2011-09

Leveraging an SNMP agent in terminal equipment for network monitoring of U. S. Navy SATCOM

McLaughlin, Robert D.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

LEVERAGING AN SNMP AGENT IN TERMINAL EQUIPMENT FOR NETWORK MONITORING OF U. S. NAVY SATCOM

by

Robert D. McLaughlin, Jr.

September 2011

Thesis Advisor:	Alex Bordetsky
Second Reader:	Glenn Cook

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Leveraging an SNMP Agent in Terminal Equipment for Network Monitoring of U.S. Navy SATCOM		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Robert D. McLaughlin, Jr.			
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)		**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. IRB Protocol number N.A.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

This research describes and analyzes a United States Navy Satellite Communications (SATCOM) performance monitoring model in providing status information to a network monitoring console to support naval operations. The environment is characterized by potentially adverse conditions that affect satellite performance.

Current SATCOM systems are unable to provide performance information to the network's performance monitor because they are not Simple Network Management Protocol (SNMP) enabled and not integrated into the routable network. A network monitoring model defined by sense, decide, and act is central to this study. It represents enhanced monitoring by the subscriber station's monitor console for naval shipboard operations. This model delivers operational and RF environmental information to the SNMP MIB environment so that commonly used SNMP agents can request and send information for sending proper messages to the network's performance monitoring system.

The proposed solution is explored through analysis of existing monitoring models together with observations of a tactical networking field experiment, in which equipment at the edge of the network and subscriber's SATCOM terminal is monitored for gathering critical performance details.

14. SUBJECT TERMS Satellite Communications, ADNS, Master Station, Base Station, Subscriber Station, Terminal, Modem, SNMP, MIB, Monitoring, Sensors, RF Environment, RF Interference, Routable Network, SNMP Agent, SNMP Manager, Fault Monitoring, Remote Monitoring (RMON), Tactical Network Topology (TNT), Maritime Interdiction Operations (MIO), 8th Layer	**15. NUMBER OF PAGES** 131
	16. PRICE CODE

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

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

LEVERAGING AN SNMP AGENT IN TERMINAL EQUIPMENT FOR NETWORK MONITORING OF U. S. NAVY SATCOM

Robert D. McLaughlin, Jr.
Lieutenant Commander, United States Navy
B.B.A., Memphis State University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2011

Author: Robert D. McLaughlin, Jr.

Approved by: Alex Bordetsky
Thesis Advisor

Glenn Cook
Second Reader

Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This research describes and analyzes a United States Navy Satellite Communications (SATCOM) performance monitoring model in providing status information to a network monitoring console to support naval operations. The environment is characterized by potentially adverse conditions that affect satellite performance.

Current SATCOM systems are unable to provide performance information to the network's performance monitor because they are not Simple Network Management Protocol (SNMP) enabled and not integrated into the routable network. A network monitoring model defined by sense, decide, and act is central to this study. It represents enhanced monitoring by the subscriber station's monitor console for naval shipboard operations. This model delivers operational and RF environmental information to the SNMP MIB environment so that commonly used SNMP agents can request and send information for sending proper messages to the network's performance monitoring system.

The proposed solution is explored through analysis of existing monitoring models together with observations of a tactical networking field experiment, in which equipment at the edge of the network and subscriber's SATCOM terminal is monitored for gathering critical performance details.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Dr. Alex Bordetsky for his thought provoking conversations during the Tactical Network Topology (TNT) experimentation exercisers. I have gained greater understanding and experience through his innovative ideas and knowledge of network systems. I would like to express my sincere gratitude to Professor Glenn Cook for his guidance and leadership. I would also like to thank CPT. Joseph Collins (USMC) for his friendship and understanding during the difficult times I experienced during my time at the Naval Postgraduate School. Without his support, I would never have completed this thesis. Finally, I would like to dedicate this thesis to the most significant individual in my life; my wife, Yun Mi Woo-McLaughlin, for her unconditional love and constant support during the long hours of study required to accomplish this lofty goal.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

8-PSK	8-Phase Shift Key
16-APSK	16-Amplitude Phase Shift Key
ACTS	Advanced Communications Technology Satellite
ADNS	Automated Digital Network System
AOR	Area of Responsibility
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
ASCM	Anti-Ship Cruise Missile
ATM	Asynchronous Transfer Mode
AT&T	American Telephone & Telegraph Corporation
BE	Best Effort
BPSK	Binary Phase Shift Keying
BS	Base Station
BW	Bandwidth
C4I	Command, Control, Communications, Computers and Intelligence
CDMA	Code Division Multiple Access
CENETIX	Center for Network Innovation and Experimentation
CIC	Combat Information Center
CJCS	Chairman Joint Chief Staff
CNO	Chief of Naval Operations
COC	Combat Operations Center
CODEC	Coder-Decoder
COTS	Commercial Off-the-Shelf
CRC	Cyclic Redundancy Check
DAMA	Demand Assigned Multiple Access
DDP	Datagram-Delivery Protocol
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DL	Downlink
DMR	Digital Modular Radio

DNS	Domain Name Server
DoD	Department of Defense
DSC	Dynamic Service Change
DSCS	Defense Satellite Communication Systems
DTE	Data Terminal Equipment
DWTS	Digital Wideband Transmission System
EBEM	Enhanced Bandwidth Efficient Modem
EHF	Extremely High Frequency
ESEM	Ethernet Service Expansion Module
ESP	Encapsulating Security Payload
EW	Electronics Warfare
FCC	Federal Communications Commission
FEC	Forward Error Correction
FPS	Frames Per Second
FTP	File Transfer Protocol
GBS	Global Broadcast Service
GENSER	General Service
GEO	Geostationary Earth Obit
GIG	Global Information Grid
GIG-E	Gigabit Ethernet
GOTS	Government Off-the-Shelf
GPS	Global Positioning System
GRC	Ground Radio Communications
GSN	Gigabit Satellite Network
GUI	Graphical User Interface
HF	High Frequency
HP	Hewlett Packard
HPA	High Power Amplifier
HTTP	Hypertext Transfer Protocol
IBS	Intelsat Business Service
ICMP	Internet Control Message Protocol
ID	Identification

IDR	Intermediate Data Rate
IEEE	Institute of Electrical and Electronic Engineers
IF	Intermediate Frequency
ifDiscr	if description
IFF	Identification of Friend or Foe
INE	In-line Network Encryptors
INM	Integrated Network Manager
IP	Internet Protocol
IPSEC	IP Security
IPX	Internet Packet Exchange
IR	Infrared
ISO	International Organization for Standardization
IT	Information Technology
ITA	Information Throughput Adaptation
ITP	Integrated Terminal Program
JMCOMS	Joint Maritime Communications
JPEG	Joint Photographic Experts Group
JTRS	Joint Tactical Radio System
Kbps	Kilobits per second
KG	Key Generator
L-3	L-3 Communications CyTerra Corporation
LAN	Local Area Network
LDPC	Low-Density Parity-Check
LLC	Logical Link Control
LNA	Low Noise amplifier
LNB	Low Noise Block
LOS	Line-of-Sight
LSB	Least Significant Bit
MAC	Media Access Control
MAN	Metropolitan Area Network
MAP	Map
Mbps	Megabit per second

MEO	Medium Earth Orbit
MHz	Megahertz
MIB	Management Information Base
MIL	Military
Milstar	Military Strategic and Tactical Relay
MIO	Maritime Interdiction Operations
MODEM	Modulator Demodulator
MPEG	Moving Pictures Expert Group
MSB	Most Significant Bit
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCTAMS	Naval Computer and Telecommunications Area Master Station
NCW	Network Centric Warfare
NDI	Non-Developmental Item
NIPERNET	Non-secure Internet Protocol Router Network
NLOS	Non-Line-of-Sight
NMIOTC	Maritime Interdiction Operational Training Center
NMT	Network Management Terminal
NNTP	Network News Transfer Protocol
NOC	Network Operations Center
NPM	Network Performance Monitor
NPS	Naval Postgraduate School
NTP	Naval Telecommunications Procedures
nuc	Nuclear
NWC	Network Centric Warfare
OFDM	Orthogonal Frequency Division Multiplexing
OID	Object Identifier
OQPSK	Orthogonal Quadrature Phase Shift Keying
OS	Operating System
OSI	Open System Interconnection
OTH	Over The Horizon
P2P	Peer-to-peer

PDU	Protocol Data Unit
PHY	Physical Layer
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PKI	Public Key Infrastructure
PMP	Point-to-Multipoint
POP3	Post Office Protocol Version 3
PPP	Point-to-Point Protocol
PtP	Point-to-Point
QAM	Quadrature Amplitude Mode
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
rad	Radiation
RCA	Radio Corporation of America
REG	Registration
REQ	Request
RF	Radio Frequency
RFC	Request for Comment
RFI	Radio Frequency Interference
RMON	Remote Monitoring
RNG	Ranging
R&S	Routing and Switching
RSP	Response
RX	Receiver
SA	Security Association
SAT	Satellite
SATCOM	Satellite Communications
SBC	Subscriber Station Basic Capability
SCPC	Single Channel Per Carrier
SDU	Service Data Unit
SF	Service Flow

SFID	Service Flow Identifier
SHF	Super High Frequency
SIP	Session Initiation Protocol
SIPRNET	Secure Internet Protocol Router Network
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SONET	Synchronous Optical Networking
SRBOC	Super Rapid Blooming Off-board Chaff
SS	Subscriber Station
SSPA	Solid-State Power Amplifies
STD	Standard
STEP	Standard Tactical Entry Point
SYNCOM	Synchronous Communication Satellite
TacLANE	Tactical Local Area Network Encryption
TAO	Tactical Action Officer
TCP	Transmission Control Protocol
TDMA	Time-Division Multiple Access
TEK	Traffic Encryption Key
TFTP	Trivial File Transfer Protocol
TNT	Tactical Network Topology
TWT	Traveling-wave Tube
TX	Transmitter
UCD	Uplink Channel Descriptor
UDP	User Datagram Protocol
UFO	UHF Follow-On
UHF	Ultra High Frequency
UL	Uplink
U.S.	United States
USU	United States Navy
VHF	Very High Frequency

VoIP	Voice Over Internet Protocol
VTC	Video Teleconference
WAN	Wide Area Network
WMI	Windows Management Instrumentation
WWW	World-Wide Web

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE OF STUDY

The purpose of this study is to determine the best method that can be used to provide the subscriber station's network monitor console the ability to monitor the satellite terminals operational status through the use of a Simple Network Management Protocol (SNMP) agent.

