2005-09

A study of the IEEE 802.16 MAC Layer and its utility in augmenting the ADNS Architecture to provide adaptable intra-strike group high-speed packet switched data, imagery, and voice communications

Pryor, Jameau R.; Johnson, Ballard V.

Monterey, California. Naval Postgraduate School

https://hdl.handle.net/10945/1977

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A STUDY OF THE IEEE 802.16 MAC LAYER AND ITS UTILITY IN AUGMENTING THE ADNS ARCHITECTURE TO PROVIDE ADAPTABLE INTRA-STRIKE GROUP HIGH-SPEED PACKET SWITCHED DATA, IMAGERY, AND VOICE COMMUNICATIONS.

by

Ballard V Johnson
Jameau R Pryor

September 2005

Thesis Co-Advisors: Rex Buddenberg
John Gibson

Approved for public release; distribution is unlimited.

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

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: A Study of the IEEE 802.16 MAC Layer and its Utility in Augmenting the ADNS Architecture to Provide Adaptable Intra-Strike Group High-Speed Packet Switched Data, Imagery, and Voice Communications.	**5. FUNDING NUMBERS**
6. AUTHOR(S) Ballard V Johnson and Jameau R Pryor	
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

13. ABSTRACT (maximum 200 words)

This research evaluates the Medium Access Control Layer (MAC) of the IEEE 802.16 Wireless standard and its utility in augmenting the IP (Internet Protocol) router based Automated Digital Network System (ADNS). This research explores the need for a high throughput, high speed network for use in a network centric wartime environment and how commercial off-the-shelf (COTS) technologies that take advantage of the IEEE 802.16 wireless protocol can satisfy these requirements. The intent of this research is to prove that IEEE 802.16 systems can provide the ADNS with a viable alternative in order to enhance its capabilities and mitigate its limitations.

This research includes a discussion on the current configuration of the ADNS architecture and its uses in the Carrier Strike Group (CSG). This research also analyzes the IEEE 802.16 MAC layer and identifies and tests its unique quality attributes that make it a viable high speed, high throughput communication link for point-to-point and point-to-multipoint naval applications.

14. SUBJECT TERMS IEEE 802.16, WiMax, Wireless, Network, ADNS, COTS, MAC, Intra-strike Group Communications, Packet Switched Data	**15. NUMBER OF PAGES** 85
	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

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

A STUDY OF THE IEEE 802.16 MAC LAYER AND ITS UTILITY IN AUGMENTING THE ADNS ARCHITECTURE TO PROVIDE ADAPTABLE INTRA-STRIKE GROUP HIGH-SPEED PACKET SWITCHED DATA, IMAGERY, AND VOICE COMMUNICATIONS.

Ballard V Johnson
Lieutenant, United States Navy Reserve
B.S., Georgia Institute of Technology, 2001

Jameau R Pryor
Lieutenant Commander, United States Navy
B.S., Southern University and A&M College, 1994

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN
INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL
September 2005**

Authors: Ballard V Johnson

Jameau R Pryor

Approved by: Rex Buddenberg
Thesis Co-Advisor

John Gibson
Thesis Co-Advisor

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research evaluates the Medium Access Control Layer (MAC) of the IEEE 802.16 wireless standard and its utility in augmenting the IP (Internet Protocol) router based Automated Digital Network System (ADNS). This research explores the need for a high-throughput, high-speed network for use in a network centric wartime environment and how commercial off-the-shelf (COTS) technologies that take advantage of the IEEE 802.16 wireless protocol can satisfy these requirements. The intent of this research is to prove that IEEE 802.16 systems can provide the ADNS with a viable alternative in order to enhance its capabilities and mitigate its limitations.

This research includes a discussion on the current configuration of the ADNS architecture and its uses in the Carrier Strike Group (ESG). This research also analyzes the IEEE 802.16 MAC layer and identifies and tests its unique quality attributes that make it a viable high-speed, high-throughput communication link for point-to-point and point-to-multipoint naval applications.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS AND ACRONYMS

ADNS	Automated Digital Network System
AK	Authorization Key
ARQ	Automatic Repeat Request
ATM	Asynchronous Transfer Mode
BE	Best Effort
BR	Bandwidth Request
BS	Base Station
BW	Bandwidth
C2	Command and Control
CDMA	Code Division Multiple Access
CEC	Cooperative Engagement Capability
CID	Connection Identifier
CINGARS	Channel Ground and Airborne Radio System
CJCS	Chairman Joint Chief Staff
CODEC	Coder-Decoder
COTS	Commercial Off the Shelf
CPLT	Complete
CRC	Cyclic Redundancy Check
CS	Convergence Sublayer
CSG	Carrier Strike Group
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DNS	Domain Name Server
DOD	Department of Defense
DONCIO	Department of the Navy, Chief Information Officer
DSA	Dynamic Service Addition
DSC	Dynamic Service Change
DSCH	Distributed Scheduling
DSCP	Differential Services Code Point
DSD	Dynamic Service Deletion
DWTS	Digital Wideband Transmission System
EHF	Extremely High Frequency
FTP	File Transfer Protocol
GIG	Global Information Grid
GRC	Ground Radio Communications
HDC	Helicopter Direction Center
HF	High Frequency
HTTP	Hypertext Transfer Protocol
ID	Identification
IEEE	Institute of Electrical and Electronic Engineers
IM	Information Management

IP	Internet Protocol
IT	Information Technology
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
LLC	Logical Link Control
LPI	Low Probability of Intercept
LPD	Low Probability of Detection
LOS	Line-of-Sight
LSB	Least Significant Bit
MAC	Medium Access Control Layer
MAGTAF	Marine Air-ground Task Force
MAN	Metropolitan Area Network
MAP	Map
Mbps	Megabit per second
MHz	Megahertz
MOS	Mean Opinion Score
MPEG	Moving Pictures Expert Group
MSB	Most Significant Bit
MSH	Mesh
NLOS	Non-Line-of-Sight
NNTP	Network News Transfer Protocol
nrtPS	Non-Real-Time Polling Service
NWC	Network Centric Warfare
OFDM	Orthogonal Frequency Division Multiplexing
OS	Operating System
OSI	Open System Interconnection
P2P	Peer-to-peer
PDU	Protocol Data Unit
PHY	Physical Layer
PKI	Public Key Infrastructure
PM	Poll-Me Bit
PMP	Point-to-Multipoint
POP3	Post Office Protocol Version 3
PtP	Point-to-Point
QAM	Quadrature Amplitude Mode
QoS	Quality of Service
REG	Registration
REQ	Request
RF	Radio Frequency
RNG	Ranging
RSP	Response
rtPS	Real-Time Polling Service
s	Seconds
SA	Security Association
SBC	Subscriber Station Basic Capability

SDU	Service Data Unit
SF	Service Flow
SFID	Service Flow Identifier
SMTP	Simple Mail Transfer Protocol
SS	Subscriber Station
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
TFTP	Trivial File Transfer Protocol
TEK	Traffic Encryption Key
UCD	Uplink Channel Descriptor
UDP	User Datagram Protocol
UGS	Unsolicited Grant Service
UL	Uplink
VoIP	Voice Over Internet Protocol
VRC	Vehicle Mounted Radio Communications
VTC	Video Teleconference
WAN	Wide Area Network
WSC	Waterborne Special Communications
WiFi	Wireless Fidelity
WiMAX	Wireless Interoperability for Microwave Access
WirelessMAN	Wireless Metropolitan Area Networks

ACKNOWLEDGMENTS

We would like to thank Rex Buddenberg and John Gibson specifically for their tremendous support and guidance throughout this process. We would also like to extend our appreciation to the Science Applications International Corporation (SAIC) ADNS laboratory personnel, specifically Yau Keung Hom, Cal Goodrich, Ed Hucke and Sean Vuong for their ADNS equipment support and advice.

Jameau would like to thank God, his parents, Laordice Pryor and James Pryor Jr., his wife, Tiffany, and his kids Britton, Gabriel and Caleb for their constant support and understanding during the research and development of this thesis.

I. INTRODUCTION

A. CARRIER STRIKE GROUP (CSG) COMPOSITION

A CSG consists of an array of ships with varying capability and the ability to support and or defend the Aircraft Carrier. Various types of communications needs exist among the units in each strike group. The basic composition of the group are one (CV/CVN) aircraft carrier, one or more (CG) Aegis class cruisers, one or more (DDG) Spruance/Arleigh Burke class destroyers, one (FFG) Perry class frigate, and one or more (SSN) Los Angeles class submarines. The carrier is typically placed within layers of defense. Each ship has a specific defense capability and is arranged in order to provide the most logical protection for the strike group. An Aegis cruiser is normally in charge of the anti-air activities of the group, a destroyer (DD/DDG) is typically in charge of the undersea and surface warfare activities, and a frigate is in charge of the undersea warfare. An attack submarine may or may not be attached to the group, depending upon the tasked mission. When one is attached, it is typically in charge of the anti-submarine and anti-surface warfare. Finally, the group is accompanied by a support ship, usually an (AOE) Supply class ship.

Each of the various mission roles has its command and control (C2) support requirements that demand effective and efficient communications. The number of different stovepipe systems necessary for the proper function of each of these ships is staggering. However, they do have one characteristic in common: The data transmitted by the different systems can be encapsulated and transferred via TCP/IP.

B. COMMON CSG COMMUNICATIONS SYSTEMS AND DATA TYPES

Due to a lack of actual information, a few assumptions must be made about the requirements of the basic systems that are necessary for a CSG to operate effectively. The current high frequency (HF) systems and their assumed data types are as follows:

- Bridge to Bridge radio, providing ship-to-ship voice,
- Ground Radio Communications (GRC-211) radio transceiver, providing voice and data,
- the GRC-171 radio group, voice and data

- Link 4A/11 data and voice, data
- Vehicle Mounted Radio Communications (VRC-90) radio group Single Channel Ground and Airborne Radio System (SINCGARS), voice and data
- Waterborne Special Communications (WSC-3) Line-of-sight (LOS) radio for voice/teletype/digital data,
- Prifly/Helicopter Direction Center (HDC) radio, data,
- Digital Wideband Transmission System (DWTS), digital voice/data/imagery, and
- Cooperative Engagement Capability (CEC), data.

C. DEPARTMENT OF DEFENSE (DOD) DESIRED END STATE

1. DOD Transformation to Network Centric Warfare (NCW) Operations

A Network Centric operation is what the DOD is attempting to attain via a total organizational transformation. A network centric operation is defined as an environment in which information superiority is enabled and combat power is increased by connecting or networking sensors, shooters and decision makers in an effort to achieve shared awareness. The key features that the DOD is seeking are to tag data, make data available, visible and useable via posting, and enabling of many-to-many exchanges amongst network users. The idea to transform to Network Centric organization was initiated by the observance of the commercial sector’s ability to develop and leverage information superiority and translate it into an advantage by shifting to Network Centric operations. The commercial sector’s success has been enabled by the exploitation of new technology and the decision to restructure their organizations and processes to provide more value to the customer.

The DOD is interested in following suit, just in a different arena and with different customers. The arena is the battlespace and the customers/users are the war fighters. In light of the DODs transformation endeavor to a Network Centric organization, the addition of the IEEE 802.16 system to the CSG is another avenue to take advantage of current technology to assist in developing and leveraging information superiority. The addition of the IEEE 802.16 base station (BS) and subscriber stations

(SS) to the Automatic Digital Network System (ADNS) will open a broadband pipe available to the carrier strike group to conduct intra-group communications and effectively reserve ADNS bandwidth for other, more distant entities, thereby creating more value for the war fighters by enhancing the ability to obtain more information simultaneously. This will generate more accurate, timely information, which in turn, will lead to better knowledge of the battlespace and situational awareness.

According to the Commander of the Joint Chiefs of Staff's (CJCS) Joint Vision 2020, the transformation of the joint force to reach full spectrum dominance rests upon information superiority as a key enabler and our capacity for innovation. Network connectivity promotes and supports mission accomplishment in Strike, Intelligence Surveillance and Reconnaissance (ISR), Force Protection, and Logistics. The development of a global information grid (GIG) will provide the network-centric environment required to achieve this goal. It will enhance combat power and contribute to the success of non-combat military operations.

D. TRANSFORMATION SUPPORT

IP connectivity and interoperability in a robust network that allows one to attain information superiority is the overarching goal. An example of the success and benefits of IP connectivity is the ADNS. The ADNS provides a standardized networking architecture using mobile ad-hoc networking between joint platforms on one autonomous system. Connectivity reaches users at useful data rates over a common radio frequency (RF) path to support tactical requirements. IP connectivity improves communication efficiency, increases data reliability, and brings information dominance to the battlefield. (From: Ref 23)

The Navy systems that would most likely benefit from the addition of the IEEE 802.16 system are the systems that are used for Intra-Strike Group communications, to include tactical, operational, and administrative data. They all reside in the high-frequency ranges and most are capable of LOS transmissions. Because each system has been developed to serve very specific purposes using custom forms of communications, few are compatible or interoperable. Most acquisition efforts created turnkey systems for each need as it was identified. The idea of establishing a common communications infrastructure to be shared by the various application domains was rarely considered.

This generated an enormous number of stand-alone, special purpose, or stovepipe, systems that further fragmented the Navy C2 infrastructure into isolated specialized systems and equipment. The one element that each system does have in common is the use of the HF range of the RF spectrum. Further, the Navy employs the use of telephone voice quality equipment with a bandwidth of approximately 64kbps, thereby imposing a physical limit on all of its systems, even if it is capable of a higher rate of data transmission.

These factors, in addition to the impact of running the gauntlet of research and development in the bureaucratic and military system lead to high development and maintenance costs and the introduction of systems that are obsolete by the time they became operational. In the fast-paced world of high technology, components that are more than two-years old, for the most part, are considered obsolete or out-dated. So, the question arises: Can the Navy significantly reduce development and maintenance costs and time used to develop and deploy systems by taking advantage of existing technology and using current off-the-shelf equipment that incorporates the wireless metropolitan area network (IEEE 802.16) standard? The authors of this thesis assert that incorporating COTS IEEE 802.16 compliant equipment into the ADNS architecture will provide a key component in response to this question.

As early as the mid-80's, the concept of interoperability has been identified as crucial to transforming a Network Centric DOD and is now a part of systems development, not just in the Navy, but in the DOD in general, as evidenced by the following quotes from the Department of the Navy Chief Information Officer (DONCIO) and Marine Corps leadership personnel.

> We will select IM/IT investments that improve combat capability, war fighting readiness and mission performance. These investments will be assessed, qualified and validated as part of the Department of the Navy's planning, programming budgeting and execution process and will permit us to extract the utmost from our scarce resources. (From: Ref 23)

> … leverage technologies that allow us to more effectively share and expedite the flow of useful information. The increase in situational awareness through integrated command and control systems and a

> common operating picture, both for peacetime functions and on the battlefield will dramatically increase our effectiveness and enhance the flexibility and responsiveness that are the signature characteristics of our Corps. (From: Ref 10)

In addition to the focus on connectivity and interoperability is the need for independent groups and forces to coordinate and act decisively and quickly to a wide range of possible scenarios that require intra-group and inter-group synchronization.

> The global concept of operations will dispense combat striking power by creating additional independent operational groups capable of responding simultaneously around the world. This increase in combat power is possible because technological advancements are dramatically transforming the capability of our ships, submarines and aircraft to act as power projections forces netted together for expanded war fighting effect. (From: Ref 9)

Nonetheless, interoperability has remained a very elusive goal. What is interoperability? According to *dictionary.com* it is “the ability to exchange and use information (usually in a large heterogeneous network made up of several local area networks).” (From: Ref 17) An Institute of Electrical and Electronics Engineers (IEEE) standards website defines it as, “The capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units. In short, ‘interoperability’ means communication/ execution/ data transfer without knowing the nature of the implementations (e.g., the endpoints of communication, the execution environment, data repositories, etc.)” (From: Ref 15) The Joint Pub 1-02, states that interoperability is the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together. According to the DOD, interoperability is the condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users.

Although the definition is straight-forward, the attainment is difficult, especially when so many legacy systems remain critical to mission accomplishment. Perhaps a first step to achieving interoperability is to approach it from a layered standpoint, similar to the development of network protocols, in order to make the problem manageable and scalable. One such approach would decouple the exchange of data from the generation, interpretation, and display of that data. Once the transfer or exchange of the data is considered in isolation from the other aspects of interoperability, it becomes clear that the most direct avenue to attaining interoperable data exchange is by using the well-demonstrated and understood IP standards and the design of an open-ended network that maintains or surpasses the current service available to each application through the tangle of CSG communications. Where reliable or timely data transfer is required TCP and the Real-Time protocol offer services above the data forwarding functionality of IP.

