addressing these limitations is the primary concern of this research.

The limitations of current communications systems are of greater importance in light of the Marine Corps’s vision of future Ship-to-Objective Maneuver (STOM) operations in support of Operational Maneuver from the Sea (OMFTS). STOM will demand robust networking capabilities of C4I systems in support of forces that are OTM and may be “Over-the-Horizon” (OTH). STOM networks will also need to be flexible enough to include support for the integration of all available naval, joint, and national C4I capabilities.

To address these issues, the Marine Corps envisions a STOM networking architecture built around the Joint Tactical Radio System (JTRS). JTRS is the DoD’s attempt to develop software-defined ground, airborne, and maritime tactical radios that are capable of transmitting multiple waveforms within each radio. These waveforms will include both legacy (e.g., UHF, HF, SINCGARS, HaveQuick, Link 11) and the new Wideband Networking Waveform (WNW).

The WNW enabled radios will operate as wireless gateways that can interconnect various tactical headquarters operating on the battlefield. The Marine Corps sees a STOM scenario that would have a network consisting of a large number of low-power wireless local area networks (WLANs) interconnected by a self-organizing WAN of WNW capable JTRS nodes. The WNW network would thus be required to keep pace

with the fastest moving elements of the combat forces, in addition to providing network connectivity from the rear areas and/or sea base. With the demanding requirements of STOM, it is easy to see that the development of the WNW, or equivalent networking standard, by the DoD is crucial in developing a networking architecture which will provide reliable connectivity throughout the battlespace.

While the DoD is looking at the development of the WNW to address future tactical networking issues, an emerging wireless networking standard exists within the commercial world that may offer an alternative and/or complimentary approach to address STOM networking requirements. The Institute of Electrical and Electronics Engineers (IEEE) 802.16 standard specifies the Air Interface for fixed broadband wireless access systems. Compared with previously developed wireless standards, IEEE 802.16 standard is a next-generation technology that promises to operate over greater distances, provide more bandwidth, take advantage of a broader range of frequencies, and support a greater variety of deployment architectures, including NLOS operation.

The IEEE 802.16 standard specifies a Media Access Control (MAC) layer that is designed to accommodate different Physical layer (PHY) requirements for different environments. The MAC is capable of supporting thousands of users with DSL-comparable guaranteed service levels and a QoS capable of supporting voice or video applications. The standard offers multiple deployment options in that it is designed specifically for the Point-to-Multipoint (PMP) wireless access environment as well as Point-to-Point (PTP) modes. The IEEE 802.16 standard is designed to carry any higher layer or transport protocol such as ATM, Ethernet or Internet Protocol (IP). It is expected that networks based on the IEEE 802.16 standard will have a range up to 30 miles and the ability to transfer data, voice and video at shared data rates up to 120 Mbps for LOS transmission in the 10-66 GHz frequency range and 70 Mbps NLOS in the 2-11 GHz frequency range. [Ref 1] Future IEEE 802.16 standards will add support for mobile platform communications and mesh networking capabilities.

The robust capability of this standard lends itself to numerous potential military applications. This research evaluates the IEEE 802.16 standard and technologies that are currently being developed in the commercial sector. The research will also look at how

IEEE 802.16 might address the shortcomings of existing military radio and data systems; specifically, with respect to the goals of the WNW and the requirements of STOM communications. The objective is to investigate and make recommendations on the adaptations necessary to make IEEE 802.16 compliant equipment suitable to military needs.

Potential benefits of Commercial off the Shelf (COTS) adaptation of IEEE 802.16 include:

- Routable networks that can interconnect other network segments such as LANs and WANs via routers
- The capability to handle multicast traffic
- The capability to handle different quality of service needs
- Cost savings at least an order of magnitude less expensive than equivalent 'grey box' military equipment

In order to determine whether the IEEE 802.16 standard would be suitable for future military communications requirements, we compared the standard to the basic requirements of all radio WANs, the goals of the WNW and the requirements of STOM. In each case the standard was able to meet the requirements or goals identified with only a few adaptations. Based on our analysis, it is apparent that the IEEE 802.16 standard offers enormous potential for adaptation in future tactical radio networks.

Based on our research, we find that the standard would require adaptations in two general areas: frequency range and encryption. The goal of developing an additional PHY specification would be to increase the flexibility of the standard to communicate in frequencies below 2 GHz, which is the lowest specified frequency in the current IEEE standard. The modification of the encryption scheme of the standard, while not the focus of this thesis, is also a requirement for military adaptation of the standard.

Our research also included testing of pre-standard equipment to evaluate its ability to support various architectures, QoS levels, and NLOS requirements. While this equipment was not IEEE 802.16 standard compliant, its MAC design was largely based on the IEEE 802.16 standard. This equipment was found to perform quite well, and

further confirmed that the IEEE 802.16 standard would be a suitable technology for adaptation to future military radio networks.

# I. INTRODUCTION

## A. BACKGROUND

The tenets of Network Centric Warfare (NCW) are:

- A robustly networked force improves information sharing
- Information sharing enhances the quality of information and shared situational awareness
- Shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command [Ref 2]

The US military believes that by achieving these tenets, their forces should in turn increase combat mission effectiveness in addition to improving its operational flexibility. Transforming today's platform-centric force into a network-centric one, which can effectively be employed in Allied and coalition operations, is a priority for each of the US military services. [Ref 2]

Operations Desert Storm, Enduring Freedom (OEF) and Iraqi Freedom (OIF) all demonstrated the challenges with data connectivity to our maneuvering forces in support of NCW. During these conflicts the “Digital Divide” between the Major Subordinate Commands (MSC) and the maneuvering forces was more pronounced when forces were dispersed over large distances in Afghanistan and Iraq (i.e., beyond the reach of the wired tactical network). [Ref 3] The DoD saw firsthand that the limitations of current radio frequency (RF) based tactical networks in terms of bandwidth, on-the-move (OTM), and non line-of-sight (NLOS) capabilities. The requirements of achieving a force that is securely and robustly connected, while providing medium to high data throughput, has pushed systems such as the Single Channel Air-Ground Radios Systems (SINGARS) and Enhance Position Location Systems (EPLARS) to their respective limits. Gaps in their capabilities rendered the tenets of NCW out of reach for maneuvering forces at critical times on the battlefield during OIF and OEF. Employing a manner to address this gap is the primary concern of this research.

The lessons learned in both Iraq and Afghanistan has illustrated the need to improve networking capability to address current system deficiencies. While tactical

satellite (TACSAT) communications systems offer an alternative to terrestrial RF based systems in this regard, they too have their limitations. Recent operations proved that TACSAT systems were capable of reaching fixed forward sites, but had very limited capability to reach mobile units. This issue is of importance in light of the Marine Corps's vision of future Ship-to-Objective Maneuver (STOM) in support of Operational Maneuver from the Sea (OMFTS).

The OMFTS objective is to substantially reduce the size and type of units placed ashore. Formally published as a doctrinal publication in 1996 by the Department of the Navy (DoN), OMFTS will be characterized by the provision of sea-based logistical support and the extensive use of the sea for operational advantage. Amphibious maneuver would in turn replace the ship-to-shore movement seen in traditional US Naval and Marine Corps doctrine. By using the sea as an avenue for friendly movement (dominant maneuver) and a barrier to an enemy (force protection), OMFTS will permit US Naval Forces to better project expeditionary power directly against an enemy's center of gravity or critical vulnerability. [Ref 4]

STOM is the tactical extension of OMFTS whereby landing forces will strike directly from the ships to the objective without requiring building forces at the beachhead. STOM will emphasize sea-based command and control (C2), logistics, and fire support. Securing the beachhead for C2 and logistics will no longer be needed and amphibious operations terminate with mission accomplishment, not the transfer of command ashore. [Ref 4] STOM operations will thus demand robust networking capabilities supporting forces which are OTM and may be "Over-the-Horizon" (OTH). Just as important, STOM networks will need to be flexible enough to include support for the integration of all available naval, joint, and national Command, Control, Communications, Computers and Intelligence (C4I) capabilities.

To address these issues, the Marine Corps envisions a STOM networking architecture built around the Joint Tactical Radio System (JTRS). JTRS is the Department of Defense's (DoD) attempt to develop software-defined ground, airborne, and maritime tactical radios that are capable of transmitting multiple waveforms within

each radio. These waveforms will include both legacy (e.g., UHF, HF, SINCGARS, HaveQuick, and Link 11) and the new Wideband Networking Waveform (WNW).

WNW radio sets will operate as wireless gateways that can interconnect various tactical headquarters operating on the battlefield. The Marine Corps sees a STOM scenario that would have a network consisting of a large number of low-power wireless local area networks (WLANs) interconnected by a self-organizing WAN of WNW capable JTRS radios. The WNW network would thus be required to keep pace with the fastest moving elements of the combat forces, in addition to providing network connectivity from the rear areas and/or sea base. To prevent fragmentation of the network due to distance or terrain, airborne WNW capable relay nodes will augment the terrestrial portion of the WAN backbone. [Ref 5] With the demanding requirements of STOM, it is easy to see that the development of the WNW, or equivalent waveform, by the Department of Defense (DoD) is crucial developing a networking architecture which will provide reliable connectivity to throughout the battlespace.

While the DoD is looking at the development of the WNW to address future tactical networking issues, an emerging wireless networking standard exists within the commercial world that may offer an alternative and/or complimentary approach to address STOM networking requirements. The Institute of Electrical and Electronics Engineers (IEEE) 802.16 standard specifies the Air Interface for fixed broadband wireless access systems. Compared with previously developed wireless standards, IEEE 802.16 standard is a next-generation technology that promises to operate over greater distances, provide more bandwidth, take advantage of a broader range of frequencies, and support a greater variety of deployment architectures, including NLOS operation.

The IEEE 802.16 standard specifies a Media Access Control (MAC) layer that is designed to accommodate different Physical layer (PHY) requirements for different environments. The MAC is capable of supporting thousands of users with DSL-comparable guaranteed service levels and a QoS capable of supporting voice or video applications. The standard offers multiple deployment options in that it is designed specifically for the Point-to-Multipoint (PMP) wireless access environment as well as Point-to-Point (PTP) modes. The IEEE 802.16 standard is designed to carry any higher

layer or transport protocol such as ATM, Ethernet or Internet Protocol (IP). It is expected that networks based on the IEEE 802.16 standard will have a range up to 30 miles and the ability to transfer data, voice and video at shared data rates up to 120 Mbps for LOS transmission in the 10-66 GHz frequency range and 70 Mbps NLOS in the 2-11 GHz frequency range. [Ref 1] Future IEEE 802.16 standards will add support for mobile platform communications and mesh networking capabilities.

The robust capability of this standard can potentially lend itself to numerous military applications. This research evaluates the IEEE 802.16 standards and technologies that are currently being developed in the commercial sector and how they might address shortcomings of existing military radio and data systems; specifically, with respect to the issues surrounding the STOM communications.

## **B. OBJECTIVES**

This research evaluates the IEEE 802.16 standards and technologies that are currently being developed in the commercial sector. Our discussions on IEEE 802.16 will focus on the MAC layer characteristics as they are currently implemented within the various IEEE 802.16 standards. We intend to compare the commercially developed IEEE 802.16 standard with the military developed JTRS Wideband Networking Waveform (WNW) in order to investigate and make recommendations on the COTS adaptations necessary to make IEEE 802.16 suitable as a complimentary technology within the STOM scenario.

## **C. RESEARCH QUESTIONS**

1. What are the STOM C2 and networking requirements?
2. Is IEEE 802.16 capable of meeting the STOM C2 networking requirements?
3. Can the IEEE 802.16 standard meet the same specifications of the JTRS WNW?
4. What adaptations would be needed for the military implementation of the IEEE 802.16 Standard?

## **D. SCOPE**

The scope of the research will include:

1. A discussion of networking requirements in a STOM scenario.
2. A discussion on the JTRS program and the Wideband Networking Waveform.
3. Analysis of the IEEE 802.16 standards in terms of potential DoD tactical applications will be addressed with emphasis on potential employment related to the STOM Networking.
4. Recommendations for an 'adapt from COTS' list of militarization features that US DoD services would need for future employment of the evolving IEEE 802.16 standards.

## **E. METHODOLOGY**

The methodology used to fulfill the requirements for this thesis will consist of the following:

1. Analysis of current STOM networking requirements.
2. Analysis of the IEEE 802.16 standards.
3. Comparison of IEEE 802.16 and the JTRS WNW.
4. Development of a working demonstration of a military application using IEEE 802.16-compliant (or pre-standard prototype) equipment.

## **F. ORGANIZATION OF THESIS**

This thesis is organized as follows:

**Chapter I** Introduction – provides a brief description of the objectives of the thesis, the scope, organization and methodology of study.

**Chapter II** STOM Research Study – Provides an overview of STOM networking requirements and planned capability of the WNW

**Chapter III** WNW Research Study – Provides an overview of the planned capability of the WNW

**Chapter IV** IEEE 802.16 Standard Overview

**Chapter V** Comparison of IEEE 802.16 to the WNW and STOM Requirements

**Chapter VI** Implementation and Testing-Provides overview of our testing with pre-standard IEEE 802.16 equipment

**Chapter VII** Adapt From COTS Discussion

**Chapter VIII** Summary and Follow-on Research- This chapter provides a short summary of the thesis and addresses possible future research.

## II. IDENTIFYING SHIP TO OBJECTIVE MANEUVER NETWORKING REQUIREMENTS

### A. INTRODUCTION

This chapter provides an overview of STOM and discusses issues associated with this doctrine from a networking perspective. This discussion will include the role that the JTRS has within STOM's proposed networking architecture. The intent is to identify the characteristics of STOM networking and to discuss how the JTRS is planned to address these requirements.

### B. OVERVIEW

STOM is the execution of combined-arms maneuver through and across the water, air, and land of the littoral battlespace directly to inland objectives. It is a tactical concept for the conduct of amphibious operations in support of OMFTS. The key aspect of STOM is that its aim is not to seize a beach for lodgment, but to project combat units ashore in their fighting formations and to sustain them against a decisive objective in order to ensure mission accomplishment. In STOM operations, the surface battlespace could begin in excess of 25 nautical miles (nm) OTH and could extend as far inland as 175 nm. [Ref 5]

The USMC STOM overview document states that the doctrine:

- **Focuses on the operational objective** and provides increased flexibility for landing force commanders to strike enemy critical vulnerabilities. No longer tied to phased operations and the cumbersome development of suitable beachheads, the landing force will concentrate on rendering the enemy ineffective. [Ref 6]
- **Treats the sea as maneuver space.** For the force that controls it, the sea is both a protective barrier and highway of unparalleled mobility. Turning the enemy's vulnerable flank, or exploiting gaps in his positions, the landing force thrusts combat units by air and surface deeply into his defensive array. Such maneuvers unhinge the enemy position, making his dispositions increasingly vulnerable and, finally, untenable. [Ref 6]
- **Emphasizes intelligence, deception, and flexibility** to drive planning, option selection, and maneuver execution. The common tactical

picture provided to all commanders by advanced command and control systems, combined with the inherent flexibility of STOM, will allow the landing force to exploit such gaps. [Ref 6]

- **Applies strength against weakness** and projects combat power through gaps located or created in the adversary's defenses. These gaps are not necessarily geographical; they may be exploitable weaknesses, such as limited night fighting capability, poor command and control, lack of endurance or low morale. [Ref 6] Figure 1 provides a general overview of STOM Scheme of Maneuver.
- **Creates overwhelming tempo and momentum.** Air and surface units maneuver from ships to inland positions faster than the enemy can effectively react. The landing force maintains the initiative and operates at a pace that allows it to dictate the terms of engagement. Operational surprise, through a combination of secrecy, deception, ambiguity, electronic warfare, lethal attack, and tactical successes, delays enemy recognition and disrupts his response. [Ref 6]
- **Integrates all elements in accomplishing the mission.** Whether operating in a joint or combined environment, the naval forces will employ all available assets in support of STOM in order to maximize the effectiveness of the landing force. [Ref 6]

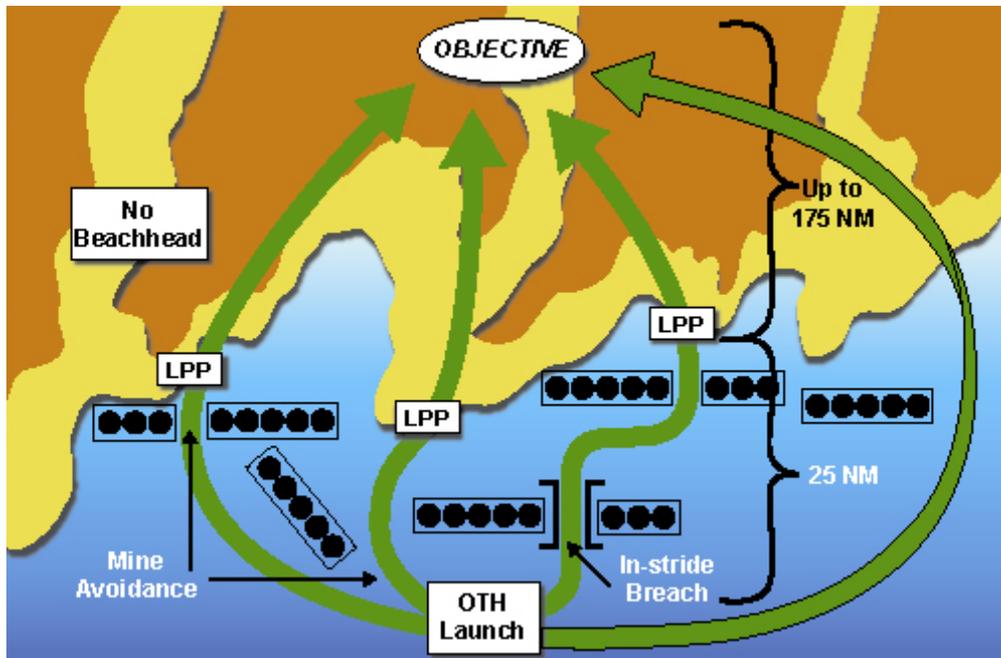


Figure 1. STOM Scheme of Maneuver (From: Ref 6)

The *STOM Concept of Employment (COE)* document emphasizes that STOM operations will be increasingly nonlinear—with operations taking place over large distances with widely dispersed forces. It also emphasizes that the objective of STOM is to generate and maintain overwhelming tempo through maneuver from the sea and to avoid the operational pause associated with a traditional force beachhead.

### **C. STOM NETWORK REQUIREMENTS**

An IEEE 802.16 “Adapt from COTS” implementation in STOM would attempt to address the networking architecture requirements as defined in the STOM Concept of Employment document from HQMC dated April 2003. This document specifies that networks in STOM would have five key characteristics. These include:

#### **1. Self-Organization**

Increased tempo of operations in a STOM scenario will require that its network to be self-organizing and meshed (vice point-to-point) network to the maximum extent possible. STOM will require establishing additional mobile, ad hoc networks that tie into dissimilar networks that carry needed information for the new mission. The varying Quality of Service requirements of the diverse users will allow the network to be capable of adapting to network congestion, loss of nodes, and topology changes while continuing to deliver the most important and urgent information. [Ref 6]

#### **2. Ubiquitous Communications Relays**

To affect a self-organizing meshed network, C2 nodes must not only act as transceivers (data sources/sinks, end systems) but as relay devices as well. STOM’s meshed network will require cooperative, multihop relay systems at C2 nodes for routing and forwarding traffic between distant nodes within the network. Similar to the routing that takes place on the Internet, forwarding would occur via a “best path” determination, which is based on factors such as distance and hardware capabilities. For example, vehicle-mounted radios are preferred relays over man-packed systems because of their greater power output and range. When factors such as intervening terrain or rapid movement make tactical unit C2 nodes insufficient, C2 node equipped aircraft provide range extension to prevent network fragmentation. [Ref 6]

### **3. Common Operational Picture (COP)**

The COP of all forces involved in the STOM operation is critical in a fluid battlespace. The nodes of the Marine Air-Ground Task Force (MAGTF) C2 system must be able to automatically or manually determine their own position location via the Global Positioning System (GPS) and transmit COP/CTP updates simultaneously to all applicable warfighter C2 display nodes. With this capability, commanders at all levels can reasonably expect all those within the unit to see the same relevant picture linked to mission, task, and purpose. This requires the means to broadcast or multicast the required information while maximizing use of the available bandwidth. [Ref 6]

### **4. Cooperative Engagement**

The MAGTF C2 system architecture enables “cooperative engagement” between platforms and sensors synchronized by commanders. The purpose of cooperative engagement is to support the commander’s decision making (e.g., directing the focus and distribution of maneuver forces and fires in multiple engagements) process. A cooperative engagement capability requires an enhanced quality of information—information that is relevant, timely (urgent), precise, and actionable. [Ref 6]

### **5. Consolidated Networks**

Joint C2 system nodes that are able to seamlessly operate with each other regardless of their location (ground, air, or sea-based) consolidate the number of current parallel networks. A consolidated network requires that bandwidth management measures be employed to efficiently use available bandwidth. The current multitude of dedicated voice channels must be replaced with a limited number of command voice channels and general-purpose data channels. Most information that is distributed is standard, redundant, or easily repeatable data such as friendly unit locations, target locations, or 9-line Close Air Support (CAS) briefs. [Ref 6]

## **D. SUMMARY**

The ability of WNW to effectively operate in STOM operations will permit greater flexibility and striking power capability while limiting the need to establish a preponderance of combat power ashore prior to offensive operations. While the added networking requirements to operate in a STOM scenario are robust, recent operations

illustrate the viability of this doctrinal shift. The Navy's Transformation Roadmap states that:

Both Operation ENDURING FREEDOM and Operation IRAQI FREEDOM demonstrated the potential of STOM by allowing the seizure of Forward Operating Base Rhino and critical oil production facilities at Al Zubayr directly from the sea base. Future STOM operations in the Global War on Terror must be capable of similar operations, at expanded ranges, in a shorter time period, and against a higher threat, without the benefit of available Host Nation support or extended planning and rehearsal opportunities. [Ref 7]

While traditional command centers may continue to be established ashore during sustained operations, the networking architecture for STOM will need to allow for the dynamic establishment of networks (both voice and data) between multiple organizations. The network would also have to account for both sea and shore based C2 nodes in the battlespace and dynamically support greater distances. This will require a C2 structure, and networking architecture to support it, which is capable of coordinating widely dispersed and advancing MAGTF and Joint forces within the battlefield. STOM's networking architecture will demand ad-hoc networking capabilities in addition NLOS, OTH and OTM communications between C2 nodes on the battlespace. In summary, the military requires its radio wide area network (WAN) to act as a seamless extension of the wired tactical network for mobile platforms.

THIS PAGE INTENTIONALLY LEFT BLANK

### **III. JTRS WIDEBAND NETWORKING WAVEFORM OVERVIEW**

#### **A. INTRODUCTION**

The DoD is in the process of fielding the JTRS to address the need for improved tactical communications on the battlefield. The software defined radios (SDR) of the JTRS program should increase communications capabilities through higher data throughput than legacy radios. Improved interoperability will be achieved by using common hardware components and standardized software architectures. This chapter provides an overview of the JTRS WNW and discusses issues associated with it as it applies to STOM. This discussion will include the role that the JTRS WNW has within STOM's proposed networking architecture. The intent is to identify likely requirements for an IEEE 802.16 "adapt from COTS" list by using WNW for comparison.