B. THESIS QUESTIONS

The thesis will attempt to answer the following questions:

- What U.S. Navy environmental sensors and monitoring tools are used to monitor a satellite terminal's status and environment?
- Are SNMP Agents implemented on U.S. Navy satellite station terminals?
- How can the U.S. Navy use SNMP concepts to monitor a satellite terminal's operational status?

C. SCOPE AND LIMITATIONS

The goal of this thesis is to identify a way to provide the subscriber's network monitoring consol the ability to monitor the subscriber's satellite terminal operational status through the use of an SNMP Agent. This study will include, but is not limited to, fault and environmental monitoring capabilities for U.S. Navy satellite communications systems and related terminals, SNMP and SNMP Agents on these systems, and the management information bases (MIBs) associated with network monitoring.

D. MAJOR CONTRIBUTIONS OF THIS THESIS

The benefits of this research provide a method for sending the subscriber terminal's operational status to the subscriber's network monitoring console. In addition, this research results in providing an example SNMP agent for improving the monitoring capability of the U.S. Navy satellite communications equipment.

E. BACKGROUND

Satellite systems provided a large portion of the commercial long distance connectivity in earlier times. Today's Navy Satellite Communications (SATCOM) systems are primarily used for extending the reach for communications to mobile platforms and satisfy the need for ad hoc connectivity. SATCOM provides the necessary physical medium for making the connection between two access points (stations) possible however satellite components are not part of a routable network.

Network and satellite systems work totally independent of each other without recognizing that the other exists. Neither the subscriber or base station terminal equipment has been integrated into the Internet's routable network; they simply hang off of the edge of the network to extend a pathway for data to flow between specific access points. The routable network behind the subscriber and base stations is not visible by the routable network and the routers only identify the path by which data flows over the connection from one router to the next. Any routable network, when a connection is broken, the routing is updated to reflect the change allowing the data to continue to flow.

Satellite base stations and subscriber stations have no backchannel and are not seen by the routable network. In addition, the U.S. Navy has not developed SATCOM systems to be adaptable to adverse environments. One might ask, "Why should the subscriber or base station need environmental sensors?" The answer, in short, is to be able to adapt to the environment as it changes. The stations need to be able to sense interference and adapt to the changing environment for sustaining any portion of the vital link. Therefore, the intent of this research is to analyze the SATCOM system, available sensors, and network monitoring tools for fully integrating a satellite monitoring capability into the U.S. Navy's routable network monitoring capability. As a result, the satellite suite should achieve greater flexibility for sustaining the extended Internet during times of less than favorable conditions.

The United States Navy has a need for providing SATCOM with the ability to sustain the extended Internet even if the subscriber station's satellite transmitter was to fail or if a significant amount of Radio Frequency Interference (RFI) rendered the

transmit capability ineffective. Unfortunately, the subscriber station does not have the ability to monitor their satellite terminal status (fault monitoring) or the ability to monitor the operational RF environment of the terminal (RFI monitoring) for interference that would limit performance. In addition, the network monitoring tools deployed by the subscriber's network support team can only monitor the status of known nodes, of which the satellite terminal is not included. Therefore, the routable network behind the satellite connection cannot monitor the satellite terminal status.

F. ORGANIZATION OF THE THESIS

This thesis is organized into the following chapters:

Chapter I: Introduction

This chapter provides a general outline of the work and the fines of the problem addressed by this research.

Chapter II: Background

This chapter provides a brief history of both commercial and satellite systems and presents basic information necessary to gain a better understanding of satellite communications.

Chapter III: Network Management

This chapter provides a brief history of the Internet and presents information necessary to gain a better understanding of routable networks, ADNS, environmental sensors, network monitoring tools, an SNMP agent available for supporting satellite communications systems, RMON, and the concept of the 8th Layer.

Chapter IV: Analysis of Management Capabilities

This chapter will provide an analysis of the network monitoring capabilities of U.S. Navy SATCOM and the available technologies discussed in Chapters II and II.

Chapter V: Case-Studies

This chapter discusses two field experiments (Tactical Network Topology [TNT] and Maritime Interdiction Operations [MIO]), focused on how to monitor an SHF satellite link and extended network using SNMP means and .

Chapter VI: Conclusion

This chapter provides analysis findings, the conclusion, and recommendations for a possible way ahead. In addition, this chapter discusses further research identified from ideas and questions raised during the thesis.

II. BACKGROUND

Satellite communications (SATCOM) are the life-blood for vital naval messaging and intelligence data essential to achieving successful mission accomplishment for the United States Navy's afloat forces and other mobile customers in support of the United States' national security. SATCOM systems need the capability of being monitored by the subscriber's network monitoring tools that already exist. This chapter provides the background necessary to gain a better understanding of SATCOM and how its components operate in order to focus on monitoring the essential elements of the system.

A. SATELLITE HISTORY

Satellite communications has been in existence for a relatively short time. It is important to understanding that this form of communications came on stage at different era than the Internet, having distinctive and special operational requirements, but for similar purposes as the Internet. From the start of Satellite communications in 1945 with Arthur C. Clarke's article, "Extra-Terrestrial Relays," this technology has grown independently of other forms of communications with a unique design (Whalen, n.d.).

Since 1945, there have been numerous milestones in its development. The following paragraphs briefly discuss historical satellite and Internet chronological events.

1. Commercial Satellites

In the fall of 1945, Arthur C. Clarke, an electronics officer in the Royal Air Force, wrote an influential article describing television programming provided by manned satellites orbiting above the earth (Whalen, n.d.). In a speech in 1954, and followed by an article in 1955, AT&T's Bell Telephone Laboratories' John R. Pierce thoroughly explained the advantages of a "communications 'mirror' in space, a Medium Earth Orbit (MEO) 'repeater' and a Geostationary orbiting (GEO, 24-hour) 'repeater'" (Whalen, n.d.). In 1960, the Federal Communications Commission (FCC) received a request from AT&T to launch an experimental communications satellite (Whalen, n.d.). As a result,

AT&T built its own TELSTAR satellite, a MEO vehicle, by 1961 (Whalen, n.d.). In addition, the National Aeronautics and Space Administration (NASA) awarded RCA a contract to build RELAY, an active MEO communications satellite. AT&T also contracted Hughes Aircraft Company for the construction of SYNCOM, a GEO satellite (Whalen, n.d.). These efforts resulted in the successful operation of two TELSTARs, two RELAYs, and two SYNCOMs by 1964 and the launch of EARLY BIRD on April 6, 1965 (Whalen, n.d.). This was the beginning of man's interest in Global satellite communications (Whalen, n.d.).

NASA headed in the right direction as it moved towards the development of the Advanced Communications Technology Satellite (ACTS) that include Simple Network Management Protocol (SNMP) interfaces into satellite and transmission equipment. ACTS will be part of the NASA and ARPA joint sponsored development of the Gigabit Satellite Network (GSN) (Bergamo & Hoder, n.d.). "Typical applications will include connection of distributed SONET/ATM fiber 'islands' over satellite, wide-area distributed supercomputer networking, high-definition digital TV, and high-speed file transfer" (Bergamo & Hoder, n.d.). "Management of the network is performed using a Network Management Terminal (NMT) and is based on standard SNMP and Internet protocols. The earth stations can also be remotely monitored and controlled via the satellite channel or via the terrestrial Internet (Bergamo & Hoder, n.d.). Through NASA's research and development of ACTS, satellite technology has begun to be a true extension of the Internet rather than a piece of equipment hanging off of it. For a Selective Communications Satellite Chronology, see Appendix A.

2. Military Satellites

United States military satellite saw its beginning with the Army accomplishing RADAR contact with the moon in 1946 (Martin, n.d.*a*). "In 1954, the Navy began communications experiments using the moon as a reflector, and by 1959, it had established an operational communication link between Hawaii and Washington, D.C." (Martin, n.d.*a*).

The Department of Defense (DoD) began satellite communication systems development in the 1960s alongside of the U.S. space program (Martin, n.d.*a*). In addition, the DoD had to consider unique military operational requirements such as protecting against signal jamming, providing service to global regions previously unsupported and management of system resources as required (Martin, n.d.*a*).