Fundamental to attaining interoperability is a sound architecture. The introduction of the ADNS system has provided the development of a sound architecture and facilitates interoperability by providing a means of standardizing data exchange through IP encapsulation. With the successful implementation of ADNS, the issue becomes one of enhancing the system to meet all of its demands more directly and efficiently.

E. ADNS

The ADNS is a system that uses adapt-from-Commercial-off-the-shelf (COTS) equipment and protocols, processors and Cisco routers approach to create a robust and flexible networking environment. Interfaces to all RF media from HF to extremely high frequency (EHF) provide access to the available communications links. ADNS provides the following capabilities:

- It is a routable network that provides Wide Area Network (WAN) access for multiple-security level networks.
- The system allows for IP connectivity among a diverse group of users.
- Bandwidth reservation per security level (enclave)
- Ship-to-ship LOS links with IP video teleconference (VTC) (DWTS)
- Ship-to-tactical shore Marine Air-Ground Task Force (MAGTF) support
- Pier-side network access
- Traffic distribution over multiple links
- Adjustable bandwidth guarantees
- Application prioritization

- Improved link monitoring tools
- Application monitoring.

ADNS is composed of the three functional elements: Integrated Network Management (INM), Routing and Switching (R&S) and Channel Access Protocol (CAP). INM uses adapt-from-COTS equipment and tactical (TAC-4) workstations to provide the flexibility to alter communications to match the current available equipment and mission priorities. The tasks of providing an interface and conducting routing and switching is handled by the R&S subsystem. R&S uses Cisco routers, a suite of routing protocols and the COTS Integrated Services Digital Network (ISDN) and Asynchronous Transfer Mode (ATM) switches to accomplish its functions. The CAP equipment coordinates the management of data. In addition, CAP monitors network quality of service (QoS) and reports loading and errors to the INM. (From: Ref 29)

The known limitations of the ADNS system are as follows:

- Ship's application priorities are fixed and cannot easily be changed.
- Only one of three different enclave bandwidth allocations can be selected.

The introduction of ADNS is a step in the right direction for Navy transformation to a net-centric service.

F. SUMMARY

The architecture and IP routing ability inherent in the ADNS system enable two important requirements of the transformation to Network Centric operations: a common medium and the ability to attach end systems to the network easily.

THIS PAGE INTENTIONALLY LEFT BLANK

II. INTENTION

A. COTS IEEE 802.16 WILL ENHANCE THE EFFECTIVENESS OF ADNS

The purpose of this study is to assess the effectiveness of augmenting the bandwidth available to systems for tactical use among the members of the CSG across a common, low-cost, adaptable medium. The goal is in accordance with the DONCIO vision and mission statements and enhances the creation of a joint network centric environment that fosters knowledge dominance for the Navy. The goal focuses on the network and transport layers of the Open System Interconnection (OSI) model to determine whether or not the different types of traffic can be encapsulated and routed across a wireless packet-switched network. In order to answer this question, we first need to identify the current systems and the characteristics of the output traffic generated by their components. Once these characteristics are determined, one can ascertain whether the output is suited for encapsulation. If the data can be encapsulated, then one can assume that they are indeed routable. Once the determination is made that the data traffic is routable, one can use COTS IEEE 802.16 equipment to test and assess whether the Media Access Control (MAC) layer of the IEEE 802.16 wireless protocol can provide similar or better quality of service (QOS), security and usability than is currently provided to the strike group platforms. In addition, any limitations encountered will be identified and analyzed. Where possible, the thesis will present potential solutions in order to mitigate the limitations that have been discovered. The intention is to create a highly robust information transfer system with the proper architecture that allows easy connectivity of components and can adapt to the ad hoc nature of CSGs. The addition of COTS IEEE 802.16 system will be compliant with the ship-borne interface of the ADNS architecture, including updated technology. ADNS provides a standardized networking architecture that enables the use of mobile ad-hoc networks between joint platforms on one autonomous network. What remains is to expand the link BW available through such means as the incorporation of the IEEE 802.16 compliant equipment. Due to the flexibility of the network architecture, connecting the wireless assets to the ADNS router interfaces easily creates a wireless Metropolitan Area Network (Wireless MAN). This implementation would assist in addressing the issue of last-mile interoperability at the tactical level.

B. COTS IEEE 802.16 DATA TRANSMISSION CAPABILITIES

It remains to be shown whether or not these traffic types can be collected, encapsulated, and transferred using COTS IEEE 802.16 equipment and then be unwrapped and presented to the intended application in the expected format. The advent of ADNS has shown that the various current data and information types can in fact be transmitted through a routable network effectively. The architecture of ADNS allows the connection of COTS IEEE 802.16 equipment. However, two issues remain to be considered: The allocation of the available bandwidth (BW) and the priority or order of different data when the bandwidth limit is reached. These issues go beyond the scope of this study and would be better addressed by the operations community.

C. COTS IEEE 802.16 BENEFITS

The introduction of the COTS IEEE 802.16 equipment to the ADNS architecture would allow the exploitation of the following:

- WiMax (IEEE 802.16) enables routable wireless networks (seamless interconnection to the internet) by virtue of the use of the 802.2 Logical Link Control (LLC);
- WiMax offers wireless broadband at data rates far in excess of those typically in use by the military today, and
- Large-scale manufacturing, technology advances and commercial adoption have lead to very low cost devices, when compared to military equivalents.

Equipment compliant with the IEEE 802.16 standard offers several advantages over the current stovepipe communications systems. Theoretically, it is possible to achieve shared data rates up to 75 Mbps in a single sector of the base stations using only 20 MHz of BW at a range of 30 miles. This is a much larger pipe (bandwidth) to work with in contrast to the small BW offered by current Navy equipment. This results in quicker dissemination of the critical data that is inherent of any tactical situation, and furthermore it allows near-real time reactions to orders and changes in the battlespace picture. COTS IEEE 802.16 compliant equipment is very flexible, able to handle and transmit different types of traffic. The only requirement is to encapsulate the data, after which it is routable to any host connected to the IP network. In addition, COTS IEEE

802.16 compliant equipment offers flexible channel BW that fosters scalability. For example, a subscriber at 20 MHz can divide the allocation into two 10MHz sectors or four 5MHz sectors. Further, increasing the power on more narrow sectors allows one to increase the number of users while maintaining range and considerable throughput. WiMAX also incorporates the use of dynamic adaptive modulation. It allows the base station to automatically trade throughput automatically for range by reducing the highest modulation scheme, 64 Quadrature Amplitude Modulation (64-QAM) to 16-QAM phase key shifting, thereby reducing throughput but increasing range. In addition, the IEEE 802.16 standard supports some of the newer initiatives, including mesh topology, a broadcast point-to-point mechanism, and the various smart antenna techniques that allow expansion of the coverage area.

The IEEE 802.16 standard also supports applications requiring low latency services, such as voice and video. This stipulation will greatly enhance the quickness and robustness of response options of the actors in the NCW environment.

Furthermore, the IEEE 802.16 standard allows rapid integration of emerging technology. Commercial systems are far outpacing the current capability of DOD systems, resulting in frustration for commanders. They are aware that such capabilities are available, yet they are not able to employ the IT equipment in a timely manner within existing program channels. The DOD will find that the commercial IEEE 802.16 is the most beneficial alternative because of the advantages and capabilities of the equipment available at mass-production costs scales.

Overall the potential enhancement in capability due to the introduction of COTS IEEE 802.16 systems would allow for a considerable increase in information power. Information power assists in achieving information superiority and information superiority may be translated into a very advantageous increase in combat power.

D. ADJUSTMENTS TO COTS IEEE 802.16

1. Transmission Modes

The intended use of the system with respect to the mode of transmission must be considered when planning the system deployment. Whether the transmission is directed to a particular user, a collection or group of users via multicast, or broadcast to the entire network population will determine the necessary protocol for the mode. In the case of multicasting or broadcasting the User Data Protocol (UDP) must be used. UDP is an alternate transfer protocol standard to the (TCP). It is a light-weight protocol in that it does not provide error recovery, or flow and congestion controls functions, as does TCP. Though the transfer mechanism of TCP is more robust than UDP, TCP is strictly a point-to-point protocol and supports neither broadcast nor multicast traffic. TCP only allows two hosts to establish a connection and exchange information. TCP guarantees that data received will be delivered to the target application in order and error-free.

2. Converting Equipment from Commercial to Military

In applying these COTS standards to the military domain the following issues must be considered:

- Range (distance) capability;
- WiMax uses a scheduling MAC, which provides stability and positive QoS control;
- Datalink layer security. WiMax added a security sub-layer Public Key Infrastructure (PKI), which provides security for the MAC messages and prevents denial of service, and theft of service type attacks, however it does not necessarily meet the NSA standard for sensitive data protection.
- Physical layer security. None of the commercial wireless standards provide this type of security, which is a firm requirement for the military domain (e.g. wireless fidelity (WiFi) uses spread-spectrum, which is good for jam-resistance but has a high probability of interception nor does it provide NSA-certified data protection). Requirements such as Low Probability of Intercept/Detection (LPI/D) and techniques including link cryptography could be “bolted onto” these standards by replacing/modifying the applicable layer or encapsulating the data prior to access to the link control, i.e., by robust IP encapsulation. This is possible because of adherence to the layered protocol model.
- Timing. Only applies to satellite systems in which the (physical) frame length is exceeded by the return trip propagation time.
- Multi-cast support.

These issues are beyond the scope of this research.

III. IEEE 802.16 MAC LAYER IDENTIFICATION AND ANLAYSIS

A. MAC LAYER INTRODUCTION

An IEEE 802.16 uses radio waves to propagate or transfer data providing support for two-way Point-to-Multipoint (PMP) and Mesh (MSH) topology. Because the network capacity is limited in bandwidth, the MAC layer of the protocol attempts to optimize the use of the valuable link resource by means of a scheduling algorithm. In the scheduling algorithm, the MAC provides a designated time as specified by the uplink map (UL-MAP) message in which each subscriber station (SS) takes its turn in uploading information to the base station (BS). Information can then be either sent to an entity to request further information from a source outside the network, or it can be broadcast to the designated SSs during the time assigned by the downlink map (DL-MAP) message allocated by the BS. The MAC is connection-oriented, meaning that it designates a connection for each service flow (SF), allowing it to assign an amount of BW needed for transmission of the service. The SFs, identified by their Connection Identifier (CID), provide a method for uplink (UL) and downlink (DL) management for the BS and the SS. Each CID has an associated set of QoS parameters. In accordance with the QoS parameters associated with the CID, the BS grants BW allocation for uplink to the SS on a per connection basis. Downlink is broadcast from the BS. A SS must request service flows from the BS and can terminate SFs.

B. PROTOCOL DATA UNIT (PDU) CREATION

The MAC PDU is a data unit that is transferred among peer entities or between different sub-layers of the MAC protocol. The MAC Service Data Unit (SDU) is a data unit that is transferred between adjacent layers of the MAC protocol. The PDU is created with a fixed-length generic MAC header, followed by the payload, as illustrated in Figure 1. The optional, variable length payload field allows the MAC PDU to carry messages of a higher-layer traffic type without knowledge of its contents.

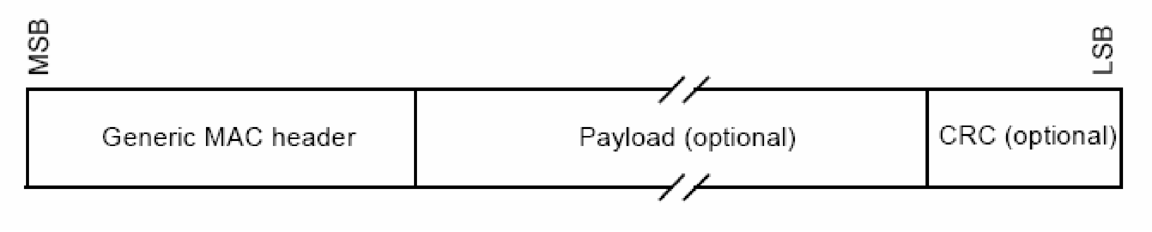


Figure 1. MAC PDU Format (From: Ref 16)

To conserve valuable air-link resources, the MAC may fragment SDUs to fit into an air-link allocation or may pack smaller SDUs into a larger PDU to fill an air-link allocation. Below, Figure 2 shows the PDUs and SDUs in the protocol stack:

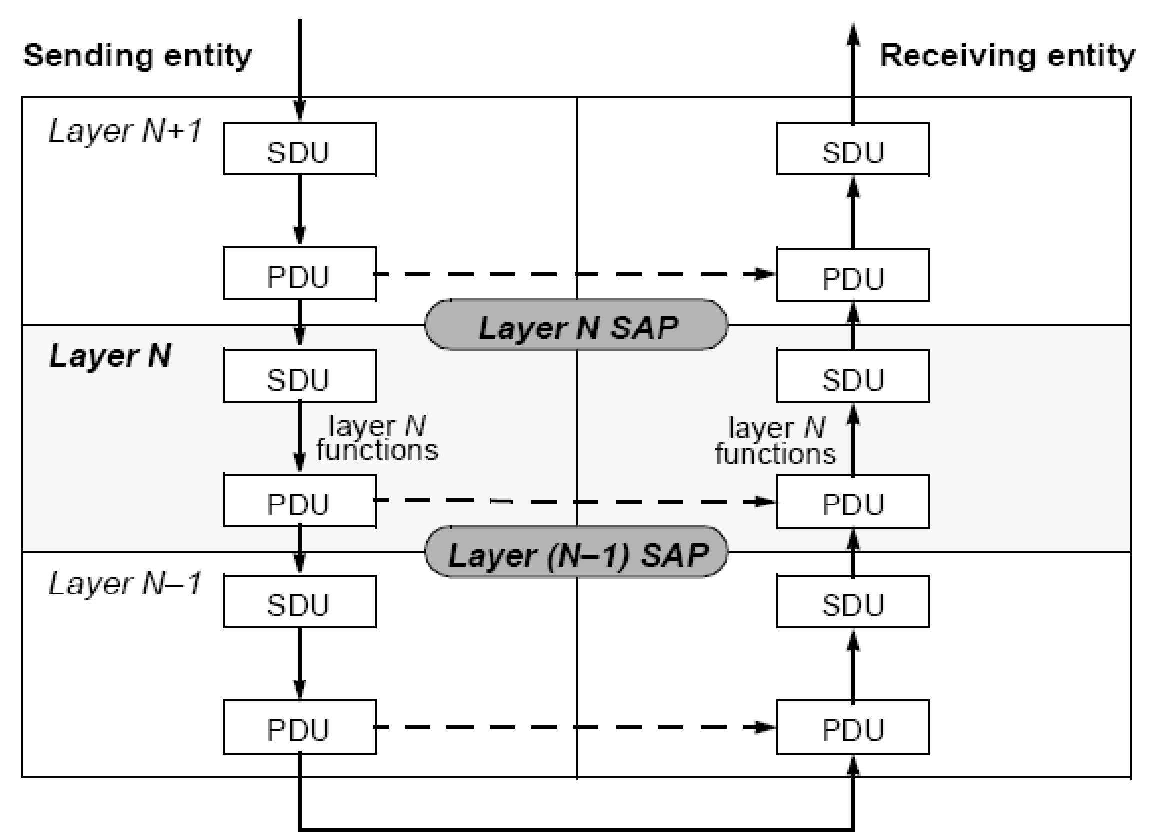


Figure 2. PDU and SDU in Protocol Stack (From: Ref 16)

1. MAC Header Types

Two MAC header types are used in the IEEE 802.16 protocol: The generic MAC header and the BW request header. The generic MAC header is used to begin PDUs that contain either MAC management messages or convergence sub-layer (CS) data. The MAC PDUs may also contain amplifying information about its associated unique service in one of the five subheaders: Mesh, Fragmentation, FAST-FEEDBACK_Allocation, and Grant Management. The BW request header is used to request additional BW and does not contain a payload.

2. MAC Management Messages

The MAC management messages are the primary means of communication and control between the BS and the SSs. These messages are separated into broadcast, initial ranging, primary management and basic connection types. The MAC management messages are listed in Appendix A.

3. Encryption of MAC PDUs

A PDU may be encrypted if the connection being used is established with a security association (SA). An SA is a set of security information that the BS and the SS share in order to support secure communications. If the PDU is to be encrypted, then the sender will perform encryption and data authentication of the payload only, as illustrated in Figure 3. The receiver will in turn perform decryption and data authentication.