#### **B. JOINT TACTICAL RADIO SYSTEM OVERVIEW**

##### **1. Overview**

The DoD realized two key facts following the First Gulf War in 1991 which were the impetus for change in the RF battlefield communications systems. First, the DoD needed to field systems that could keep pace with the expanding requirements of the operating forces. Second, DoD needed radio systems capable of delivering higher throughput compared to the legacy systems used by our combat forces today. [Ref 8]

Most of the existing tactical radio systems fielded by DoD are based on legacy technologies dating as far back as the 1960s. This fact yields systems that require extensive depot level equipment or component changes to implement new capabilities. The singular functionality design of legacy radios does not allow incremental or modular upgrades to increase the choices of waveforms and the bandwidth within those waveforms, or to modify message system standards. The bottom line is that these radio systems are not flexible enough to meet the evolving demands of the US military services. [Ref 8]

At the tactical level, JTRS will replace SINCGARS and Enhanced Position Location Reporting System (EPLRS) radios that produce their signals through their

hardware alone and consequently lack much of the flexibility of SDRs. The JTRS modular design of software and hardware is intended to facilitate upgrades and the replacement of functional components. By combining functions and using common components, this program will reduce the number of radios needed by the military (250,000 JTRS radios, compared to 750,000 legacy radios currently in use). [Ref 11]

The US military's post-Gulf War emphasis on Network Centric Warfare and Information Superiority has increased the bandwidth requirements on the modern "digital" battlefield. Shifting from platform centric warfare, which had previously characterized modern warfare, the DoD envisions future conflicts where networks connecting platforms play the leading role. The belief is that forces that fight using NCW would be able to change the conflict continually, and can accelerate the speed of change. [Ref 9] Thus, the efficient dissemination of information to distributed warfighting participants would now be the key to success. This information would include imagery, the "tactical scene" via tactical data messages, messaging information, and real-time interactive applications such as digital secure voice. [Ref 10]

Pushing the aforementioned data down to the tactical level requires an increasing amount of bandwidth and is taxing legacy systems to the limit. Migration to NCW will only increase the need for more robust networking capabilities to support future operations. For example, according to the Joint Forces Command, U.S. forces in OIF had access to 42 times the bandwidth available in Desert Storm via TACSAT and terrestrial RF based networks. However, despite this improvement US forces experienced continuing shortages in the availability of bandwidth. [Ref 1] This is way JTRS is programmatically considered as a crucial link in the DoDs future vision of the Global Information Grid. (See figure 2)

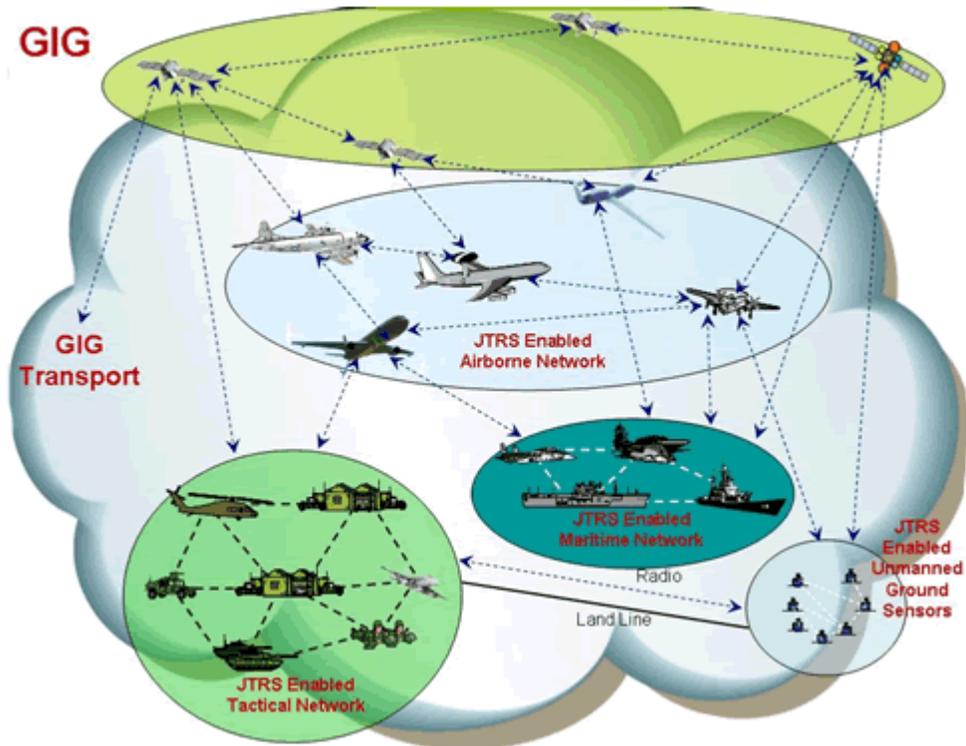


Figure 2. JTRS within the Global Information Grid (From: Ref 11)

The current shortcomings in tactical data networking transmission to maneuvering forces that would operate in STOM operations can mostly be attributed to deficiencies in high bandwidth NLOS and OTM capabilities in today's RF based tactical networks (e.g., EPLRS and SINCGARS). JTRS will introduce the new Wideband Networking Waveform (WNW), which is intended to address the demanding networking requirements of future conflicts. All four military services see the WNW as a critical part in providing network connectivity on the future battlefield. For the Marine Corps, JTRS radios using the WNW, operating as wireless bridges, will interconnect various tactical C2 nodes operating out of Expeditionary Fighting Vehicles (EFV), High Mobility Multipurpose Wheeled Vehicles (HMMWV), or Light Armored Vehicles (LAV).

## 2. JTRS Wideband Networking Waveform<sup>1</sup>

The WNW is intended to provide a new wireless environment to supplant 20- to 30-year-old legacy waveforms which are struggling to keep up with the increasing NCW bandwidth requirements. A recent Congressional Budget Office study on battlefield communications determined that current tactical radio systems provide insufficient data throughput to support the future exchange of command-and-control and fire-support data. [Ref 8] Such time critical data would be vital for the successful operation implementation of STOM.

The JTRS WNW network is planned to provide connectivity of both backbone links (tier 2) and subnet links (tier 1) and provide gateway functionality between the two. (See Figure 3) The WNW is planned to be capable of operating in several different modes such as anti-jamming, low probability of detection (LPD) and intercept (LPI), and a mode for bandwidth efficiency that permits large amounts of data to move in low-bandwidth environments. Conversely, a big-pipe, high-data-rate mode also is part of the waveform in order to provide tactical WAN capability. [Ref 12]

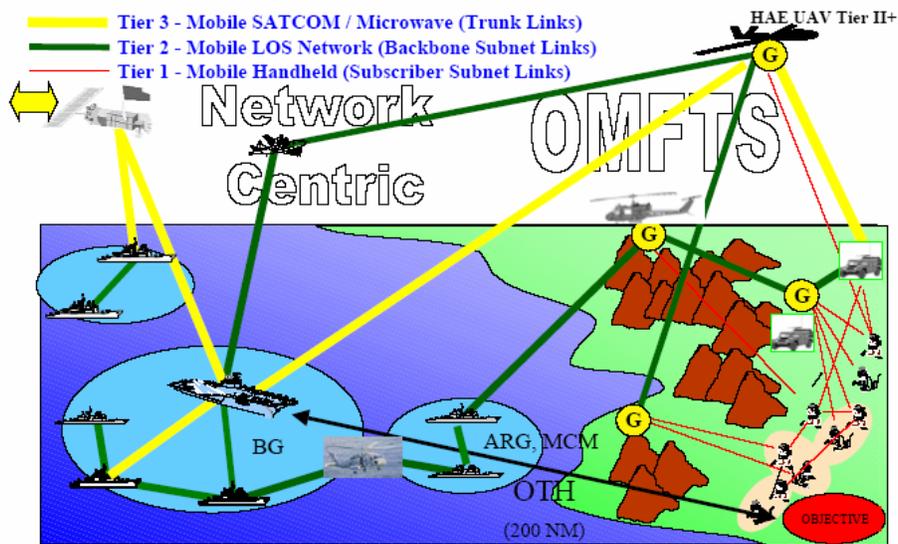


Figure 3. JTRS Interconnected Network (From: Ref 12)

<sup>1</sup> The specifications of the WNW in this research are based on the *Performance Specification JTRS Software Waveform, Wideband Networking Waveform (WNW)* document dated 6 Aug 02 and are current as of this writing.

### 3. WNW Employment within STOM

Depending on the radio's size, weight, and power requirements the WNW will be employed in a variety of ways. The primary role of the WNW will be in providing connectivity between Combat Operations Centers (COCs), ground mobile nodes (e.g. HMMWV, LAV, AAV) and airborne platforms. As with many of the Marine Corps' digital radios, the OTH capability of the WNW JTRS nodes will still require airborne (manned or unmanned) relay platforms. (See Figure 4)

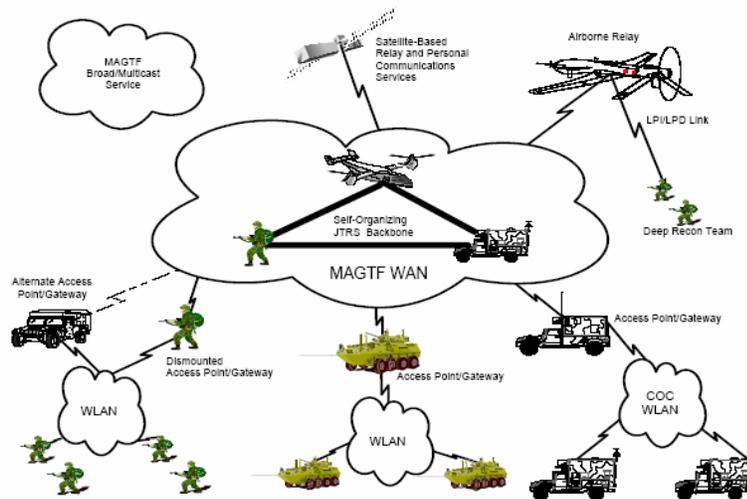


Figure 4. JTRS Concept of Employment (From: Ref 12)

Once the WNW can be implemented on hand-held radios, it will be operated by small tactical units. This will provide wideband LAN functionally down to the lowest tactical levels. (See Figure 5) For a truly network centric force, these lower echelon radios will be capable of providing interconnection within units and automatic relays to other units. [Ref 6]

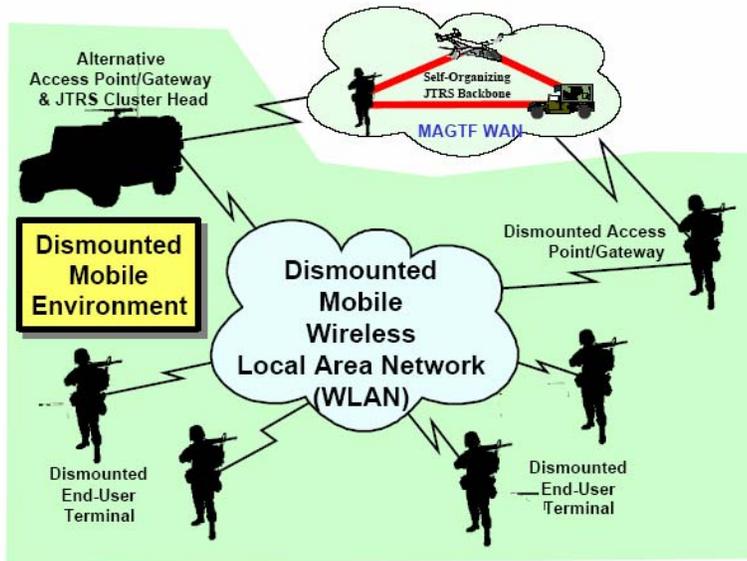


Figure 5. Dismounted Mobile WLAN (From: Ref 12)

## C. WNW PLANNED OPERATING REQUIREMENTS

### 1. Performance Characteristics

The JTRS's WNW will support point-to-point operation modes that optimize the throughput and latency between two nodes. The data rates of the WNW link will be optimized by negotiated automatic changes based on channel conditions or restricted modes of operation. The specified throughput rates will have to be sufficient to support a broad range of data, voice, and video applications in a mobile network. Currently, it is planned for the JTRS WNW to support user throughputs greater than 2 Mbps as a threshold and 5 Mbps as an objective for most common operating conditions/scenarios. [Ref 12]

With these data rates, the WNW will far exceed the throughput of today's SINCGARS and EPLRS systems. The SINCGARS is undergoing enhancements that include: reduced co-site interference; improved error detection and correction; reduced network access delay; and a GPS interface to obtain accurate time and position location. Even with these improvements, SINCGARS will only increase information throughput from 1.7 kbps to 4.8 kilobits per second (kbps). Test results indicate that the enhanced SINCGARS radio will be able to reliably pass data at 4.8 kbps up to a range of 35 km in a benign environment. The EPLRS system, which now incorporates Very High Speed

Integrated Circuit (VHSIC) technology, can provide throughput to individual EPLRS users from 4 kbps to 12 kbps. [Ref 13] Secure Mobile Anti-jam Reliable Tactical-Terminals (SMART-T), which provides some MAGFT WAN capability, currently has an average effective throughput of 481 kbps. The point-to-point (PTP) throughput rates of these systems are summarized in Table 1.

Radio	Point-to-Point Data Throughputs	
	Max Engineering (kbps)	Average Effective (kbps)
SINCGARS	16	1.7
EPLRS	128	13.3
SMART-T	4620	481

Table 1. Throughput Comparisons for MAGTF Communication Systems (From Ref 8)

The other performance characteristics of the WNW will be dependent on the capabilities in terms of power and antenna type of the host platform. JTRS systems will be employed on airborne, maritime and ground platforms in a diverse range of environments. The range, power and propagation requirements will thus be dependent on the type of platform that which the JTRS is employed on. The planned requirements taken as described in the WNW FDD are summarized in Table 2.

## 2. Networking Requirements

The JTRS WNW will be used in widely varying mission scenarios. JTRS employment may range from a few radios in a small area, a few radios in a fairly large area, many radios in a small area, to many hundreds of radios spread over a large area. In any network there could be a mixture of very short distances and very long distances between radios. Operating environments will range from desert to urban to mountainous to at sea. Some deployments may have single links joining areas of nodes to form a large network. To maintain flexibility, and to support operations like STOM, the WNW is planned to accommodate the “ad-hoc” or mesh networking capabilities within many different types of terrain and topologies.

Item	Description
Range (LOS point-to-point)	Air-to-Air* at least 370 km (200 nmi) Air-to-Ground/Surface* at least 370 km (200nmi) Ground-to-Ground at least 10 km (5.4 nmi) Ship-to-Ship at least 28 km (15 nmi) Ship-to-Shore at least 28 km (15 nmi)
Power Control	The JTRS WNW shall automatically control power to reduce the amount of interference and allow for frequency reuse.
Terrain/Propagation Environment	The JTRS WNW shall be able to operate in all tactical RF propagation environments such as hilly, mountainous, dense vegetation, desert, and urban terrain. The JTRS WNW shall be robust and adaptable to support connectivity during rapidly changing distances and orientations between nodes. The JTRS WNW shall adapt to the presence of Doppler effects, fading, multipath, and other RF channel conditions in the operating environments and host platform operating profiles.
Frequency Spectrum	WNW and host JTRS shall incorporate adequate flexibility with respect to operating frequency, bandwidth, modulation, and power
Noise Environment	The JTRS WNW shall be able to operate in tactical RF propagation environments. These propagation environments include unintentional (atmospheric, background, self-interference, and co-site interference) and intentional (jamming) noise.
Anti-Jamming Capabilities	The JTRS WNW shall include an anti-jam (AJ) feature of operation for protection to prevent the enemy disruption of services.

Table 2. WNW Performance Characteristics (After Ref 12)

The characteristic of a mesh network is that there is no central orchestrating device. Instead, each C2 node may act as a relay point for other nodes. In the partially meshed topology that we would likely see in the STOM scenario, nodes are connected to only some, not all, of the other nodes. Although not specifically mentioned in the WNW specification document, the “ad-hoc” networking requirements imply extensive use of the developing area of Mobile Ad-hoc Networking (MANET). The Internet Engineering Task Force (IETF) MANET Working Group offer insight to the challenges that would be faced in a STOM ad-hoc network topology. They state that:

MANETs must contend with a difficult and variable communication environment. Packet transmissions are plagued by the usual problems of radio communication, which include propagation path loss, signal multipath and fading, and thermal noise. These effects vary with terminal movement, which also induces Doppler spreading in the frequency of the transmitted signal. Finally, transmissions from neighboring terminals, known as multi-access interference, hostile jammers, and impulsive interference, e.g., ignition systems, generators, and other non-similar in-band communications, may contribute additional interference. [Ref 9]

The network’s dynamic management of complex routing information would be the biggest challenge as the maneuvering forces move toward the objective. However, mesh networks would be more reliable than other kinds of networks, because if a single

node goes down, other nodes are available. The mesh capabilities of the WNW based network would in turn provide lower echelon units interconnectivity as well as provide automatic relays/forwarding to surrounding units. Table 3 depicts a summary of the networking characteristics planned for the WNW.

Item	Description
Mesh and ad-hoc networking	The WNW shall provide self-organizing, self-healing networks capable of responding to dynamic changes in connectivity. The WNW network shall provide routing and management protocols/schemes that can rapidly respond to ad hoc changes in network topology caused by such things as node addition and deletion, node movements, antenna shadowing or orientation, terrain masking, or interference.
Network Size	The WNW network shall have the capability to integrate an initial network of 150 nodes spread over the operational area into a single network within 15 minutes of system initialization.
Topology	The WNW network shall integrate any node operating in the area of operation into the network. The nodes may be operating at altitudes of between sea level and 65,000 feet above sea level
Mobility Management	The JTRS WNW network design shall support connectivity to and between ground or surface mobile platforms moving at speeds relative to other platforms in excess of 120 mph while maintaining network connectivity and traffic transmission integrity. The JTRS WNW network design shall support network connectivity and traffic transmission integrity to and between airborne platforms for speeds relative to other platforms up to 900 knots at altitudes of tens of feet to over 65,000 feet above sea level.

Table 3. WNW Networking Requirements (After: Ref 12)

### 3. Network Services

In radio networks the bandwidth available will always be less than the demand offered and a means of Quality of Service (QoS) control is required. [Ref 15] In general terms, QoS refers to the conditions within a network that will support the delivery of time sensitive or low redundancy services with a minimal perception of degradation. It encompasses the following:

- Control of throughput rate
- Control of overall delay or latency
- Control of packet-to-packet delay (jitter)
- Control of bit error rate (bit error rate)

Unlike in the commercial world, where everyone has a more or less equal footing, military network environments often need to assign priority to users or even individual

packets. An example of this is the tactical data exchange. Tactical data messages are generally single-datagram messages containing information on the location, bearing, identification, etc., of entities detected by sensors. Differential Services that would be implemented in the WNW would ensure that important messages, such as a possible WMD attack message, were given priority over less important messages, such as a friendly, slow- moving tanker's heading. [Ref 33]

Additional layers of complexity of the network due to mesh routing and the “ad-hoc” networking topology would further tax the network environment that will likely have restricted communication resources, limited bandwidth, and possible degradation and/or denial of service. [Ref 33] Table 3 depicts a summary of the networking services planned for the WNW.

Item	Description
Traffic support	The WNW network will be used to support unicast, multicast, and broadcast of traffic types to include large data files (>1 Megabyte), video, video teleconferencing, voice, and short or formatted message traffic.
QoS	The WNW shall support Quality of Service (QoS) mechanisms to support differential handling of traffic classes according to their service requirements. The mechanisms shall include precedence handling that discriminates among traffic based on its mission importance. To support an integrated mix of traffic types, including a variety of data, voice, and video, in a variety of operating conditions, the ability to preset and negotiate QoS parameters should be supported. At a minimum, the WNW shall support both DiffServ(RFC 2474) and IP Precedence (RFC 791).
Packet Delivery	The WNW link layer shall provide packet delivery schemes that support assured (acknowledged) and best effort (unacknowledged) message delivery. Assured delivery to broadcast or multicast recipients should use network efficient methods. Receive-only nodes will receive only best effort delivery.
Channel Access	<p>The WNW link layer shall provide channel access schemes which:</p> <ol style="list-style-type: none"> <li>a) Manage access from multiple nodes that are in line of sight of each other</li> <li>b) Minimize packet collisions between these nodes or at nodes in line of sight of two transmitting nodes which are not in line of sight (“hidden node” problem)</li> <li>c) Maximize simultaneous transmission to receivers that are not in line of sight of each other (“exposed node” problem)</li> <li>d) Provide fair access between nodes transmitting data with the same precedence in the network.</li> </ol>
Multimedia Traffic	In addition to data traffic, the WNW will carry real-time traffic, including voice and video. Voice and video have strict requirements on delivery delay (latency), delay variation (jitter), and packet drop rates. The WNW shall support QoS mechanisms to ensure optimum performance for multimedia traffic, including data, voice, and video.

Table 4. WNW Requirements for Network Services (after Ref 12)

#### 4. Network Layer Addressing

Network Layer addressing can be divided into three specific categories: unicast, broadcast and multicast traffic. During unicast transmission, one machine talks directly with another machine. During broadcast transmissions all machines absorb the traffic, regardless of their interest in receiving the information. Multicast could be considered selective broadcast, whereas information is sent to a selective number of machines. The broadcast nature of many RF networks and the need for broad dissemination of information to warfighting participants makes multicast the general case for information flow in the tactical environment.

Mechanisms which can enhance the effectiveness of an network to provide resource reservation, priority, and service quality guarantees are imperative the highly dynamic and “ad-hoc” nature of STOM operations. While, the ability to multicast information presents challenges in addressing and routing, it would be imperative to help conserve valuable network resources. Table 5 depicts how the WNW is planned to accommodate network addressing.

Item	Description
Network Layer Addressing	The WNW network shall use Internet Protocol addressing schemes, including support for subnet addressing and unique and group addresses
Routing	The WNW network shall use routing protocols/schemes that support: a) Unicast, multicast, and broadcast transmissions to nodes or users on any part of the WNW network, or on other military or commercial networks; b) Scalable networks of from 2 to 1,630 nodes which may be densely or sparsely distributed across an operational area; c) Ad hoc changes in network topologies caused by such things as node addition and deletion, node movements, antenna shadowing, terrain masking, or interference without overwhelming the network with routing overhead information; d) Nodes with varying functionality/modes e) Route transit as well as local traffic.

Table 5. WNW Requirements for Network Layer Addressing (After: Ref 12)

#### 5. Information Assurance and Security

As with any military system, information assurance (IA) and security is of paramount importance. Information assurance can be described in four general categories: availability, confidentiality, authenticity, and integrity. Confidentiality is the characteristic that the information being transmitted is only being made available the

authorized person at authorized times and in appropriate manner. Integrity is when the information sent is received without modifications without the owner's knowledge. Authentication is when the state/purported originator of the information is the true originator. And finally, availability is having access to the data in a reasonable amount of time.

While the WNW's IA specifications depicted in Table 6 are rather broad, the requirement for NSA Type-1 is specifically mentioned. NSA's Type-1 encryption would secure the entire WNW packet. This would provide secure communication of data and network header information (COMSEC and NETSEC) for all network layers. Concerns for denial of service attacks, traffic analysis monitoring, etc., usually dictate that tactical RF communication networks provide link layer security mechanisms like NSA's Type 1. To address transmission security (TRANSEC) issues such traffic flow analysis and enemy jamming, the WNW will be required to be capable of operating in LPI/LPD and anti-jamming (AJ) mode. The TRANSEC modes of operation would have to be balanced with the need for security versus the network throughput requirements, environment, frequency band (s) of operation, synchronization requirements, and threat. The degree to which these functions are implemented would be configurable by a network administrator or the JTRS operator.

Item	Description
Confidentiality	The JTRS WNW and associated JTR Set shall provide for NSA Type 1 protection for user data transmitted and shall provide header cover.
Availability	The JTRS WNW shall provide the means to recover from loss of cryptographic or TRANSEC synchronization and to resynchronize.
Integrity	The JTRS WNW and associated cryptographic functions shall provide anti-spoofing features to assure that user data packets exchanged through wired and wireless networks cannot be maliciously or unintentionally modified.
Identification and Authentication	The JTRS WNW shall provide the means to identify and authenticate nodes attempting to join the network. High grade authentication as defined by NSA shall be employed. The WNW shall employ identification, authentication, and authorization and security association mechanisms to support key management functions through wired and wireless networks. Access controls shall be employed to limit WNW reconfiguration to the appropriate personnel or organizations.
Waveform Cryptographic Functions	Type 1 cryptographic algorithm(s) shall be used to protect classified and sensitive user information transmitted through wireless networks. Required cryptographic functions include encryption and decryption of data, identification and authentication, header cover or protection (may also be provided through readdressing techniques), and TRANSEC key stream generation.
TRANSEC	TRANSEC design features (s) shall consider throughput requirements, environment, frequency band (s) of operation, synchronization requirements, and threat. The TRANSEC design should minimize the probability of intercept (LPI) for LPI modes and maximize anti-jam (AJ) capabilities within the envelope of the throughput requirements and spectrum availability. The level of LPI and AJ capabilities should be adaptable to accommodate degradations in the environment.

Table 6. WNW Requirements for Information Assurance and Waveform Security (After: Ref 12)

## 6. Program Status

The intent of the JTRS program office was for the WNW to be developed in stages: stage 1, a wide-band waveform available by 2004; stage 2, a midband waveform that has a (LPI/LPD capability by 2005; stage 3, a midband waveform with "anti-jam" capability by 2005; and stage 4, a narrow-band, special-access waveform by 2006. [Ref 8] However, the development of the WNW has been delayed as of this report and estimates on when this capability will be fielded were not forthcoming.