In the article "A History of U.S. Military Satellite Communications Systems" Donald H. Martin states that "the first U.S. military communication satellites were of an experimental nature and used low-altitude orbits" (Martin, n.d.*a*). "They were developed to provide basic experience with satellites and to explore what satellite communications could do" (Martin, n.d.*a*). Actual military use would come about later.

Significant events showing the chronology of Military Communications Satellites from 1945 to 2010 are illustrated by Figures 1 and 2.

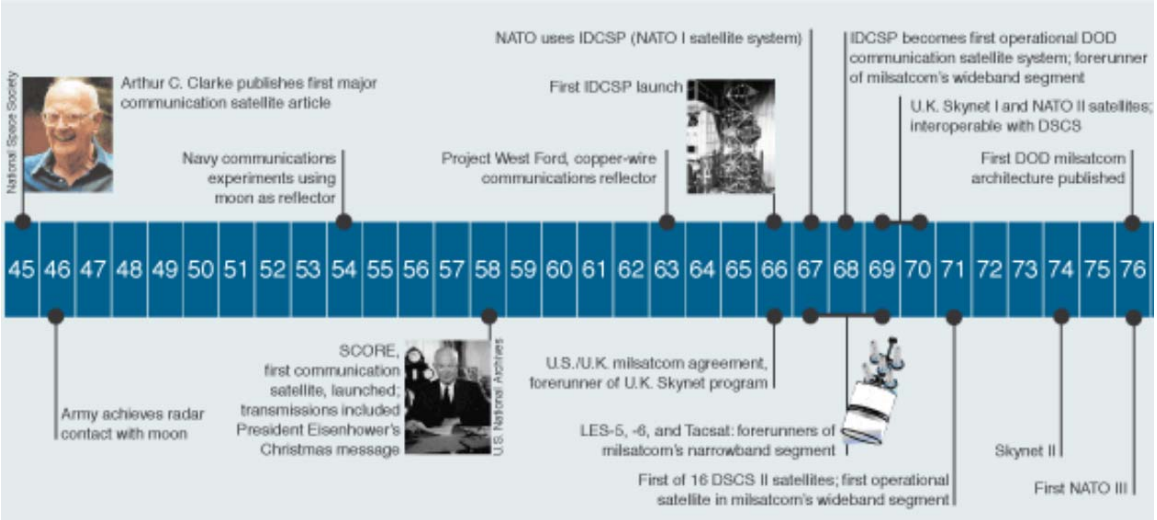

Figure 1. Military Communications Satellites from 1945 to 1976
(After Martin, n.d.*b*)

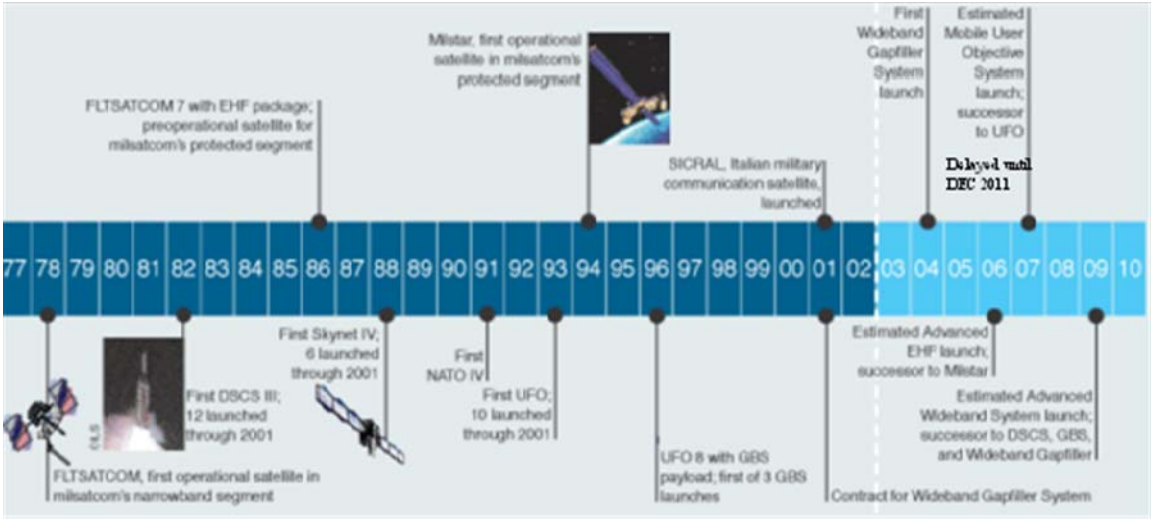

Figure 2. Military Communications Satellites from 1977 to 2010 (After: Martin, n.d.*b*)

Martin focuses on the improvements and growth of satellite technology (Martin, n.d.*a*). He states that:

- "U.S. military satellite communications have improved and expanded greatly over the past four decades, from SCORE through DSCS III, UFO, and Milstar" (Martin, n.d.*a*).
- "Capabilities have grown dramatically with the development of satellite and electronics technologies" (Martin, n.d.*a*).
- "Higher-power and wider-bandwidth satellites have enabled increased information transmission to an ever-wider assortment of terminal types deployed with an increasing number and variety of military units" (Martin, n.d.*a*).

Martin explains that "as military satellite communication systems improve, they continue to provide information superiority to the U.S. military. This enables our military forces to remain dominant in the increasing speed and diversity of their actions during times of peace as well as times of conflict" (Martin, n.d.*a*).

See Appendix B for a Selective Military Satellite Chronology, which supports the growth of SATCOM technology.

B. WHAT SATCOM COMPONENTS TO MONITOR

There are many functions executed to sustain a satellite communications connection. It is important to understanding the intricacies of how satellite terminals make the physical connection between mobile or fixed sites and a Master Station, also known as the Earth Terminal. In addition, it is very important to have a clear understanding of the system as a whole and how it operates. Understanding is the key to finding the solution for monitoring the extended internet using SATCOM terminals.

To better understand the entire SATCOM picture, this chapter will explain some basic parts of the satellite connection that extends the Internet through the use of satellite systems. This chapter will include the functions of the bent pipe / transponder satellite relay, the terminal equipment, and modem operation during transmit and receive.

Through laying a solid foundation for understanding the current technology in place today, the possibilities of future implementations can be more clearly understood. Therefore, the new management concept presented in this thesis can become a satellite communications equipment management reality.

1. The “Bent Pipe”

Satellites are used for relaying data back and forth between mobile terminals and Earth Terminals like a “bent pipe” would redirect the flow of water. The “bent pipe” concept represented in Figure 3 is a transponder that acts as a repeater based on using a medium for sending a received data stream back to the earth (Roddi, 2001, p. 587).

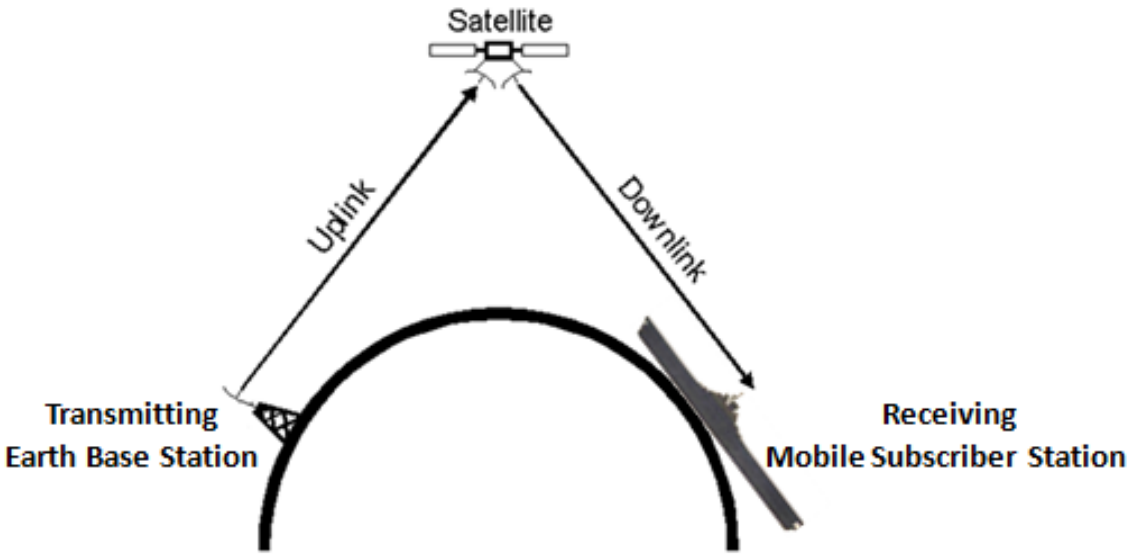

Figure 3. Basic "Bent Pipe" Representation (After "SatCom basics tutorial," n.d.)

In the case of satellite unprocessed relays, the only processing performed on the RF signal is a change in the RF frequencies used for terrestrial uplink to downlink or satellite-to-satellite crosslink and the amplification of the RF signal so the transmission can reach its intended access point (Roddi, 2001, p. 587). The earth station transmitter will send signals to the satellite receiver as an uplink. The received uplink signals will be down converted, amplified by the High Power Amplifier (HPA), and then transmitted down to the earth station receiver by the satellite ("IP Basic Course," 2008, p. 5-32). Filtering is performed to reduce noise in the re-transmitted signal, frequency conversion is accomplished to separate the uplink and downlink, and amplification is performed to compensate for path losses ("IP Basic Course," 2008, p. 5-32).