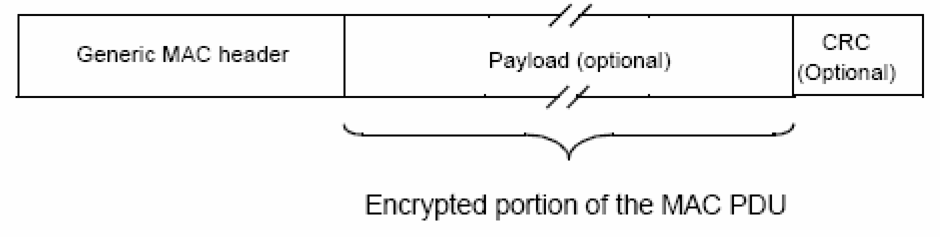


Figure 3. MAC PDU Encryption (From: Ref 16)

4. Error Control

Error control may be accomplished by optionally using either a Cyclic Redundancy Check (CRC) or enabling the Automatic Repeat Request (ARQ) mechanism. The CRC is a hash function used to produce a checksum in order to detect errors in the transmission of the packets. The CRC is appended to the payload of the MAC PDU. The ARQ mechanism, when enabled on a per connection basis, automatically requests retransmission of the packets in which it detects an error.

C. NETWORK ENTRY

Each SS station must follow a strict policy in order to join an IEEE 802.16 wireless network. The procedure for the SS to join the network is shown in Figure 4.

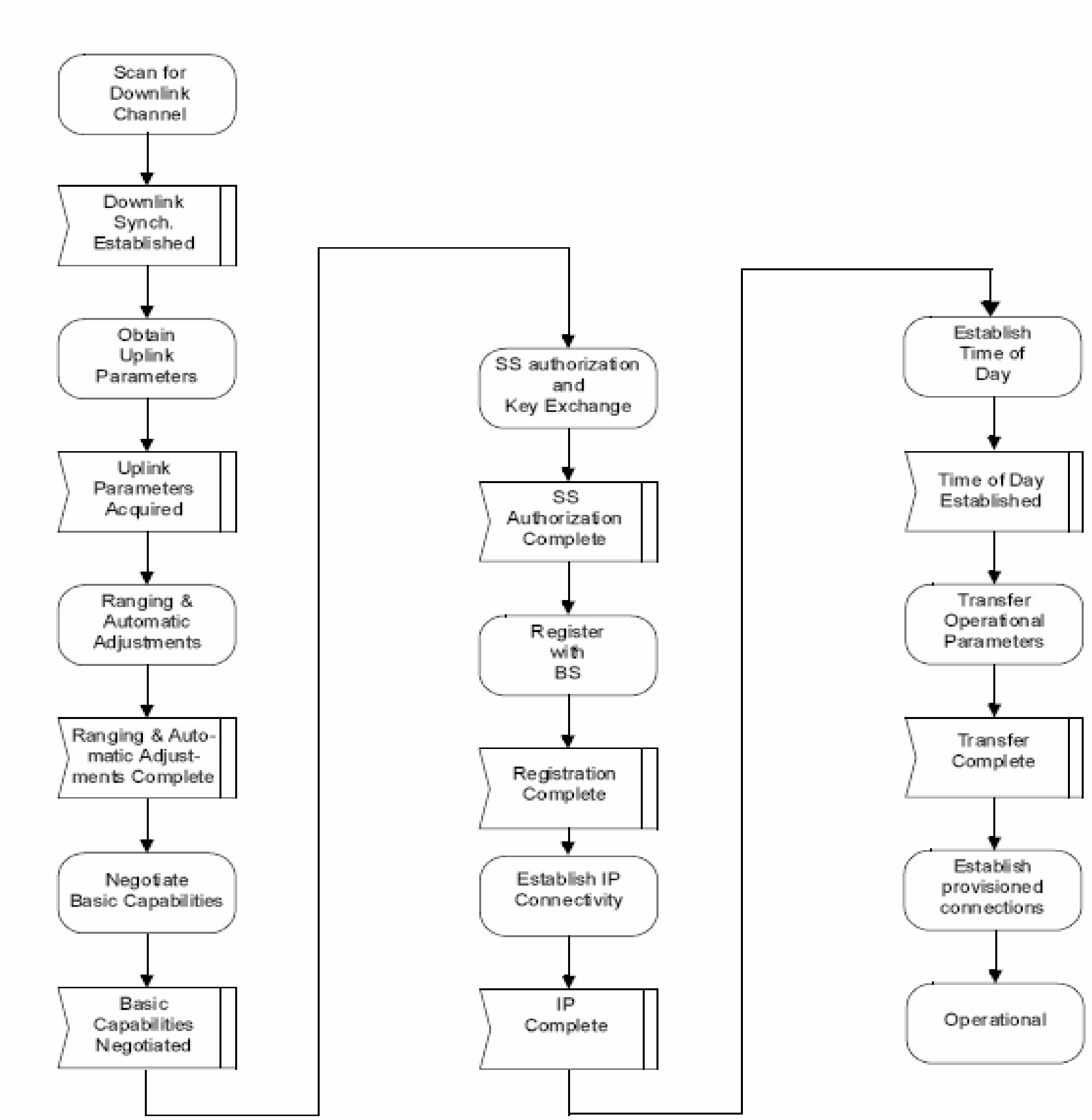


Figure 4. SS Initialization Overview (From: Ref 16)

1. Scan for DL Channel and Establish Synchronization with the BS

The SS checks to see if the operational parameters are stored to reacquire the DL channel. This operation is performed to identify whether or not the SS was previously online and had experienced a signal loss. If no operational parameters are detected, the

SS scans the possible channels of the DL frequency band of operation in order to acquire a valid DL channel. The SS then synchronizes its physical (PHY) layer parameters with the BS's PHY layer parameters. After the PHY layer synchronization, the SS will acquire channel-control parameters for the DL and then the UL. The SS then attempts to achieve MAC synchronization with the BS by obtaining the DL parameters via the DL-MAP management messages. The SS achieves MAC synchronization when it has received at least one DL-MAP message.

2. Obtain Transmit Parameters

The transmit parameters are obtained in order to establish an UL window in which the SS can transmit information to the BS. The BS sends an Uplink Channel Descriptor (UCD) message to the SS containing the UL parameters. After receiving the UCD message, the SS evaluates the channel description parameters in order to ensure that the UL parameters are suitable for use. Assuming that the parameters are suitable, the SS extracts the UL parameters for use. The SS then extracts the time synchronization from the next DL-MAP message so that both the BS and SS are coordinated in their efforts to transmit information. After the SS has synchronized its system clock to that of the BS, the SS waits for the BW allocation map from the BS. This map provides the scheduling as to when the SS can send messages to the BS. After receiving the BW allocation map, the SS can then transmit in accordance with the MAC operation and the BW allocation mechanism.

3. Perform Initial Ranging

Ranging is the process of acquiring the correct timing offset and power adjustments needed for the SS to transmit and to receive information to and from the BS. The SS synchronizes to the DL and learns the UL channel characteristics through the UCD MAC management messages. After synchronization, the SS will scan the UL-MAP message to find the initial ranging interval. The SS then composes a Ranging Request (RNG-REQ) message to be sent in the initial ranging interval as if it were collocated with the BS. The SS then resends this message iteratively with increasing power until it receives a response containing its MAC address. After the response is received, the SS calculates the maximum signal strength. This signal strength is the power from the successful transmission of the last message.

4. Negotiate Basic Capabilities

After initial ranging is performed, the SS sends a SBC-REQ message to the BS to inform it of the SS's basic capabilities, which are necessary for effective communication. The SS includes the physical parameters supported by the SS and the properties of the SS needed for the BW allocation purposes. If the BS can support the basic capabilities necessary for the SS, the BS replies with a Subscriber Basic Capabilities Response (SBC-RSP) message.

5. Authorize SS and Perform Key Exchange

The BS then performs an authorization and key exchange with the SS. The details of this procedure are beyond the scope of this thesis.

6. Perform Registration

The SS then sends a Registration Request (REG-REQ) message to the BS to begin the process of registration, which allows the SS entry into the network. The REG-REQ message contains the following parameters: IP version, SS capabilities encodings, vendor Identification (ID) encodings, vendor specific information, CS capabilities, and ARQ parameters. The BS responds by sending a Registration Response (REG-RSP) message that assigns the SS a secondary management CID, thus allowing the SS to become manageable.

7. Establish IP Connectivity

After registration is completed, the SS obtains an IP address by invoking Dynamic Host Configuration Protocol (DHCP) mechanisms. The DHCP mechanism automatically assigns an IP address to the SS while the SS is configured to use the network.

8. Establish Time of Day

The SS's secondary management connection will request the time of day, via User Datagram Protocol (UDP). The BS then responds, also via UDP, with the time of day, unauthenticated and accurate only to the nearest second. The time of day is required for time-stamped logged events that the management system must retrieve.

9. Transfer Operational Parameters

After the DHCP is completed, the SS downloads the SS configuration file using the Trivial File Transfer Protocol (TFTP). The SS configuration file contains the software upgrade filename configuration setting, software server IP address, authorization node IP address, registration node IP address, provisioning node IP address, and the vendor-specific configuration settings. Once the configuration file has been successfully downloaded, the SS sends a TFTP Complete (TFTP-CPLT) message.

10. Set-Up Connections

The SS is now on the network, and the BS sends a Dynamic Service Addition Request (DSA-REQ) message to the SS for pre-provisioned SFs that belong to the SS. The SS responds with a Dynamic Service Addition Response (DSA-RSP) message confirming the SF. The SS sends a DSA-REQ to the BS in order to request more SFs.

11. Contention Resolution

During initial ranging and request intervals, collision can occur between two or more SS that are attempting to enter the network. If a collision does occur, the standard contention resolution used is a truncated binary-exponential back off.

D. SERVICE FLOWS

The IEEE 802.16 protocol specifies scheduling services for data transport on a per connection basis. These connections are assigned a CID and are then scheduled for transmission depending on the amount of resources available and the necessary QoS parameters.

1. Quality of Service (QoS)

Each connection has only one data service that is defined by a set of QoS parameters. The QoS is guaranteed by the transmission ordering and scheduling on the air interface for each service flow according to its respective QoS parameters for that connection, as defined by its CID. There are four QoS services: Unsolicited Grant Service (UGS), Real-time Polling Service (rtPS), Non-real-time Polling Service (nrtPS), and Best Effort (BE).

a. Unsolicited Grant Service (UGS)

The UGS is designed to support real-time service flows that have a constant bit rate, such as voice over internet protocol (VoIP) and VTC services. This is accomplished by generating fixed-time allocations for the use of the bandwidth on a periodic basis, thus eliminating the overhead and latency needed for a SS to request the bandwidth from the BS.

b. Real-time Polling Service (rtPS)

The rtPS is designed to support real-time services that periodically send variable-length data packets such as moving pictures expert group (MPEG) video. In rtPS, the BS polls the SS for the amount of BW that the SS needs to transmit its data to provide for optimum data transport efficiency.

c. Non-real-time Polling Service (nrtPS)

The nrtPS is designed to support non-real-time services that send variable length data packets such as Joint Photographic Expert Group (JPEG) files. In nrtPS, the BS polls the SS on a regular basis, usually on an interval of one second or less.

d. Best Effort Service (BES)

The BES service is designed to provide efficient service for traffic whose packets do not need to be received in a specific order, such as web traffic. In BE, the SS uses contention request opportunities to request BW allocation.

2. Bandwidth Allocation and Request Mechanisms

When a connection is established between a BS and an SS, the SF is assigned a CID. This CID has an associated set of QoS parameters. For connections using UGS the bandwidth allocation does not change, but for the other QoS types, the SS must request bandwidth according to how many resources are needed for their respective transmission. The SS is allocated resources through requests, grants, and polling, as shown in Figure 5.

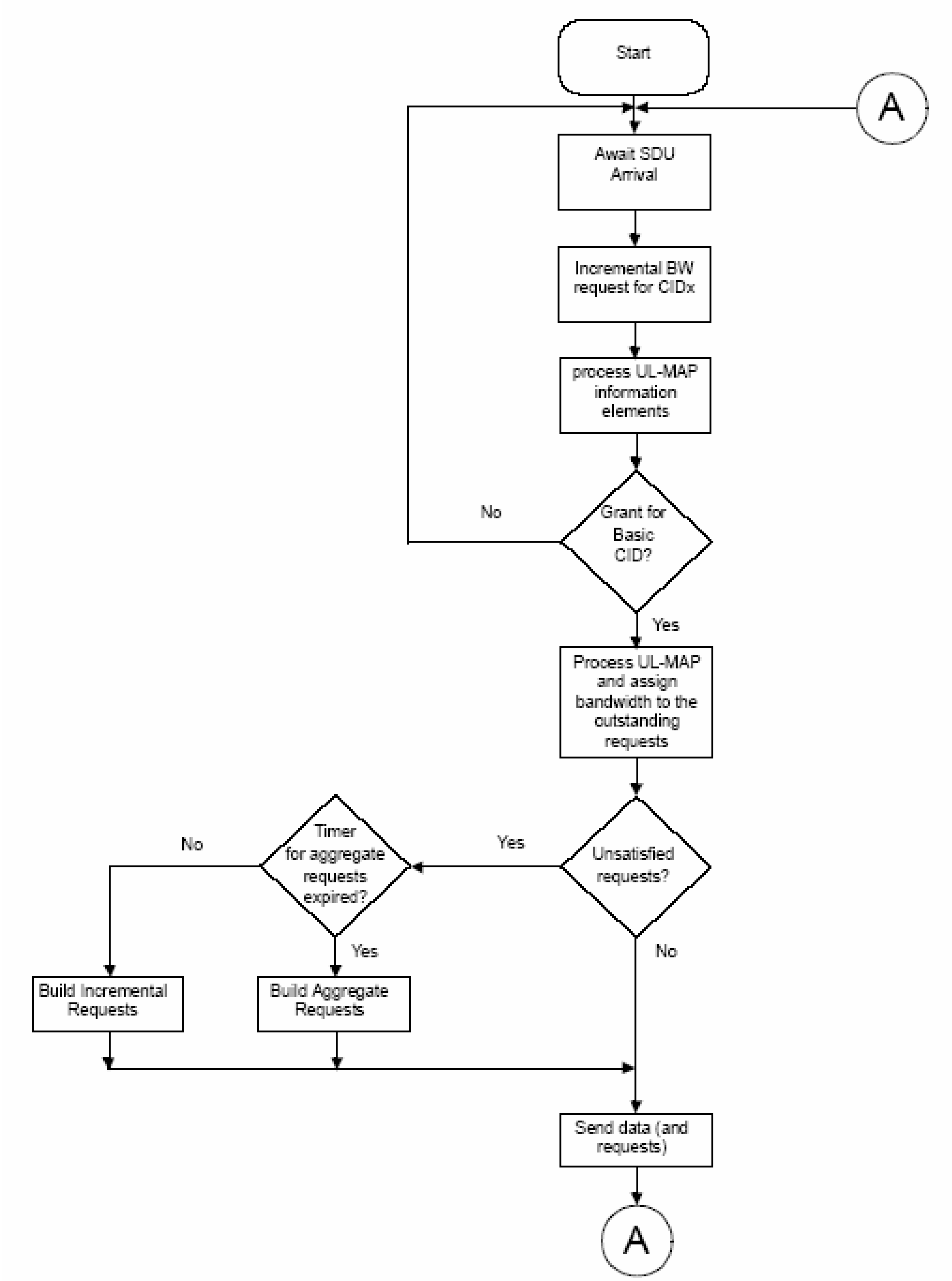


Figure 5. SS Request/Grant Flow Chart (From: Ref 16)

a. Requests

In order for a SS to tell the BS that it needs an UL BW allocation, the SS must submit a request. The SS station transmits its request during any UL allocation and makes its request in terms of the number of bytes required to carry the MAC header and payload.

b. Grants

After a SS requests an allocation from the BS, the BS grants the SS an amount of the BW depending on the connection's associated QoS parameters and the amount of resources available for the transmission. The SS can then transmit its information for the connection in its allocated grant. If a grant provides a shorter transmission opportunity than needed, the SS can either discard the SDU or perform back-off and request again.

c. Polling

The BS allocates BW to the SSs for the purpose of effectively managing BW utilization. This process is known as polling. The BW can be allocated to an individual SS or to a group of SSs. In unicast polling, the SS is polled individually by the BS. The BS provides an allocation for the SS to request BW in the UL-MAP, and if BW is required by an SS, the SS sends a BW request during this time. To save BW, the BS may initiate multicast or broadcast polling in which a group of SSs are polled. In this process, the BS provides an UL allocation for a group of SSs to request BW at the same time. Only SSs that need BW reply. In the event of a collision, the standard contention resolution that is used is truncated binary exponential back off.