Part of the reason behind the fielding delays is the fact that the technologies behind JTRS and the WNW are still emerging. These delays in development are posing significant risk to their respective tactical fielding. A recent analysis sponsored by the Army noted the high level of risk associated with the JTRS program's successful

completion were due to the multitude of engineering challenges that it faces. Elements that contribute to that assessment include the complexity of the software development required, the size and weight constraints imposed on the radios, the amount of power that they will consume, the heat that they will dissipate, and interference problems that are anticipated among the waveforms when the radios are co-located. [Ref 8]

It will cost the DoD an estimated \$40 billion price tag to replace every radio with the JTRS. A GAO report of the status and outlook of the JTRS states the following:

The program still faces several managerial and technological challenges that could affect the Department of Defense's (DOD's) ability to develop and procure JTRS radios successfully. These include managing requirements and funding, maturing key technologies, integrating system components, testing, and developing secure communications. The most significant challenge we identified is the lack of a strong, joint-management structure. [Ref 8]

As a consequence, several program development efforts, such as handheld radios, have been delayed. In the meantime, the services will have to purchase more existing radios with fewer communications capabilities, which may further delay the delivery of the new tactical wideband waveform for mobile users<sup>2</sup>.

#### **D. SUMMARY**

Both the Marine Corps and the Navy are firmly committed behind the concepts of OMFTS and STOM; as seen by the procurement of major weapon systems such as the JTRS, the Expeditionary Fighting Vehicle, and the MV-22 Osprey which support these doctrinal concepts. However, the risks associated with the development of the JTRS and its WNW capability pose a valid question as to whether the JTRS and its WNW will be fielded in time to support these operations in the near future.

---

<sup>2</sup> DoD received a recommendation from Congress in July 2004 to relax restrictions on the services which inhibited them from purchasing additional "legacy" systems. DoD had wanted the services to keep their radio procurement funds focused on JTRS vice procurement of "legacy" radio systems.

## **IV. IEEE 802.16 STANDARD OVERVIEW**

### **A. INTRODUCTION**

This chapter will explore the IEEE 802.16 standards, the capabilities they enable and their advantages over current wireless networking technologies. We will begin with a general discussion of the standard, followed by a brief comparison of the IEEE 802.16 and IEEE 802.11 standards. Subsequent sections will discuss network architectures, and features of the standard.

### **B. WHAT IS IEEE 802.16?**

The IEEE 802.16 is a standard, designed by the IEEE, for local and metropolitan area network (MAN) fixed broadband wireless access. The IEEE 802.16 standard itself is titled "Air Interface for Fixed Broadband Wireless Access Systems" and was approved by the IEEE on 6 December 2001. The standard applies to frequencies between 10 and 66 GHz, while the IEEE 802.16a standard covers frequencies between 2-11 GHz. However, the MAC portion of the standard is entirely frequency independent, and thus leaves open the possibility of future adaptations of the standard.

Systems designed using the IEEE 802.16 standard will be capable of performance comparable to cable, DSL or T1 systems, with shared data rates up to 120 Mbps for LOS transmission in the 10-66 GHz frequency range and 70 Mbps NLOS in the 2-11 GHz frequency range. [Ref 1] These systems will be able to provide simultaneous support to "more than 60 businesses at T1 level and hundreds of homes with DSL rate connectivity at 20 MHz bandwidth". [Ref 1] In addition to these capabilities, IEEE 802.16 systems will be capable of providing:

- Long range operation: radius up to 30 miles
- Non Line of Sight (NLOS) performance
- Ability to operate in high multipath environment
- Guaranteed service levels
- Superior scalability

- QoS capable of supporting voice and video applications
- High Spectral efficiency
- Routable networks within an IEEE 802 framework
- Ability to support multicast traffic

The primary advantages of IEEE 802.16 systems over wired systems include: cost savings, quick setup and more complete coverage. While IEEE 802.16 systems are not inexpensive, the costs are still much less than those associated with wired systems. Cost savings are achieved by eliminating the need for wired infrastructure investment and monthly leasing expenses. Installing an IEEE 802.16 system and establishing service requires relatively little time when compared to the three months it might take to establish T1 service in some areas. [Ref 1] While DSL services may not be available in areas that are too far from the local telephone company switch, and similar services are often not available in areas of low subscriber density, IEEE 802.16 service can easily and cost effectively reach these areas.

Typical applications for IEEE 802.16 in the commercial sector may include cellular backhaul, broadband on demand and best connected wireless service. IEEE 802.16 is particularly well suited for providing these services. In a cellular backhaul role, IEEE 802.16's robust bandwidth management makes it a reliable alternative to leased wire. This technology is particularly well suited for businesses that relocate frequently within a metropolitan area, such as construction companies, and trade shows. These companies are able to provision wireless broadband service quickly as they move from one location to another without the need to re-wire. Similarly, the development of hand off procedures between IEEE 802.16 networks will allow a user to roam from network to network, connecting to the best available service in each area. [Ref 17]

### **1. Comparison of IEEE 802.11 and IEEE 802.16**

In recent years IEEE 802.11 has experienced a widespread adoption in residential, corporate and even military settings. The IEEE 802.11 has been used primarily in a data access role, through the creation of "hotspots", a small area where network users can roam unencumbered by wires. Additionally, IEEE 802.11 has been used to provide

extension of existing networks into areas where cabling might be impractical or cost prohibitive, building to building connectivity, last mile data delivery, and connectivity for small office /home office (SOHO) networks and mobile offices.

For reasons that will be outlined below, IEEE 802.11 is not well suited for "backbone" or core data distribution roles within a network, or as a public access medium. Among IEEE 802.11's primary limitations are its relatively short range, poor scalability, and security vulnerabilities. Table 7 shows a comparison of IEEE 802.11 and IEEE 802.16 standards.

As shown in Table 7, the signal from the typical IEEE 802.11 access point (AP) propagates only about 200 yards. This limits the mobility of users and requires the use of many access points for large coverage areas. In addition to IEEE 802.11's inherent range limitations, this standard is very vulnerable to the effects of multipath, and fresnel zone blocking. These vulnerabilities limit IEEE 802.11x's ability to operate in environments with many vertical obstructions and to support NLOS communications.

IEEE 802.11's use of the Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) access control protocol lies at the heart of its poor scalability. In this protocol, APs "sense" whether there is any traffic on the wire prior to transmitting, and transmit only when the medium is clear. Unfortunately, due to signal propagation delays and hidden node problems, the possibility of collisions always exists, and this probability increases dramatically as more users are added to the network. As users increase, collisions increase, eventually creating a situation where retransmissions and collisions begin to severely limit throughput.

The IEEE 802.11 standard has been plagued by security vulnerabilities associated with the Wireless Equivalent Privacy (WEP) encryption protocol. For reasons that are beyond the scope of this thesis, the WEP protocol is particularly vulnerable to encryption cracking. WEP has been considered so vulnerable, that the IEEE has developed a replacement, the WIFI Protected Access (WPA) protocol, which will be available in equipment following the 802.11i protocol.

Feature	802.11	802.11b	802.11a	802.11g	802.16	802.16a
Assigned Spectrum	2.4 GHz	2.4 GHz	5.8 GHz	2.4 GHz	10-66 GHz	2-11 GHz
Access Control	CSMA- CA	CSMA- CA	CSMA-CA	CSMA- CA	TDMA / DAMA	TDMA / DAMA
Maximum Throughput	2 Mbps / user	11 Mbps / user	54 Mbps / user	54 Mbps / user	124 Mbps / channel	70 Mbps / channel
Propagation Distance	200 yards	200 yards	200 yards	200 yards	> 1 mile	Several miles
Network Architectures	PMP	PMP	PMP	PMP	PTP, PTCM	PMP, PTCM, Mesh
Modulation	Frequency hopping- direct sequence	Frequency hopping - direct sequence	OFDM	OFDM	QUAM, PSK	OFDM
Adaptive Modulation?	No	No	No	No	Yes	Yes
Full Mobility?	No	No	No	No	No	Upcoming
QOS?	No	No	No	No	Yes	Yes

Table 7. Comparison of 802.11 vs. 802.16 (After: Ref 18)

The IEEE 802.11 standards enjoy two advantages: price and prevalence. Currently IEEE 802.11 network interface cards available can be purchased for about \$60, and APs can be had for less than \$100. The second advantage IEEE 802.11 networks currently enjoy is that they are more prevalent than ever before. Today it is not uncommon to find hotspots in airports, bookstores, coffee shops, etc. This prevalence results in more users of this protocol, which in turn produces a more widespread acceptance of the technology by vendors and providers.

In contrast to the IEEE 802.11 standards, equipment based on the IEEE 802.16 standards boasts longer ranges, more robust signals capable of NLOS communication, the ability to handle many users while supporting high QOS and guaranteed service levels, and superior security. In addition to these advantages, future versions of the standard will support full mobility and mesh networking capabilities. It is also important to note that

the price of IEEE 802.16 equipment is expected to drop once it becomes more commonly available. IEEE 802.16's capabilities and standards will be covered in more detail in the next section.

The IEEE 802.16 standard is the ideal standard for a public access medium. Its ability to support thousands of users simultaneously is primarily due to its use of time division multiple access (TDMA) with demand assigned multiple access (DAMA) scheduling for MAC procedures. The specifics of IEEE 802.16's MAC protocol will be examined in greater detail in later sections.

## **2. WiMax and Interoperability**

The Worldwide Interoperability for Microwave Access (WiMax) forum is an organization of equipment and component suppliers dedicated to promoting the adoption of IEEE 802.16 compliant equipment. [Ref 1] This organization tests and certifies products for interoperability and standards compliance. Additionally, the WiMax forum creates what it calls system profiles, which are *specific implementations, selections of options within the standard, to suit particular ensembles of service offerings and subscriber populations*. [Ref 18] The goal of these system profiles is to increase the adoption rate of IEEE 802.16 equipment by simplifying the setup of this equipment. Prominent members of WiMax include Intel Corporation, Fujitsu, Motorola, AT&T, and many others.

## **C. THE IEEE 802.16 STANDARDS**

The creation of the Wireless MAN standard is important because it results in a research and development costs savings to equipment manufacturers, which in turn insures interoperability of the equipment they produce and ultimately leads to a reduced risk on the part of equipment operators. The fact that the standard has been developed within the IEEE 802.x framework means that it is possible to both bridge and route traffic to other IEEE 802.x networks (e.g., .11, .3, etc.). In addition to these benefits, a standard provides minimum performance criteria for equipment manufacturers to meet.

The following is a list of the IEEE 802.16 family of standards along with a brief summary and the current status of each. It is important to note that in July 2004, the

IEEE approved the draft standard known as IEEE 802.16 - 2004 which combines the IEEE 802.16, IEEE 802.16a, and the IEEE 802.16.c standards into one document.

- IEEE 802.16- The "Air Interface for Fixed Broadband Wireless Access Systems" was approved on December 2001. Designed for Wireless MANs operating in the 10-66 GHz frequency range. [Ref 19]
- IEEE 802.16.2- Addresses recommended practices for the operation of multiple fixed broadband wireless systems. Published in 2001, this standard applies to the 10-66 GHz frequency range. [Ref 19]
- IEEE 802.16a- This extension to the IEEE 802.16 standard addresses the operation of systems in the 2-11 GHz frequency range, for both licensed and unlicensed operation. This standard was approved in Jan 2003. [Ref 19] A substandard that addresses Mesh network architectures is included as part of this standard. [Ref 18]
- IEEE 802.16c- Specifies system profiles designed to improve interoperability in the 10-66 GHz frequency range. This standard was approved in December 2002. [Ref 19]
- IEEE 802.16e- Addresses both fixed and mobile operations in licensed bands in the 2-6 GHz frequency range. [Ref 19] Mobile operation is designed for vehicles moving up to 150 km/hour.
- IEEE 802.16f - Addresses mesh networking architectures.

#### **D. DEPLOYMENT ARCHITECTURES**

A typical IEEE 802.16 network is made up of one central base station (BS) that communicates with one or more Subscriber Stations (SS). This communication can take place in several different network architectures to include:

- Point-to-point (PTP): Connections between two nodes, in this case a BS and a SS. PTP links have the advantage of extended range over PMP links.
- Point-to-multipoint (PMP): A connection between one BS and multiple SS nodes. Generally involves the use of sector or omni-directional antennas to create a coverage area with more than one SS. This architecture supports multicast communication.

- Point-to-consecutive point (PTCM): Involves the creation of a closed loop through multiple PTP connections.
- Mesh: IEEE 802.16a substandard, where each node is able to route data adaptively to its destination. Mesh architectures are self organizing and self healing.

## **E. THE PHYSICAL LAYER (PHY)**

The IEEE 802.16 standard and the IEEE 802.16a standard each specify a separate air interface due to differences in frequency range, but they both use the same MAC protocol. This ability to apply one MAC to multiple PHY interfaces has much potential application in both commercial and military applications. The two separate air interface standards make it possible for operators to take advantage of the strengths of either frequency range dependent on the deployment situation. For military purposes, it may be possible to adapt the IEEE 802.16 standard to employ a PHY that is better suited to military operations. These military applications will be discussed further in Chapter Seven of this thesis.

### **1. 10-66 GHz Systems**

Higher frequency microwave signals in the 10-66 GHz frequency range are addressed in the IEEE 802.16 standard. This standard supports only LOS operation and has shorter ranges of only a few kilometers, when compared to lower frequency systems. [Ref 18] This frequency range is capable of supporting data rates up to 120 Mbps. [Ref 21] The primary advantage of this frequency range over others is the abundant availability of bandwidth. Unlike the lower frequency ranges where frequency bands are often less than 100MHz wide, most frequency bands above 20GHz can provide several hundred megahertz of bandwidth. [Ref 18] Additionally, channels within these bands are typically 25 or 28 MHz wide. [Ref 21]

IEEE 802.16 utilizes a single carrier modulation (WirelessMAN-SC) using either (1) quadrature phase shift keying (QPSK), (2) 16-bit quadrature amplitude modulation (QAM) or (3) 64 QAM. [Ref 25] Communication on the downlink, which typically involves one BS talking to multiple SSs, is handled using time division multiplexing (TDM). The uplink uses TDMA combined with DAMA techniques. [Ref 21] The uplink

channel is divided into various time slots and the assignment of those slots is dynamically controlled by the MAC of the BS and based on the moment to moment needs of the system.

IEEE 802.16 allows for both time division duplexing (TDD) and frequency division duplexing (FDD). In TDD, the uplink and downlink take turns transmitting on a shared channel, while FDD allocates separate channels to each. The standard also supports half duplex FDD where the uplink and the downlink share one channel much like in TDD.

Another feature unique to the higher frequency IEEE 802.16 standard is the use of adaptive burst profiling. Adaptive burst profiling makes it possible for the radio to make adjustments to the modulation and coding schemes being used in response to changing environmental conditions and the resulting signal quality. [Ref 20] Systems using adaptive burst profiling will constantly monitor signal quality and make adjustments on a frame by frame basis, shifting between the more efficient and less robust QAM to the less efficient but more robust QPSK as needed.

## **2. 2-11 GHz Systems**

The IEEE 802.16a standard addresses lower frequency microwave signals in the 2-11 GHz frequency range. Signals in this frequency range have many advantages over higher frequency signals to include the ability to penetrate walls, NLOS performance, longer ranges than higher frequency signals (over 30 miles using highly directional antennas), support for more complex modulation, and higher robustness and spectral efficiency. [Ref 18] Indeed, many of the IEEE 802.16 PHY's most advantageous capabilities are found in this frequency range.

IEEE 802.16a uses orthogonal frequency-division multiplexing (OFDM) with a 256-point transform. [Ref 20] A brief description of OFDM is provided below:

Orthogonal FDM's (OFDM) spread spectrum technique distributes the data over a large number of carriers that are spaced apart at precise frequencies. This spacing provides the "orthogonality" in this technique which prevents the demodulators from seeing frequencies other than their own. The benefits of OFDM are high spectral efficiency, resiliency to RF interference, and lower multi-path distortion. [Ref 22]

IEEE 802.16a also uses TDM and TDMA to schedule uplink and downlink transmissions. Additionally, it uses TDD and FDD in much the same way that IEEE 802.16 systems do.

### **3. Error Control**

IEEE 802.16 uses two methods to control errors in the PHY: Forward Error Correction (FEC) and Automatic Retransmission Request (ARQ).

#### *a. Forward Error Correction*

FEC is common to both air interfaces. IEEE 802.16 normally uses Reed-Solomon GF (256) FEC, but has the option of using the more robust Block Turbo code to either increase the range of the BS or increase throughput. [Ref 22] A brief description of Reed Solomon FEC is provided below:

Reed-Solomon error correction is a coding scheme which works by first constructing a polynomial from the data symbols to be transmitted and then sending an over-sampled plot of the polynomial instead of the original symbols themselves. Because of the redundant information contained in the over-sampled data, it is possible to reconstruct the original polynomial and thus the data symbols even in the face of transmission errors, up to a certain degree of error. [Ref 23]

#### *b. Automatic Retransmission Request*

ARQ is a PHY characteristic that is used to deal with errors occurring due to propagation anomalies. [Ref 22] ARQ involves the retransmission of individual bits of data that may have been lost in the original transmission. The efficiency of retransmitting individual bits makes it possible to correct errors before the data is sent to a higher layer for processing. ARQ is a feature of IEEE 802.16a only and is not specified in the IEEE 802.16 standard. [Ref 22]

### **4. Framing**

The IEEE 802.16 PHY uses frames of 0.5, 1 or 2 milliseconds in duration. Each frame is divided into physical slots that are 4-QAM symbols long. Physical slots are used for bandwidth allocation and PHY transitions. In TDD systems, each frame is divided between the uplink and downlink subframe portions. For each frame, the downlink subframe is transmitted first, followed by a transmit/receive gap that allows the hardware time to switch between transmitting and receiving, which is then followed by the uplink

subframe. [Ref 21] There is also a brief time gap between frames. In FDD systems, transmitting and receiving occur simultaneously on separate channels. [Ref 21]

**a. Downlink Subframe**

As shown in Figure 6, each downlink subframe begins with a preamble followed by a frame control section that contains a downlink map (DL-MAP) message and an uplink map (UL-MAP) message. The frame start preamble is a 32-symbol sequence generated by repeating a 16-symbol sequence. The frame control section is used to pass control information for the channel to all SSs, and this data is not encrypted. [Ref 21]

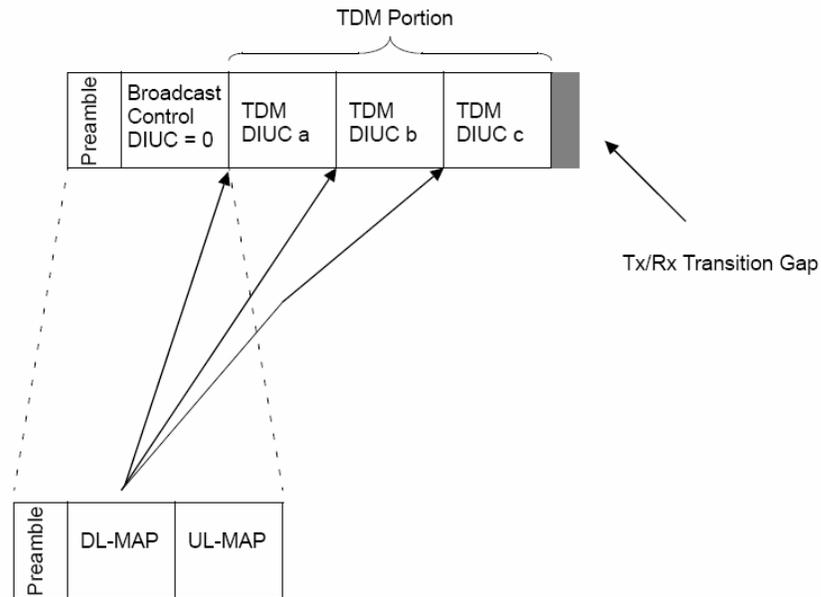


Figure 6. TDD Downlink Subframe Structure (From: Ref 21)

The DL-MAP portion of the frame control section provides listening SSs with the characteristics of the downlink channel. This information includes: PHY synchronization (i.e., schedule of physical layer transitions to include modulation and FEC changes), a downlink channel descriptor message (DCD), a programmable 48-bit BS identifier, and the number of data elements to follow. [Ref 21] The DCD and the BS identifier identify the channel and the BS, respectively, and thus together are useful for

situations where a SS is on the border of multiple IEEE 802.16 sectors or cells. The DL-MAP message shall be organized as shown in Table 8.

Syntax	Size	Notes
DL-MAP_Message_Format() {		
<b>Management Message Type = 2</b>	8 bits	
<b>PHY Synchronization Field</b>	Variable	See appropriate PHY specification.
<b>DCD Count</b>	8 bits	
<b>Base Station ID</b>	48 bits	
<b>Number of DL-MAP Elements <math>n</math></b>	16 bits	
Begin PHY Specific Section {		See applicable PHY section.
for ( $i = 1; i \leq n; i++$ ) {		For each DL-MAP element 1 to $n$ .
DL_MAP_Information_Element()	Variable	See corresponding PHY specification.
if !(byte boundary) {		
<b>Padding Nibble</b>	4 bits	Padding to reach byte boundary.
}		
}		
}		
}		

Table 8. The DL-MAP message format (From: Ref 21)

The UL-MAP is used to communicate uplink channel access allocations to the SSs. Information provided in the UL-MAP includes: Uplink channel identifier, uplink channel descriptor (UCD), number of information elements to map, allocation start time and map information elements. The UCD is used to provide SSs with information regarding the required uplink burst profile. The map information elements message identifies the SS this information applies to by using a connection identifier (CID). This message also provides an uplink interval usage code (UIUC) and offsets that are to be used by the SS to transmit on the uplink. The uplink interval usage code is used to specify the burst profile to be used by the SS on the uplink. The UL-MAP message shall be organized as shown in Table 9.

The frame control section is typically followed by a TDM portion where downlink data is transmitted to each SS. These TDM sections are used for transmitting data or control messages to specific SSs. Each of these transmissions is carried out according to the burst profile negotiated between the BS and the SS and data is transmitted in order of decreasing robustness. [Ref 20]

Syntax	Size	Notes
UL-MAP_Message_Format() {		
Management Message Type = 3	8 bits	
Uplink Channel ID	8 bits	
UCD Count	8 bits	
Number of UL-MAP Elements <i>n</i>	16 bits	
Allocation Start Time	32 bits	
Begin PHY Specific Section {		See applicable PHY section.
for ( <i>i</i> = 1; <i>i</i> <= <i>n</i> ; <i>i</i> ++) {		For each UL-MAP element 1 to <i>n</i> .
UL_MAP_Information_Element()	Variable	See corresponding PHY specification.
}		
}		
}		

Table 9. The UL-MAP message format (From: Ref 21)

The recipient SS is specified in the MAC header of the each data transmission, not in the DL-MAP portion of the frame control message. This makes it necessary for full duplex SSs to listen to all downlink subframes in order to filter out their data. [Ref 20]

In FDD systems with half duplex capability, the TDM portion of the downlink subframe may be followed by a TDMA portion designed to allow half duplex systems to regain synchronization with the BS. In this case, a separate preamble would precede each TDMA slot as shown in Figure 7. Burst profiles parameters and the presence of a TDMA portion will vary on a frame by frame basis as dictated by bandwidth and service demands. [Ref 20]

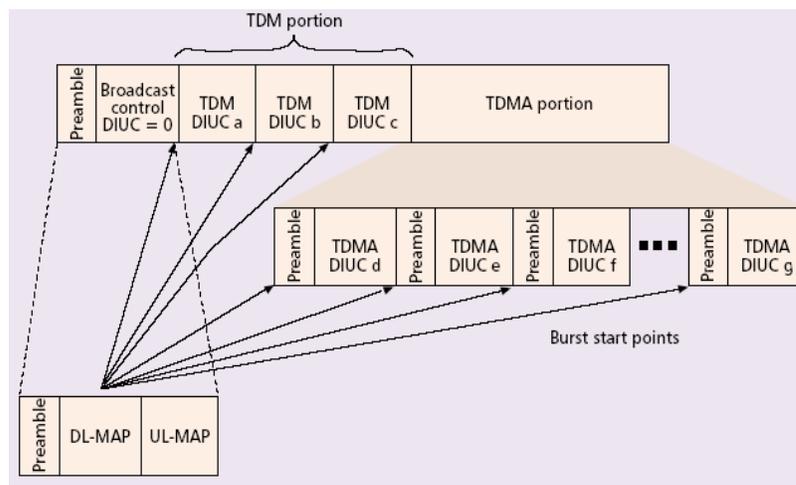


Figure 7. The downlink subframe structure (From: Ref 20)

### *b. Uplink Subframe*

The uplink subframe is used for SSs to transmit information to the BS. A typical uplink subframe structure is shown in Figure 8.