The majority of communication satellites are orbital relays that carry several transponders (Roddi, 2001, p. 587). The transponder, illustrated in Figure 4, is a piece of the communications satellite that creates the channel formed between a transmit and a receive antenna by a string of interconnected functional circuits (Roddi, 2001, p. 587).

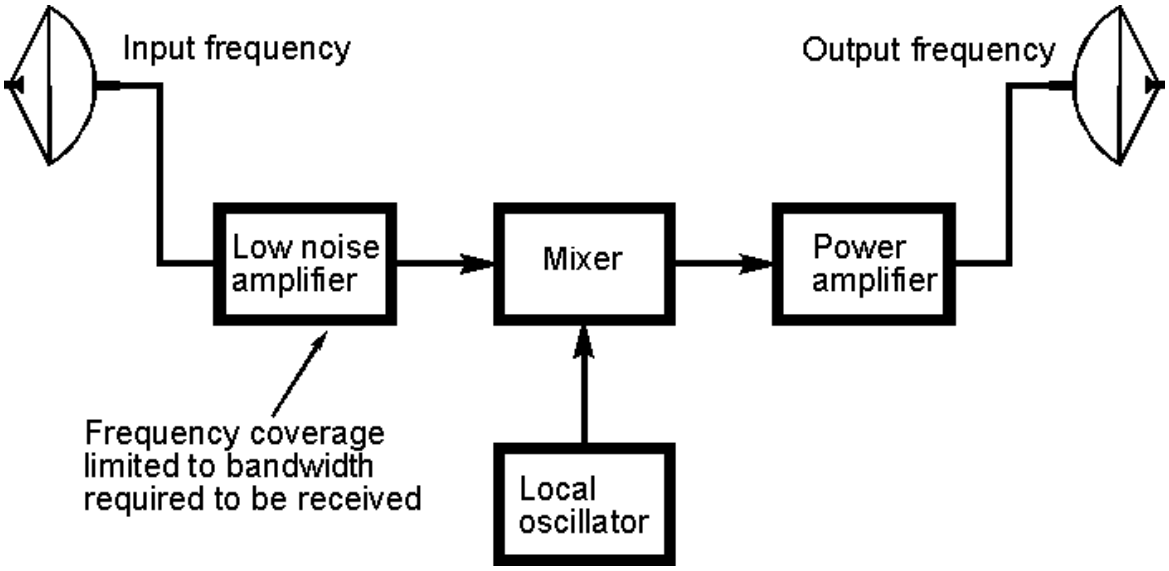

Figure 4. Basic Satellite Transponder Block Diagram (After "SatCom basics tutorial," n.d.)

Donald Roddi describes the typical composition of a transponder in his book "Satellite Communications" as:

- "An input and output band pass filter; for eliminating noise created from frequencies outside the usable bandwidth" (Roddi, 2001, p. 587).
- "A LNA; for amplifying the very weak receive signal that has been attenuated due to the distance the RF signal travels from the earth station to the satellite" (Roddi, 2001, p. 587).
- "A frequency converter; for changing the received signal (satellite uplink) to the transmit signal (satellite downlink) frequency" (Roddi, 2001, p. 587).
- "A power amplifier (either TWT or solid state); for increasing the strength of the signal to be transmitted" (Roddi, 2001, p. 587).

In some cases, satellites possess the ability to demodulate, decode, encode and then modulate the received signal (Roddi, 2001, p. 587). Figure 5 shows a comparison between a basic retransmitted signal from transponder satellites and a signal that is processed on-board for re-transmission. Satellites with on-board processing functionality possess a variety of transponder known as "regenerative" (Roddi, 2001, p. 587). This

type of on-board processing capability is very advantageous but also much more expensive while increasing the complexity of the circuitry placed aboard the satellite (Roddi, 2001, p. 587).

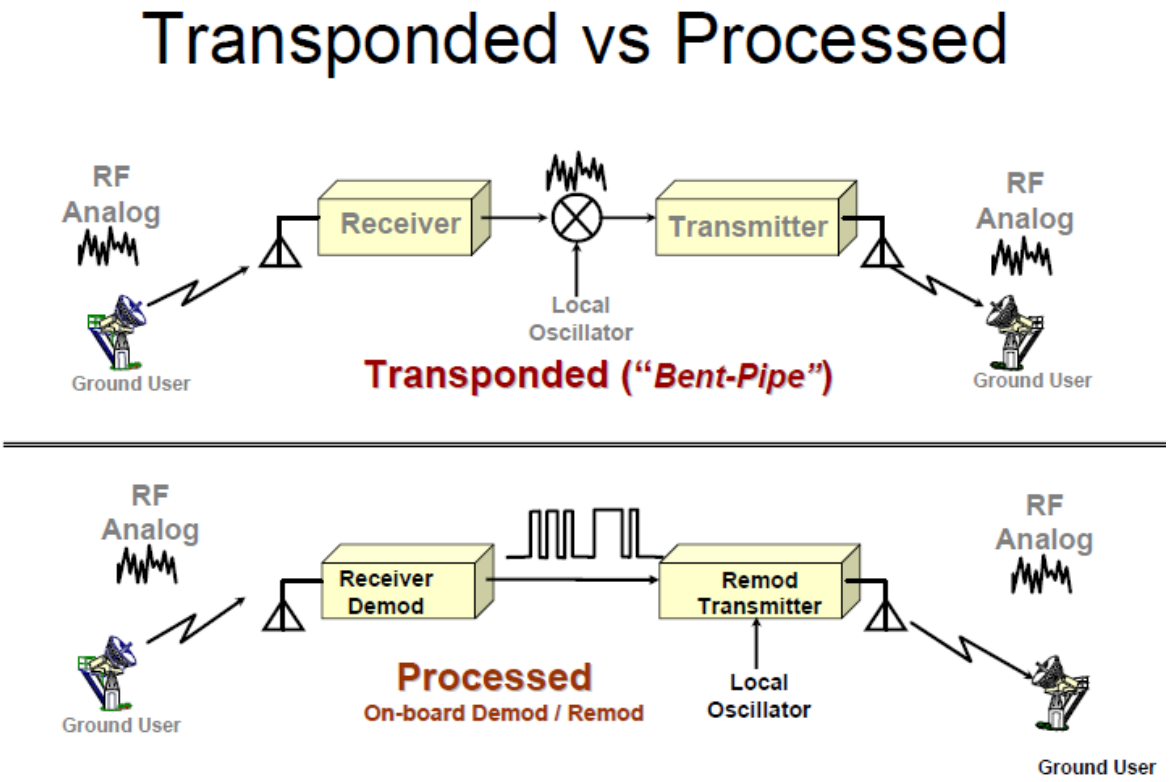

Figure 5. Transponder vs. Processed (From "IP Basic Course," 2008, p. 5-32)

Satellites with on-board processing handle the uplink and downlink signals autonomously ("IP Basic Course," 2008, p. 5-32). The noise and signal distortion is removed from the uplinked signal through the on-board processes ("IP Basic Course," 2008, p. 5-32). Once processed, "the reconstructed signals are then modulated, multiplexed, and up-converted to be transmitted at the downlink" ("IP Basic Course," 2008, p. 5-32). As a result, the link performance is increased and the receive signal at the subscriber station or base station is much cleaner ("IP Basic Course," 2008, p. 5-32).

2. Satellite Terminal Equipment

Satellite terminals, fixed or mobile, are standalone systems with a single access via line of sight to a specified access point known as a Base Station, Master Station, or Standard Tactical Entry Point (STEP) Site, as seen in Figure 6 ("SatCom Tutorial," 2007, p. 1).

Figure 6. Standard Tactical Entry Point (STEP) Site
(From "Earth Station" Card00742_fr.jpg, n.d.)

According to the Satellite Terminal Station Law and Legal Definition stated in 47 United States Code–Section 702, "the term 'satellite terminal station' refers to a complex of communication equipment located on the earth's surface, operationally connected with one or more terrestrial communication systems, and capable of transmitting telecommunications to or receiving telecommunications from a communications satellite system" ("Sat Term Sta Law & Legal Def," n.d.).

Both earth and mobile stations have many major subsystems which consist of the antenna, the transmitter chain, and the receiver chain ("SatCom Tutorial," 2007, p. 5). In addition to these subsystems, the master station has an environmental control system and the station control system ("SatCom Tutorial," 2007, p. 5). The antenna focuses radiated energy into a very concentrated narrow beam and directs this energy towards a satellite

located in a specified point in space (“SatCom Tutorial,” 2007, p. 5). In addition, the antenna directs incoming energy from the space based vehicle into the feed horn for further processing by the Low Noise Block (LNB) and receiver chain (“SatCom Tutorial,” 2007, pp. 5–6). The antenna equipment can discriminate (identify the difference) between transmitted and received Radio Frequency (RF) signals through specialized RF diverter known as a diplexer (“SatCom Tutorial,” 2007, pp. 5–6). The environmental control system provides the earth station equipment and antennas the necessary heating and cooling requirements in order to enable prolonged operations, while the station control system is used to control the azimuth and elevation pointing of the antenna, as well as the earth station (“SatCom Tutorial,” 2007, pp. 5, 12).