E. COMPARISON OF IEEE 802.16 AND 802.11

1. Scalability

In IEEE 802.11 technologies, medium access is granted using a contention-based medium access control system. This system causes a geometric reduction in the efficiency of the BW, thus reducing the throughput, as more users are added. In contrast, the IEEE 802.16 MAC layer is designed to support hundreds of users in one RF channel due to its scheduling based access algorithm.

2. Coverage

The IEEE 802.11 standard uses a Code Division Multiple Access (CDMA) multiplexing technique that has the requirement of low-power consumption. Due to this requirement, IEEE 802.11 systems can cover approximately a few hundred meters. The IEEE 802.16 systems were designed for higher power and use an Orthogonal Frequency-Division Multiplexing (OFDM) technique. This scheme allows for optimal performance in all types of propagation environments, including LOS and NLOS environments, and an increased range to tens of kilometers.

3. Quality of Service

The IEEE 802.16 MAC layer assures collision-free data access, thus increasing BW efficiency and throughput, through the use of its Grant/Request protocol for access to its medium. By assigning QoS parameters to the grants that were requested, IEEE 802.16 systems can support differentiated service levels and assures a bound on delay. On the contrary, an IEEE 802.11 system with its contention-based medium access system cannot deliver the QoS of an IEEE 802.16 system.

F. SUMMARY

The IEEE 802.16 standard employs a scheduling algorithm to grant access to the medium, thus allowing for such quality attributes as scalability, increased coverage, and QoS. These qualities make an IEEE 802.16 system a natural fit for use in delivering data, video, and voice in order to augment the ADNS.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TESTING

A. INTRODUCTION

The purpose of this chapter is to determine whether or not IEEE 802.16 COTS equipment can be used to provide a high-speed, high-throughput wireless link from pier-to-ship and ship-to-ship configurations in order to augment the ADNS system.

B. OBJECTIVES

The objectives for the tests were outlined as follows:

- Report on the effectiveness of IEEE 802.16 for Naval applications
    - Ship-to-Ship while at sea
    - Ship-to-Pier Point-to-Point (PtP) application
    - Pier-to-Ship Point-to-Multipoint (PMP) application
- Effectiveness for ADNS
    - Efficacy as a WAN
    - Deployment topology options (PMP or mesh)
    - QoS capabilities
- Usability and training issues for deployment
    - WAN characteristics
    - Interface options (Ethernet, serial, other)
    - Throughput and response time.

C. METHODOLOGY

The authors went to the ADNS Point Loma testing facility in San Diego, California, to set up a network simulation augmented with IEEE 802.16 COTS equipment that would be typical of that used with the ADNS system. The networks were set up in a testing facility, so no ships were used. All of the equipment was housed in the testing facility, except for the antennas for the wireless connections.

1. Equipment

a. Computers

Multiple laptop computers were used to simulate the nodes and generate IP traffic at the ends of the network. The main characteristics of each computer are shown in Table 1.

Computer	Purpose	Operating System	Speed	Memory
Averatec	Console	MS Windows XP	1.66 GHz	512 MB DDR
Panasonic Toughbook	Endpoint	Windows NT 2000	1.66 GHz	512 MB DDR
Panasonic Toughbook	Endpoint	Windows NT 2000	1.66 GHz	512 MB DDR
Apple G4 Powerbook	Endpoint	Mac OS X Tiger	1.5 GHz	512 MB DDR

Table 1. Computer Characteristics

b. Ethernet Switch

A 3Com switch was used to allow the computer running the console application of the IxChariot tool to talk to the computer that generated the IP traffic. This was necessary so that the computer that generated IP traffic did not also have to use valuable resources collecting and analyzing the received data, thus providing a more accurate result. The main characteristics of the 3Com switch are shown in Table 2.

Make	3Com
Model	4226T
Ports	24 Auto-sensing 10BASE-T/100BASE-TX, two 10BASE-T/100BASE-TX/1000BASE-T
Media Interfaces	RJ-45
Ethernet Switching Features	Full-rate non-blocking on all Ethernet ports, full/half-duplex auto negotiation and flow control, multicast Layer 2 filtering, 802.1 Q VLAN support, 802.1p traffic prioritization, IGMP snooping

Table 2. Ethernet Switch Specifications (After: Ref 1)

c. Routers

The ADNS system uses COTS Cisco 3620 and 3640 routers; therefore, these routers were used in the simulation of the ADNS system. The 3640 router is used on the shipside of the topology and the 3620 router is used on the pier side of the topology. The main characteristics of the 3620 and 3640 routers are shown in Table 3.

Router	3620	3640
Purpose	Shore	Ship
Processor Type	80 MHz IDT R4700 RISC	100 MHz IDT R4700 RISC
Flash Memory	16 MB	16 MB
System Memory	32 MB DRAM	32 MB DRAM
Network Module Slots	Two Slots	Four Slots
Performance	20-40 kpps	50-70 kpps

Table 3. Router Specifications (After: Ref 11)

d. Antennas

An omni-directional antenna was used for the BS, and directional antennas were used for the two SSs. The BS's antenna was set up on top of the testing facility, and the two SS's antennas were set up approximately 15 meters from the BS's antenna. The main characteristics of the antennas are shown in Table 4.

Antenna	Omni-directional
Model	HyperGain HG5808U
Frequency	5725-5280 MHz
Gain	8 dBi
Horizontal Beam Width	360 DEG
Vertical Beam Width	16 DEG
Impedance	50 Ohm
Maximum Input Power	100 Watts
VSWR	< 1.5:1 avg
Connector	N Female

Table 4. Antenna Specifications (After: Ref 29)

e. IEEE 802.16 Equipment

Redline Communications' AN50e equipment was used for the BS and the SSs. The AN50e system is pre-standard equipment that closely resembles the IEEE 802.16 protocol. The main characteristics are shown in Table 5, and the complete system specifications are shown in Appendix A.

System Capability	LOS, Optical-LOS, and non-LOS (OFDM)
RF Band	5.470-5.850 GHz, TDD
Channel Size	20 MHz (5 MHz steps)
Data Rate	Up to 49 Mbps avg Ethernet rate
Max TX Power	20 dBm (region specific)
Rx Sensitivity	-86 dBm @ 6 Mbps (BER of 1x10e-9)
IF Cable	Up to 228 m (750 ft)
Network Attributes	Transparent bridge, automatic link distance ranging, 802.3x, 802.1p, DHCP pass-through, 802.1Q VLAN, encryption
Modulation	BPSK to 64 QAM (bidirectional dynamic adaptive)
Dynamic Channel Control	DFS, ATPC
MAC	PTP, PMP, concatenation/fragmentation, ARQ
Range	Beyond 80 km (50 mi) LOS @ 48 dBm EIRP
Network Connection	10/100 Ethernet (RJ-45)
System Configuration	HTTP Interface, SNMP, CLI, console (RS-232)
Network Management	SNMP: standard/proprietary MIBs
Power	110-240 VAC 50/60 Hz, 18-72 VDC, dual

Table 5. Redline AN50e Characteristics (After: Ref 3)

f. IxChariot

IxChariot is a software program that performs traffic-pattern analysis by emulating real-world application data. The IxChariot system consists of application scripts, a console, and endpoints (EPs). Application scripts tell the EPs to make the same calls to the network protocol stacks and produce the same load on the stacks as the applications they are designed to imitate. The console tells the EPs how to emulate a particular application by sending them an application script and other test setup information. The EPs are lightweight software agents that are installed on client and server computers that collect information about network transactions and send this information back to the console for analysis and reporting.

2. Tests

In all the tests, an ad hoc network was set up and tested to act as a control. Then the ADNS routers were added, and the networks were retested, and the results were compared. The networks were tested with the IxChariot test tool.

a. Ship-to-Ship

In accordance with Figure 6, one laptop running the console application and one laptop generating the IP traffic were connected to the 3Com switch, which was then connected to a Redline IEEE 802.16 transceiver configured as the BS unit. Another laptop running the EP program was connected to a Redline IEEE 802.16 transceiver configured as a SS and connected to the BS via wireless link. This topology was used as the control for the Ship-to-Ship configuration.

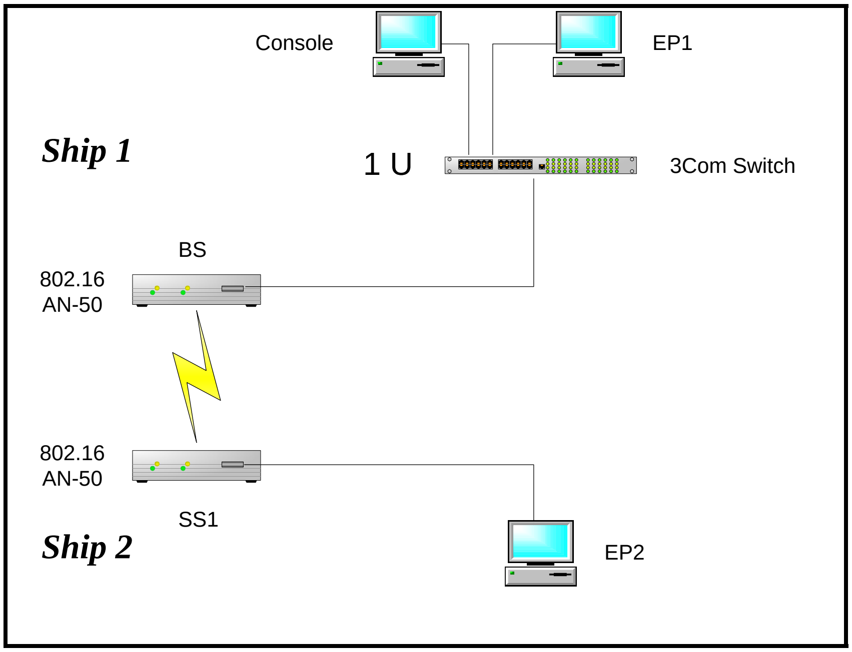


Figure 6. Ship-to-Ship Control Network Diagram

As illustrated in Figure 7, one laptop running the console application and one laptop generating the IP traffic were connected to the 3Com switch, which was then connected to a Cisco 3640 router. The router was then connected to a Redline IEEE 802.16 transceiver configured as the BS unit. Another laptop running the EP program was connected to another Cisco 3640 router, and the router was connected to a Redline IEEE 802.16 transceiver configured as a SS. The SS was connected to the BS via a wireless link. This topology was used as the simulation for the Ship-to-Ship configuration of the ADNS system augmented with IEEE 802.16 COTS equipment.

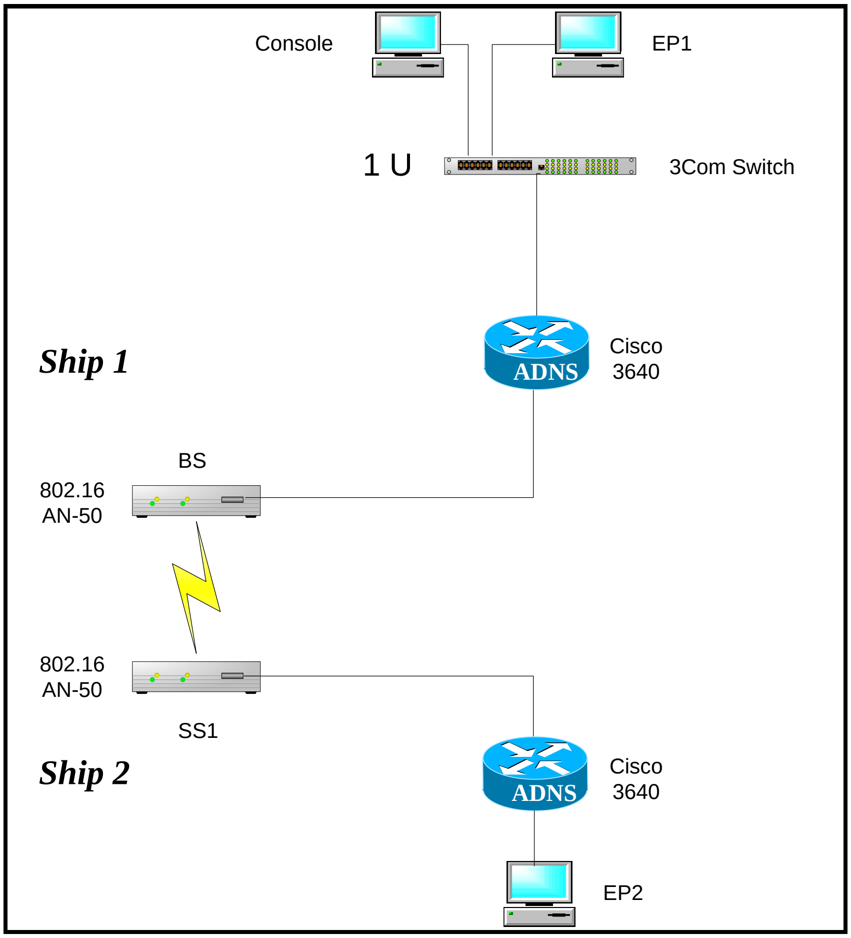


Figure 7. Ship-to-Ship ADNS System Augmented with IEEE 802.16 COTS Equipment Network Diagram

b. *Pier-to-Ship*

As shown in Figure 8, one laptop running the console application and one laptop generating the IP traffic were connected to the 3Com switch, which was then connected to a Redline IEEE 802.16 transceiver configured as the BS unit. Another laptop running the EP program was connected to a Redline IEEE 802.16 transceiver configured as a SS, which was connected to the BS via a wireless link. This topology was used as the control for the Pier-to-Ship configuration.

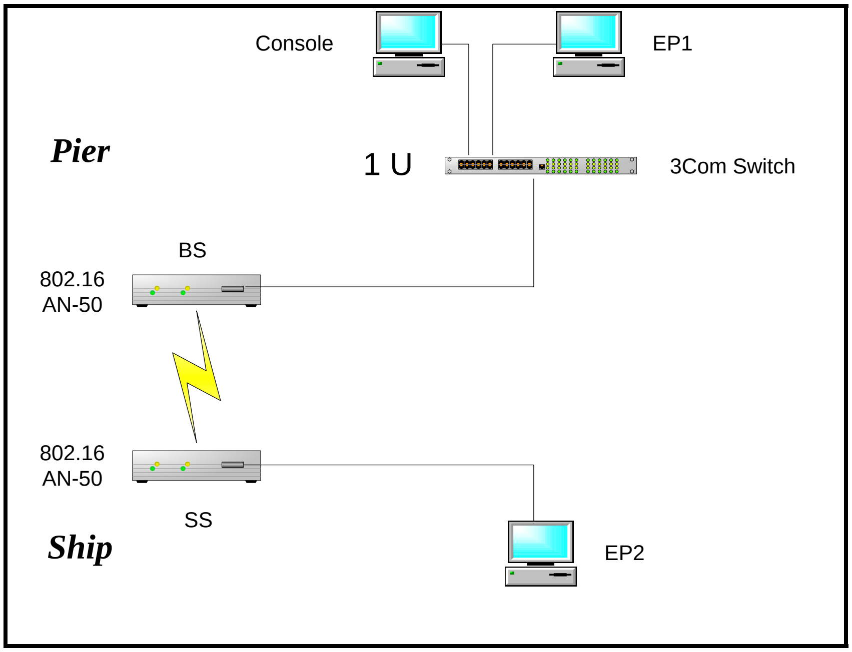


Figure 8. Pier-to-Ship Control Network Diagram

Figure 9 illustrates the setup of the simulation for the Pier-to-Ship configuration of the ADNS system augmented with IEEE 802.16 COTS equipment. One laptop running the console application and one laptop generating the IP traffic were connected to the 3Com switch, which was then connected to a Cisco 3640 router. The router was connected to a Redline IEEE 802.16 transceiver configured as the BS unit. Another laptop running the EP program was connected to another Cisco 3620 router and the router was connected to a Redline IEEE 802.16 transceiver configured as a SS. The SS was connected to the BS via wireless link.