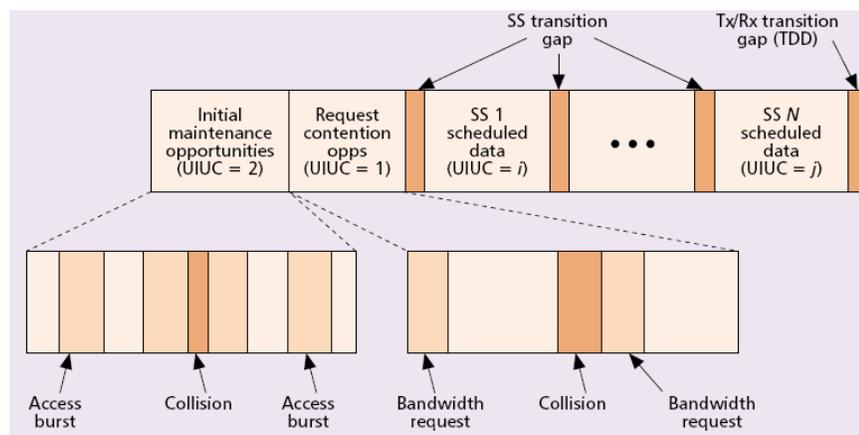


Figure 8. The uplink subframe structure (From: Ref 20)

There are three possible burst classes that may be present in any uplink subframe:  
[Ref 21]

- Contention based initial maintenance or initial access opportunities
- Contention based opportunities defined by request intervals as a response to multicast or broadcast polling
- Non-contention based and scheduled intervals allocated to specific SSs in UL-MAP bandwidth grants from the BS

Any of these three burst classes may be present in any frame, in any order and in any quantity per frame as dictated by the BS scheduler in a UL-MAP message.  
[Ref 21]

Initial maintenance/access timeslots include extra guard time to account for SS trying to acquire initial access and who have not yet resolved timing issues related to their range from the BS. [Ref 20] Additionally, collision time gaps, SS transition time gaps and transmit/receive time gaps are used to reduce the possibility excessive collisions.

## 5. Transmission Convergence (TC) Sublayer

The TC sublayer exists between the PHY and the MAC. The TC sublayer takes variable length MAC protocol data units (PDU) and organizes them within fixed length FEC blocks prior to transmission. [Ref 20] A 1-byte pointer is then added to the at the beginning of the TC PDU to indicate the first byte of the next MAC PDU within the TC PDU. In the event of lost data transmissions, this pointer allows for resynchronization between the SS and the BS. [Ref 20] The TC PDU format is shown in Figure 9.

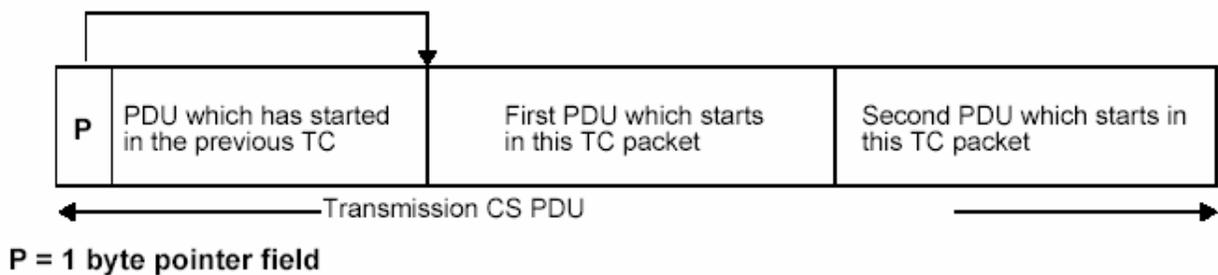


Figure 9. The TC PDU format (From: Ref 21)

## F. MEDIUM ACCESS CONTROLLER LAYER (MAC)

The IEEE 802.16 MAC is the mechanism responsible for the efficient sharing of the available medium. The IEEE 802.16 MAC is upper layer PHY protocol independent, with the capability of supporting services to include legacy TDM voice and data, IP connectivity, or packetized applications like VOIP. It is also capable of supporting either continuous or bursty traffic and ensuring that QoS is in keeping with the type of traffic being transmitted. Additionally, the IEEE 802.16 MAC is capable of supporting Asynchronous Transfer Mode (ATM) and guaranteed frame rate (GFR) services. [Ref 20]

Through a variety of methods that we will discuss shortly, the MAC is able to provide differentiated service to users on the same medium. Most importantly, the MAC is able to guarantee a specified service level and required QoS for each connection. As an example, one sector of a BS is capable of supporting guaranteed T1 service to business customers while simultaneously providing best effort DSL services to other customers within the same service area. [Ref 21]

## 1. Connection Orientation

A connection is a unidirectional mapping between base station and subscriber station medium access control peers for the purpose of transporting a service flow's traffic. [Ref 25] IEEE 802.16 is a connection oriented protocol, where all services are mapped to a connection. This is true even for inherently connectionless services. [Ref 20] While each SS has a unique 48-bit MAC address, this number is not used to reference the multiple connections associated with each SS. Instead, connections are referenced using a 16-bit CID. CIDs are used for all interactions with the BS to include bandwidth requests, connection QoS control, and routing data to the appropriate sublayer.

When a SS is first introduced into a network, the BS will assign three management connections in each direction. [Ref 20] Each connection is used for transmitting messages of different lengths and urgency. The three management connections and the type of messages they transmit are as follows:

- The basic connection - short, time critical MAC and radio link control messages
- The primary management connection - longer, more delay tolerant messages (ex. authentication or connection setup messages)
- The secondary management connection - standards based messages such as DHCP, TFTP and SNMP messages.

There are various types of connections to support many of the IEEE 802.16 MAC's various functions. A second group of connections, known as transport connections, are established according to the services being supported and the required QoS and traffic parameters. [Ref 20] These connections are not to be confused with layer 4 or Transport layer connections found in the OSI model. Transport connections are typically assigned in pairs. Other connections might be established for contention based initial access, broadcast transmissions, multicast transmissions, etc.

## 2. The MAC PDU

### a. PDU Description

The definition of a MAC PDU is as follows:

The MAC PDU is the data unit exchanged between the MAC layers of the BS and its SSs. A MAC PDU consists of a fixed length header, a variable length payload, and an optional cyclic redundancy check (CRC). [Ref 20]

More specifically, PDUs are exchanged among peer entities in the same protocol layer, from higher to lower layers in the downward direction and from lower to higher layers in the upward direction. This exchange of PDUs is shown in Figure 10 below. In the downward direction, each layer encapsulates the higher layer PDU into the MAC SDU format before passing it on to the next layer. [Ref 21]

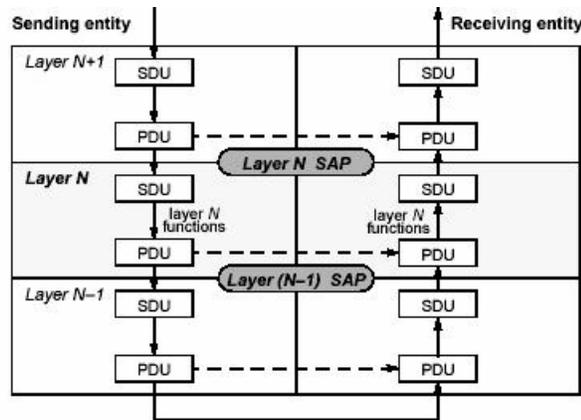


Figure 2—PDU and SDU in a protocol stack

Figure 10. PDU and SDU in a Protocol Stack (From: Ref 21)

**b. Construction of the MAC PDU**

Prior to transmission, the MAC can take advantage of several methods of MAC PDU construction to maximize the efficiency of the transmission. The MAC PDU construction process is shown in Figure 11.

The following methods are used in the construction of MAC PDUs:

(1) Concatenation. Involves the concatenation of multiple MAC PDUs into one transmission. [Ref 21] May be done for either uplink or downlink transmissions.

(2) Fragmentation. Involves the division of a MAC SDU into several MAC PDUs. [Ref 21] May be used to support services where the MAC SDU size may be very large, such as video applications. Fragmentation may also be done in both the uplink or downlink directions.

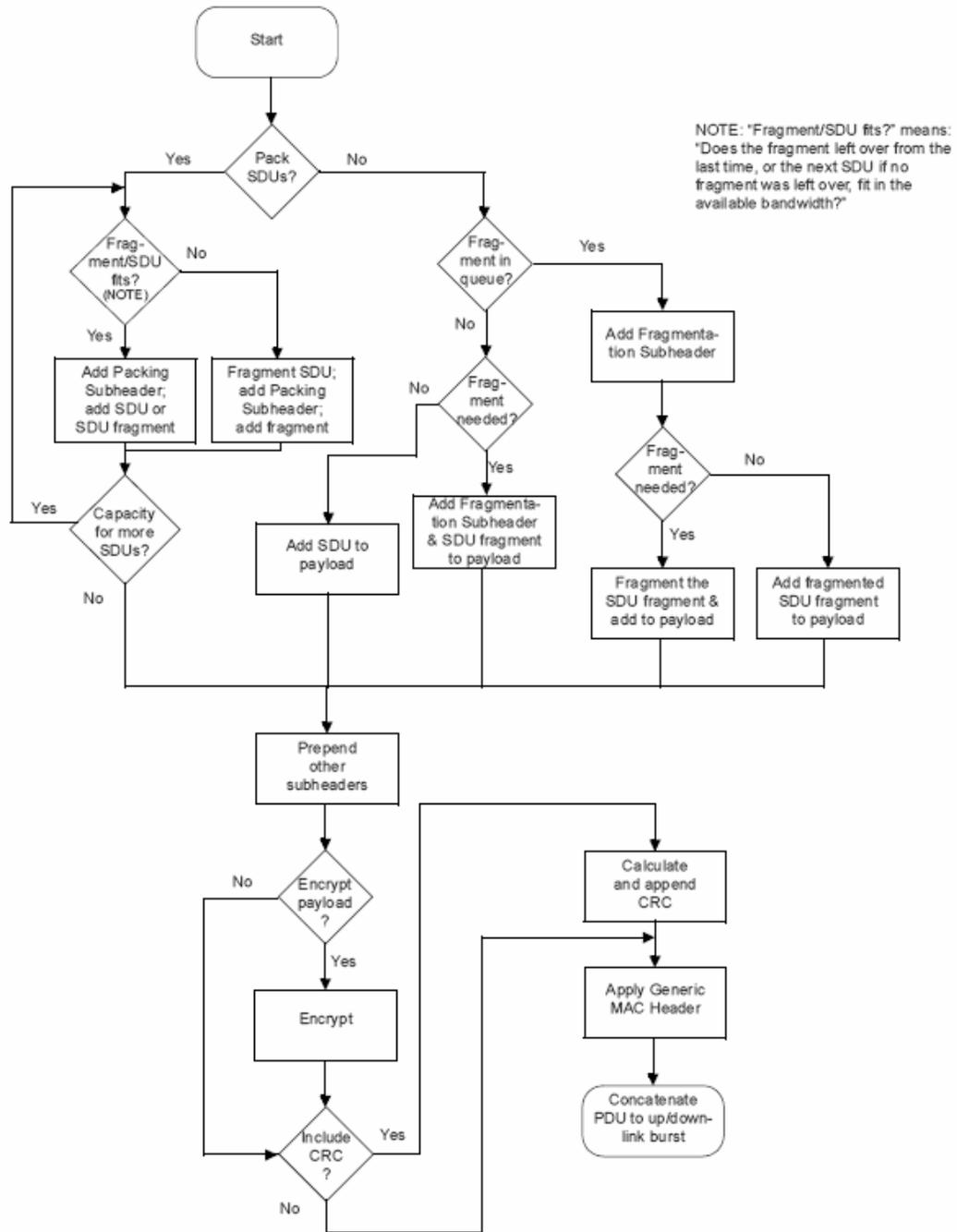


Figure 11. Construction of the MAC PDU (From: Ref 21)

(3) Packing. Involves the packing of multiple MAC SDUs into one MAC PDU. [Ref 21] The connection must be authorized to carry variable length packets in order to take advantage of packing. Packing may be done in either the uplink or the downlink at the discretion of the transmitting station.

### 3. Sub-layers

The MAC is made up of three sublayers: the Service Specific Convergence Sublayer (CS), the MAC Common Part Sublayer (MAC CPS), and the Privacy Sublayer. The sublayers are organized as shown in Figure 12, with the CS on top as the interface to higher layers, the MAC CPS below the CS, and the Privacy Sublayer below the MAC CPS. Between each sublayer lies a service access point, which acts as an interface between the two layers it borders. It is important to note that the CS SAP acts as the interface to layer 3 - i.e. to a router or protocol stack in the end system.

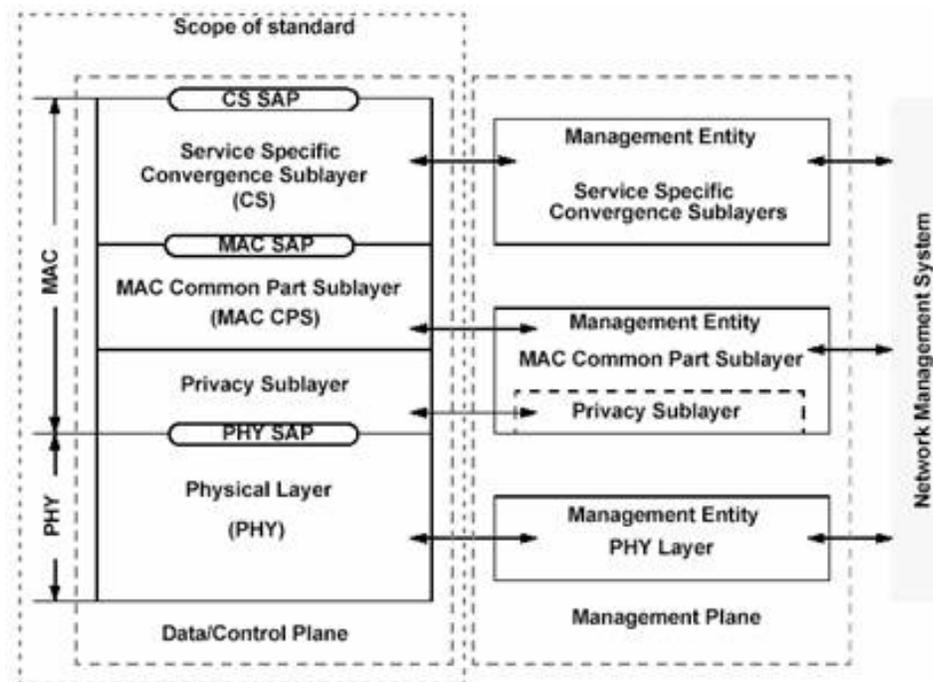


Figure 12. IEEE 802.16 Protocol Layering (From: Ref 21)

#### a. Convergence Sublayer

The CS is used for mapping services to and from IEEE 802.16 MAC connections. More technically, the CS accepts, classifies and processes PDUs received from a higher layer, delivers CS PDUs (or SDUs in the case of a lower layer) to the appropriate MAC SAP, and receives CS PDUs from peer entities. [Ref 21] *Classification is the process by which a MAC SDU is mapped onto a particular connection for transmission between MAC peers.* [Ref 21] Figure 10 is a generic

representation the processing of PDUs and SDUs through the sublayers. In simpler terms the CS functions as follows:

The primary task of the sublayer is to classify service data units (SDUs) to the proper MAC connection, preserve or enable QoS, and enable bandwidth allocation. The mapping takes various forms depending on the type of service. In addition to these basic functions, the convergence sublayers can also perform more sophisticated functions such as payload header suppression and reconstruction to enhance airlink efficiency. [Ref 20]

There are two specifications for CSs, the ATM CS, for ATM services and the packet CS, for mapping packet services such as IPv4, IPv6, Ethernet, and virtual local area network (VLAN). [Ref 20]

The MAC CPS provides much of the IEEE 802.16 MAC's core functionality to include: system access, bandwidth allocation, connection establishment, and connection maintenance. [Ref 21] This layer is also responsible for applying connection specific QoS through appropriate transmission scheduling. Much like the functioning of the CS, the MAC CPS receives SDUs from higher layers via the SAP and provides appropriate disposition based on a variety of parameters. Much of the details behind these MAC CPS functions will be covered in detail in the subsequent sections. Figure 13 shows a typical classification and mapping sequence between a BS and a SS.

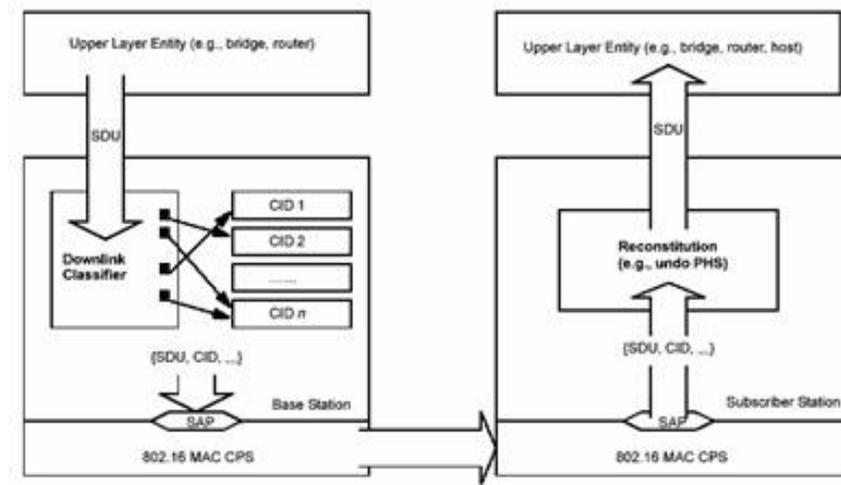


Figure 13. Classification and CID mapping (From: Ref 21)

***b. Privacy Sublayer***

The privacy sublayer is responsible for encryption between the BS and the SS. The privacy sublayer protects privacy by guarding users against theft of service and unauthorized access to the network. [Ref 21] This sublayer employs a client / server key management protocol and digital certificate based SS authentication. Security issues will be covered in more detail in a subsequent section of this chapter.

***c. Payload Header Suppression***

In order to increase the efficiency of MAC SDU exchange between the CS and other entities, it is possible to suppress the repetitive portions of payload headers. [Ref 21] In each case the sending entity will suppress the payload header and the receiving entity will rebuild the suppressed portions of the payload header.

**4. Radio Link Control**

The IEEE 802.16 Radio Link Controller (RLC) is responsible for the management of adaptive burst profiles, power control and ranging. A different burst profile is used for each channel as determined by the RLC, based on "a number of factors, such as rain region and equipment capabilities". [Ref 20] Under favorable link conditions, the RLC will employ the most bandwidth efficient burst profiles available, and will revert to less efficient burst profiles when link conditions become less favorable. Through the use of adaptive burst profiles IEEE 802.16 is able to support a link a planned link availability of 99.999%. [Ref 20] The adjustment of burst profiles, power and ranging parameters is controlled by the BS, which monitors signal quality on the uplink and manages requests from associated SSs to make adjustments on the downlink. [Ref 20] Power control and initial ranging begin immediately upon initial channel acquisition and will be described below.

**5. Network Entry and Initialization**

Figure 14 shows the stages of an error free initialization of a SS entering a network. There are many possible branches from this procedure that may be invoked due to errors during initialization. This initialization procedure is designed to eliminate the need for manual configuration of each SS. [Ref 20]

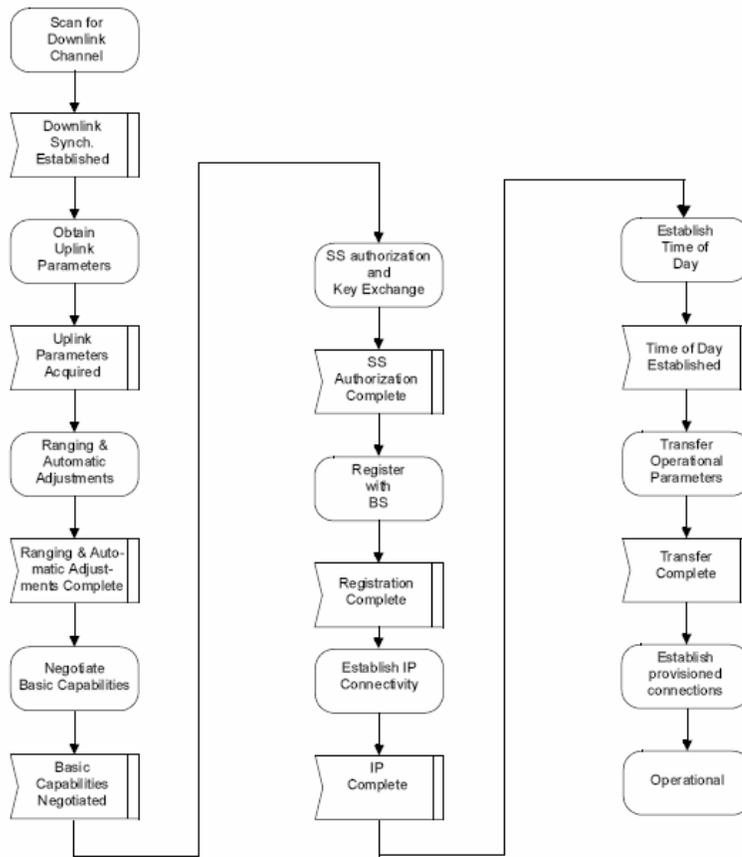


Figure 14. SS Initialization Overview (From: Ref 21)

Each step in the initialization process will be covered in detail below:

**a. Scanning and Synchronization to the Downlink**

SSs are designed to scan their frequency lists for active downlink channels immediately upon installation or following any period of signal loss. [Ref 21] In the case of signal loss, the SS will store the operational parameters of the last signal and will try to reestablish that connection. After acquiring a channel with a valid downlink signal, the SS will attempt to synchronize the PHY by listening for DL-MAP management messages. The SS will continue to listen for DL-MAP management messages and in the case of missing DL-MAP messages, the SS will repeat the scanning and synchronization process.

**b. Obtaining Transmit Parameters**

Once a DL-MAP message has been detected, the MAC sublayer will listen for downlink and uplink transmission parameters. By listening for UCD messages from

the BS, the SS is able to determine a usable uplink channel. UCD messages are broadcast messages, sent out periodically, providing pertinent parameters for all available uplink channels. [Ref 21] The SS will collect UCD messages for each available channel, and will attempt to establish communications on a suitable channel. If communications fail on one channel, the SS will move on to the next suitable channel until a connection is established or the list has been exhausted, in which case it will begin the scanning process again. [Ref 21]

**c. *Ranging and Power Adjustment***

As described in the IEEE 802.16 standard, *Ranging is the process of acquiring the correct timing offset such that the SS's transmissions are aligned to a symbol that marks the beginning of a minislot boundary.* [Ref 21] Timing offset is dictated by the distance of the SS to the BS and the corresponding signal propagation delay. The SS begins this process by scanning UL-MAP messages for an available maintenance interval. Once an available maintenance interval has been determined, the SS will send a Ranging Request (RNG-REQ) message, within this contention based initial maintenance period, to the BS at the minimum power level. If this transmission does not receive a response, the SS will increase the power level incrementally as necessary, but not to exceed the maximum specified transmission power. The BS will reply with a Ranging Response (RNG-RSP) message, which specifies the appropriate timing advance and power adjustment for the SS, as well as the basic and primary managements CIDs. [Ref 20]

**d. *Negotiation of Basic Capabilities***

The SS will use SS Basic Capability Request (SBC-REQ) messages to report its capabilities to the BS. This message provides the SS's PHY capabilities, supported modulation and coding schemes, and duplexing methods supported. [Ref 20] The BS will then respond using the SS Basic Capability Response (SBC-RSP) message to detailing which of the SS's capabilities it will support. [Ref 21] This response will be used to adjust the burst profile to the most efficient usable profile. Up to this point all previous transmissions are carried out using the most robust burst profile available.

***e. Authorize SS to Perform Key Exchange***

Authorization and key exchange will be covered in more detail in the security section to follow.

***f. Registration***

According to the IEEE 802.16 standard, Registration is the process by which the SS receives its Secondary management CID and thus becomes manageable. [Ref 21] This is accomplished through the Registration Request (REG-REQ) message sent by the SS and the Registration Response (REG-RSP) message sent by the BS.

***g. Establish IP Connectivity***

The SS may also include the version of IP it uses in the REG-REQ. If not included the BS will authorize the use of the default IPv4 for the Secondary Management Connection. [Ref 21] The SS and the BS will then use Dynamic Host Configuration Protocol (DHCP) on the Secondary Management connection to complete IP connectivity.

***h. Establish Time of Day***

Time of day is used for time stamping of logged events by both the BS and the SS. The SS again uses the Secondary Management connection to retrieve the time from the server. The transmission is sent via user datagram protocol (UDP). The time returned from the server is combined with the SS's timing offset in order to determine the current local time. [Ref 21]

***i. Transfer Operational Parameters***

The SS will use TFTP to transfer the SS configuration file. The configuration file contains the configuration settings for a variety of parameters used in the operation of the SS.