A terminal creates a medium for making the physical connection between mobile remote terminal and a master station access point, so that information/data can pass between them. The terminals function in producing this medium is through the up conversion to a Radio Frequency and the amplification of the RF signal, using a High Power Amplifier (HPA), for the transmitted signal to reach the satellite orbiting in space (“SatCom Tutorial,” 2007, p. 7–9). The terminal also performs down conversion of the received RF signal through the use of a Low Noise Block (LNB). The resulting Intermediate Frequency (IF) signal is sent to the modem for further processing (“SatCom Tutorial,” 2007, p. 10–11).

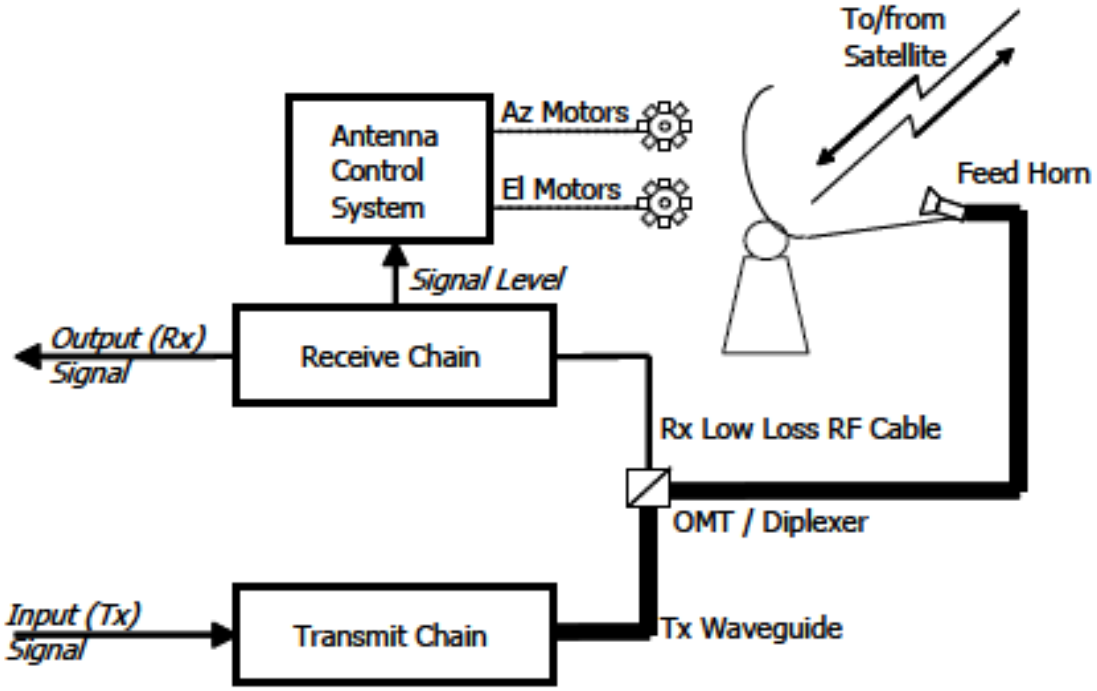

Figure 7. Terminal Equipment Block Diagram (From "SatCom Tutorial," 2007, p. 5)

The mobile satellite terminal block diagram provided in Figure 7 illustrates both transmit and receive paths, and the antenna control of the mobile system. In addition, the terminal equipment performs dish pointing and satellite tracking using the receiver's peak signal level, illustrated in Figure 7, so that the best RF signal is made available for the satellite termination ("SatCom Tutorial," 2007, p. 12–13).

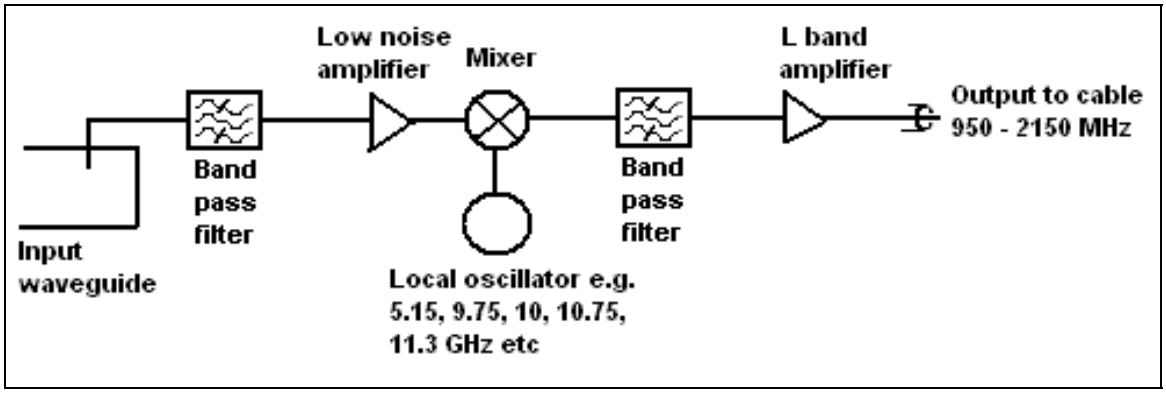

Figure 8. Low Noise Block (LNB) / Down Converter Diagram (From Johnston, 2007)

The LNB is a device in the receive side of a satellite dish that converts very low RF signals, received from the associated satellite, into a lower IF signal (Johnston, 2007). The processing of the received RF signal performed by the LNB is known as down converting (Johnston, 2007). Down converting is performed through the filtering, mixing, and amplification of the received signal, as seen in Figure 8 (Johnston, 2007).

Both stationary and mobile terminals use very similar, but have unique features for the platform they support due to size, frequency, and physical placement.

3. Modems

The word modem stands for modulator-demodulator. A modem is basically a piece of equipment that converts an incoming signal (either analog or digital data stream) into a usable signal ("Modem," n.d.). The modem uses the modulation of an analog carrier signal for the encoding of an incoming intelligible data stream, such as digital information, to produce an intermediate frequency (IF) that can be easily transmitted as a radio frequency (RF) signal ("Modem," n.d.). The modem demodulates a carrier signal to decode received information in order to reproduce the original information ("Modem," n.d.). To better understand how a modem functions a block diagram of a generic satellite modem is shown in Figure 9, so that the internal structure can be viewed ("Satellite Modem," n.d.).

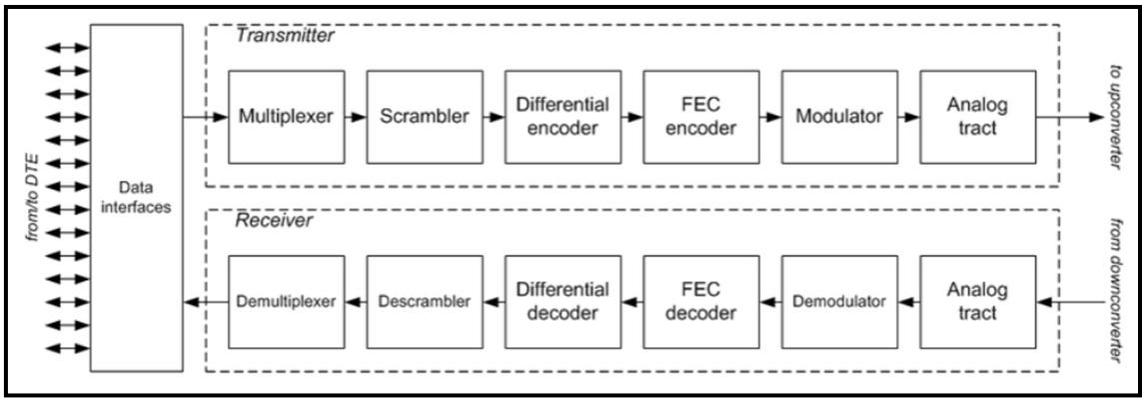

Figure 9. Generic Satellite Modem Block Diagram (From Satellite Modem, n.d.)

When looking at the modem transmitter function (Figure 9), Data Terminal Equipment (DTE) sends data to be transmitted via the Data interface, is multiplexed,

scrambled, Differential encoded, Forward Error Correction (FEC) encoded, modulated, sent through the Analog tract, which is a reconstruction filter, and then sent to the up converter for transmission ("Satellite Modem," n.d.). Similarly, the modem receiver performs several processes to the received signal from the down converter. The modem receiver section adjusts the IF signal and obtains envelope components in the Analog tract section, performs demodulation of the signal, decodes the FEC, performs Differential decoding, descrambles the signal, and then sends the demultiplexed data to the data interfaces ("Satellite Modem," n.d.).