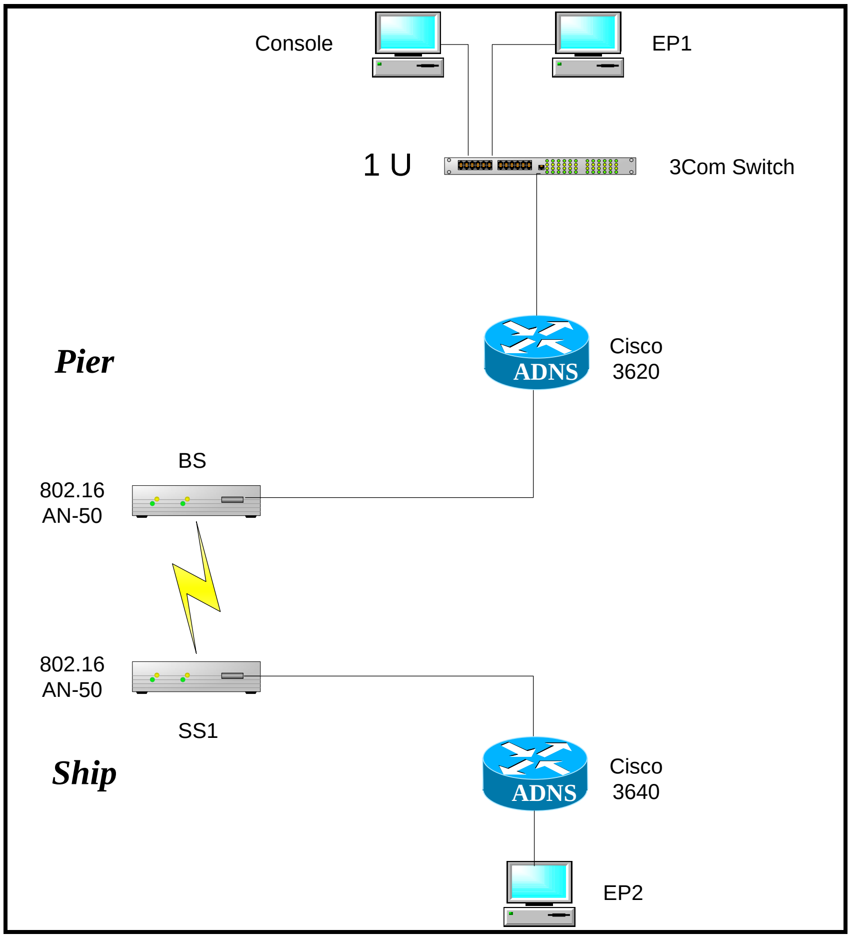


Figure 9. Pier-to-Ship ADNS System Augmented with IEEE 802.16 COTS Equipment Network Diagram

c. Pier-to-Ship Multipoint

One laptop running the console application and one laptop generating the IP traffic were connected to the 3Com switch, which was then connected to a Redline IEEE 802.16 transceiver configured as the BS unit, as depicted in Figure 10. Two laptops running the EP programs were connected to Redline IEEE 802.16 transceivers configured as SSs, which were connected to the BS via wireless link. This topology was used as the control for the Pier-to-Ship Multipoint configuration.

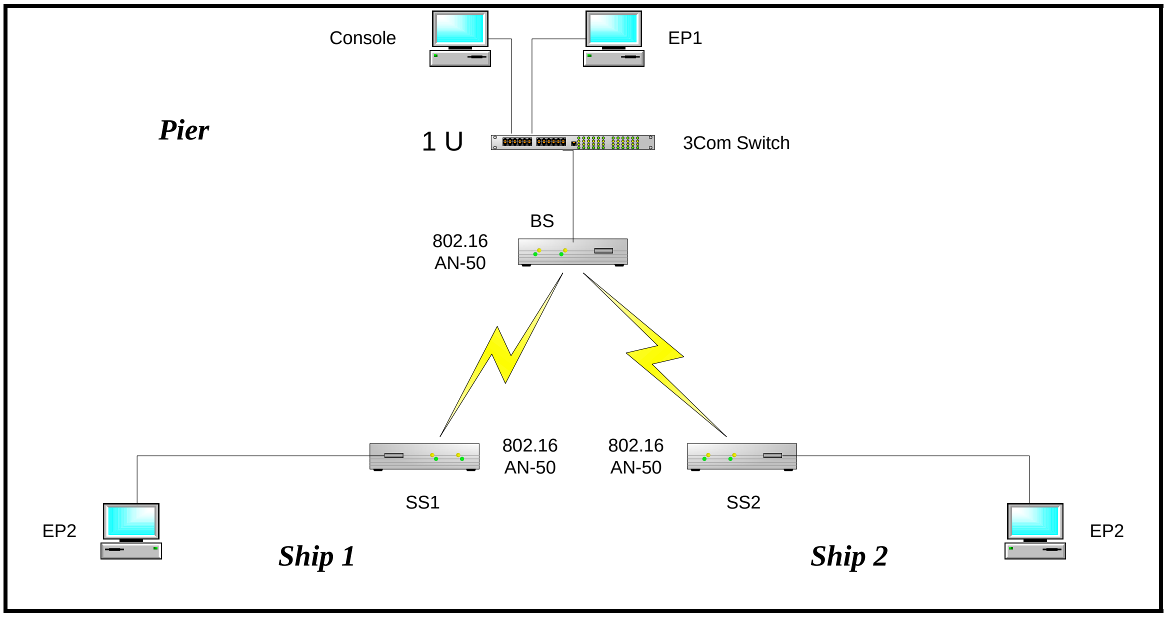


Figure 10. Pier-to-Ship Multipoint Control Network Diagram

Figure 11 shows one laptop running the console application and one laptop generating the IP traffic connected to the 3Com switch, which was then connected to a Cisco 3620 router. The router was connected to a Redline IEEE 802.16 transceiver configured as the BS unit. Two laptops running the EP programs were connected to two Cisco 3640 routers, and the routers were connected to two Redline IEEE 802.16 transceivers configured as SSs. The SSs were connected to the BS via wireless link. This topology was used as the simulation for the Pier-to-Ship multipoint configuration of the ADNS system augmented with IEEE 802.16 COTS equipment.

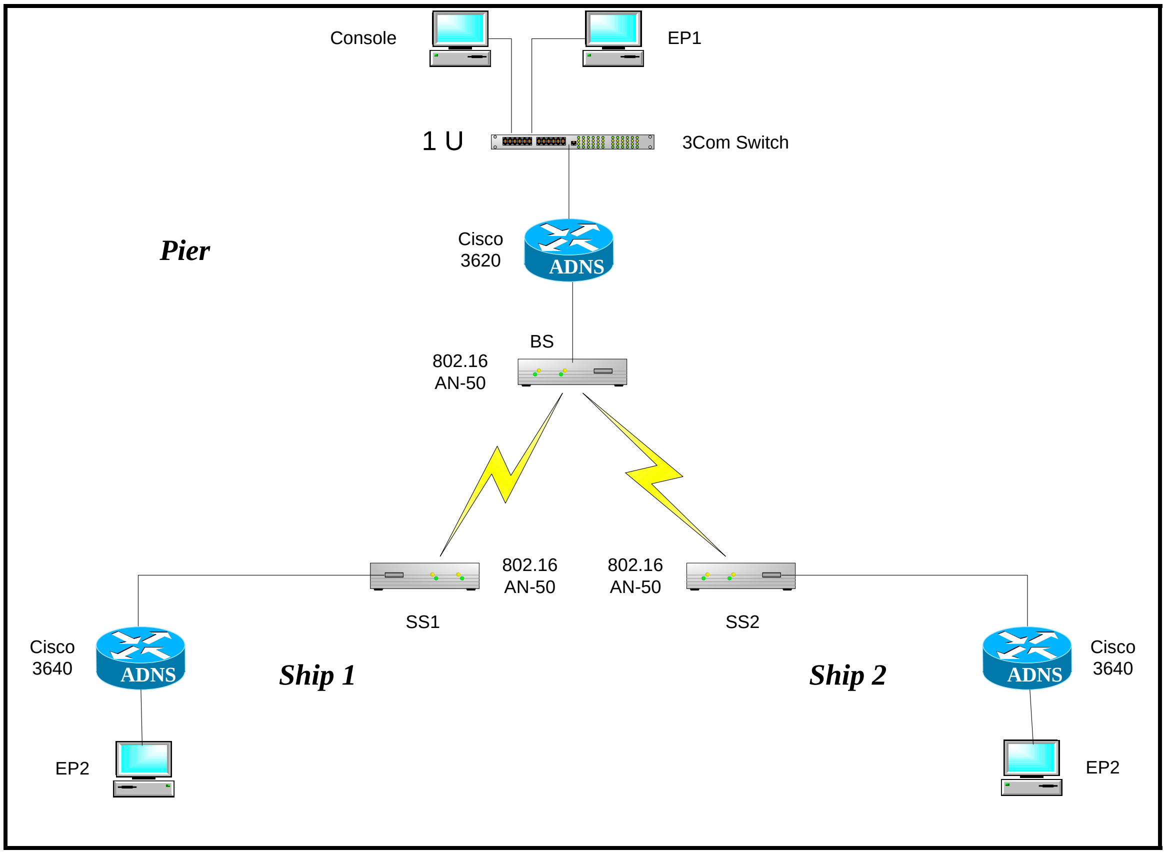


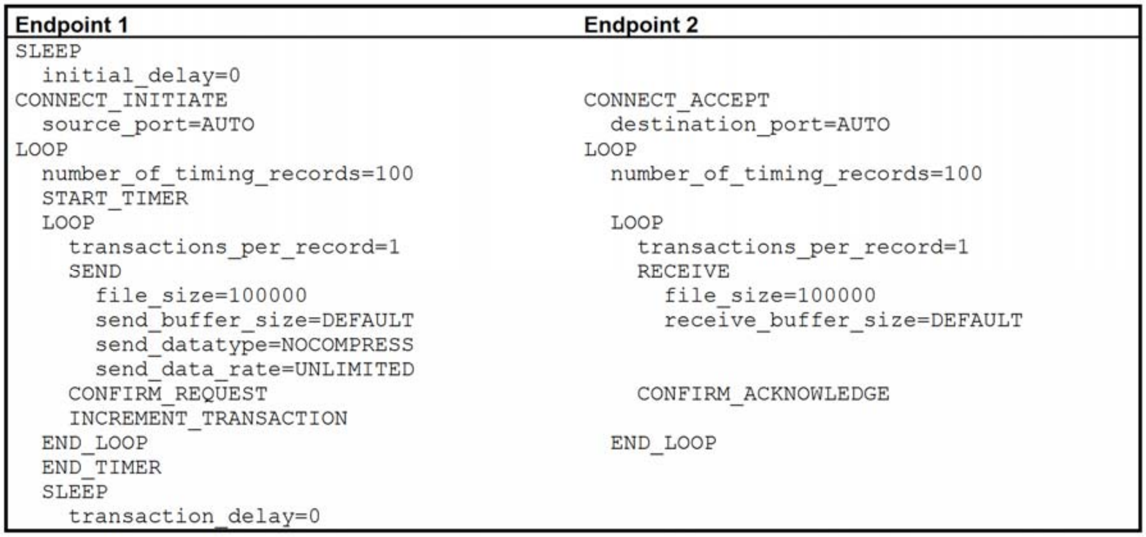
Figure 11. Pier-to-Ship Multipoint ADNS System Augmented with IEEE 802.16 COTS Equipment Network Diagram

3. IxChariot Test Plans

Each of the following IxChariot test plans was executed on the aforementioned configurations in order to determine the characteristics of the network. The results were recorded and analyzed to ensure that the proposed network would satisfy the required quality attributes.

a. Maximum Throughput

The maximum throughput test was designed to determine the rate at which the network sends or receives data. For this test, the IxChariot File Send, Long Connection script FILESNDL was used. This script sends a 100kb file in both directions between the endpoints so that there were sufficient data to fill the pipe. This script is shown in Figure 12.

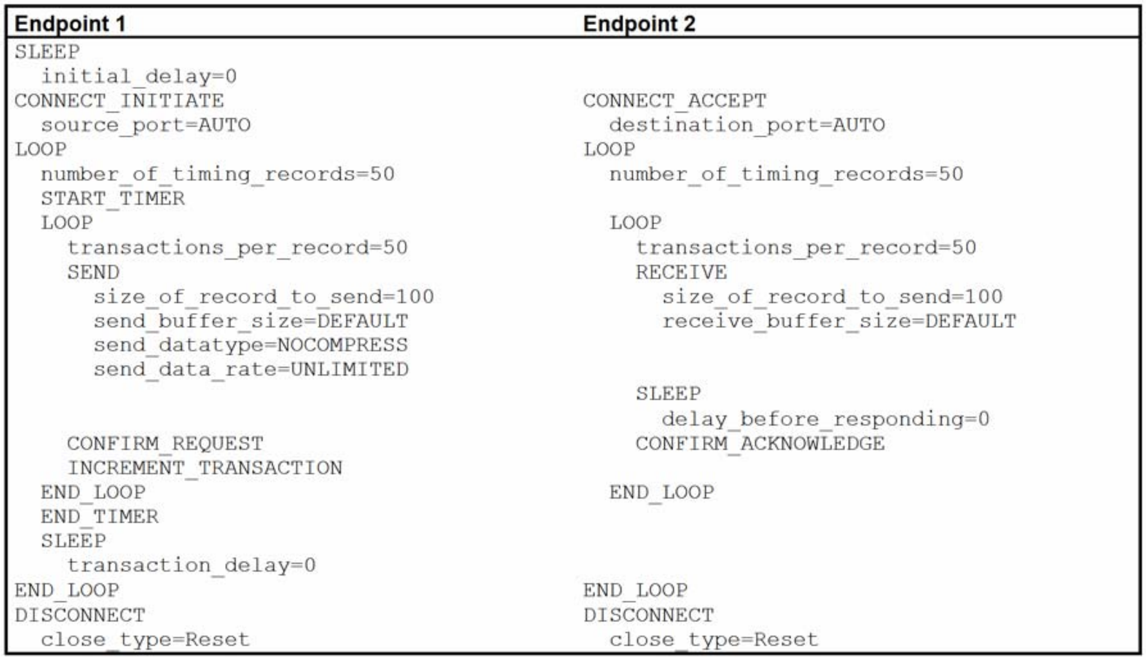


```
Endpoint 1                                Endpoint 2
SLEEP
  initial_delay=0
CONNECT_INITIATE                          CONNECT_ACCEPT
  source_port=AUTO                          destination_port=AUTO
LOOP                                      LOOP
  number_of_timing_records=100              number_of_timing_records=100
  START_TIMER
  LOOP                                      LOOP
    transactions_per_record=1                 transactions_per_record=1
    SEND                                      RECEIVE
      file_size=100000                          file_size=100000
      send_buffer_size=DEFAULT                  receive_buffer_size=DEFAULT
      send_datatype=NOCOMPRESS
      send_data_rate=UNLIMITED
    CONFIRM_REQUEST                           CONFIRM_ACKNOWLEDGE
    INCREMENT_TRANSACTION
  END_LOOP                                  END_LOOP
  END_TIMER
  SLEEP
    transaction_delay=0
```

Figure 12. FILESNDL.scr – The File Send, Long Connection Script Used in IxChariot

b. Maximum Response Time

The maximum response time test was designed to determine the system's latency, or the time delay between the moment something is initiated to the moment one of its effects begin. For this test we used the IxChariot script CREDITL. This script transfers a 100-byte file bounded by the latency of the network. The CREDITL script is show in Figure 13.



```
Endpoint 1                                Endpoint 2
SLEEP
  initial_delay=0
CONNECT_INITIATE                          CONNECT_ACCEPT
  source_port=AUTO                          destination_port=AUTO
LOOP                                      LOOP
  number_of_timing_records=50               number_of_timing_records=50
  START_TIMER
  LOOP                                      LOOP
    transactions_per_record=50                transactions_per_record=50
    SEND                                      RECEIVE
      size_of_record_to_send=100                size_of_record_to_send=100
      send_buffer_size=DEFAULT                  receive_buffer_size=DEFAULT
      send_datatype=NOCOMPRESS
      send_data_rate=UNLIMITED

                                              SLEEP
                                                delay_before_responding=0
    CONFIRM_REQUEST                           CONFIRM_ACKNOWLEDGE
    INCREMENT_TRANSACTION
  END_LOOP                                  END_LOOP
  END_TIMER
  SLEEP
    transaction_delay=0
END_LOOP                                  END_LOOP
DISCONNECT                                DISCONNECT
  close_type=Reset                          close_type=Reset
```

Figure 13. CREDITL.scr – The Credit Send, Long Connection Script Used in IxChariot

c. Triple Play

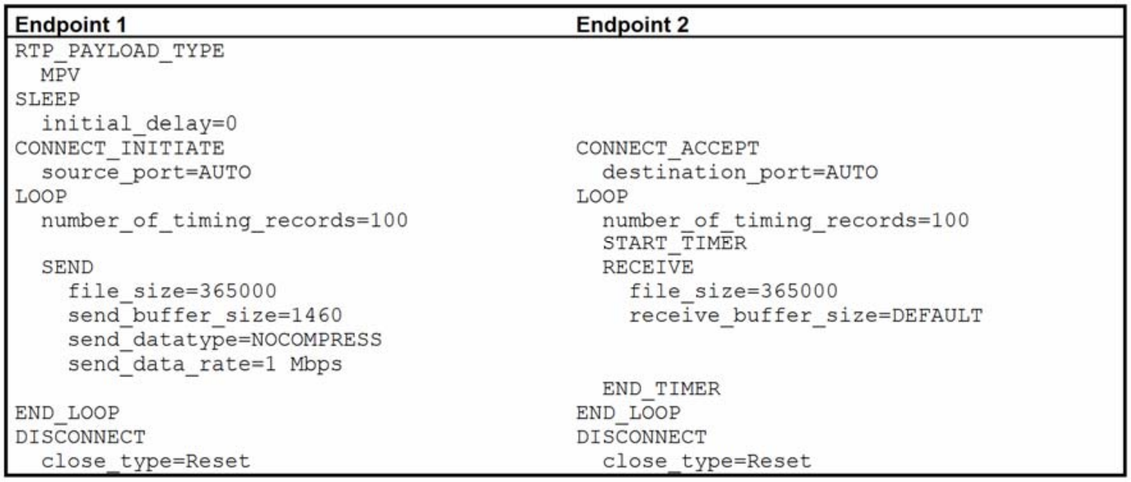
The triple play test was designed to evaluate the performance of the networks using real-world applications that use the three protocols that handle voice, video, and data. This test would also yield a simplistic QoS analysis. First we created the baseline traffic types, Internet, video and VoIP in order to see how the traffic is run in isolation. Then all the traffic types were combined, and the network was reassessed in terms of throughput, latency, and data loss.