***j. Set Up Connections***

The SS will next begin to establish connections for pre-provisioned service flows, where a service flow is defined as the unidirectional transport of packets on either the uplink or the downlink. [Ref 20] Each service flow is associated with a specific set of QoS parameters for the supported service. These service flows utilize a two phase activation model where a service flow may be admitted (BS has resources reserved, but service is not active), or active (BS has resources reserved and service is active). A third possible state for a service flow is the provisioned state, where the BS

has assigned a service flow identifier, but has not reserved any resources for this service flow. [Ref 21]

## **6. Bandwidth Requests and Grants**

IEEE 802.16 manages the allocation of bandwidth by using a request / grant protocol. In this protocol, SSs request bandwidth allocations from the BS through a variety of methods, which will be explored in more detail below. As previously discussed, the BS makes bandwidth assignments by allocating transmission timeslots (via TDMA) only to those SSs that have submitted a request for bandwidth (via DAMA). The BS will use UL-MAP messages to relate the bandwidth allocations to all SSs on the network.

IEEE 802.16 subscriber stations can be divided into two classes based on how they handle bandwidth grants. The first class of SS accepts bandwidth grants for each connection, or on a grant per connection (GPC) basis. The second class of SS is able to accept grants for all of the SS's bandwidth needs, or on a grant per SS (GPSS) basis. These are covered in more detail below:

### ***a. GPC***

The GPC SS receives grants only for specific connections (to include management connections) and as a result must request bandwidth for each individual connection as needed. In addition, the GPC SS must request additional bandwidth to meet any unexpected RLC requirements. For these reasons, GPC systems are less efficient than GPSS systems, but they are also simpler. [Ref 20]

### ***b. GPSS***

The GPSS SS receives one bandwidth grant, which it uses to meet the needs of all its connections. As a result, the SS itself must manage how much bandwidth is allocated to each connection. In situations where one connection requires more bandwidth than expected, the SS has the option of 'stealing' bandwidth (referred to as bandwidth stealing in the IEEE 802.16 standard) from another connection to cover the temporary bandwidth shortage. The BS is also responsible for priority queuing based on traffic types. The SS can then send a request to the BS requesting that its bandwidth grant be increased to meet its new needs. GPSS SSs are the only class of SS available in the 10-66 GHz frequency range. [Ref 20]

Bandwidth grants are provided based on a self-correcting protocol as opposed to an acknowledged protocol. [Ref 20] In this protocol, if the SS does not receive a bandwidth grant in reply to a bandwidth request, the SS will assume that the request was either lost or could not be fulfilled, and will simply send another request to the BS, without having to wait for some acknowledgement of the original request. This protocol eliminates the overhead associated with acknowledgement messages.

## **7. Bandwidth Requests**

SSs typically will request bandwidth incrementally as new bandwidth requirements arise, and the BS will add the requested bandwidth to the total perceived requirement for the SS.

### ***a. Request Periods***

With incremental requests, the BS has no way of knowing whether it has granted the correct total requirement of bandwidth to the SS, since the total granted bandwidth may be affected by lost grant request packets. Due to this possibility, the SSs may request bandwidth incrementally or on an aggregate basis. [Ref 21] Aggregate requests are used to reset the BS's perception of the total bandwidth requirement of the SS. When a BS receives an aggregate request, it will store the requested bandwidth value as the new total requirement for the requesting SS. [Ref 21]

There are a variety of methods available for a SS to request bandwidth allocations from the BS. Bandwidth requests may be related to the BS during bandwidth request periods specifically dedicated to a SS or during contention periods. The method of polling used by the BS to inform the SSs of upcoming bandwidth request periods is what determines whether the bandwidth request period is a dedicated or contention request period. Polling methods will be covered in the following section.

### ***b. Bandwidth Request Header***

In addition to bandwidth request periods allocated via polling, SSs may request bandwidth allocations at any time by sending the BS a bandwidth request MAC PDU with a bandwidth request header and no payload. [Ref 20] This method of bandwidth request may be used in any bandwidth grant for GPSS SSs and in either grant request intervals or data grant intervals for a specific connection.

*c. Piggyback Request*

A similar method for requesting bandwidth is to use a grant management subheader to piggyback a request for additional bandwidth for the same connection within the MAC PDU. [Ref 20]

**8. Polling**

Polling is the process used by the BS to allocate bandwidth request opportunities to SSs. When the BS wants to notify a SS of an upcoming bandwidth request opportunity, it will use an UL-MAP message information element (IE) to do so. [Ref 21] The UL-MAP IE will grant sufficient bandwidth for the SS or SSs to submit their bandwidth requests during the specified request period. Bandwidth request opportunity allocations may be made on a unicast, multicast or broadcast basis as described previously in section 4.b. of this chapter. A brief description of each polling method is provided below:

*a. Unicast polling*

In unicast polling, a SS is polled individually by the BS. The SS will reply with stuff bytes if the granted bandwidth is not needed. [Ref 21] The process by which the BS conducts unicast polling is shown in Figure 15 below.

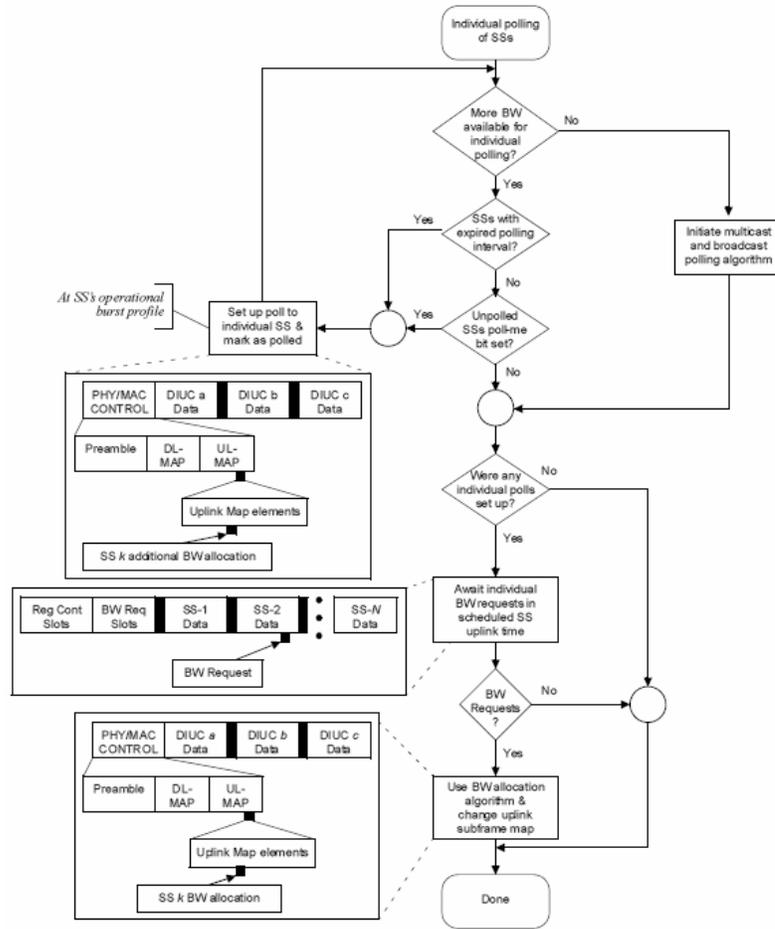


Figure 15. The Unicast Polling process (From: Ref 21)

***b. Multicast and Broadcast Polling***

The BS will resort to multicast or broadcast polling when insufficient bandwidth is available to individually poll SSs. [Ref 21] Multicast and broadcast polling is also done via the UL-MAP message in the same fashion as for unicast polling. The BS reserves some CIDs for multicast or broadcast groups as specified in Table 10. The primary difference here is that the polling message is directed toward a multicast or broadcast CID instead of an individual CID or SS.

Interval description	Uplink map IE fields		
	CID (16 bits)	UIUC (4 bits)	Offset (12 bits)
Initial Ranging	0000	2	0
Multicast group 0xFFC5 Bandwidth Request	0xFFC5	1	405
Multicast group 0xFFDA Bandwidth Request	0xFFDA	1	605
Broadcast Bandwidth Request	0xFFFF	1	805
SS 5 Uplink Grant	0x007B	4	961
SS 21 Uplink Grant	0x01C9	7	1136
*	*	*	*
*	*	*	*
*	*	*	*

Table 10. Sample Uplink Map with multicast and broadcast IE (From: Ref 21)

**c. Poll-Me Bit**

The poll-me bit is used by SSs using the Unsolicited Grant uplink scheduling service (UGS) to notify the BS that they need to be polled. The UGS will be covered in more detail in the following section. The poll-me bit is part of the grant management subheader. Once the poll-me bit has been detected, the BS will issue a unicast poll to the SS requesting it. [Ref 21] Figure 16 below shows the process for using the poll-me bit.

**9. Uplink Scheduling Services**

IEEE 802.16 uses predefined uplink scheduling services to increase the efficiency of uplink transmissions on each connection based on the service being provided by that connection. [Ref 21] The four defined uplink scheduling services are: Unsolicited Grant service, Real Time Polling service, Non-Real Time Polling service, and Best Effort service. The scheduling service that a connection will use is determined at the time of that connection's set up. [Ref 20] Each uplink scheduling service is further defined below:

**a. Unsolicited Grant Service**

This service is used primarily for synchronous, real time services which generate fixed units of data periodically, such as ATM constant bit rate (CBR), T1/E1 over ATM or Voice over IP without silence suppression. [Ref 21] In this service, the BS provides

periodic fixed size data grants, as negotiated during connection setup, without the need for the SS to send bandwidth requests.

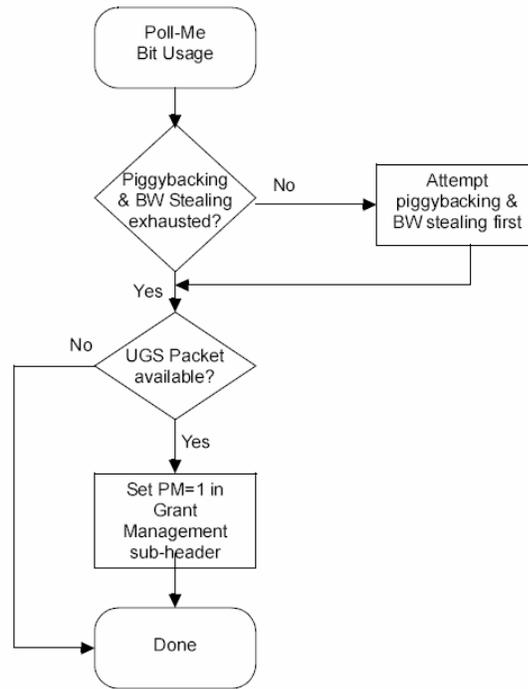


Figure 16. Poll-me bit usage (From: Ref 25)

This unsolicited granting of bandwidth eliminates the overhead and latency associated with bandwidth requests and as a result helps to reduce jitter and delay jitter. [Ref 20] More stringent jitter requirements may be met through the use of output buffering.

The SS is able to provide feedback to the BS concerning the state of service flows by employing the slip indicator flag in the grant management subheader. [Ref 21] The slip indicator flag is used to indicate a queue backlog, which may be caused by a variety of factors to include lost grants or clock skew with outside networks. Once the BS has been notified of the slippage, it can grant additional bandwidth in order to eliminate the backlog.

***b. Real Time Polling Service***

This service is designed to meet the needs of real time services needing to transmit periodic, variable sized data packets. This service is well suited for applications such as streaming video or audio, or VoIP. [Ref 20] A suitable military application might be in missile guidance systems, where a missile in flight might require periodic tracking

information updates. Real time polling works by allocating periodic dedicated (unicast) bandwidth request opportunities to each connection. Because the SS must explicitly request bandwidth, there is more overhead and latency associated with this service than with Unsolicited Grant service, however, some efficiency is gained through the use of variable sized data packets.

*c. Non Real Time Polling Service*

This service works the same way as the Real Time Polling service, except that connections use contention based access opportunities to transmit bandwidth requests. [Ref 21] Unicast polling opportunities are also used to guarantee at least a minimal reserved traffic rate, although these opportunities are less frequent than those found in Real Time polling. Non-Real Time Polling is well suited for supporting services that can tolerate some delay jitter, such as high bandwidth FTP, Internet connections, and ATM GFR. Non-Real Time polling also utilizes the traffic priority parameter, contained in the SS configuration file and established at connection setup, to determine which service flows have priority in relation to others. As stated in the IEEE 802.16 standard, given two service flows identical in all QoS parameters besides priority, the higher priority service flow should be given lower delay and buffering preference. [Ref 21]

*d. Best Effort Service*

There are no throughput or delay guarantees associated with this service. Connections use contention based opportunities to request bandwidth. Additionally the SS may use unicast or unsolicited opportunities to request bandwidth. [Ref 21] The availability of unicast opportunities is subject to the load of the network and is not guaranteed. The best effort service is the most bandwidth efficient because it does not reserve bandwidth for a station that may or may not be using it.

**10. Quality of Service**

There are various parameters associated with QoS in the IEEE 802.16 standard. These parameters are used at the establishment of a service flow to determine the QoS requirements of a supported service. Below are some of the QoS parameters specified in the IEEE 802.16 standard:

- QoS parameter set type - specifies the proper application of the QoS parameter set to either a provisioned, admitted or active set. [Ref 21]

- 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. [Ref 21]
- 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. [Ref 21]  
Table 11 provides an example of the Request/Transmission Policy.
- Tolerated jitter - specifies the maximum delay variation (jitter) for a connection. [Ref 21]
- Maximum latency - specifies maximum latency between receipt of packet on the network interface and forwarding to the RF interface. [Ref 21]
- Fixed length versus variable length SDU indicator - indicates whether data packets must be fixed length or may be variable length. [Ref 21]

Type	Length	Value	Scope
[24/25].16	4	Bit #0 – Service flow shall not use broadcast bandwidth request opportunities. Bit#1-Reserved. Bit #2 – The service flow shall not piggyback requests with data. Bit #3 – The service flow shall not fragment data. Bit #4 – The service flow shall not suppress payload headers (convergence sublayer parameter) Bit #5 – The service flow shall not pack multiple SDUs (or fragments) into single MAC PDUs. Bit #6 – The service flow shall not include CRC in the MAC PDU. All other bit positions are reserved.	DSx-REQ DSx-RSP DSx-ACK

Table 11. Request Transmission Policy Example (From: Ref 25)

## 11. Security

The IEEE 802.16 privacy sublayer provides users privacy by encrypting the link between the BS and the SS, and it provides protection against theft of service by encrypting service flows within the network. [Ref 21] The privacy sublayer employs an authenticated client/server key management protocol that is capable of supporting the Advanced Encryption Standard (AES). [Ref 20] In this protocol the BS, acting as the server, controls key distribution to the SS, which acts as the client.

The privacy sublayer employs two component protocols to carry out all security related tasks. [Ref 21] The first is an encapsulation protocol, which is used for the encryption of data packets across the network. This protocol defines the rules associated with using *cryptographic suites to encrypt the MAC PDU payload. Cryptographic suites are defined as pairings of data encryption and authentication algorithms.* [Ref 21]

The second component of the privacy sublayer is the Privacy Key Management Protocol (PKM). [Ref 21] PKM is used to provide secure distribution of keys between the BS and SSs. This protocol is further used by the BS and the SS to keep synchronization of keying data between them, and by the BS to control access to network services.

### *a. Packet Data Encryption*

When encryption is enabled on an IEEE 802.16 system, not all packets or even all portions of packets will be encrypted. In order to facilitate ranging and registration, all MAC management messages are sent in the clear. Additionally, encrypted data packets contain an encrypted payload with an unencrypted header. [Ref 21] The unencrypted MAC PDU header will contain information specific to the encryption such as an encryption control field, an encryption key sequence field, and the corresponding CID. [Ref 21] This information is used by the receiving BS or SS to decrypt the MAC PDU payload. Figure 17 shows the format for an encrypted MAC PDU.

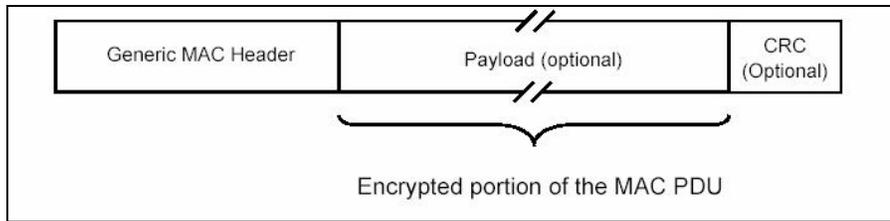


Figure 17. MAC PDU Encryption (From: Ref 6)

***b. Key Management Protocol***

All IEEE 802.16 SSs shall contain a manufacturer issued X.509 digital certificate, which is used for SS authentication and initial authorization key exchange. [Ref 21] The digital certificate will contain the SS's public key as well as its MAC address. Upon authentication, the BS will use the SS's public key to encrypt the authorization key (i.e., a shared secret), and the authorization key will be used to encrypt any subsequent data and key exchange. In addition to digital certificates, all SSs have either factory installed RSA private/public key pairs, or the appropriate algorithms to generate these keys dynamically. [Ref 21] The RSA public-key encryption algorithm, and strong symmetric algorithms are used by the PKM protocol to facilitate key exchange.

***c. Security Associations***

A security association (SA) is defined as the set of security information a BS and one or more of its client SS in order to support secure communications. [Ref 21] Upon initialization, each SS will establish at least one SA with the BS. With the exception of the basic and primary connections, all new connections are mapped to a SA.

**G. SUMMARY**

IEEE 802.16 is a well conceived standard from an organization with a good history of producing sound standards. [Ref 18] The fact that the WiMax alliance has undertaken the task of ensuring interoperability should accelerate the adoption of the standard and help to produce high quality equipment standards. The IEEE 802.16 standard offers superior performance, support for large numbers of users, robust links, and the future promise of mobility, and mesh networking among other things. The IEEE

802.16 standard is fertile ground for military experimentation and testing, and with a few adaptations, may produce a communications transformation within DOD.

## **V. COMPARISON OF IEEE 802.16 TO THE WNW AND STOM REQUIREMENTS**

### **A. INTRODUCTION**

In this chapter we will compare the IEEE 802.16 standard to the WNW specification as outlined in Chapter Three of this thesis. Additionally, we will examine whether the IEEE 802.16 standard meets the requirements of STOM as outlined in Chapter Two. We will begin by outlining the basic requirements for a WAN radio network and comparing how the IEEE 802.16 and the WNW propose to meet these requirements. The goal of these comparisons is to identify where the IEEE 802.16 standard might fall short of the capabilities of the WNW and the requirements of the radio WANs and STOM, and to identify where the standard meets or exceeds these requirements. This information will be used in chapter eight of this thesis to identify adaptations necessary for the IEEE 802.16 standard to replace the WNW, and to generate a comprehensive 'adapt from COTS' list.

### **B. REQUIREMENTS FOR RADIO WAN**

The basic requirements for the efficient functioning of any IP based radio network are (1) routable networks, (2) the ability to support multicast traffic, (3) layer 2 QoS control, (4) layer 2 security, and (5) manageability. [Ref 24] These requirements are outlined below, along with how the WNW and the IEEE 802.16 standards will address these requirements. Since both the WNW and the IEEE 802.16 standards are concerned with passing IP protocol based data via a radio, it is appropriate to compare the two technologies side by side to determine which of the two is likely to perform this function more efficiently and/or effectively. While the WNW has yet to be developed, we will rely on what is known about the WNW so far and the goals of the waveform as outlined in Chapter Three.

#### **1. Routable Networks**

The first requirement for an IP-protocol radio network is the ability of the radio to transmit and receive data as IP-protocol packets. The transmission of data in this format

makes it possible to support network addressing, which makes it possible to efficiently route this data within the network. The WNW is currently being designed to support the IPv4 and IPv6 protocols. Similarly, the IEEE 802.16 standard supports both IPv4 and IPv6.

## **2. Ability to Support Multicast Traffic**

A second requirement for the efficient functioning of a radio WAN is the ability of the network's radios to support multicast traffic. As outlined previously in this thesis, this ability to support multicast traffic adds greatly to the efficiency of the network because it makes it possible to send the same message to many destination hosts using only one transmission. Both the WNW specifications and the IEEE 802.16 standard are designed to support the transmission of multicast traffic.

## **3. QoS Control**

This requirement essentially boils down to the ability of the radio network to support scheduling and bandwidth allocation schemes that are in keeping with the type and priority of the traffic being transmitted. This includes the requirements for traffic prioritization, support for real time traffic requiring deterministic data delivery, and the ability to keep latency, jitter, and BER below certain thresholds. The WNW has a goal of being able to support assured (acknowledged) and best effort message delivery services. This will include the differential handling of traffic based on traffic class service requirements and assigned precedence. Unfortunately, since the specification is still in development, it is not possible to examine exactly how the WNW will support proper QoS control. In contrast, the IEEE 802.16 standard appears to have an effective and efficient protocol for QoS control as outlined in the previous chapter. The IEEE 802.16 standard easily supports various QoS requirements.

## **4. Layer 2 Security**

The primary concern of layer 2 security is the ability to resist traffic analysis efforts. [Ref 24] Traffic analysis resistance is accomplished by encryption of the header information being transmitted. The WNW standard has as a goal the ability to support NSA Type-1 encryption, which encrypts the payload and the entire header. The IEEE 802.16 standard also supports the ability to encrypt the payload, but does not support the

encryption of header information. This is one vulnerability of the IEEE 802.16 standard that must be corrected before it can be adapted to military applications.

## **5. Manageability**

Network management requirements can be satisfied by allowing the use of SNMP within the network. [Ref 24] Both the WNW and IEEE 802.16 standards will support the use of SNMP for network management. [Ref 12, 21]

### **C. COMPARISON OF IEEE 802.16 AND THE JTRS WNW**

In order to provide as fair a comparison as possible of the WNW and IEEE 802.16 standards, we will follow the general outline used to present the WNW in chapter three. This outline will allow us to briefly compare and contrast the capabilities of both standards in the following general categories: (1) Performance Characteristics, (2) Networking Capabilities, (3) Network Services, (4) Information Assurance and Security, and (5) Program Status. In some areas the comparison categories may be modified in order to reduce redundancy. It is important to keep in mind that the IEEE 802.16 standard has been specified in a standards document, while the WNW standard is still being developed, therefore any comparisons of the two standards will be based on the goals of the WNW standard as outlined in the WNW Functional Description Document.

#### **1. Performance Characteristics**

##### ***a. Adaptive modulation***

Both the WNW and IEEE 802.16 standards will support adaptive modulation based on link conditions.

##### ***b. Supported Data Rates***

It is difficult to make an effective comparison of supported data rates because there are many factors to consider that might influence the determination of what standard would ultimately provide the most aggregate throughput. Besides the advertised throughput rates, other factors to consider might include channel size, number of channels supported simultaneously, robustness of the link under adverse conditions, and the frequency range of transmissions. Assuming that the stated data rates for the WNW standard apply to a single channel, the objective data rate is 5 Mbps, with 2 Mbps as a

threshold. [Ref 13] In contrast, the IEEE 802.16 standard is able to support single channel shared data rates up to 120 Mbps for LOS transmission in the 10-66 GHz frequency range and 70 Mbps NLOS in the 2-11 GHz frequency range. [Ref 21] Based on this simplified comparison, IEEE 802.16 promises to deliver much higher data rates than the WNW standard.

***c. Automatic Power Control***

Both the WNW and IEEE 802.16 standards will support automatic power control.

***d. Range***

The WNW Functional Description Document specifies ranges for air-to-air, air-to-ground, and ground-to-ground transmissions, while the IEEE 802.16 standard only specifies ranges for ground-to-ground transmissions. For ground-to-ground transmission, the WNW claims a 10km (6.2 miles) range, while the IEEE 802.16 standard can support ranges up to 30 miles. [Ref 21] This topic warrants additional experimentation and comparison since many factors may affect a transmission's range to include antenna height, terrain, and weather among others.

***e. Propagation Environment Support***

With respect to propagation environments supported, both standards will provide a robust signal with a high degree of resistance to the effects of multipath and fading. Similarly both standards will be able to operate in varying environmental conditions such as jungle, mountainous, or urban terrain. The WNW Functional Description Document does not directly address whether the WNW will perform under NLOS, OTH or BLOS conditions. By contrast, the IEEE 802.16 standard document goes to great length to specify that equipment based on the standard will be capable of NLOS, OTH and BLOS communication. [Ref 21] IEEE 802.16's PHY independence means that the standard may be adapted to additional frequency ranges where propagation behaviors may differ greatly.