This thesis refers to satellite modems which are used for establishing the data transfers using a communications satellite as a bent pipe, otherwise known as a relay ("Satellite Modem," n.d.). There is a broad variety of satellite modems available for satellite communications. There are some devices referred to as modems that only perform one of the two previously described functions (only modulate or demodulate, but not both) ("Satellite Modem," n.d.). Therefore, a modem with only a modulator is used for encoding data for the uplink or upload of a satellite and a modem with only a demodulator is used for decoding or downloading data from a satellite connection ("Satellite Modem," n.d.). In addition, modems can use many different types of modulation schemes, error correction codes, and framing formats. A few modulation schemes include, but are not limited to, Binary phase shift keying (BPSK), Quadrature Phase Shift Keying (QPSK), Orthogonal Quadrature Phase Shift Keying (OQPSK), and Quadrature Amplitude Modulation (QAM) ("Satellite Modem," n.d.). Popular error correction codes include Convolutional codes, Reed-Solomon codes, and superior error correction codes such as low-density parity-check (LDPC) and turbo codes ("Satellite Modem," n.d.). Some frame formats supported by a variety of satellite modems include Intelsat business service (IBS) framing, Intermediate data rate (IDR) framing, MPEG-2 transport framing, E1 and T1 framing ("Satellite Modem," n.d.). Modems are initially configured with these settings in order to use current satellite communications ("Satellite Modem," n.d.).

ViaSat, based out of Carlsbad, California, provides equipment and services for military and commercial communications, primarily in satellite related technologies,

currently provides the satellite terminal modems for the U.S. Navy (Freeman, 2009). ViaSat provides various standard modems for use in satellite communications.

Figure 10. MD-1366 Enhanced Bandwidth Efficient Modem (EBEM) (From "High Speed Modems," 2011)

The ViaSat MD-1366 Enhanced Bandwidth Efficient Modem (EBEM) shown in Figure 10 was chosen by the U.S. Government as "the new standard (MIL-STD-188-165B) for high-speed, high-performance, flexibility and compatibility in a Single Channel Per Carrier (SCPC) modem" ("MD-1366 EBEM," 2008-2011). The MD-1366 EBEM meets the requirements for high-speed satellite communications available for both military and commercial use ("High Speed Modems," 2011). This modem performs with satellite terminals operating at the X, C, Ku, and Ka band frequencies, supporting user data rates from 64 kbps to 155 Mbps ("High Speed Modems," 2011). The EBEM incorporates advanced modulation schemes such as BPSK, QPSK, OQPSK, 8-Phase Shift Keying (8-PSK), 16-Amplitude PSK (16-APSK) while providing backwards compatibility to the majority of SCPC modems currently in existence ("MD-1366 EBEM," 2008-2011). ViaSat provides an optional Ethernet Service Expansion Module (ESEM) for this modem, enabling an Ethernet interface for supporting Ethernet based protocols ("MD-1366 EBEM," 2008-2011). With the ESEM in place, the Ethernet port could be used for interface with a personal computer using the "c" prompt, a graphical user interface (GUI), or an automated management system for command line entries

("MD-1366 EBEM," 2008–2011). In addition, this modem does bring to bear an Information Throughput Adaptation (ITA), which provides increased available throughput by automatically converting the power margin resulting in the automatic raising and lowering of the system data rate as the downlink power increases and decreases ("MD-1366 DISA Certified," 2011).

C. SUMMARY

The purpose of this chapter was to present basic information necessary to gain a better understanding of satellite communications and how its components operate. Through providing a solid foundation of the technology in place and taking an in depth look into each element of the satellite system, we can now focus on identifying the essential elements necessary to improve the overall operation of the extended Internet connection.

In the next chapter, this thesis will present the information necessary to gain a better understanding of routable networks, ADNS, environmental sensors, network monitoring tools, an SNMP agent available for supporting satellite communications systems, Remote Monitoring (RMON), and the concept of the 8th Layer.

THIS PAGE INTENTIONALLY LEFT BLANK

III. NETWORK MANAGEMENT

A. ROUTABLE NETWORKS

The Internet has been in existence for a relatively short time. Since its birth in 1969, this technology has grown into a routable network that supports many forms of communication. As a routable network, it has come to support mobile platforms and secluded areas through being extended by various wireless technologies. Of interest is the routable network that supports the extended Internet to the U.S. Navy's afloat networks through Satellite Communication systems.

The Internet is a global interconnection of networks that uses the Transmission Control Protocol (TCP) and the Internet Protocol (IP) (TCP/IP) as a standard Internet Protocol Suite. Throughout the years Internet resources and services have expanded for both commercial and private use. Various resources and services such as the World Wide Web (WWW), e-mail, Voice over Internet Protocol (VoIP), and Video Telecommunications (VTC) are available through the Internet. Since the introduction of communications, there have been numerous milestones in the development of the Internet. For a Selective Internet Chronology, see Appendix C.

B. ADNS MONITORING APPROACH

Automated Digital Network System (ADNS) provides network connectivity between the Navy's ships and Naval Computer and Telecommunications Area Master Station (NCTAMS) for exchanging classified and unclassified data ("IP Basic Course," 2008, p. 9–21). The primary function of the ADNS is to provide connectivity for Navy shipboard networks from ship-to-ship and ship-to-shore for the transfer of Internet Protocol (IP) data. Shipboard users can connect to other Navy platforms, facilities, or Wide Area Networks (WANs) provided by the Defense Information Systems Agency (DISA). ADNS is designed to facilitate the monitoring, management, and routing of (IP) data over various RF and physical mediums (Naval Network Warfare Command, 2008, p. 2-30).

Naval Telecommunications Procedures 4 (E) states that “the ADNS system provides Wide Area Network (WAN) connectivity to the shore by passing IP data over available RF mediums using Point-to-Point Protocol (PPP) for link establishment and maintenance” (Naval Network Warfare Command, 2008, p. 2-30). ADNS can dynamically route IP data by selecting any available RF link to connect to a shore base station (Naval Network Warfare Command, 2008, pp. 2-30, 2-31).

The ADNS is a robust networking environment and backbone to the Department of Defense’s (DoD) Joint Maritime Communications (JMCOMS). ADNS uses commercial off-the-shelf (COTS) routers, processors, and protocols to create a highly flexible networking atmosphere that interfaces with “all RF media from HF to EHF provides the total throughput and access needed” (“ADNS,” n.d.). ADNS consists of three functional elements: Integrated Network Manager (INM), Routing and Switching (R&S), and Channel Access Protocols (CAPs). Figure 11 illustrates the basic components and relative position of a typical ADNS system. The basic ADNS installation shown in the illustrations consists of a Local Area Network (e.g., SIPRNET, NIPRNET, and GENSER), CISCO Routers, an INM, In-line Network Encryptors (INEs), and Tactical Local Area Network Encryption (TacLANE) devices illustrated by the KG-194A, and SATCOM terminals, which include modems. The Navy’s ADNS incorporates the use of Cisco brand 3640 and 3620 routers, whereas the 3640 router is usually found in shipboard installations and the 3620 router is put in place at shore-based facilities (“Cisco 3600,” n.d.).

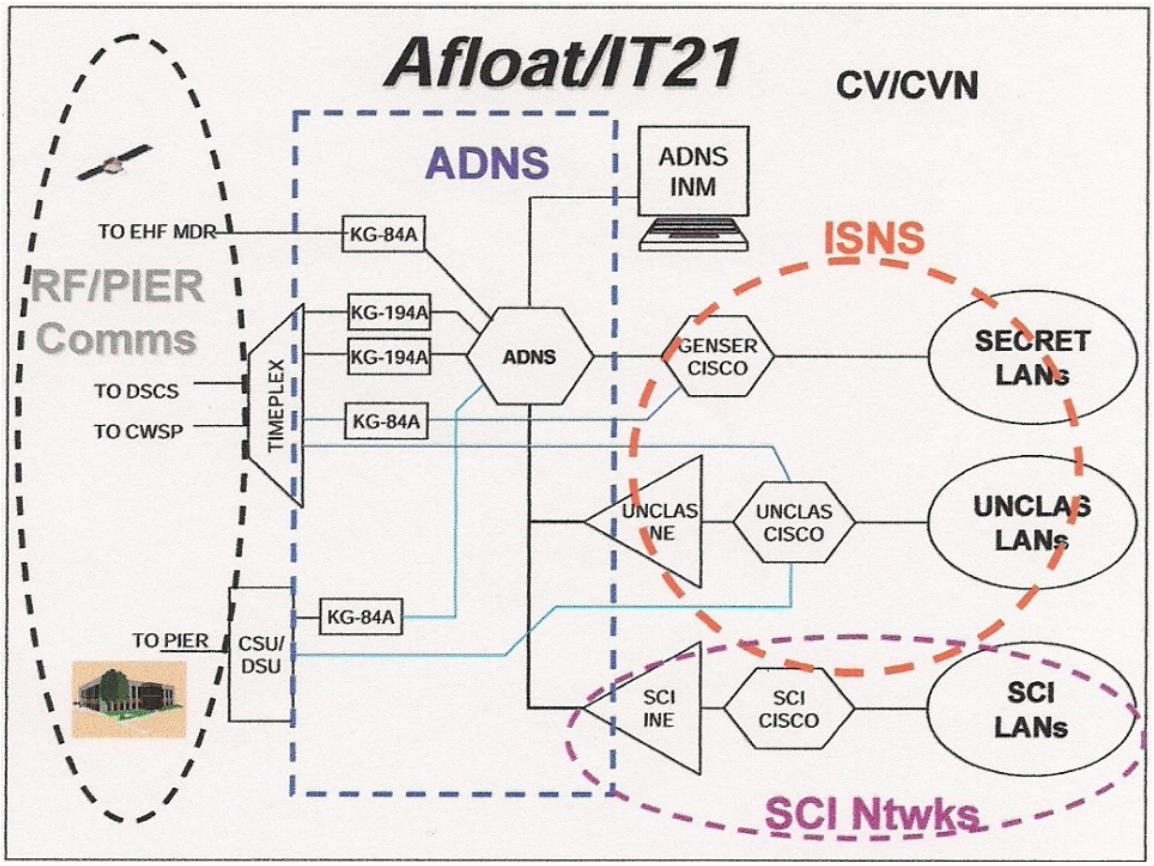

Figure 11. CVN Network Topology (From: CVN Network Topology "IW & IP Basic Officer Course," 2008, p. 2-23)