The Internet traffic type consists of web accesses, mail, ftp, P2P, and various forms of business traffic designed to serve as a constant source of background Internet traffic. Nine pairs of IxChariot traffic were used to simulate the Internet traffic, as shown in Table 6.

Script Filename	Protocol	TCP/UDP Port	User Delay (ms)	Transaction Delay (ms)	Response Delay (ms)
DNS.scr	UDP	53		10	10
FTPget.scr	TCP	20	1000	10	1000
FTPput.scr	TCP	20	1000	10	10
HTTP_Secure_Transaction.scr	TCP	443		10	
HTTPgif.scr	TCP	80		10	10
HTTPtext.scr	TCP	80		10	10
NNTP.scr	TCP	119		10	10
POP3.scr	TCP	110		10	
SMTP.scr	TCP	25		10	

Table 6. Internet Traffic Setup (From: Ref 20)

The video traffic type emulates video streams to simulate the behavior of video traffic through the network by streaming a 1.0 Mbps video stream in both directions. For this test, we used the Cisco IP/TV, MPEG Video Stream script IPTVv as, shown in Figure 14.



```
Endpoint 1                                  Endpoint 2
RTP_PAYLOAD_TYPE
  MPV
SLEEP
  initial_delay=0
CONNECT_INITIATE                            CONNECT_ACCEPT
  source_port=AUTO                            destination_port=AUTO
LOOP                                        LOOP
  number_of_timing_records=100                number_of_timing_records=100
                                              START_TIMER
  SEND                                        RECEIVE
    file_size=365000                            file_size=365000
    send_buffer_size=1460                       receive_buffer_size=DEFAULT
    send_datatype=NOCOMPRESS
    send_data_rate=1 Mbps
                                              END_TIMER
END_LOOP                                    END_LOOP
DISCONNECT                                  DISCONNECT
  close_type=Reset                            close_type=Reset
```

Figure 14. IPTVv.scr – The Cisco IP/TV, MPEG Video Stream script used in IxChariot.

The VoIP traffic type emulates voice traffic using several different types of codec algorithms and measures the Mean Opinion Score (MOS) of the voice conversations. Six VoIP pairs were created with each using a unique codec type (G7.11u, G.711a, G.723.1-ACELP, G.723.1-MPMLQ, G.729 and G.726). Each pair was then replicated to go in the reverse direction in order to simulate bidirectional traffic. All twelve pairs were replicated twice to create a total of 36 VoIP pairs to evaluate how the network would respond to a multitude of VoIP traffic.

D. TEST RESULTS

1. Maximum Throughput

The results summarized in Table 7 were obtained from running the maximum throughput tests on the associated network topologies. As expected, a slight decrease occurred in the throughput when the ADNS routers were added to the network. Despite this slight decrease, there was still sufficient throughput to allow for a multitude of applications to be run in all of the tested topologies.

Topology	Control	ADNS
Ship-to-Ship	16.454	13.935
Pier-to-Ship PtP	15.454	16.199
Pier-to-Ship PMP	19.853	16.244
Ship-to-Ship PMP	10.917	9.500

Table 7. Max Throughput Results (Mbps)

2. Maximum Response Time

The results summarized in Table 8 were obtained from running the maximum response time tests on the associated network topologies. The response time is the amount of delay between the request from a computer and the moment at which the response to the request is received. This characteristic is what the user of the network usually perceives as actual speed of the network, therefore the lower the response time, the faster the network. In evaluating response time there are three important limits based on rationale defined by Rob Miller, a behavioral scientist who has specialized in task behavior:

- 0.1 second is about the limit for having the user feel that the system is reacting instantaneously, meaning that no special feedback is necessary except to display the result.
- 1.0 second is about the limit for the user's flow of thought to stay uninterrupted, even though the user will notice the delay. Normally, no special feedback is necessary during delays of more than 0.1 but less than 1.0 second, but the user does lose the feeling of operating directly on the data.
- 10 seconds is about the limit for keeping the user's attention focused on the dialogue. For longer delays, users will want to perform other tasks while waiting for the computer to finish, so they should be given feedback indicating when the computer expects to be done. Feedback during the delay is especially important if the response time is likely to be highly variable, since users will then not know what to expect.
  (From: Ref 27)

The results from the testing of all of the network topologies are three orders of magnitude less than the limit where the user will actually feel that service is intermittent. Therefore from a user's perspective the network would seem uninterrupted.

Topology	Control		ADNS	
	avg	max	avg	max
Ship-to-Ship	0.001	0.002	0.001	0.003
Pier-to-Ship PtP	0.001	0.002	0.002	0.002
Pier-to-Ship PMP	0.002	0.003	0.003	0.004
Ship-to-Ship PMP	0.002	0.003	0.003	0.004

Table 8. Max Response Time Results (s)

3. Triple Play

The results summarized in Table 9 were obtained by running the Internet baseline tests for their associated topologies. As expected, the throughput was still sufficient to carry a large amount of web traffic and the average response time was still below the 1.0 second cutoff for the user to feel that the service is uninterrupted. The max response time does indicate that the users will notice some slight delay on a few of their transactions with the use of the Internet, but it is still not high enough or frequent enough to cause the user's experience to be any less satisfactory than that of a user of any other standard network.

Topology		Throughput (Mbps)	Avg Response Time (s)	Max Response Time (s)
Ship-to-Ship	Control	11.219	0.552	3.286
	ADNS	10.328	0.599	3.700
Pier-to-Ship PtP	Control	11.219	0.552	3.286
	ADNS	12.021	0.533	3.130
Pier-to-Ship PMP	Control	19.042	0.612	3.907
	ADNS	18.571	0.621	3.974
Ship-to-Ship PMP	Control	6.293	0.661	3.926
	ADNS	6.378	0.698	5.103

Table 9. Internet Baseline Results

The results summarized in Table 10 were obtained by running the video baseline tests for their associated topologies. The test was set up so that a 1Mbps video would stream in both directions between the users, simulating a VTC-type application. Because only 1Mbps would need to be transferred in both directions, the required throughput would be 2Mbps. In the Pier-to-Ship PMP-topology, the test was set up to stream the video in both directions between the pier and both ships and also in both directions between each ship, thus requiring the max throughput to be 6Mbps. The results in Table 10 show that there is sufficient throughput to stream the videos with no loss of bytes.

Topology		Throughput (Mbps)	Bytes Lost (%)
Ship-to-Ship	Control	1.998	0
	ADNS	1.998	0
Pier-to-Ship PtP	Control	1.998	0
	ADNS	1.998	0
Pier-to-Ship PMP	Control	5.995	0
	ADNS	5.995	0
Ship-to-Ship PMP	Control	1.999	0
	ADNS	1.998	0

Table 10. Video Baseline Results

A more easily interpreted determination of whether or not the network could handle streaming video would result from surveying the graphs of the throughput. Figure 15 shows the throughput for the video baseline test in the ADNS Pier-to-Ship PMP topology. The data source evaluated was chosen since it used the most throughput and would have the highest need for the resources of the network. The graph shows no significant deviations from the 1Mbps throughput needed to stream each video successfully, thus indicating that the network will support this type of application.

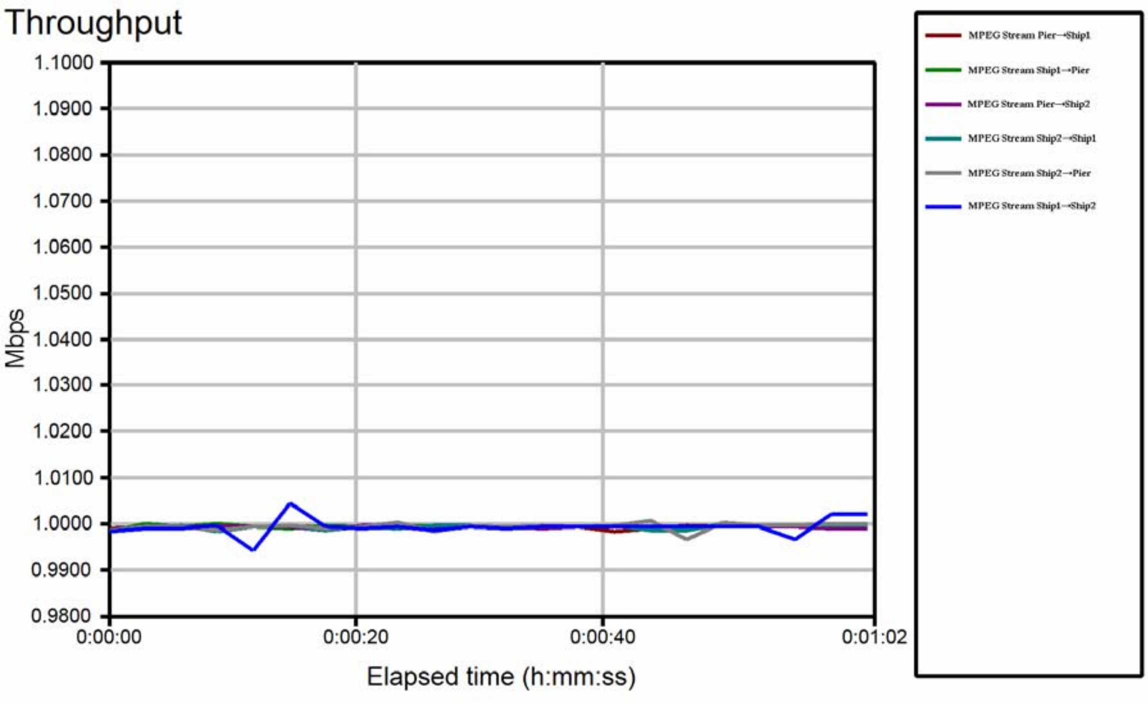


Figure 15. Throughput for the Video Baseline Test in the ADNS Pier-to-Ship PMP Topology

The results summarized in Table 11 were obtained by running the VoIP baseline tests for their associated topologies. The best indicator that the network would support the VoIP protocol is the MOS. Users would have a better experience with their voice call with a higher MOS. In the Ship-to-Ship and Pier-to-Ship point-to-point topologies, the average MOS score is high enough to predict that the user would experience good performance.

Topology		Throughput (Mbps)	MOS	Jitter Max (ms)	Bytes Lost (%)
Ship-to-Ship	Control	1.033	4.07	5	0
	ADNS	1.032	4.07	24	0
Pier-to-Ship PtP	Control	1.033	4.07	5	0
	ADNS	1.032	4.07	13	0
Pier-to-Ship PMP	Control	1.033	3.05	38	0
	ADNS	1.032	3.05	39	0
Ship-to-Ship PMP	Control	1.033	2.54	38	0
	ADNS	1.032	2.54	34	0

Table 11. VoIP Baseline Results

In the Pier-to-Ship PMP topologies, the average MOS is around 3, indicating that the users would have a fair experience with their voice calls. These numbers are slightly lower because an Apple Operating System (OS), whose system clock could not be synchronized with the other system clocks, was used as the EP for one of the ships. The graph in Figure 16 shows that VoIP simulations that relied on the system clock from the Apple OS had an MOS estimate of 1 because of the high amount of perceived delay because the system clocks were not synchronized. The remainders of the VoIP simulations' MOS estimates were between 3.6 and 4.4, the same level as the tests of the other network topologies. This leads to the inference that if the system clocks had been synchronized, all of the users would have had a satisfactory VoIP call.

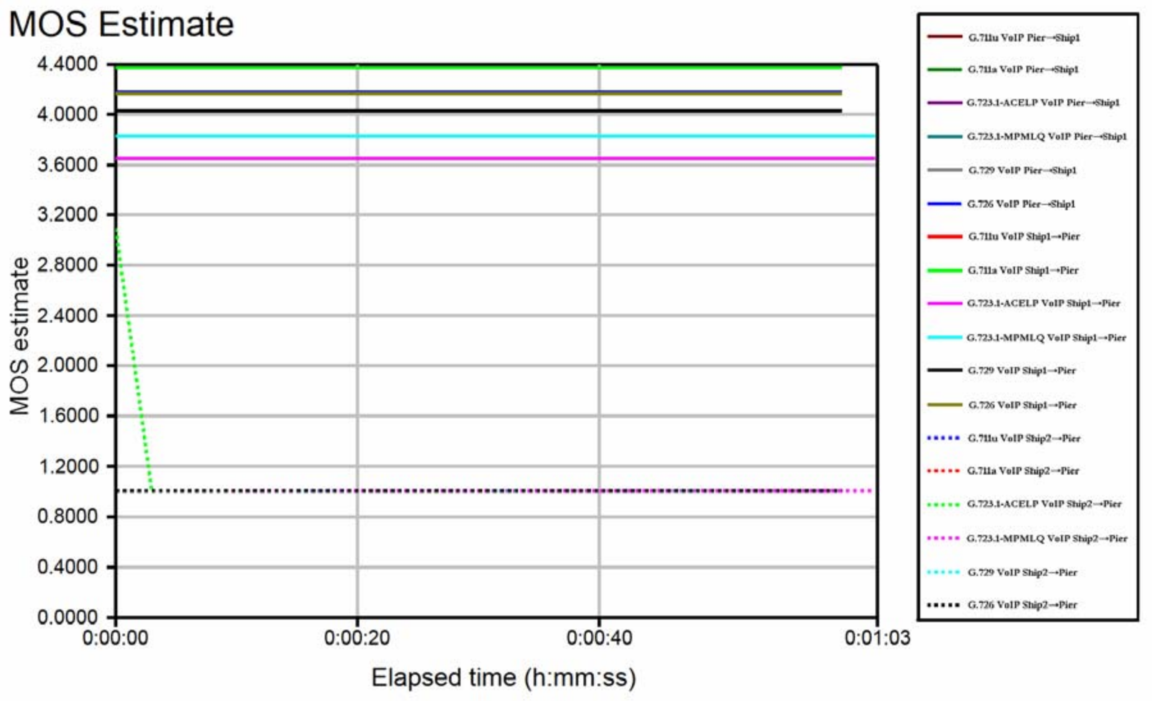


Figure 16. MOS Estimate for the VoIP Baseline Test in the ADNS Pier-to-Ship PMP Topology

The results summarized in Table 12 were obtained by running all of the previous tests on their associated topologies simultaneously. As expected, the throughput stayed relatively the same and was therefore sufficient to handle all the information types transferred. The average response time also remained below the 1.0 second cut-off for the user to feel that the system was uninterrupted. MOS results were the same as in the baseline test indicating that the composite flow of traffic did not hinder the performance of the voice calls.