***f. Frequency Spectrum***

With respect to supported frequencies sets, the goal of the WNW is to provide *adequate flexibility with respect to operating frequency, bandwidth, modulation,*

*and power.* [Ref 12] In contrast, the IEEE 802.16 standard is specified to support frequencies between 2-11 GHz and 10-66 GHz. In order to maximize the effectiveness of the IEEE 802.16 standard, adaptations should be included to support a wider range of frequencies, especially in the lower frequency bands. Due to IEEE 802.16's MAC layer frequency independence, adaptations to other frequency ranges are possible.

***g. Noise Environments***

The goals of the WNW standard state that it will be able to operate in *tactical RF propagation environments* where unintentional and intentional (jamming) noise will be present. The IEEE 802.16 standard does not address clearly whether or not it will operate effectively in such hostile noise environments. However, it is useful to note that one of the strengths of the IEEE 802.16 standard in general is its ability to operate in high noise environments.

***f. Anti-jamming capabilities***

The WNW functional description document states that the WNW will include an anti-jam feature to prevent the intentional disruption of service. While the IEEE 802.16 standard does not specify an anti-jamming capability, the use of OFDM in the lower frequency ranges provides a signal that is resilient to RF interference. This capability should be tested to determine how resistant the OFDM signal is to RF interference.

**2. Networking capabilities**

***a. Network size***

The WNW functional description document states that the network will be scalable from 2 to 1,630 nodes. [Ref 12] By contrast, the IEEE 802.16 standard should be able to support *thousands of users*. [Ref 21] It is important to note that neither of these values are definitive, and they are likely to vary widely based on network conditions, the nature of traffic being transmitted, and numerous other factors.

***b. Topology***

The WNW functional description document states that the *WNW network shall integrate any node operating in the area of operation into the network*. [Ref 13] This will allow nodes to exit and reenter the network as necessary. Similarly, the IEEE

802.16 standard has procedures where SSs begin scanning and synchronizing with any available network automatically after startup or service interruption. This process can be further controlled by specifying what BS SSs should be associating to. In effect, this also allows the SS to depart from the network and to reenter the network as needed. Additionally, both the WNW and IEEE 802.16 standards will support mesh, and point-to-point topologies. The WNW does not specify whether the WNW standard will support a point-to-multipoint topology, a capability that is currently supported by the IEEE 802.16 standard.

***c. Mobility management (Layer 1)***

The WNW will support nodes moving in excess of 120 mph (relative to the companion node). [Ref 123] Similarly, the IEEE 802.16 standard will support SSs moving at up to 93mph (150km/hr). [Ref 19] While the WNW will be capable of supporting ground-to-air communications up to 65,000 feet in altitude, there are no specifications for altitudes supported by the IEEE 802.16 standard. Clearly, more testing of IEEE 802.16's capabilities will be required in order to determine whether or not it will be able to match the WNW's speed and altitude of communications figures.

**3. Network services**

***a. Traffic Support***

Both the WNW and IEEE 802.16 will be able to support unicast, multicast and broadcast traffic types. Additionally, both will be able to transmit various types of traffic to include video and voice communications.

***b. QoS control***

As discussed in the previous section, both the WNW and IEEE 802.16 will be able to support traffic of varying QoS requirements.

***c. Packet Delivery***

The WNW will support both *assured (acknowledged) and best effort (unacknowledged) message delivery*. [Ref 12] By contrast, IEEE 802.16 employs an

unacknowledged scheme with a variety of error checking mechanisms to assure complete message delivery. [Ref 21] Additionally, IEEE 802.16 employs ARQ to address the retransmission of any lost data before higher layers of the OSI model are involved. While it is difficult to compare which of the two schemes will be more spectrally efficient, the IEEE 802.16 scheme is considered to be very efficient.

**d. Channel Access**

It is unclear as to what MAC procedures will be adopted for the WNW. The WNW functional description document specifies that the link layer will *manage access from multiple nodes that are in line of sight of each other* and that it will provide fair access while eliminating the exposed node and the hidden node problems, but it does not provide any more information. [Ref 12] By contrast, IEEE 802.16 has very well defined MAC procedures, which are extremely bandwidth efficient, combining DAMA, and TDMA access schemes to provide access to network resources.

**4. Information Assurance and Security**

**a. Confidentiality**

Both the WNW and IEEE standards will provide for the confidentiality of transmitted information through the use of encryption. As mentioned previously, one important difference to note here is that the WNW will encrypt both header and payload data, while the IEEE 802.16 standard only specifies the encryption of payload data.

**b. Availability**

The WNW Functional Description Document states that the WNW will provide the means to recover from loss of cryptographic or TRANSEC synchronization and to resynchronize. [Ref 12] While it is difficult to examine exactly how these mechanisms will compare in terms of efficiency due to a lack of more detailed information, the IEEE 802.16 standard also includes comparable re-synchronization features to deal with any loss of connectivity.

**c. Integrity**

The WNW will include anti-spoofing features to prevent the malicious or unintentional modification of user data packets. [Ref 12] By contrast, the IEEE 802.16 standard specifies that authentication of the user is handled during the connection setup

and all subsequent data is encrypted based on a the exchange of cryptographic keys during this setup. Since user authentication information is not included in every packet, it may be possible to spoof a user, although this is highly unlikely since it would require an attacker to use the correct cryptographic keys for the exchange of spoofed packets.

*d. Identification and Authentication*

The WNW will employ NSA defined authentication procedures, as well as security association and key management functions. Additionally, mechanisms will exist to limit WNW modifications to only authorized personnel. [Ref 12] The IEEE 802.16 standard also specifies identification and authentication procedures. These procedures employ not only security associations, but also X.509 digital certificates for the identification and authentication of SSs. [Ref 21]

*e. Waveform cryptographic functions*

The WNW will employ type 1 cryptographic algorithms for the encryption and decryption of data, identification and authentication, header cover and TRANSEC key stream generation. [Ref 12] By contrast, IEEE 802.16 will employ RSA private/public key pairs or appropriate algorithms for these purposes. [Ref 21] It is difficult to make a determination concerning the relative strength of either of these two techniques, and this will likely be a useful area of study for future research.

**5. Program status and Standard maturity**

Program status and standard maturity are areas where the WNW and the IEEE 802.16 standards differ greatly. The WNW standard is still in its infancy, while the IEEE 802.16 standard actually encompasses several other standards in various stages of development, as outlined in chapter four. While the IEEE 802.16 family of standards is not yet complete, it is likely that these standards will be completed well before the WNW standard is solidified. Currently, it is possible to purchase equipment that is IEEE 802.16a-compliant from multiple vendors, and more equipment is in the process of being developed.

During our research we noticed that there is a lot of excitement and momentum surrounding the IEEE 802.16 protocol that should serve to speed its adoption. Also helping to speed this adoption is the existence of the WiMax forum, whose purpose it is

to ensure that all IEEE 802.16 compliant equipment is interoperable. This organization should serve to speed the adoption of IEEE 802.16 compliant equipment in much the same way that the Wi-Fi Alliance helped to speed the adoption of IEEE 802.11 standard products.

By contrast, the WNW standard currently exists in no more than a functional description document. As can be seen by the comparison of the two technologies, the IEEE 802.16 standard actually fulfills many of the goals of the WNW. It is possible that with some adaptation, the IEEE 802.16 standard could serve as an excellent platform on which to build the WNW standard.

#### **D. COMPARISON OF IEEE 802.16 AND STOM REQUIREMENTS**

In order for the IEEE 802.16 standard to meet the unique network architecture requirements of STOM, it must possess five key characteristics as outlined in the *STOM Concept of Employment* document. [Ref 4] A brief explanation of each of these five key characteristics is shown below, along with an explanation of how the IEEE 802.16 standard might be able to meet the requirements of each.

##### **1. Self-Organization**

The IEEE 802.16 standard will meet this characteristic's requirement that a network be meshed to the maximum extent possible, through the completion of the IEEE 802.16f standard, which focuses on IEEE 802.16's mesh networking capabilities. Additionally, this characteristic requires *establishing additional mobile, ad hoc networks that tie into dissimilar networks that carry needed information for the new mission*. [Ref 5] The IEEE 802 Handoff Study Group is currently working on enabling the handoff of users between different 802.x networks. The U.S. military could take advantage of the work this group is doing, by ensuring the availability of communications equipment that supports 802.x networking.

##### **2. Ubiquitous Communications Relays**

STOM requires ubiquitous communications relays that will support cooperative, multi-hop relaying and routing of traffic to distant nodes via a best path determination algorithm. Due to the fact that this standard is still under development, it is not possible to specify exactly how message routing will take place under the IEEE 802.16f standard.

### **3. Common Operational Picture (COP)**

STOM requires that nodes possess the capability to automatically or manually determine their own position location via the GPS and transmit COP/CTP updates simultaneously to all applicable warfighter C2 display nodes. [Ref 5] The primary enabler for this capability is the ability to send broadcast and multicast messages. As discussed previously, the IEEE 802.16 standard does support the transmission of broadcast and multicast messaging. With the appropriate adaptations, the IEEE 802.16 standard should be able to support the determination and reporting of positions via the GPS.

### **4. Cooperative Engagement**

Cooperative engagement is achieved through the synchronization of sensors and platforms in such a way that it enhances the commander's decision making process. This capability requires an enhanced quality of information—information that is relevant, timely (urgent), precise, and actionable. [Ref 5] There is no reason to believe that the IEEE 802.16 standard would not be able to support this requirement for higher quality information. However, only detailed experimentation and testing will reveal the IEEE 802.16 standard's ability to support all of the requirements associated with the STOM characteristic of cooperative engagement.

### **5. Consolidated Networks**

In order to achieve consolidated networks, it is necessary to implement bandwidth management measures that allow for the efficient distribution of available bandwidth. In such a scenario, dedicated channels will give way to shared channels where aggregate bandwidth is shared on a demand assigned basis. The IEEE 802.16 standard excels in its ability to efficiently distribute bandwidth on a demand assigned basis, while still meeting the diverse QoS needs of many simultaneous users at different service levels. It is these particularly strong MAC procedures that we believe are one of the areas where the IEEE 802.16 standard can make the most significant contribution to the improvement of efficiency in current military networks.

## **E. CONCLUSIONS**

A comparison of and the IEEE 802.16 standard against the requirements of the WNW, radio WANs, and STOM reveals that the IEEE 802.16 standard comes very close to fulfilling all of the requirements outlined. It is likely that with a few adaptations, further maturity of the standard, and further testing, the IEEE 802.16 standard will be able to achieve all of the outlined requirements. While it is not likely that the IEEE 802.16 standard in its entirety will ever replace the WNW specification, its ability to achieve most of the WNW's goals makes it a good point of departure for the future development of the WNW standard. In particular, the WNW would benefit greatly from the adaptation of MAC procedures as outlined in the IEEE 802.16 Standard. The fact that this standard is significantly more mature than the WNW standard, adds to its attractiveness for military adaptation. This approach is likely to save significant development time and research dollars in the JTRS program, while producing a standard that has been tested thoroughly in the commercial sector before being applied to military equipment.

THIS PAGE INTENTIONALLY LEFT BLANK

## **VI. IMPLEMENTATION AND TESTING**

### **A. INTRODUCTION**

The purpose of this chapter is to provide an overview of the “hands-on” testing conducted during the course of our research. While the focus of the thesis has been on the “Adopt from COTS” modifications required from the IEEE published standard, we also wanted to work with pre-standard IEEE 802.16 equipment in order to validate its capabilities.

### **B. METHODOLOGY**

During the spring and summer of 2004, the authors approached the practical application aspect of their research by using the following methodology:

- First, by conducting familiarization training and OTM and PTP NLOS Testing using pre-standard IEEE 802.16 equipment. (March 2004)
- PTP NLOS testing using pre-standard IEEE 802.16 equipment (May 2004)
- PMP NLOS and LOS Testing using pre-standard IEEE 802.16 equipment (Aug 2004)

The first experiment was conducted in support of the USMC Transformational Communication research by Captain Gilbert Garcia (USMC), Captain David Joseforsky (USMC), Lieutenant Manny Cordero (USN), and Lieutenant Albert Seeman (USN). The experiments were conducted from March 7-11, 2004 at Camp Roberts, CA and included testing of the same pre-standard equipment which we would eventually test for our research. The following scenarios were tested using pre-standard equipment: Command and Control On-the-Move Network Digital Over-the-Horizon Relay (CoNDOR), communications on-the-move, and NLOS communications. Broadband links were established in a PTP deployment and we integrated seamlessly with other networking technologies (to include Free Space Optics and IEEE 802.11 links). These links were then routed into wired networks as a proxy for the terrestrial GIG. While the IEEE 802.16a standard was not intended to address OTM communications, the testing equipment testing at Camp Roberts during this experiment proved OFDM based systems

were capable of establishing and maintaining OTM communication links in excess of 20 Mbps. The authors used the lessons learned during this week as a point of departure for our own experimentation using a PMP deployment. The detailed results of the testing during this experiment can be found in Ref 25.

The second opportunity for testing was with Lieutenant Ryan Blazeovich (USN) the NPS STAN 6 experiment<sup>3</sup>. During this testing several PTP links were established using Redline Communication's model AN-50 equipment at distances that ranged from 1 to 6 miles. This testing also included additional exploration of IEEE 802.16's OTM communication capabilities. Please refer to the Ref 26 for detailed explanation of the IEEE 802.16 testing completed during the STAN 6 experiment.

## **C. PMP TESTING (AUG 2004)**

### **1. Introduction**

The authors conducted thesis research with IEEE 802.16 pre-standard equipment from 11-15 August 2004. The testing conducted at the Camp Roberts National Guard base located near Paso Robles, CA. Additional participants in the experiment research included: Dave Rumore (Redline Communications), Don Mullin (Redline Communications), and Capt Max Green (USMC) from the Marine Corps Tactical Systems Activity (MCTSSA). The emphasis of this experiment was to test IEEE 802.16 PMP capabilities in both LOS and NLOS conditions. The QoS and throughput characteristics of the established links would be measured to test the capabilities of IEEE 802.16 technologies.

---

<sup>3</sup> Surveillance and Tactical Acquisition Network. NPS and industry partners have been conducting intensive unmanned aerial vehicle field studies at Camp Roberts to improve operational capabilities for small UAVs (SUAV). Current tests are evaluating SUAV sensor performance, especially for target detection and identification, counter detection, plane stability, and human factors in extended field operations. In addition to SUAV tests, the NPS team is examining wireless communication issues and data transfer from unmanned underwater vehicles.

## 2. Equipment

### a. *Redline Communications*<sup>4</sup>

The pre-standard equipment that was chosen to base our testing on was developed by Redline Communications, a broadband wireless company that is in Toronto, Canada. Redline's product offered the most cost effective option for broadband wireless testing for our purposes. Appendix A provides details specifications of the AN-50 system which is summarized below. (See Figure 18 for a picture of the AN-50 system)

AN-50 Characteristics include:

- Capable of Non-line-of-sight (NLOS) and Optical-Line-of-Sight (OLOS) deployments
- Operates in the 5.8 GHz (unlicensed Band)
- Capable of over-the-air rates up to 72 Mbps
- Sustained Ethernet rates of up to 45Mbps
- Range capability beyond 15 miles (24 km)
- Transparent Ethernet bridge
- 10/100 BaseT interface
- Over-the-air 64-bit encryption

An additional consideration in using Redline Communications equipment was its close resemblance to the MAC and PHY properties of the 802.16a standard. Redline Communications is a prominent member of the WiMax committee as well as the IEEE Standards working group. This fact allows them to have significant influence in the evolution of the IEEE 802.16 family of standards. Some of the characteristics of the AN-50 which are similar to the approved IEEE 802.16a standard are:

- PHY
  - OFDM based
- MAC
  - Provides dynamic adaptive modulation and coding
  - Extensive QoS provisioning capabilities
  - Time Division Duplexing implementation
  - Request and grant polling for SS requesting additional bandwidth

---

<sup>4</sup> Redline Communications is the only vendor which has produced an 802.16a compliant product (the AN-100) by the summer of 2004. Their AN-100 system operates in the licensed 3.5 GHz frequency range and is design to for WiMax interoperability. Due to the logistics with operating in the frequency band (namely the coordination with the Federal Communications Commission), we decided instead to pursue pre-standard equipment for testing the capabilities of the protocol. The AN-50 provides most of the 802.16a characteristics while offering us the flexibility of operating in the unlicensed frequency band.



Figure 18. Redline Communications AN-50 System<sup>5</sup> with Antenna and 5.8 GHz Transceiver Radio (From: Ref 35)

***b. Antennas***

Four different types of antennas were used during the testing. In a PMP deployment, the base station would typically consist of a wide-beam, or sector, antenna in order to provide the service to the greatest number of SSs in within the beams width. The flexibility gained from using the sector antenna comes with the price of distance the link can reach (with all other things, such as power, being equal). This can be attributed to the path loss and the lower gain of sector antennas. Table 12 describes the specification of the antennas used.

Antenna	Weight and Size	Gain
Omni Directional	Weight: .4 kg Size: 30x4 cm;	9dBi
1 ft Flat Panel (9 degree beam width)	Weight 1.5 kg Size: 30x30 cm	23 dbi
2 Ft Flat Panel (4.5 degree beam width)	Weight: 5.0 kg Size: 60x60 cm	28 dBi
1 ft Flat Panel (60 degree sector beam width)	Weight: 7.0 kg Size: 65x21.6 cm	17 dBi

Table 12. Antenna Specifications

<sup>5</sup> Most broadband wireless vendors are either building their own proprietary MAC, re-using the IEEE 802.11 MAC, or are awaiting the arrival of the Intel/Fujitsu chipsets due in FY 05.

### 3. Testing Terrain

The distances we tested ranged from a few hundred meters to several kilometers in both LOS and NLOS deployment. The terrain which the links traversed can be characterized as hilly with scattered trees and scrub brushes. Back of the envelope calculations and the use of a vendor provided link budget tool assisted in our determination of antenna deployments. Figure 19 provides an overview picture of the test location.

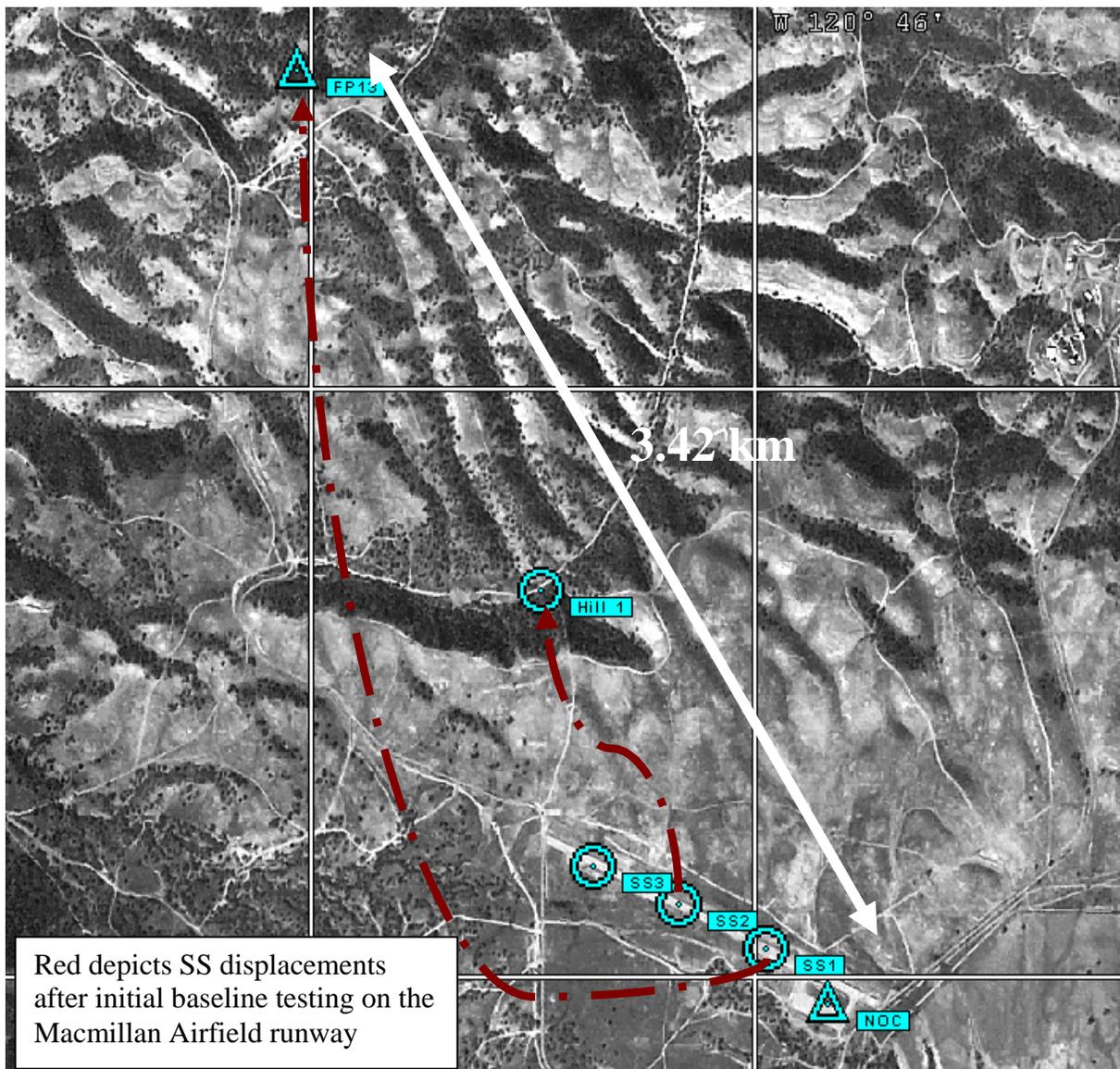


Figure 19. Overhead View of Testing Area

## 4. Network Description

### a. Hardware devices

The methodology was to take measurements at the Ethernet ports of each node. We also wanted to minimize the degradation of performance of the network caused by adding additional networking and wireless devices. Hence, the network was simplified to include only layer 2 devices (which included the wireless bridges and 3Com switches) and the laptops which were connected to take the measurements of the network's performance. Laptops which were used to capture testing data were either connected directly to the AN-50 Ethernet port or indirectly via a switch. We chose to use 1 BS and 3 SS to reflect typical command hierarchy of three subordinate commands per major command. Figure 20 provides a general overview of the devices used during the testing.

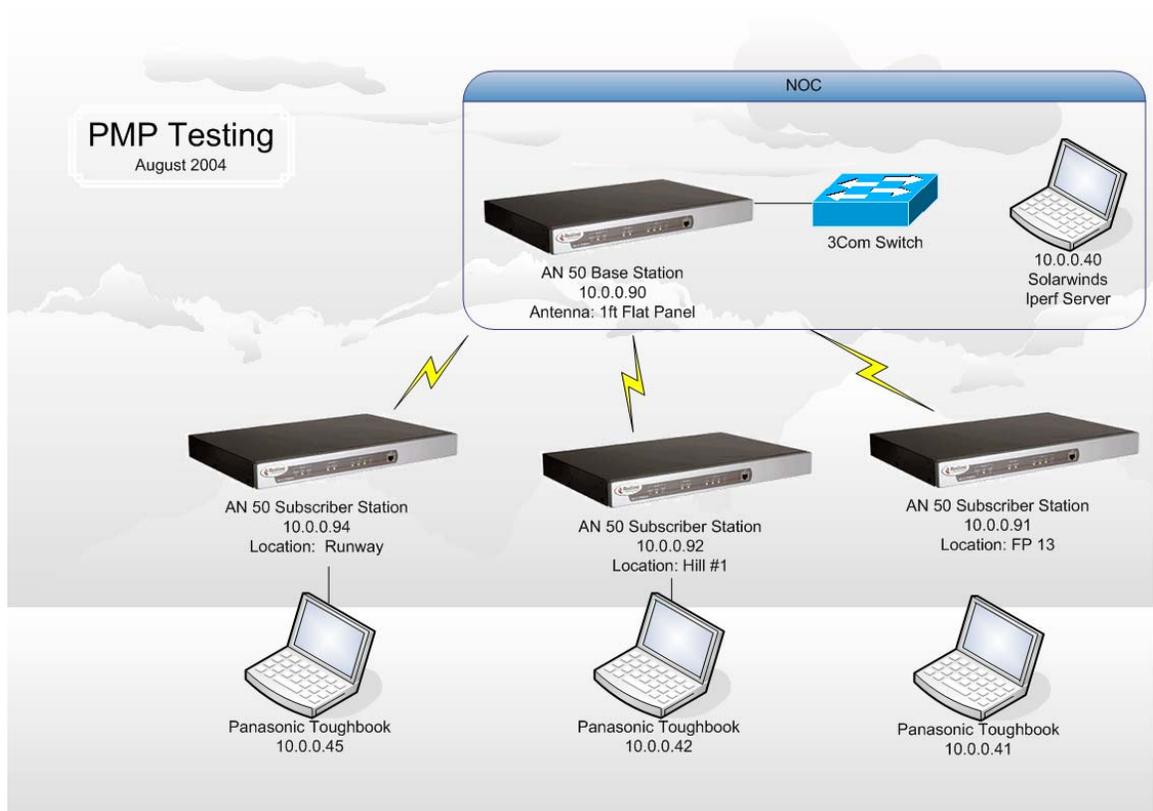


Figure 20. Network Diagram

### ***b. Software Tools***

We used Solarwinds® as the networking management tool inside the NOC. It provided us with the ability to track network performance and view the real-time statistics of the network. The family of applications which comprise the Solarwinds® application monitors and collects data from routers, switches, servers, and any other SNMP-enabled devices located on the network. Each device in our experimentation was configured with SNMP enabled to permit this functionality.