According to GlobalSecurity.org, ADNS provides the following improvements:

- "Furnishes autonomous, digital, interoperable, joint and secure LAN/WAN management and control for RF assets on demand to Navy deployed personnel aboard ships and at shore sites" ("ADNS," n.d.).
- "Ensures worldwide communications connectivity via the RF assets included in the Digital Modular Radio (DMR) and Integrated Terminal Program (ITP)" ("ADNS," n.d.).
- "Automates all communications systems-replaces several unique subnetworks with a single integrated network hub" ("ADNS," n.d.).
- "Provides Integrated Network Management (INM) which resolves problems caused by overloading or underutilization of existing communications circuits, yielding a 4X increase in multispectrum throughput efficiency over legacy systems" ("ADNS," n.d.).
- "Applies NDI COTS/GOTS router, switching and packet data technologies enabling reduced life cycle costs" ("ADNS," n.d.).

The Automated Digital Network System (ADNS) network management has been established aboard ships and shore facilities alike. This management system seeks the best path delivery of data. Once a route is identified as congested the ADNS management system seeks an alternate best path for data delivery. Navy personnel in the rate of Information Systems Technology operate the INM, which includes a Simple Network Management Protocol (SNMP) management console. Tools like HP Open View are used to monitor the status of the network connectivity.

In cases where a receive (downlink) stream is degraded (the modem is no longer receiving or passing information), the ADNS router's SNMP Agent will no longer see dataflow resulting in that path being considered as either infinitely congested or the path no longer available. In addition, the ADNS router SNMP Agent will detect that the path is constrained (infinite congestion), will not pass packets to that path, and the routing table is updated to reflect the change in connectivity. Once the anomaly disappears and/or the system returns to normal operating parameters (up condition), the modem will again pass information to the ADNS router, the SNMP Agent will detect dataflow, and the routing table will updated and again push packets to that path.

Bao and Garcia-Luna-Aceves state in their "Link-State Routing in Networks with Unidirectional Links" paper that for routing protocols to work an up-stream and down-stream path must exist for routing information to be past between connected routers in order to sustain the connection (Bao & Garcia-Luna-Aceves, n.d.). The key to this statement is that routing information could be passed over separate satellite links that create the existence of many up-stream and down-stream paths. The routable network that supports the Internet is extended to the U.S. Navy's afloat networks through satellite communications systems. Therefore, if a subscriber station were to have a loss of transmit capability the ADNS routers could communicate through the routable network in order to continue passing routing information.

C. SNMP MONITORING APPROACH

Regis Bates introduces Simple Network Management Protocol (SNMP) in Chapter 32 of his book "Network Management SNMP" as "the Internet standard protocol for monitoring and managing devices connected to" IP networks (Bates, 2002, p. 576). There are three versions of SNMP; each subsequent version introduced additional capabilities.

- SNMP version 1 (SNMPv1) was the first rendition of the SNMP protocol. "SNMPv1 operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX)" ("SNMP," n.d.).
- SNMPv2 is a revision of version 1 which includes several improvements in "performance, security, confidentiality, and manager-to-manager communications" ("SNMP," n.d.). SNMPv2 introduced the GetBulkRequest for single retrieval requests of management data in large amounts ("SNMP," n.d.).
- SNMPv3 only provides added cryptographic security and remote configuration enhancements while making no changes to the protocol itself. In addition, this version looks a bit different from previous versions due to the introduction of new terminology and text conventions ("SNMP," n.d.).

SNMP "defines the data set structure of the information that each device may provide" (Bates, 2002, p. 576). This data set structure is called a Management Information Base (MIB) and has provisions for custom MIBs (Bates, 2002, p. 576). MIB contents are defined by Request for Comments (RFCs). A list of relevant SNMP standards, which apply to general network management (SNMP) and remote monitoring (RMON), is provided in Table 1 of Appendix D (Bates, 2002, p. 582).

Bates states that "devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more" ("SNMP," n.d.). Therefore, the standard set of parameters can be provided as well as an extended set of custom vendor parameters (Bates, 2002, p. 576). SNMP assumes the existence of managers and agents and is used as a device monitor and management tool in network management systems

("SNMP," n.d.). The functional relationship between manager and managed functions is illustrated in Figure 12. SNMP "consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects" ("SNMP," n.d.).

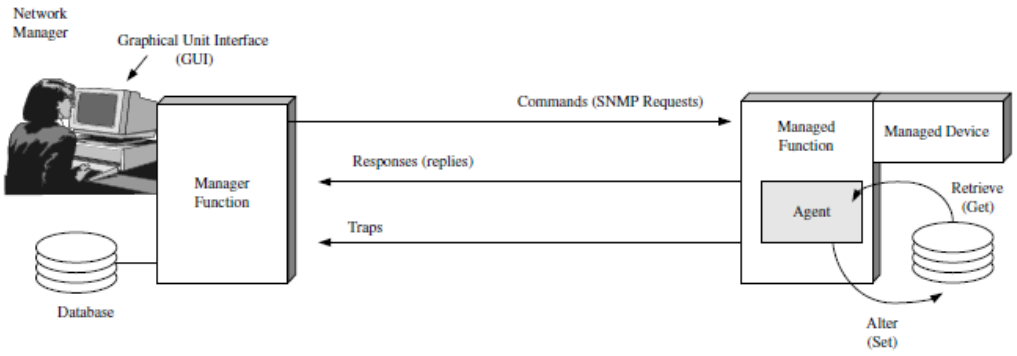

Figure 12. Manager to Managed Function Relationship (From Bates, 2002, p. 580)

Interpeak, a leader in providing networking, security and middleware software, states that "an SNMP manager is a software module in a management system, responsible for handling of configuration and statistics of the networked devices" ("SNMP," 2005). The management station translates management tasks into commands for SNMP messages that are sent on the routable network for management of SNMP capable devices ("SNMP," 2005). The manager function sends commands to the agent for obtaining status information or setting specific parameters (Bates, 2002, p. 583).

An SNMP agent must be resident on the device that is to be managed remotely over the routable network using SNMP protocols ("SNMP," 2005). "Data are collected, kept, and reported by an agent that runs on the managed device" (Bates, 2002, p. 576). The agent responds to manger commands and can send status messages if a predetermined parameter is met or exceeded (Bates, 2002, p. 583). In the case of satellite communications subscriber stations there is no SNMP agent residence on the terminal equipment.

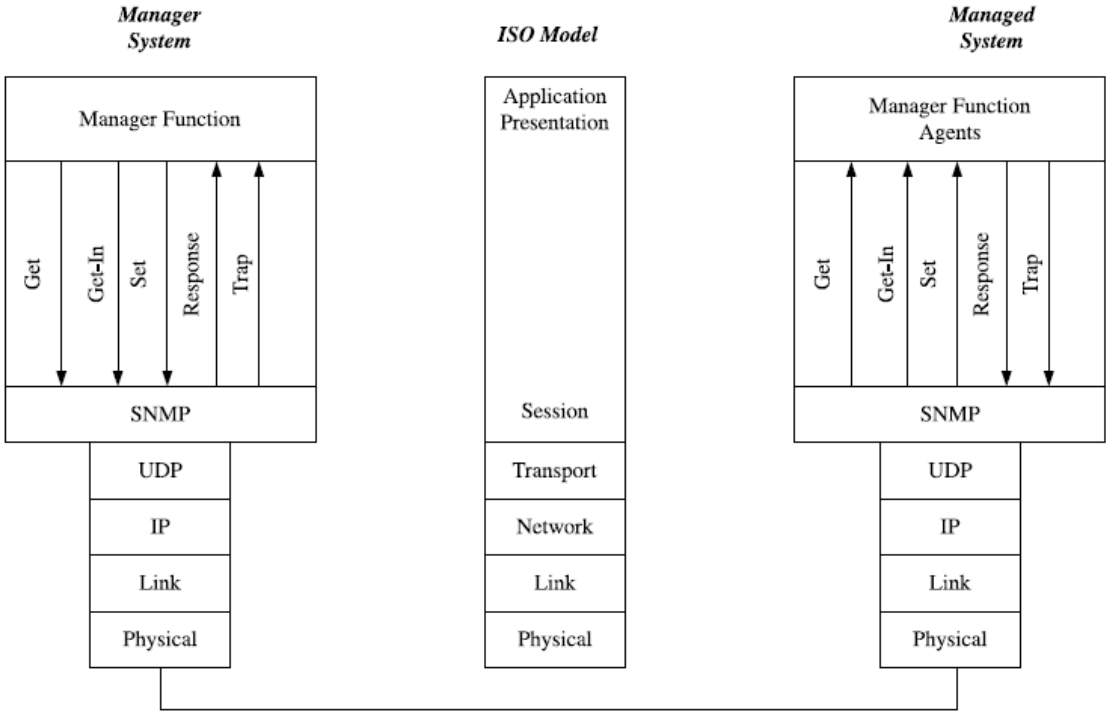

Figure 13. SNMP Function in relationship to the OSI Model
(From Bates, 2002, p. 584)

Figure 13 shows the SNMP functions in relationship to the OSI Model with SNMP running at the top of the protocol stack and User Datagram Protocol (UDP) used by the transport layer (Bates, 2002, p. 583). “From an OSI point of view, SNMP and its interaction with the manager and managed functions encompass the upper three layers of the protocol stack” (Bates, 2002, p. 584). The SNMP flow of commands and responses are shown in Figure 13, with the internationally accepted names and assigned numbers provided in the International Structure of Management Information Tree shown in Figure 14 (Bates, 2002, p. 584).