Topology		Throughput (Mbps)	Response Time (s)	Bytes Lost (%)	MOS	Jitter Max (ms)
Ship-to-Ship	Control	12.436	0.587	0	4.07	17
	ADNS	11.821	0.636	0	4.06	46
Pier-to-Ship PtP	Control	12.436	0.587	0	4.07	17
	ADNS	13.653	0.555	0	4.07	18
Pier-to-Ship PMP	Control	19.404	0.783	0.075	3	39
	ADNS	19.722	0.722	0.033	3.04	22
Ship-to-Ship PMP	Control	6.993	0.775	0.306	2.36	39
	ADNS	7.923	0.751	0.381	3.08	23

Table 12. Triple Play Results: Internet, Video and VoIP

The graph in Figure 17 shows the throughput for the triple-play test on the ADNS Pier-to-Ship PMP topology. By analyzing the graph and the tabular results for such measures as throughput and MOS, a simplistic QoS estimation can be determined. QoS is the probability that the network will meet the required traffic contract. This can be evaluated by measuring the dropped packets, delay, and out-of-order delivery of the packets. Dropped packets occur when the packets arrive when their buffers are already full, thus causing the packets to be resent, ultimately delaying the overall transmission. Delay in the packets is important in such applications as VoIP and streaming video since a delayed packet would cause the transmission to appear erratic. Out-of-order delivery of packets do not cause problems in the transmission of applications like Internet traffic, but in applications in which the order is important, such as VoIP or streaming video, an out-or-order packet will degrade the service. VoIP and video have a high priority of transmission quality and require either UGS or rtPS, and the Internet traffic would be designated to use BE service. In the graph, in Figure 17, the EPs for the transfer of video remain at 1Mbps, thus indicating that they retain quality video streaming service. The throughput for the Internet traffic rises and falls as throughput is available, thus demonstrating the assigned BE service.

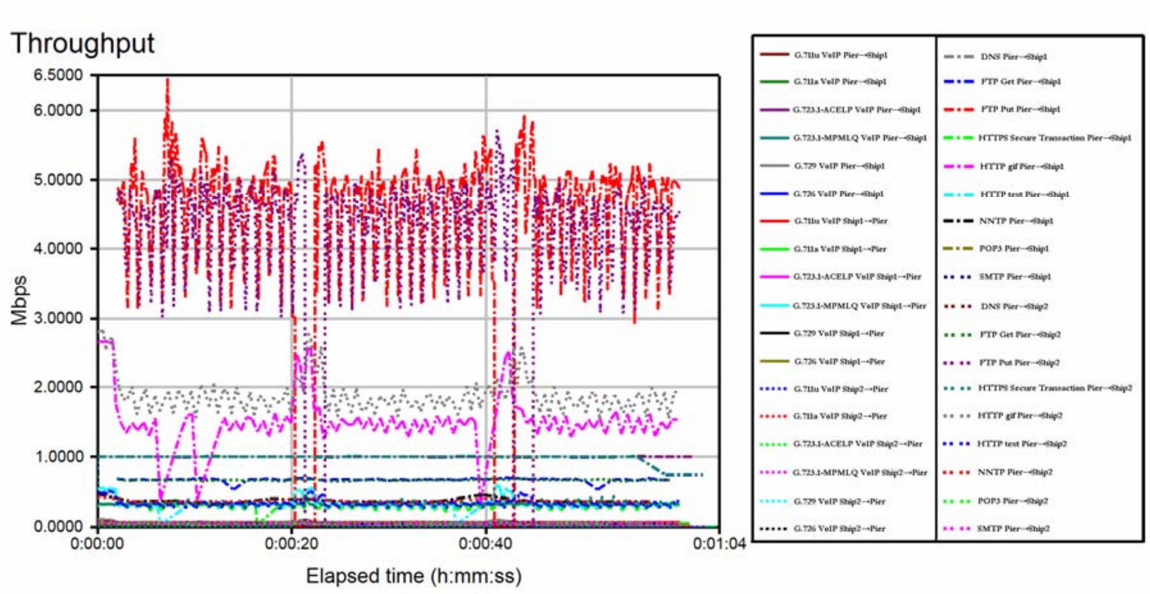


Figure 17. Throughput for the Triple-Play Test on the ADNS Pier-to-Ship PMP Topology

As traffic was added, the MOS estimates shown in Figure 18 dipped slightly due to packets being dropped. No packets were dropped consecutively, and the MOS estimates for the VoIP calls remained at their previous levels despite the composite traffic, indicative of the QoS applied to such applications.

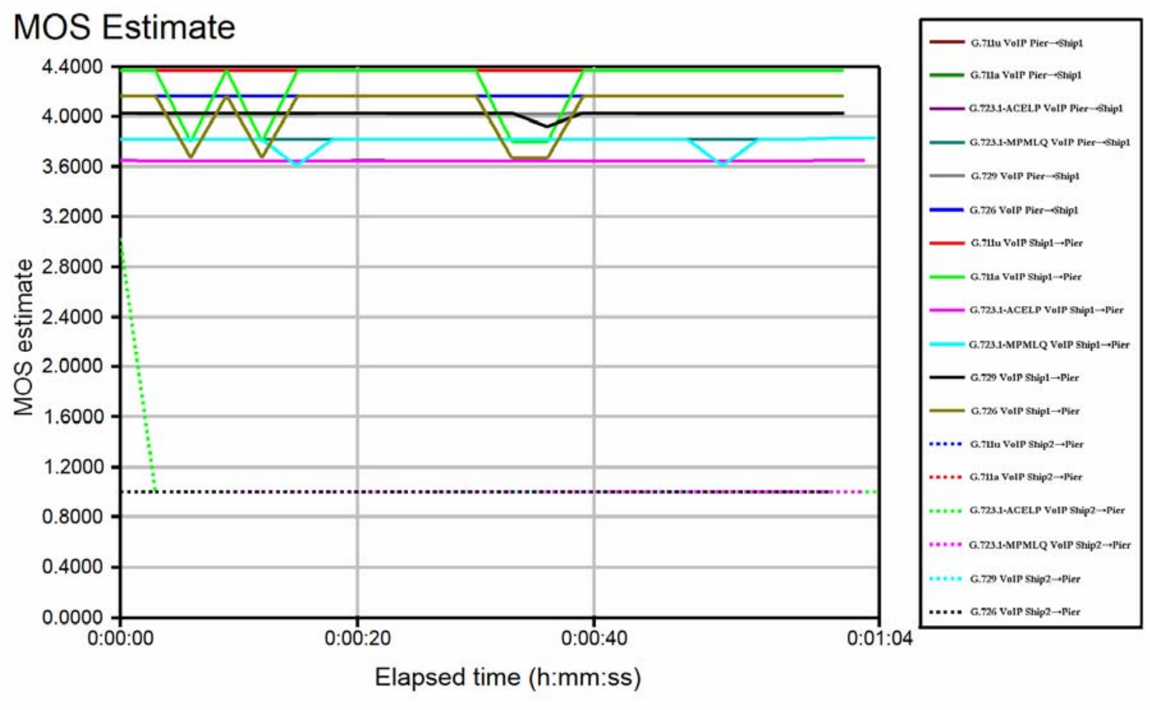


Figure 18. MOS Estimates for the Triple-Play Test on the ADNS Pier-to-Ship PMP Topology

E. SUMMARY

The aforementioned tests were designed to verify the utility of the IEEE 802.16 COTS equipment for extending the ADNS system's IP router-based ship-to-ship and ship-to-shore architecture to provide adaptable intra-strike group high-speed packet switched data, imagery, and voice communications. The maximum throughput test proved that the network could support a minimum of 9.500 Mbps and a maximum of 19.853 Mbps. Response time of the network proved to be below the level at which the user would feel that the service is intermittent. The triple-play test demonstrated that the IEEE 802.16 COTS equipment is sufficient for providing data, video, and voice communications with the intention of augmenting the ADNS system.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS

A. FINDINGS

Our research focused on the unique quality attributes of the IEEE 802.16 MAC layer and its ability to transfer data, video and voice in conjunction with the ADNS. The objectives of our research were to report on the effectiveness of IEEE 802.16 COTS equipment for naval applications in point-to-point and point-to-multipoint topologies and to report on IEEE 802.16 system's efficacy as a WAN for use in the ADNS.

1. Effectiveness of IEEE 802.16 COTS Equipment

The IEEE 802.16 MAC layer's uses a scheduling algorithm that moderates access to its medium using a grant/request mechanism. Being connection orientated, a request granted is assigned a CID with distinctive QoS parameters. These parameters are based on the needs of the transmission and the resources available. Due to these qualities, IEEE 802.16 systems can provide scalability from one to hundreds of SSs, at ranges up to tens of kilometers, and provide QoS guarantees. These advantages make COTS equipment that adheres to the IEEE 802.16 standard a viable alternative for point-to-point and point-to-multipoint naval applications.

2. Efficacy as a WAN for Use in the ADNS

The IEEE 802.16-standard compliant equipment was tested in point-to-point and point-to-multipoint topologies in order to verify its value in the ADNS architecture. Maximum throughput, maximum response time, and a "triple-play" suite of data, video, and voice tests were executed on the COTS equipment. The IEEE 802.16 system performed to expectations, delivering a maximum throughput of 19.852 Mbps and a maximum response time of 0.004 seconds. The triple-play test demonstrated the ability of the IEEE 802.16 system to provide QoS assurances successfully and to handle the demands of real-world applications that use data, video, and voice. Thus, our testing proved that the IEEE 802.16 COTS equipment could be used as a high-speed, high-throughput communication link augmentation to the ADNS. This system is capable of being deployed now.

B. FURTHER RESEARCH

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

1. Security Services

The ADNS is currently a “red” system. ADNS relies on layer 1 encryption to address the security service of confidentiality, thereby requiring the entire system, including the radio WAN portion, be run at the Secret-GENSER-NOFORN system high level. The intention of the Navy is to make the radio WAN “black;” no unencrypted classified datagrams. The plan is to implement encryption at each user’s machine prior to sending data onto the network. An IEEE 802.16 network segment could be deployed “black” within the ADNS framework by surrounding it with VPN protection. Although encryption hides the content of the data, there are other problems that exist and need to be addressed in either configuration. Issues that, theoretically, can be handled at layers one and two of the OSI model are traffic analysis, traffic flow analysis, limited probability of interception, limited probability of detection (LPI/LPD) and jam resistance.

Confidentiality, authenticity, non-repudiation and integrity aspects of data protection must be considered. Confidentiality includes the secrecy of data and the denial of access by unintended parties. It can theoretically be handled at any layer of the OSI model. By addressing confidentiality at layer 3 via VPN, you can effectively make layers 1 and 2 “black”, as they would never handle any encrypted (red) datagrams. Authenticity is ensuring that others cannot imitate the data and/or pretend to be someone else and send it. Authenticity can be handled at layers 3, 4 and 7. Non-repudiation means that a host cannot do or say something and later successfully deny it. This service can also be handled at layers 3, 4 and 7. Finally, integrity, also potentially handled at either of layers 3, 4 and 7, is ensuring that the data have not been altered between the source and destination. The areas that lend themselves to being scrutinized more closely are those that are either not addressed by the IEEE 802.16 standard or are vulnerable, based on the nature of the equipment used at that layer. Since COTS IEEE 802.16 equipment resides at layers 1and 2 of the OSI model, the issues at this layer have been addressed by the standard and the upper layers of the OSI exceed the scope of this thesis, so that leaves the confidentiality issue at layers 1 and 2. The placement of a VPN box at each router should effectively address the service issues at these levels, by effectively hiding the IP addresses of the equipment that resides behind it. The solution mentioned here, addressing confidentiality at layer3, would be out of scope for IEEE 802.16.

The IEEE 802.16 standard has addressed the security issues that were prevalent in the IEEE 802.11 standard. Further research should be conducted to address the changes to the COTS IEEE 802.16 equipment that is necessary to meet or exceed the current NSA Standard for security in RF transmissions.

2. Mesh Topologies

The IEEE 802.16 standard has provisions for mesh topologies. Due to the natural design of a CSG, the range of communications could be enhanced by an order of magnitude through the use of mesh topologies. It remains to be shown whether or not the IEEE 802.16 systems' messages can be relayed and controlled at Physical and Datalink Layers, and can be leveraged for us in a CSG.

Due to IEEE 802.16's BS and SSs configuration, the information must travel to the BS to be relayed to an addressed SS. This means that the entity that is configured as the BS should be centrally located in respect to the SSs. Dynamic role assignment should be investigated to determine the flexibility of the IEEE 802.16 architecture to changes in the relative location of the base station.

Additionally, analysis of the ability of SSs to forward the information to SSs in another network, thereby, acting as a bridge between tow or more geographically adjacent networks should be performed. If feasible, the SSs connecting the networks serve as a gateways or borders hosts/routers between those networks.

The IEEE 802.16 standard does not mention the ability to configure or reconfigure the SS to take on the role of a BS in situations suggested here. Further research should be conducted to address the necessary changes to COTS IEEE 802.16 equipment that would allow for transferring transmissions and autonomous switching of subscriber stations to base stations, thus improve the usability of the system.

3. QoS

Currently, the ADNS, acting at the network layer, does not have a mechanism to relate the priority of its output to the IEEE 802.16 transceiver.

The COTS IEEE 802.16 scheduling algorithm allows us to control QoS by adjusting BW grants. QoS is guaranteed by transmission ordering and scheduling to each service as defined by its CID. The router will have numerous data grams and will send several Differential Service Code Point (DSCP) intentions, which have to be sorted, to their respective CID. What is not defined by the standard is the mechanism by which a BS performs this process. An appropriate way to provide QoS control at the network layer is by using differential services. We can make a reasonable assumption that the ADNS routers (at both BS and SS) will have the highest priority traffic at the head of the line, so when a station gets permission to transmit, the highest priority traffic are sent first. However no mechanism exists for the SS or a BS to know how much traffic is queued at any particular DSCP queue at the router. Example: ADNS routers with four DSCP queues (probably pretty reasonable) are set up. Traffic originated by end systems on a DD goes to the ADNS router via the ship's LAN and gets sorted into these 4 queues in the router. The routers do not have a mechanism to transfer the queue size information to the IEEE 802.16 interfaces. If this information is unknown, then efficient adjustments for BW grants can not be made. An investigation of means to provide this information between the network layer and the link layer, as well as how it should be used if such an information exchange is possible, should be conducted to determine whether or not this deficiency can be reasonably mitigated.

4. Radio Frequency Characteristics Performance

The conduct of practical tests of the IEEE 802.16 compliant equipment brought to mind a key implementation consideration. The IEEE 802.16 standard does mention, generically, that its scheme allows for optimal performance in various environments. However, the IEEE 802.16 standard does not address the behavior of the Radio frequency characteristics in various naval environments. Typical naval environments include “Blue water,” or at sea, and pier-side. The two environments are radically different, and each has a profound effect on the behavior of radio frequencies. The pier-side environment has numerous sources of interference in the form of RF transmissions and physical structures. When ships are at sea, there are very few physical structures but numerous transmission sources. According to the IEEE 802.16 standard, the use of the OFDM technique is recognized as contributing to optimal performance in all propagation environments.

Further research on the performance of the IEEE 802.16 radio frequency characteristics should be conducted to document the effect that each of these naval environments has on the IEEE 802.16 equipment's OFDM scheme with respect to operational range capability.

5. Increased Range

The scope of this thesis did not deal with the PHY layer issue regarding range; however during the practical tests it became apparent that the IEEE 802.16 compliant equipment's usability would be further enhanced by an increased range. Recognized methods of increasing range are to increase power to the antennas, use of an adaptive antenna system, increasing the number of strategically placed antennas, and incorporating automated, gear driven directional antennas. The simple increase in power method is plagued by many different side-effects that include large radiating zones that affect humans negatively, interference, and distortion therefore other methods need to be researched.

Further research on the necessary adaptations to the IEEE 802.16 systems should be conducted to illustrate and document an effective, low cost method of increasing the range and utility of the IEEE 802.16 system.

C. RECOMMENDATIONS

The tests proved that IEEE 802.16 is indeed an effective augmentation to the ADNS and can successfully transmit data, video, and voice communications in conjunction with the current ADNS equipment. The IEEE 802.16 equipment enhances the ability of ADNS to fulfill its objectives by allowing a large communication pipeline to be used among the ships of a CSG. Use of this pipeline for information that is not sensitive, in effect, relieves the ADNS BW of this data. This transmission of data among ships in the CSG, via the IEEE 802.16 system, allows the minimal resources of the previously existing ADNS to be used for high priority and classified transmissions to and from C2 centers ashore. The implementation of IEEE 802.16 equipment does not counter or detract from any of the attributes of the ADNS.

There is no plausible reason that IEEE 802.16 systems should not be deployed now. The availability of low priced, effective equipment must not be ignored. The addition of IEEE 802.16 equipment is in accordance with the DOD directives toward transforming into a Network Centric operation. It allows for additions of ad-hoc networks, scalability, and the enhancement of current equipment capabilities. The employment of the IEEE 802.16 system is an inexpensive way for the Navy to take advantage of the commercial sectors advanced communication technologies. The addition of IEEE 802.16 system to the ADNS is logical, and it is recommended that the advantages associated with the IEEE 802.16 system be leveraged and exploited without delay.