Throughput measurements were taken by two separate tools: QCheck® and IPerf®. QCheck® is a Microsoft Windows®-based free network management tool that is available for download on the QCheck® website<sup>6</sup>. It has a GUI for the configuration of the testing parameters, but does not provide the capability to export the results into an external file. During our testing it was primarily used as a quick and easy to use verification tool for measurements taken by the other applications.

IPerf® is also available as a free download. It offers robust capability for link data collection. It has a command line interface on Windows® platforms and has both a GUI and command line interface when implemented on UNIX based operating systems. IPerf® can measure IP bandwidth using UDP or TCP traffic with configurable window sizes and duration. Its ability to provide a constant bit rate UDP stream is useful in simulating voice and streaming video communications over a data link. It allows for tuning various parameters, and reports bandwidth, delay jitter, and packet loss. It supports IPv6 and multicast and permits its results to be exported into an external text file for latter analysis. Figure 21 shows an example of the output from an IPerf® test.

---

<sup>6</sup> <http://dast.nlanr.net/Projects/Iperf/>

```

-----
Client connecting to 224.0.55.55, UDP port 5001
Sending 1470 byte datagrams
Setting multicast TTL to 5
UDP buffer size: 8.00 KByte (default)
-----
[148] local 10.0.0.40 port 1173 connected with 224.0.55.55 port 5001
[ ID] Interval      Transfer    Bandwidth
[148] 0.0- 5.0 sec   642 KBytes  1.05 Mbits/sec
[148] Sent 447 datagrams

```

Figure 21. Example of an IPerf® Multicast Test Output

## 5. Test Results

### a. Test #1 LOS Baseline Testing

The first test involved Redline Communication’s equipment configured in a LOS, short range PMP deployment. The purpose of this test was to determine the baseline throughput of this equipment in LOS conditions with multiple SSs. The testing was conducted with the assistance of Redline Communications representatives who provided familiarization training on configuring a PMP network and the optimization of the established links.

The SSs were distributed on McMillan Airfield’s runway at approximately 300 meters apart. The base station antenna was located on the roof of the NOC (see Figure 22) and was located 300 meters away from the closest SS on the runway. Each SS antenna was within LOS of the base station antenna at the NOC. Table 13 provides a summary of the testing configuration.



Figure 22. Base Station Sector Antenna Overlooking Runway

Line of Sight Baseline Testing (Runway Testing)				
Data Collection Worksheet				
Physical Data-	Base Station	SS #1	SS #2	SS #3
Location	10S GQ 02351 54574 NOC	10S GQ 02135 54746 Runway	10S GQ 01836 54879 Runway	10S GQ 01543 54992 Runway
Distance from Base Station	N/A	312m	622m	917m
Type of Antenna	90 degree sector	2 ft Flat Panel	2 ft Flat Panel	2 ft Flat Panel
Elevation-GPS	920	901	901	899
Density Description	LOS	LOS	LOS	LOS
Uplink Link Data-				
Uncoded Burst Rate	---	54Mb/s	54Mb/s	54Mb/s
RSSI (average received signal strength)	---	-54dBm	-57dBm	-57dBm
SINADR (average signal to interference, noise and distortion)	---	28dB	28dB	28dB

Table 13. Test 1. LOS PMP Data Sheet (Baseline)

After spending approximately 45 minutes configuring the software within the AN-50 stations, it took approximately 45 minutes to establish the three SS links (deployed with 2ft. flat panel antennas) on the runway to the base station. The authors collected the baseline PMP LOS link statistics primarily using IPerf and QCheck to verify the measurements. The IPerf data for the baseline testing was exported into a text file and then transcribed into the chart in Figure 23.

The throughput rate refers to the number of bits per second in a digital network. It is a fairly important metric in the delivery of most services such as high-resolution video that inherently requires large amounts of data to be delivered continuously. The average throughputs for the links were 25 Mbps for the farthest SS and between 19-20 Mbps for the two closest locations.

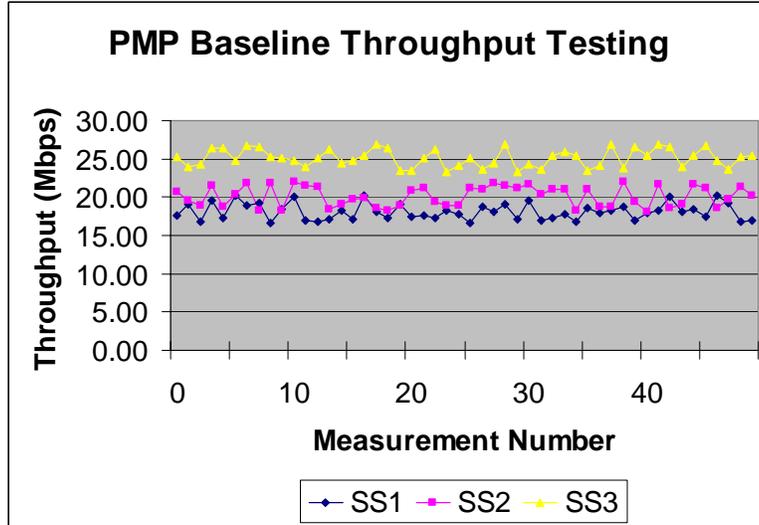


Figure 23. Baseline PMP LOS Throughput Test Results

As expected in a LOS short distance link, the packet loss for each of the sites was ~0% and the average latency for each location was under 1ms. The measure of throughput and link quality improved the farther out the SS was deployed along the runway. This could be attributed to the fact that the antenna beam was pointed in the direction of the farthest SS. We chose to do this in order to minimize the movement of the sector antenna once the SS # 1 and # 2 were deployed to Firing Point (FP) 13 and Hill # 1 (sites were on the same heading as SS#3 on the runway from the NOC).

***b. Test # 2 NLOS testing in a PMP deployment***

Following the initial base testing, two SSs were deployed to the surrounding hills of the airfield while the third SS remained deployed at the airfield. SS #1 was deployed to FP #13, which is 3.43 km from the NOC at an elevation of 988ft. The site was in a NLOS position with respect to the base station antenna and the airfield. SS #2 (See Figure 24) was located on the military crest of a hill approximately 2.00 km NLOS from the BS antenna. SS #3 remained deployed on the runway approximately 622 meters from the BS antenna.



Figure 24. Photo of Capt Munoz Deploying a 1ft 9 degree antenna at Hill #1

During past experiments, it has been the experience of the authors that the initial field set-up of the antennas is the most challenging aspect in working with broadband wireless equipment. We began the NLOS testing with the base station deployed with a 90 degree sector antenna. However, the lower gain from using this antenna prevented us from establishing a NLOS link out to FP 13 (a distance in excess of 3,400 meters with a hill and sporadic trees in between separated the SS and the BS). After multiple attempts to set up the link between the two sites, we reverted to a  $9^\circ$  beamwidth antenna with a higher gain than the sector antenna. We were then able to immediately establish the link to FP 13 (See Figure 25) as well as the links to SS#2 at Hill #1 and SS#3 located on the runway. Once the links were established, we were able to optimize the link quality by making minute adjustments to the azimuth and elevation of each antenna with the help of the vendor's link monitoring tool that can track SNR dynamically. Table 14 provides a summary of the network topology.



Figure 25. Photo of SS Antenna Deployed at FP 13

<b>Non-Line of Sight Testing (Field Testing)</b>				
<b>Data Collection Worksheet</b>				
<b>Physical Data-</b>	<b>Base Station</b>	<b>SS #1</b>	<b>SS #2</b>	<b>SS #3</b>
	10S GQ 02351 54574 NOC	10S GQ 00482 57470 FP13	10S GQ 01347 55854 Hill1	10S GQ 01836 54879 Runway
<b>Location</b>				
<b>Distance from Base Station</b>	N/A	3.42km	1.49km	.622km
<b>Type of Antenna</b>	90 degree sector	2 ft Flat Panel	2 ft Flat Panel	2 ft Flat Panel
<b>Link Characteristics</b>	----	NLOS	NLOS	LOS
<b>Elevation-GPS</b>	920	980	800	
<b>Location Notes</b>		Scattered tress and scrubs	Scattered tress and scrubs	
<b>Burst Rate</b>	---	54Mb/s	<b>54Mb/s</b>	<b>54Mb/s</b>
<b>RSSI</b>	---	-77dBm	<b>-75dBm</b>	<b>-57dBm</b>
<b>SINADR</b>	---	-18dB	<b>18dB</b>	<b>28dB</b>

Table 14. NLOS PMP Throughput Test

Figure 26 is the output of throughput rates for TCP traffic after 50 independent measurements. As expected, the throughput of the NLOS link decreased when compared to their baseline LOS testing outputs as well as the NLOS PTP we had established during

previous experiments. Of note is the fact the most dramatic degradation was to at the farthest site on FP 13, but rather on Hill #1 and SS2. This may be attributed to the fact the link from FP 13 to NOC was optimized to prior to establishing the Hill #1 link. Table 15 provides a comparison of the first 2 test outputs.

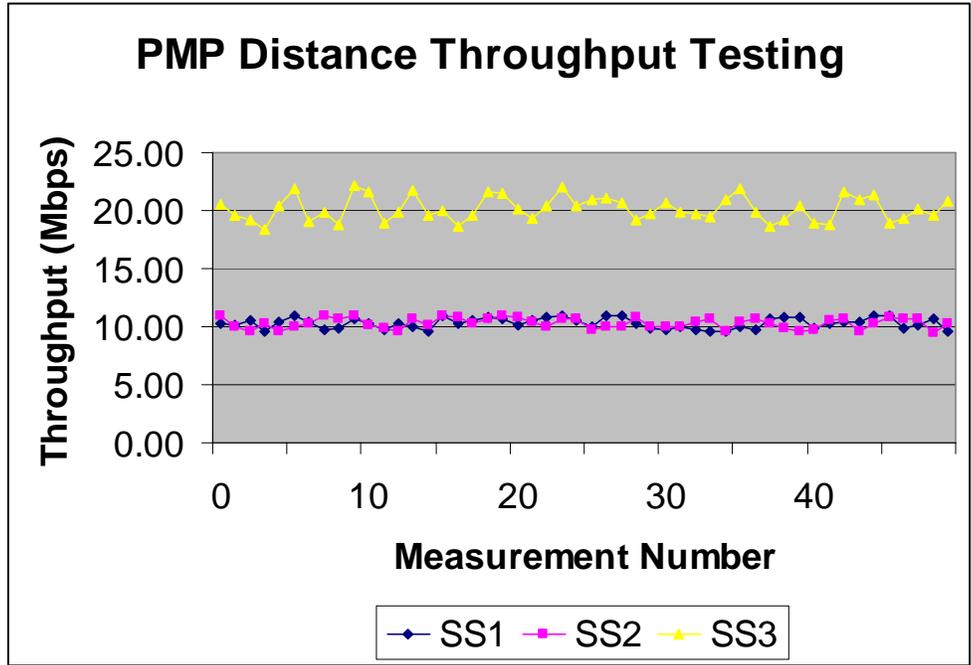


Figure 26. NLOS Throughput Test Results

	SS1 LOS Baseline (test #1)	SS1 NLOS at FP 13 (test #2)	SS 2 LOS Baseline (test #1)	SS2 NLOS at Hill 1 (test #2)	SS3 LOS Baseline (test #1)	SS3 LOS on Runway (test #2)
Throughput in Mbps	24.87	10.123	20.123	20.124	19.756	20.105
Average Latency	0	.005ms	0	.006ms	0	0
Packet Loss (3,800 total packets were transmitted)	0%	> 1%	0%	44%	0%	0

Table 15. Tests #1 and #2 Consolidated Results

*c. Test #3 Multicast Traffic Test*

For this test, locations for the SSs remained the same as the previous test. To test the link’s ability to handle multicast traffic, we configured IPerf® servers on the

SS laptops. Each SS then had its address bound to the Class D multicast group address of 224.0.55.55. From the NOC, a client IPerf® laptop sent out constant stream of UDP traffic to the multicast address. With the servers at SS1 listening for multicast traffic, we were able to measure the performance of multicast traffic in NLOS conditions. (See Figure 27 for example output)

```
-----
Client connecting to 224.0.55.55, UDP port 5001
Sending 1470 byte datagrams
Setting multicast TTL to 5
UDP buffer size: 8.00 KByte (default)
-----
[148] local 10.0.0.40 port 1173 connected with 224.0.55.55 port 5001
[ ID] Interval      Transfer      Bandwidth
[148] 0.0- 5.0 sec   642 KBytes   1.05 Mbits/sec
[148] Sent 447 datagrams
```

Figure 27. Example of IPerf® Multicast Client Test Output

The results for each SS reflected Jitter measurements of less than 0.0009 ms and 0% packet loss for each time interval. The output of the IPerf® client was then saved into text files for analysis. The data collected shows that the links were adequately robust to accept multicast traffic with only negligible packet loss. Figure 27 shows the IPerf results from FP13’s SS1. The results from FP 13 were representative of the outputs from each of the SS locations.

```
-----
Server listening on UDP port 5001
Binding to local address 224.0.55.55
Joining multicast group 224.0.55.55
Receiving 1470 byte datagrams
UDP buffer size: 8.0 KByte (default)
-----
[ 3] local 224.0.55.55 port 5001 connected with 10.0.0.40 port 1025
[ ID] Interval      Transfer      Bandwidth      Jitter      Lost/Total Data:
[ 3] 0.0- 1.0 sec   131 KBytes    1.0 Mbits/sec  0.005 ms    0/89 (0%)
[ 3] 1.0- 2.0 sec   128 KBytes    1.0 Mbits/sec  0.009 ms    0/91 (0%)
[ 3] 2.0- 3.0 sec   128 KBytes    1.0 Mbits/sec  0.007 ms    0/91 (0%)
[ 3] 3.0- 4.0 sec   128 KBytes    1.0 Mbits/sec  0.003 ms    0/87 (0%)
[ 3] 4.0- 5.0 sec   128 KBytes    1.0 Mbits/sec  0.008 ms    0/89 (0%)
[ 3] 0.0- 5.0 sec   642 KBytes    1.0 Mbits/sec  0.008 ms    0/447(0%)
```

Figure 28. Multicast Server Output of Link from FP13 to NOC

**d. Test #4. QoS Test**

The goal of this test was to capture data on the QoS characteristics of Redline equipment. Once again, data was collected using the IPerf® measurement tool. Each SS took a turn a being configured as a server while the laptop at the NOC was configured as an IPerf client. The IPerf® client would send a continuous stream of UDP traffic to simulate voice communications. The server was used to detect UDP datagram loss by the ID numbers in the datagram transmitted. Usually a UDP datagram is divided into several IP packets. Losing a single IP packet will lose the entire datagram.<sup>7</sup>

Jitter calculations were also continuously computed by the IPerf server. The client at the NOC recorded a 64-bit second/microsecond timestamp in the packet it sends out. The server then computed the relative transit time in the following format:

$$Jitter = server's\ receive\ time - client's\ send\ time$$

The client's and server's clocks do not need to be synchronized; any difference is subtracted out in the jitter calculation. Jitter is the smoothed mean of differences between consecutive transit times. With the assistance of the Redline Representatives, we were able configure varying level of QoS for each node. Because the AN-50 base station had complete control in configuring each link to the SS, we were able to configure individual sets of QoS parameters for each node. Tables 16 through 18 show the results of the QoS testing.

[148] local 10.0.0.40 port 1229 connected with 10.0.0.42 port 5001					
Run Number	Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
1	0.0-10.0 sec	6.60 MBytes	5.39 Mbits/sec	17.522 ms	3795/ 8500 (45%)
2	0.0-10.0 sec	6.56 MBytes	5.50 Mbits/sec	4.512 ms	3815/ 8493 (45%)
3	0.0-10.0 sec	7.00 MBytes	5.87 Mbits/sec	4.229 ms	3509/ 8500 (41%)
4	0.0-10.0 sec	6.89 MBytes	5.76 Mbits/sec	4.599 ms	3582/ 8500 (42%)
5	0.0-10.0 sec	6.30 MBytes	5.29 Mbits/sec	4.832 ms	4004/ 8500 (47%)
6	0.0-10.0 sec	6.62 MBytes	5.53 Mbits/sec	5.520 ms	3778/ 8500 (44%)
7	0.0-10.0 sec	6.20 MBytes	5.21 Mbits/sec	4.105 ms	3925/ 8351 (47%)
[148] Sent 8500 datagrams					

Table 16. NOC to FP 13 QoS Test Results

<sup>7</sup> Out-of-order packets cause some ambiguity in the lost packet count; IPerf assumes they are not duplicate packets, so they are excluded from the lost packet count.

[148] local 10.0.0.40 port 1215 connected with 10.0.0.45 port 5001					
Run Number	Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
1	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	1.466 ms	0/ 8500 (0%)
2	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	1.274 ms	0/ 8500 (0.059%)
3	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	0.000 ms	0/ 8500 (0%)
4	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	0.063 ms	0/ 8500 (0%)
5	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	0.003 ms	0/ 8500 (0%)
6	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	0.043 ms	0/ 8500 (0%)
7	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	0.050 ms	0/ 8500 (0%)
[148] Sent 8500 datagrams					

Table 17. NOC to Hill #1 QoS Test Results

[148] local 10.0.0.40 port 1215 connected with 10.0.0.45 port 5001					
Run Number	Interval	Transfer	Bandwidth	Jitter	Lost/Total Datagrams
1	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	1.466 ms	0/ 8500 (0%)
2	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	1.274 ms	0/ 8500 (0.059%)
3	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	0.000 ms	0/ 8500 (0%)
4	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	0.063 ms	0/ 8500 (0%)
5	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	0.003 ms	0/ 8500 (0%)
6	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	0.043 ms	0/ 8500 (0%)
7	0.0-10.0 sec	11.9 MBytes	10.0 Mbits/sec	0.050 ms	0/ 8500 (0%)
[148] Sent 8500 datagrams					

Table 18. NOC to Runway QoS Test Results

#### D. OBSERVATIONS FROM TEST RESULTS

The authors did not know what to expect in performance based on the previous experiments. Past testing had produced data rates ranging from 20-30 Mbps in PTP LOS and NLOS conditions. [Ref 30] We expected an expected deterioration of the link's throughput when deployed in the PMP scenario, but we were surprised to find that the decrease was not very significant. The link was able to sustain rate in excess of 24 Mbps in LOS conditions and in excess of 10 Mbps in NLOS conditions.

However, the degree of our optimism regarding to which our links were able to operate in NLOS conditions has to be tempered by the fact that our link did not exceed 3.5 km in distance. The challenge of establishing the NLOS FP13 link in conjunction with the Hill #1 link with a sector antenna shows that in the 5.8 GHz frequency range, NLOS technologies are only partial remedies; they do not rewrite the laws of physics. What they can do is effectively cope with partially obstructed sites by taking advantage of multipath transmissions.

In general, QoS can be defined as the conditions within a network that will support the delivery of time sensitive or low redundancy services with minimal perception of degradation. Normally, some packet loss occurs in any network, but in a wireless network the frequency of packet loss tends to be higher than in wired networks. This is typically caused by the fluctuation of background interference levels, such as sudden fades because of multipath, and variable attenuation with the changing in weather conditions. We did not observe significant fluctuations with respect to packet loss, this may be due to the static/benign environment and ideal weather conditions which our test took place in. However, the results of our PMP QoS test correspond with previous experiments conducted with NPS students during STAN experiments. Based on the past testing various deployments and conditions, it seems that IEEE 802.16 systems would provide the required QoS capabilities required for STOM operations.

## **E. SUMMARY**

The ability of our NLOS links to maintain throughput in excess of 10 Mbps as part of a PMP deployment illustrates the potential of this technology in a tactical scenario. It appears that an IEEE 802.16 MAC implementation within JTRS would support the same data requirement specified in the WNW FDD. The pre-standard system tested proved to be a good representative of the capabilities and characteristics of the IEEE 802.16a standard. The equipment also provided some insight into the challenges which will be faced an IEEE 802.16 standard implementation in a STOM tactical situation.

The pre-standard equipment showed that OFDM based technologies can effectively deal with NLOS conditions, at least over relatively short distances. This

aspect would be critical for typical STOM operations where subordinate commands will usually be deployed NLOS positions relative to adjacent units. The ability of IEEE 802.16 standard compliant equipment to take advantage of multipath signal reflections adds a capability that would be advantageous to units operating in urban environments. In such environments IEEE 802.16 standard equipment is not only resistance to multipath fading, but is able to complete otherwise difficult links by receiving the multipath signals.

## **VII. ADAPT FROM COTS RECOMMENDATIONS**

### **A. INTRODUCTION**

In this chapter we will examine the adaptations that should be made to the IEEE 802.16 standard before it can be truly viable for military communications. This chapter will also outline areas of the standard that should be tested and evaluated further.

### **B. ADAPT-FROM-COTS ITEMS**

As revealed in Chapter Five of this thesis, the IEEE 802.16 standard fulfills many of the networking requirements of STOM and many of the goals of the WNW without the need for adaptations. However, several adaptations to the standard are required in order for it to meet all of the outlined requirements. These adaptations fall into the general categories which are outlined below.

#### **1. Frequency**

The IEEE 802.16 standard should be adapted to additional PHYs in frequency ranges between 2 MHz and 2 GHz. The standard currently has two PHY specifications ranging in frequency from 2 GHz to 66 GHz. However, currently most tactical radio communications takes place in the lower frequency spectrum between 2 MHz and 400 MHz. [Ref 27] Furthermore, the JTRS radio will be capable of communication between 2 MHz and 2 GHz, and if the IEEE 802.16 standard is to truly serve as a development model for the WNW, it must be able to operate in these frequency ranges.

The development of IEEE 802.16 standards in different frequency bands will have to consider the differing characteristics of these bands. Benefits of developing an IEEE 802.16 standard to operate in the lower frequencies include dramatically increased range and increased flexibility to communicate with a wider range of platforms (i.e., aircraft and naval vessels via HF and VHF frequencies). Drawbacks of these frequency ranges include the decreased size of available frequency bands. [Ref 18] Additionally, there are likely to be many differences in the supported modulation schemes. This concept is

illustrated by the fact that the IEEE 802.16 standard is able to support OFDM in the 2-11 GHz frequency range, but will only support single channel modulation in the 10-66 GHz frequency range. [Ref 21]

## **2. Encryption**

The IEEE 802.16 standard as it is now written is vulnerable to traffic analysis and denial of service attacks because it does not layer 1 bulk encrypt layer 2 (MAC) header information or certain management and scheduling messages. Additionally, the standard does not provide for the inclusion of authentication material in each packet, and therefore is vulnerable to man-in-the-middle-attacks. These vulnerabilities would necessitate adaptations before the IEEE 802.16 standard could be used by the military for the transport of sensitive information in hostile environments.

In order to make the standard more secure, adaptations need to provide for the end-to-end encryption of all payload, header and management packet data. Additionally, the addition of at least some authentication material in management packets would prevent the spoofing of these packets by an attacker.

## **3. Antenna Pointing Mechanism**

A feature that would greatly increase the utility of this equipment for employment in tactical environments is the development of efficient antenna pointing mechanisms. This feature would greatly reduce the set up time required during tactical displacements. After repeated testing of pre-standard equipment, the authors have found that unless an omni-directional antenna was being employed, the pointing of the antenna was the most time consuming task associated with setting up the equipment. It was not uncommon to spend an hour or more trying to establish a communications link to a distant node.

## **C. SUMMARY**

Our research has found that with relatively few adaptations, the IEEE 802.16 standard may be adapted for military tactical communications. The adaptations identified would further enhance the utility of the IEEE 802.16 standard by allowing it to operate in additional frequency ranges and at a higher level of security. Additionally, adaptations to the form of the IEEE 802.16 equipment currently on the market will make the gear better

able to handle the physical rigors that today's military tactical communications hardware are subjected to.