APPENDIX A: MAC MANAGEMENT MESSAGES

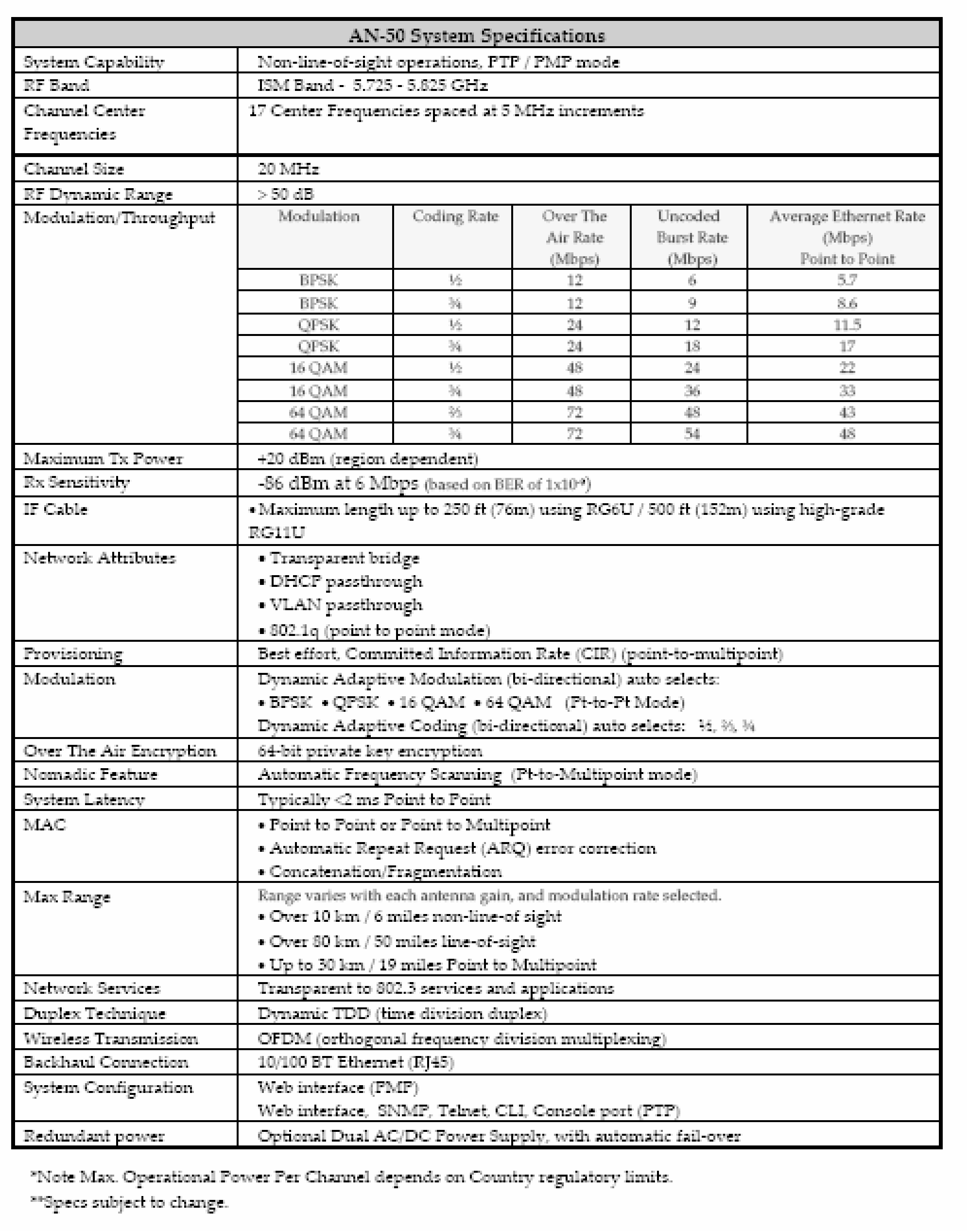
Type	Message name	Message description	Connection
0	UCD	Uplink Channel Descriptor	Broadcast
1	DCD	Downlink Channel Descriptor	Broadcast
2	DL-MAP	Downlink Access Definition	Broadcast
3	UL-MAP	Uplink Access Definition	Broadcast
4	RNG-REQ	Ranging Request	Initial Ranging or Basic
5	RNG-RSP	Ranging Response	Initial Ranging or Basic
6	REG-REQ	Registration Request	Primary Management
7	REG-RSP	Registration Response	Primary Management
8		*reserved*	
9	PKM-REQ	Privacy Key Management Request	Primary Management
10	PKM-RSP	Privacy Key Management Response	Primary Management
11	DSA-REQ	Dynamic Service Addition Request	Primary Management
12	DSA-RSP	Dynamic Service Addition Response	Primary Management
13	DSA-ACK	Dynamic Service Addition Acknowledge	Primary Management
14	DSC-REQ	Dynamic Service Change Request	Primary Management
15	DSC-RSP	Dynamic Service Change Response	Primary Management
16	DSC-ACK	Dynamic Service Change Acknowledge	Primary Management
17	DSD-REQ	Dynamic Service Deletion Request	Primary Management
18	DSD-RSP	Dynamic Service Deletion Response	Primary Management
19		*reserved*	
20		*reserved*	
21	MCA-REQ	Multicast Assignment Request	Primary Management
22	MCA-RSP	Multicast Assignment Response	Primary Management
23	DBPC-REQ	Downlink Burst Profile Change Request	Basic
24	DBPC-RSP	Downlink Burst Profile Change Response	Basic
25	RES-CMD	Reset Command	Basic

Table 13. MAC Management Messages (From: Ref 16)

Type	Message name	Message description	Connection
26	SBC-REQ	SS Basic Capability Request	Basic
27	SBC-RSP	SS Basic Capability Response	Basic
28	CLK-CMP	SS network clock comparison	Broadcast
29	DREG-CMD	De/Re-register Command	Basic
30	DSX-RVD	DSx Received Message	Primary Management
31	TFTP-CPLT	Config File TFTP Complete Message	Primary Management
32	TFTP-RSP	Config File TFTP Complete Response	Primary Management
33	ARQ-Feedback	Standalone ARQ Feedback	Basic
34	ARQ-Discard	ARQ Discard message	Basic
35	ARQ-Reset	ARQ Reset message	Basic
36	REP-REQ	Channel measurement Report Request	Basic
37	REP-RSP	Channel measurement Report Response	Basic
38	FPC	Fast Power Control	Broadcast
39	MSH-NCFG	Mesh Network Configuration	Broadcast
40	MSH-NENT	Mesh Network Entry	Basic
41	MSH-DSCH	Mesh Distributed Schedule	Broadcast
42	MSH-CSCH	Mesh Centralized Schedule	Broadcast
43	MSH-CSCF	Mesh Centralized Schedule Configuration	Broadcast
44	AAS-FBCK-REQ	AAS Feedback Request	Basic
45	AAS-FBCK-RSP	AAS Feedback Response	Basic
46	AAS_Beam_Select	AAS Beam Select message	Basic
47	AAS_BEAM_REQ	AAS Beam Request message	Basic
48	AAS_BEAM_RSP	AAS Beam Response message	Basic
49	DREG-REQ	SS De-registration message	Basic
50–255		*reserved*	

Table 14. MAC Management Messages Continued (From: Ref 16)

APPENDIX B: AN50E SYSTEM 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	½	12	6	5.7
	BPSK	¾	12	9	8.6
	QPSK	½	24	12	11.5
	QPSK	¾	24	18	17
	16 QAM	½	48	24	22
	16 QAM	¾	48	36	33
	64 QAM	⅔	72	48	43
	64 QAM	¾	72	54	48
Maximum Tx Power	+20 dBm (region dependent)				
Rx Sensitivity	-86 dBm at 6 Mbps (based on BER of $1x10^{-6}$)				
IF Cable	• Maximum length up to 250 ft (76m) using RG6U / 500 ft (152m) using high-grade RG11U				
Network Attributes	• Transparent bridge • DHCP passthrough • VLAN passthrough • 802.1q (point to point mode)				
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) Dynamic Adaptive Coding (bi-directional) auto selects: ½, ⅔, ¾				
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	• Point to Point or Point to Multipoint • Automatic Repeat Request (ARQ) error correction • Concatenation/Fragmentation				
Max Range	Range varies with each antenna gain, and modulation rate selected. • Over 10 km / 6 miles non-line-of sight • Over 80 km / 50 miles line-of-sight • Up to 30 km / 19 miles Point to Multipoint				
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 15. AN50e System Specifications (From: Ref 29)

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. "3Com Superstack 3 Switch 4226T 24-Port Plus 2 10/100/1000," Product Details [online] available from http://www.3com.com/products/en_US/detail.jsp?tab=prodspec&sku=3C17300-US&pathtype=purchase; Internet; accessed 14 September 2005.

2. Alberts, David, John Garstka and Frederick Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd ed., (CCRP, August 1999).

3. "AN50e Broadband Wireless System," *Data Sheet* [online]; available from http://www.redlinecommunications.com/products/an50/an50e.pdf; Interenet; accessed 14 September 2005.

4. "ARQ," *Wikipedia* [online]; available from http://en.wikipedia.org/wiki/ARQ; Internet; accessed 24 August 2005.

5. "Automated Digital Network System (ADNS)," *GlobalSecurity.org* [online]; available from http://www.globalsecurity.org/military/systems/ship/systems/adns.htm; Internet; accessed 15 July 2005.

6. Bedell, Paul, *Wireless Crash Course*, (New York: McGraw Hill, 2005): 476.

7. Burns, Paul, "Australian Defence Organisation CDR-01 Internet Protocol (IPv6) Transition Plan," Ball Solutions Group, Issue 1, Revision 1.5 (29 July 2005).

8. Chairman Joint Chiefs of Staff, General Henry H. Shelton. Director for Strategic Plans and Policy. Strategy Division. *Joint Vision 2020*, (Washington, D.C.: Government Printing Office, June 2000): 7.

9. Chief of Naval Operations, Admiral Vern Clark. "Sea Power 21: Projecting Decisive Joint Capabilities," *Proceedings* [online]; available from http://www.chinfo.navy.mil/navpalib/cno/proceedings.html; Internet; accessed 8 July 2005.

10. Chief of Naval Operations. Secretary of the Navy. Commandant of the Marine Corps. *Department of the Navy Information Management & Information Technology Strategic Plan FY 2004-2005*, (Washington, D.C.: Government Printing Office, 2005).

11. Cisco 3600 Series Multifunction Platforms (3620 and 3640/3640A), *Data Sheet* [online] available from http://www.cisco.com/en/US/products/hw/routers/ps274/products_data_sheet09186a0080091f6f.html; Internet; accessed 14 September 2005.

12. "CODEC," *Wikipedia* [online]; available from http://en.wikipedia.org/wiki/Codec; Internet; accessed 24 August 2005.

13. "Cyclic Redundancy Check," *Wikipedia* [online]; available from http://en.wikipedia.org/wiki/Cyclic_redundancy_check; Internet; accessed 24 August 2005.

14. *Department of Defense Dictionary of Military and Associated Terms*, (Washington, D.C.: Government Printing Office, 12 April 2001).

15. Farance, Frank, "SUO: Semantic Interoperability," [online]; available from http://grouper.ieee.org/groups/suo/email/msg07565.html; Internet; accessed 26 May 2005.

16. IEEE, "802.16: IEEE Standard for Local and Metropolitan Networks," Institute of Electrical and Electronic Engineers, October 2004.

17. "Interoperability," *Dictionary.com* [online]; available from http://dictionary.reference.com/search?q=interoperability; Internet; accessed 26 May 2005.

18. Ixia "WLAN Testing with IxChariot: Sample Test Plans," 2004.

19. Ixia, "Three Rules for Successful IxChariot Testing," 2004.

20. Ixia, "Triple Play Testing with IxChariot," 2005.

21. "Jitter," *Wikipedia* [online]; available from http://en.wikipedia.org/wiki/Jitter; Internet; accessed 24 August 2005.

22. "Latency," *Wikipedia* [online]; available from http://en.wikipedia.org/wiki/Latency; Internet; accessed 24 August 2005.

23. McNamara, J., "EXCOMM Airborne FORCEnet Overview," Computer Systems Center, Inc., (15 April 2005).

24. "Mean Opinion Score," *Wikipedia* [online]; available from http://en.wikipedia.org/wiki/MeanOpinionScore; Internet; accessed 24 August 2005.

25. Miller, R. B., "Response time in Man-computer Conversational Transactions," *Proceedings AFIPS Fall Joint Computer Conference* Vol. 33 (1968): 267-277.

26. Nair, Govindan et al., "IEEE 802.16 Medium Access Control and Service Provisioning," *Intel Technology Journal*, Volume 8, Issue 3 (August 2004):213-228.

27. Nielson, Jakob, *Usability Engineering*, The Morgan Kaufmann Series in Interactive Technologies (San Diego, Academic, 1993), 135.

28. “Quality of Service,” *Wikipedia* [online]; available from http://en.wikipedia.org/wiki/Quality_of_service; Internet; accessed 24 August 2005.

29. Redline Manual

30. “Response Time,” *Wikipedia* [online]; available from http://en.wikipedia.org/wiki/Response_time; Internet; accessed 24 August 2005.

31. “Throughput,” *Wikipedia* [online]; available from http://en.wikipedia.org/wiki/Throughput; Internet; accessed 24 August 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

GLOSSARY

The following are all from Ref 16 unless otherwise annotated.

Base Station (BS): A generalized equipment set providing connectivity, management, and control of the SS.

Codec: Codec is a portmanteau of either Compressor-Decompressor or Coder-Decoder, which describes a device or program capable of performing transformations on a data stream or signal. Codecs can both put the stream or signal into an encoded form (often for transmission, storage or encryption) and retrieve, or decode that form for viewing or manipulation in a format more appropriate for these operations. Codecs are often used in videoconferencing and streaming media solutions. (From Ref: 12)

Connection Identifier (CID): A 16-bit value that identifies a connection to equivalent peers in the MAC of the BS and SS. It maps to a service flow identifier (SFID), which defines the QoS parameters of the SF associated with that connection. SAs also exist between keying material and CIDs.

Downlink (DL): The direction from the BS to the SS.

Downlink Map (DL-MAP): A MAC message that defines burst start times for both time division multiplex and TDMA by an SS on the downlink.

Dynamic Service: The set of messages and protocols that allow the BS and SS to add, modify, or delete the characteristics of a service flow.

Jitter: In Telecommunication, jitter is an abrupt and unwanted variation of one or more signal characteristics, such as the interval between successive pulses, the amplitude of successive cycles, or the frequency or phase of successive cycles. (From Ref: 13)

Mean Opinion Score (MOS): In voice communications, particularly Internet telephone, the mean opinion score (MOS) provides a numerical measure of the quality of human speech at the destination end of the circuit. The scheme uses subjective tests (opinionated scores) that are mathematically averaged to obtain a quantitative indicator of the system performance. To determine MOS, a number of listeners rate the quality of test sentences read aloud over the communications circuit by male and female speakers. A listener gives each sentence a rating as follows: (1) bad (2) poor (3) fair (4) good (5) excellent. The MOS is the arithmetic mean of all the individual scores, and can range from 1 (worst) to 5 (best). (From: Ref 24)

Mesh (MSH): Network architecture, wherein systems are capable of forwarding traffic from and to multiple other systems.

Packing: The act of combining multiple SDUs from a higher layer into a single MAC PDU.

Point to Point (PtP): A mode of operation whereby a link exists between two network entities.

Protocol Data Unit (PDU): The data unit exchanged between peer entities of the same protocol layer. On the downward direction, it is the data unit generated for the next lower layer. On the upward direction, it is the data unit received from the previous lower layer.

Security Association (SA): The set of security information a BS and one or more of its client SSs share in order to support secure communications. This shared information includes traffic encryption keys and cipher block chaining initialization vectors.

Service Data Unit (SDU): The data unit exchanged between two adjacent protocol layers. On the downward direction, it is the data unit received from the previous higher layer. On the upward direction, it is the data unit sent to the next higher layer.

Subscriber Station (SS): A generalized equipment set provicing connectivity between subscriber equipment and a BS.

Uplink (UL): The direction from an SS to the BS.

Uplink Channel Descriptor (UCD): A MAC message that describes the PHY characteristics of a UL.

Uplink Map (UL-MAP): A set of information that defines the entire access for a scheduling interval.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dan Boger
   Naval Postgraduate School
   Monterey, California

4. Rex Buddenberg
   Naval Postgraduate School
   Monterey, California

5. John Gibson
   Naval Postgraduate School
   Monterey, California

6. Ed Hucke
   Science Applications International Corporation
   San Diego, California

7. Sean Vuong
   Space and Naval Warfare Systems Command
   San Diego, California

8. Yau Keung Hom
   Space and Naval Warfare Systems Command
   San Diego, California