THIS PAGE INTENTIONALLY LEFT BLANK

## **VIII. CONCLUSIONS**

### **A. FINDINGS**

Our discussions on IEEE 802.16 focused on the MAC and PHY characteristics as they are currently implemented within the IEEE 802.16 family of standards and how similar they are to the planned specifications of the WNW. The intent was to investigate and make recommendations on the COTS adaptations necessary to make the IEEE 802.16 standard suitable as a complimentary technology within the STOM scenario.

#### **1. Addressing the Networking Requirements**

Our comparison of the IEEE 802.16 standard against the requirements of the WNW, radio WANs, and STOM reveals that the IEEE 802.16 standard, with several adaptations, should be capable of addressing all of the identified requirements. The IEEE 802.16 standard not only addresses a majority of the WNW's networking characteristics, but it is proven to provide superior performance when compared to WNW and other tactical data networking waveforms. It is likely that with a few adaptations, further maturity of the standard, and further testing, the IEEE 802.16 standard will be able to achieve all of the outlined requirements.

#### **2. Adapt From COTS**

The IEEE 802.16 standard is a good point of departure for the future development of a wideband networking standard. The three primary area which would required more robust capability includes flexibility in operating frequency ranges, encryption, and "militarized" form factors. These recommended adaptations would enhance the utility of the IEEE 802.16 standard by allowing it to operate in additional frequency ranges and at a higher level of security in more hostile propagation environments.

### **B. FURTHER RESEARCH**

The following section provides a brief description of follow-on research possibilities and research questions that warrant further investigation.

#### **1. The IEEE 802.16e Standard**

Our research has focused on the IEEE 802.16 and the IEEE 802.16a published standards for two reasons. First, each draft provided the most current approved version of the protocols at the time of the writing of this thesis. Second, the availability of pre-

standard equipment whose MAC closely resembled the MAC of the IEEE 802.16a approved standard and enabled us to conduct hands-on testing. However, the standard which offers the greatest potential impact on STOM communications is the 802.16e standard. The 802.16e standard specifically addresses the networking issues for the mobile user. The IEEE 802.16e promises to offer connectivity for mobile users up to 90 mph. Further research should look at the potential impact that this standard will have for military applications.

## **2. MANET in STOM Operation**

STOM operations will be characterized as ad-hoc and dynamic in nature. Thus, continued research is needed to find the best solution for MANET in STOM operations. This research should include looking at how the JTRS WNW and the IEEE 802.16f Standard could address this requirement. The authors feel that performance tradeoffs with respect to security, QoS, and network management as network nodes become more mobile are key issues which should also be addressed. Interoperability issues with the wired network and a cost-benefit analysis of Layer 2 or Layer 3 solutions are also important concerns.

## **3. Mobility Management**

Participating in practical testing of the pre-standard equipment brought out a key implementation consideration. The IEEE 802.16 MAC in a PMP deployment places emphasis on the ability of the BS to control the parameters surrounding the network. Thus in a PMP deployment, the BS presents a single point of failure. In order to avoid this lack of redundancy in the network, it would be critical for the SS and BS to be able to communicate with at least another BS. With the IEEE 802.16e standard having just been approved in June 2004, more testing and evaluation will be needed to see how this standard and the IETF handle mobility of broadband wireless systems at higher layers. Higher layer mobility would involve the dynamic connection of a mobile SS to the nearest BS within its subnet as it moves into a new coverage area. This would be an area which could provide valuable information on the best way to implement the IEEE 802.16e standard in a tactical scenario.

#### **4. IEEE 802.16 Vulnerability Testing**

Information Assurance is, and will remain, a very important concern for wireless technologies. As with the IEEE 802.11, vulnerabilities of the new standard will become more apparent as IEEE 802.16 technology matures and WiMax products become increasingly available (See Appendix B for WiMax vendors). The authors believe that further research into the IEEE 802.16 Standard's security issues perspective is imperative to determine it's potential applications within the military.

#### **5. IEEE PHY Level Independence**

Our research has been focused on the IEEE 802.16 standards, which apply to the 2-10 and 10-66 GHz frequency ranges. However, the IEEE 802.16 standards were written with PHY independence in mind. We feel that validation of the ability to implement an IEEE 802.16 MAC on a military operating frequency band is the next logical step. The research should look at the requirements of a PHY waveform that is still robust to the effects multipath propagation, interference, and jamming.

#### **6. Application to Satellite Communications**

In order for the IEEE 802.16 standard to be adapted to meet the needs of satellite communications systems, it must be tolerant of the long propagation delay times associated with satellite communications. Currently, the IEEE 802.16 standard does not specify a maximum value for propagation delay tolerance, although the maximum frame duration is know to be 2ms. Further research will be required in this area to determine the standard's suitability for satellite communications.

### **C. SUMMARY**

We found relatively few adaptations are needed for the IEEE 802.16 standard for military tactical communications. The adaptations identified in the previous chapters would permit this technology to address many of the existing gaps in current tactical radio systems while leveraging the commercial sector's research and development efforts.

While this research looked solely at STOM operations, this technology demonstrates the potential for other military applications such as intra-battle group communications. With the further refinement of IEEE 802.16 with regards to mesh

extensions and the development of 802.16e chipsets in the near future the technological momentum of the standard poses an excellent opportunity for the DoD to leverage the R&D of the commercial sector to address increasing demands of NCW.

When looking at the requirements for STOM operations and the specification of the WNW, DoD should investigate further the potential the IEEE 802.16 standard as ‘an adapt from COTS’ alternative. While research into IEEE 802.16 standard is just beginning, the arrival of WiMax compliant products in the coming year will offer plenty of opportunities to explore its applicability in a tactical environment. At a minimum, the IEEE 802.16 standard makes it a good point of departure for the future development of a wideband networking standard for STOM operations.

## APPENDIX A REDLINE COMMUNICATIONS AN-50 SPECIFICATIONS

AN-50 System Specifications					
System Capability	Non-line-of-sight operations, PTP / PMP mode				
RF Band	ISM Band - 5.725 - 5.825 GHz				
Channel Center Frequencies	17 Center Frequencies spaced at 5 MHz increments				
Channel Size	20 MHz				
RF Dynamic Range	> 50 dB				
Modulation/Throughput	Modulation	Coding Rate	Over The Air Rate (Mbps)	Uncoded Burst Rate (Mbps)	Average Ethernet Rate (Mbps) Point to Point
	BPSK	1/2	12	6	5.7
	BPSK	3/4	12	9	8.6
	QPSK	1/2	24	12	11.5
	QPSK	3/4	24	18	17
	16 QAM	1/2	48	24	22
	16 QAM	3/4	48	36	33
	64 QAM	3/4	72	48	43
64 QAM	3/4	72	54	48	
Maximum Tx Power	+20 dBm (region dependent)				
Rx Sensitivity	-86 dBm at 6 Mbps (based on BER of 1x10 <sup>-9</sup> )				
IF Cable	• Maximum length up to 250 ft (76m) using RG6U / 500 ft (152m) using high-grade RG11U				
Network Attributes	<ul style="list-style-type: none"> <li>• Transparent bridge</li> <li>• DHCP passthrough</li> <li>• VLAN passthrough</li> <li>• 802.1q (point to point mode)</li> </ul>				
Provisioning	Best effort, Committed Information Rate (CIR) (point-to-multipoint)				
Modulation	Dynamic Adaptive Modulation (bi-directional) auto selects: • BPSK • QPSK • 16 QAM • 64 QAM (Pt-to-Pt Mode)				
Over The Air Encryption	64-bit private key encryption				
Nomadic Feature	Automatic Frequency Scanning (Pt-to-Multipoint mode)				
System Latency	Typically <2 ms Point to Point				
MAC	<ul style="list-style-type: none"> <li>• Point to Point or Point to Multipoint</li> <li>• Automatic Repeat Request (ARQ) error correction</li> <li>• Concatenation/Fragmentation</li> </ul>				
Max Range	Range varies with each antenna gain, and modulation rate selected. <ul style="list-style-type: none"> <li>• Over 10 km / 6 miles non-line-of sight</li> <li>• Over 80 km / 50 miles line-of-sight</li> <li>• Up to 30 km / 19 miles Point to Multipoint</li> </ul>				
Network Services	Transparent to 802.3 services and applications				
Duplex Technique	Dynamic TDD (time division duplex)				
Wireless Transmission	OFDM (orthogonal frequency division multiplexing)				
Backhaul Connection	10/100 BT Ethernet (RJ45)				
System Configuration	Web interface (PMP) Web interface, SNMP, Telnet, CLI, Console port (PTP)				
Redundant power	Optional Dual AC/DC Power Supply, with automatic fail-over				

\*Note Max. Operational Power Per Channel depends on Country regulatory limits.

\*\*Specs subject to change.

Table 19. AN 50 Specifications (From: Ref 35)

THIS PAGE INTENTIONALLY LEFT BLANK

## APPENDIX B 802.16 AND OFDM VENDORS

Vendor	Target market(s)	Product family names	Notes
Airspan	Medium and large businesses	AS4030, AS3030	Second to announce an 802.16a-compliant product
Alvarion	WISPs, telecom, utilities, rural cellular carriers	BreezeNet, BreezeAccess, BreezeLink, Walkair	Wide range of products; working with Intel on development of 802.16a chip
Aperto	WISPs, last-mile broadband wireless	PacketWave	Has products that allow for flexible channel size
Flarion	Mobile broadband access	RadioRouter	Targets mobile user and emphasizes use of Flash-OFDM
Mesh Networks	Law enforcement, ITS, emergency response, military, hotspots	MEA Mobile Broadband	Emphasizes importance of mobility
Motorola	WISPs	Canopy	Based on unlicensed 5.3- or 5.8-GHz frequency range
Navini Networks	WISPs	RipWave	Targets mobile/nomadic access; strong proponent of IEEE 802.20 standard
Proxim	Last-mile, voice and data back haul, Enterprise	Tsunami, Lynx,	Wide range of products covering most needs
Redline Communications	Telecom with long-range point to point	AN-30, AN-50, AN-100	First to market with 802.16a-compliant product
Soma Networks	WISPs, last-mile broadband wireless	Soma SoftAir	Antenna integrated into CPE
Trango	Security, video surveillance, ITS, public safety, WISPs, MUSH	Access5830, TrangoLink	Products are all in unlicensed bands
WaveRider	WISPs, campus networks	LMS and NCL series	Products operate in 900-MHz and 2.4-GHz range, allowing N-LOS
Wave Wireless Networking	WISPs, campus, business park, cellular & wireless & telecom back haul	SpeedLAN, SpeedWave solutions, also has a mesh solution	Besides regular PTP and PMP
Wi-LAN	Telecom, wireless ISP, enterprises	Libra 3000/5800, Ultima 3, AWE, VIP	Strong technology developer of W-OFDM

Table 20. WMAN Vendors (From: Ref 30)

Note: This table provides a snapshot of broadband wireless vendors as of September 2004. The vendors listed will likely fluctuate as the technologies and broadband marketplace matures.

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF REFERENCES

1. Intel Corporation. *IEEE 802.16 and WIMAX*. Broadband Wireless Access White Paper [online] [http://www.intel.com/ebusiness/pdf/wireless/intel/80216\\_wimax.pdf](http://www.intel.com/ebusiness/pdf/wireless/intel/80216_wimax.pdf) Last accessed on September 1, 2004
2. Department of Defense. *DoD Report To Congress: Network Centric Warfare* [online] [http://www.dod.mil/nii/NCW/new\\_exec\\_sum.pdf](http://www.dod.mil/nii/NCW/new_exec_sum.pdf) Last accessed on September 1, 2004
3. Communication Systems Division, Marine Corps Systems Command, Headquarters, USMC, brief *Transforming Marine Corp C4I*, Aug 2003
4. United States Marine Corps, *The STOM Concept of Operations* ONLINE <https://www.doctrine.usmc.mil/> Last accessed on September 1, 2004
5. Programs & Resources Department, Headquarters, USMC, *Marine Corps Concepts and Programs* 2004 ONLINE <http://hqinet001.hqmc.usmc.mil/p&r/concepts/concepts.htm> Last accessed on September 1, 2004
6. Department of the Navy. "Ship to Objective Maneuver." Marine Corps Combat Development Command Quantico, VA, July 1997
7. Office of Force Transformation, Department of Defense, *Naval Transformation Roadmap* ONLINE [http://www.oft.osd.mil/library/library\\_files/document\\_358\\_NTR\\_Final\\_2003.pdf](http://www.oft.osd.mil/library/library_files/document_358_NTR_Final_2003.pdf) [APR 2004](#) Last accessed on September 1, 2004
8. Congressional Budget Office, *The Army's Bandwidth Bottleneck*, Online, <http://www.cbo.gov/showdoc.cfm?index=4500&sequence=5>, Last accessed on September 1, 2004
9. Fujimoto, Masashi, *The Important Factors to Success in Digitizing Defense Forces* ONLINE <http://www.drc-jpn.org/AR-5E/fujimoto-e.htm> Last accessed on September 1, 2004
10. Alberts, David et al, *Network Centric Warfare: Developing and Leveraging Information Superiority*, CCRP Publication Series February 2000
11. JTRS, Joint Program Office Brief JTRS: Program Status, ONLINE [http://spacecom.grc.nasa.gov/icnsconf/docs/2003/11\\_D2/D2-06A-Harrison.pdf](http://spacecom.grc.nasa.gov/icnsconf/docs/2003/11_D2/D2-06A-Harrison.pdf), Last accessed on September 1, 2004

12. JTRS, Joint Program Office, *Joint Tactical Radio System (JTRS) Wideband Networking Waveform (WNW) Functional Description Document (FDD) Version 2.21*, 29 November 2001
13. Global Security.org Tactical Internet ONLINE  
<http://www.globalsecurity.org/military/systems/ground/internet-t.htm> Last accessed on September 1, 2004
14. Corson, S. and Macker J., *Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations* IETF Network Working Group January 1999
15. Buddenberg, Rex, *An Approach to Networking Requirements Analysis* ONLINE  
[http://web1.nps.navy.mil/~budden/lecture.notes/req\\_anal/req\\_anal.html](http://web1.nps.navy.mil/~budden/lecture.notes/req_anal/req_anal.html), Last accessed on September 1, 2004
16. General Accounting Office. *Challenges and Risks Associated with the Joint Tactical Radio System Program* GAO-03-879R [online]  
<http://www.gao.gov/new.items/d03879r.pdf> Last accessed on September 1, 2004
17. Intel Corporation. *Accelerating Wireless Broadband*. [online]  
[http://www.intel.com/business/bss/infrastructure/wireless/80216\\_accelerating.pdf](http://www.intel.com/business/bss/infrastructure/wireless/80216_accelerating.pdf)  
Last accessed on September 1, 2004
18. Sweeney, Daniel, *WiMax Operator's Manual: Building 802.16 Wireless Networks*, Apress Publishing, May 2004
19. Cohen, Beth and Deutsch, Debbie. *IEEE 802.16: The Future in Last Mile Wireless Connectivity*. 2003
20. Eklund, Carl et al. *IEEE Standard IEEE 802.16: A Technical Overview of the WirelessMAN Air Interface for Broadband Wireless Access*. IEEE Communications Magazine. 2002
21. IEEE Computer Society. *Air Interface for Fixed Broadband Wireless Access Systems*. 2001
22. *OFDM Tutorial*. [online] <http://www.wave-report.com/tutorials/OFDM.htm>.  
Last accessed on 24 July 2004
23. The Free Dictionary. *Reed Solomon Error Correction*. [online]  
[http://encyclopedia.thefreedictionary.com/Reed-Solomon error correction](http://encyclopedia.thefreedictionary.com/Reed-Solomon+error+correction). Last accessed on 24 July 2004

24. Buddenberg, Rex. *Radio WAN Building*. [online]  
[http://web1.nps.navy.mil/~budden/lecture.notes/r-wan/radio-WAN\\_building.html](http://web1.nps.navy.mil/~budden/lecture.notes/r-wan/radio-WAN_building.html)  
Last accessed on 22 Aug 04
25. Garcia, Gil and Joseforsky, David. *Transformational Communications Architecture for the Unit Operations Center (UOC); Common Aviation Command and Control System (CAC2S); and Command and Control On-the-Move Network, Digital Over-the-Horizon Relay (CoNDOR)*. Master Thesis. Naval Postgraduate School. June 2004
26. Blazeovich, Ryan *Wireless, Long Haul, Multi-Path Networking: Transforming Fleet Tactical Networking Operations with Rapidly Deployable, Composable, Adaptive, Multi-Path Networking in Austere Environments*. Master Thesis. Naval Postgraduate School. September 2004
27. Integrated Publishing. *Radio Operator's Handbook*. [online]  
[http://www.tpub.com/content/USMC/mcr3403b/css/mcr3403b\\_8.htm](http://www.tpub.com/content/USMC/mcr3403b/css/mcr3403b_8.htm) Last accessed on 1 Sep 04.
28. Eriksen, David, *Improving the Command A Control Organization In Expeditionary Operations*, Master's Thesis, Naval Postgraduate School, 2003
29. Boom, Derrick. *Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks*. Masters Thesis. Naval Postgraduate School. September 2004
30. Chandra, Madhavi W. *Extensions to OSPF to Support Mobile Ad Hoc Networking* IEF Working Group July 2004
31. Kenyon, Henry, *Joint Tactical Radio System Underway*, Signal Magazine August 2002
32. Bulk, Frank. *Giving Wireless MAN Some Muscle*. [online]  
[http://cnscenter.future.co.kr/resource/hot-topic/wlan/1505ws1\\_file.pdf](http://cnscenter.future.co.kr/resource/hot-topic/wlan/1505ws1_file.pdf) Last accessed on 24 Aug 04
33. Adamson, B., *RFC 1677 - Tactical Radio Frequency Communication Requirements for IPng* ONLINE <http://www.faqs.org/rfcs/rfc1677.html>, Last accessed on September 1, 2004
34. NSA Website. Global Information Grid. ONLINE  
<http://www.nsa.gov/ia/industry/gigscope.cfm?MenuID=10.3.2.2>, Last accessed on September 10, 2004
35. Redline Communications Website. ONLINE  
<http://www.redlinecommunications.com> Last Accessed on September 14, 2003

THIS PAGE INTENTIONALLY LEFT BLANK

## GLOSSARY

Bandwidth. Bandwidth is a term used to describe the rate at which information moves from one electronic device to another—usually expressed in terms of bits per second—over phone lines, fiber optic cable, or wireless telecommunications systems.

Communication. Communication is information transfer, among users or processes, according to agreed conventions.

Data Rates. The aggregate rates at which data pass a point in the transmission path of a system.

Gateway. A gateway in a communications network is a network node equipped for interfacing with another network that uses different protocols. A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires that mutually acceptable administrative procedures be established between the two networks. A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.

Global Information Grid. The Global Information Grid (GIG) will be a net-centric system operating in a global context to provide processing, storage, management, and transport of information to support all Department of Defense (DoD), national security, and related Intelligence Community missions and functions—strategic, operational, tactical, and business-in war, in crisis, and in peace.

GIG capabilities will be available from all operating locations: bases, posts, camps, stations, facilities, mobile platforms, and deployed sites. The GIG will interface with allied, coalition, and non-GIG systems.

The overarching objective of the GIG vision is to provide the National Command Authority (NCA), warfighters, DoD personnel, Intelligence Community, business, policy-makers, and non-DoD users with information superiority, decision superiority, and full-spectrum dominance. [Ref

Information Assurance. Information Operations (IO) that protect and defend information and information systems by ensuring their confidentiality, authenticity, availability, integrity, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.

---

Note: Unless noted, these definitions are reprinted from the JTRS ORD 30 Jan 2001

Integrity. Integrity is the property that data, systems, services, and other controlled resources have not been altered or destroyed in an unauthorized manner. It is the quality of an information system (IS) that reflects the logical correctness and reliability of the operating systems and the logical completeness of the hardware and software that implement the protection mechanisms.

Inter-Networking. Inter-networking is the process of inter-connecting two or more individual networks to facilitate communications between nodes of the inter-connected networks. Each network may be distinct, with its own addresses, internal protocols, access methods, and administration.

Latency. Latency is a quality or state of being that is marked by suspension of activity, or delay, in performing an operation. In an information transfer operation; latency is a measure of the time that elapses at various stages of the transfer. The information latency that is attributable to the communications means is the elapsed time from when a user terminal submits information to the means until the information is submitted to the intended user terminal.

Network. A network is an inter-connection of three or more communicating entities.

Network Administration. Network administration is a group of network management functions that provide support services; ensure that the network is used efficiently; and ensure that prescribed service quality objectives are met. Network administration may include activities such as network address assignment, assignment of routing protocols and routing table configuration, and directory service configuration.

Network Architecture. Network architecture is the design principles, physical configuration, functional organization, operational procedures, and data formats used as the basis for the design, construction, modification, and operation of a communications network.

Network Management. Network management is execution of a set of functions required for controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a telecommunication network. Network management includes performing functions such as initial network planning, frequency allocation, predetermined traffic routing to support load balancing, cryptographic key distribution authorization, configuration management, fault management, security management, performance management, and accounting management.

Node. A general term used to describe either a terminal connection point common to two or more branches of a network; a switch forming a network backbone; patching and control facilities; technical control facilities.

Non-Line of Sight. As the term is most commonly employed, it refers to radio equipment capable of dealing with the consequences of obstructions that occur within the

Fresnel zone but do not block optical line of sight. What is really being claimed here is not the ability to reach completely obstructed sites but to cope with multipath with a high degree of effectiveness. [Ref 16]

Protocol. A protocol is a formal set of conventions governing the format and control of interaction among communicating functional units. In layered communications system architecture, a protocol is a formal set of procedures that are adopted to facilitate functional inter-operation within the layered hierarchy.

Radio Channel. A radio channel is an assigned band of frequencies sufficient for radio communication. The bandwidth needed for a radio channel depends upon the type of transmission and the frequency tolerance.

Radio Net. An organization of radio sets directly communicating on a common channel or frequency.

Radio Network. An interconnection of three or more radio sets communicating with each other, but not necessarily on the same channel or frequency (e.g. a multi-channel network that may choose one or more available channels for a communications session between its nodes).

Three Tiered Communication Architecture. Each of the service's communication architectures can be broken down into three primary tiers of communication links. The lowest level is Tier 1 which refers to the edges of the network and normally consist of stub networks that can either be single subnets or small Internets and are not required to relay non local traffic. Tier 2 refers to the primary mission of the WNW providing a communications backbone to the Tier 1 networks and support the relay of transit as well as relay traffic. Tier 3 refers to external networks that are not a part of the WNW that support transit and local traffic. These include trunk networks, satellite communications and other radio networks. Tiers 2 and 3 connect together at several points to provide an adaptable internetwork that appears seamless to the user.

Transmission Security (TRANSEC). A component of COMSEC resulting from the application of measures taken to protect transmissions from interception and exploitation by means other than cryptanalysis (Cryptanalysis is defined as "Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and /or key employed in the encryption.). Transmission security is the protection of the communications paths against attack. Defensive measures include anti-jam, low probability of detection, low probability of intercept, spread spectrum techniques such as frequency hopping and direct sequence spreading, and protected distribution.

Type 1: A type 1 product is a classified or controlled cryptographic item endorsed by NSA for securing classified and sensitive U.S. Government information, when appropriately keyed. The term refers only to products, and not to information, key, services or controls. Type 1 products contain classified NSA algorithms. They are

available to U.S. Government users, their contractors, and federally sponsored non-U.S. Government activities subject to export restrictions in accordance with International Traffic in Arms Regulation.

Wide-Band. A wide band circuit may have a bandwidth wider than normal for the type of circuit, frequency of operation, or type of modulation. In common usage, "wide-band" refers to a high capacity for information transfer. In this thesis, wide-band refers to a networked radio waveform that has a node-to-node capacity for information transfer of 512 Kbps or greater.

Waveform. A waveform is the representation of a signal as a plot of amplitude versus time. In general usage, the term waveform refers to a known set of characteristics, e.g. SINCGARS or EPLRS "waveforms".

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center  
Fort Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. Marine Corps Representative  
Naval Postgraduate School  
Monterey, California
4. Director, Training and Education, MCCDC, Code C46  
Quantico, Virginia
5. Director, Marine Corps Research Center, MCCDC, Code C40RC  
Quantico, Virginia
6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)  
Camp Pendleton, California
7. Rex Buddenberg  
Naval Postgraduate School  
Monterey, CA
8. Dan Boger  
Naval Postgraduate School  
Monterey, CA
9. Commandant (G-CC)  
US Coast Guard  
Washington, VA 20593
10. Glen Elfers  
Transformation Communications  
System Aerospace Corp  
El Segundo, CA

THIS PAGE INTENTIONALLY LEFT BLANK