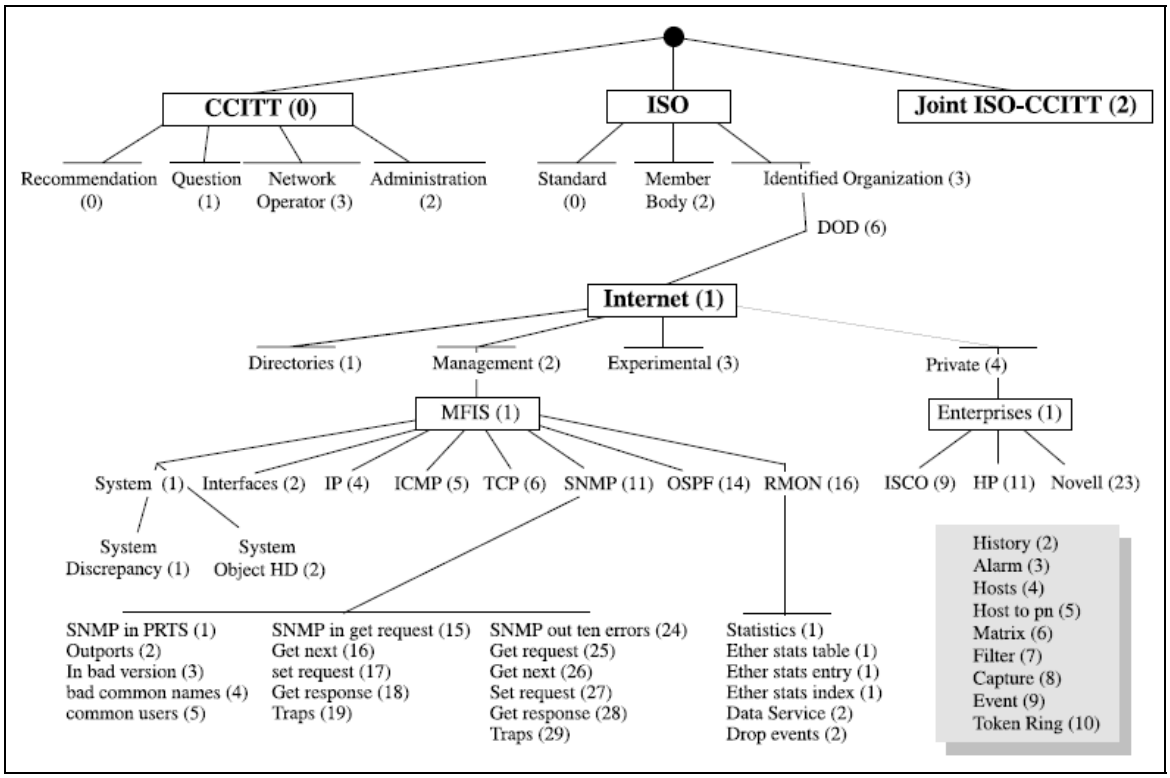

Figure 14. International Structure of Management Information Tree (From Bates, 2002, p. 583)

Looking at the SNMP message illustrated in Figure 15, the SNMP message is encapsulated within the protocol layers. Each layer usually has some leader, header information and trailer bits (Bates, 2002, p. 584). “The link layer frame carries the IP packet across the link layer connection to the next router. The IP datagram header has the routing information that lets the routers direct this packet to its final destination (Bates, 2002, pp. 584–585). When using a satellite communications system to make this connection, the path would be from the subscriber station’s router to the base station’s router and then on to the final destination. “The SNMP message is contained within the UDP datagram” (Bates, 2002, pp. 584–585). “The version field insures that we are conversing with another agent of the same version. The community field is important because it is the security function. Our SNMP function can therefore only collect information from members of our own community” (Bates, 2002, p. 585). This prevents competitors from obtaining information from equipment connected to the Internet. “The

Protocol Data Unit (PDU) type specifies whether there is a GetRequest, GetNextRequest, SetRequest, Response, or a Trap. The error fields are used to identify SNMP errors, such as tooBig, noAccess, or badValue. The error pointer points to the location of the offending data field. Each Object Identifier (OID) then is included, followed by its value" (Figure 14) (Bates, 2002, p. 585).

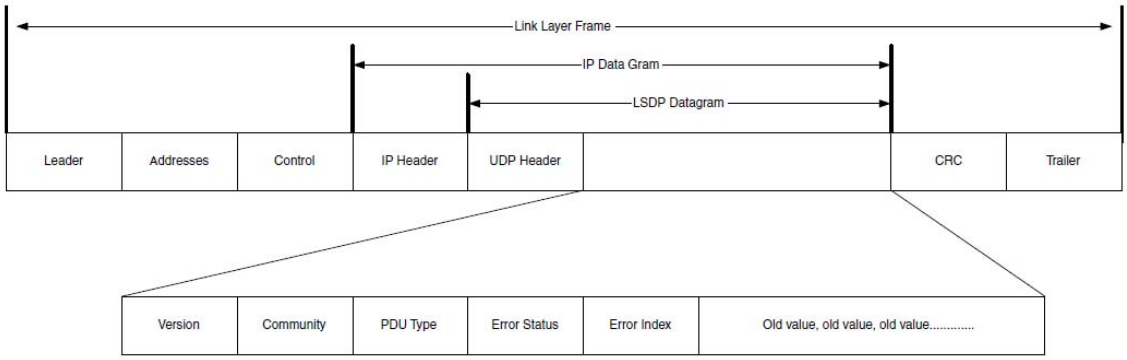

Figure 15. SNMP Message within Protocol Layers (From Bates, 2002, p. 584)

D. RMON

Remote Monitoring (RMON) is an extension of the SNMP MIB that allows network monitors and consoles to exchange data for meeting specific network monitoring needs ("RMON," n.d.). This standard monitoring specification provides network administrators with the flexibility to select specific network-monitoring probes and clients for obtaining distinctive networking features ("RMON," n.d.). The number of RMON MIB variations has grown as the technology of the routable network has improved; for example, the Token Ring RMON and SMON MIBS have been created to specifically manage analyze their perspective Token Ring and Switched networks ("RMON," n.d.).

The two versions of RMON are RMON1 and RMON2. Most new networking equipment comes with RMON preinstalled or built in ("RMON," n.d.). RMON1 and RMON2 MIB Group functions can be reviewed using Tables 2 and 3, respectively, in Appendix D. The RMON1 and RMON2 are focused at different network layers of the

OSI model. RMON1 is used for basic network monitoring and is only used for network monitoring at the MAC and PHY layers of the OSI model illustrated in Figure 16 (“RMON,” n.d.). RMON2, illustrated in Figure 16, is used for monitoring those OSI layers above the MAC with focus on Transport and Application layers (“RMON,” n.d.). “RMON2 allows network management applications to monitor packets on all network layers” (“RMON,” n.d.).

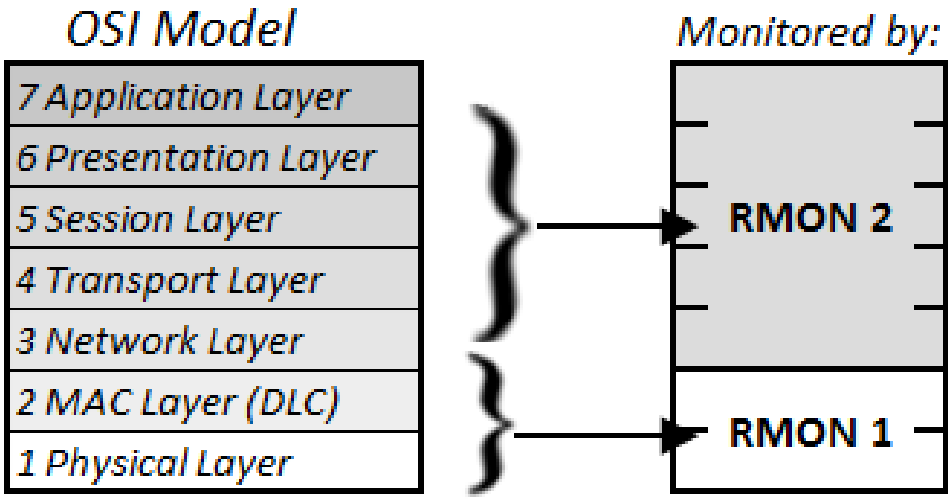

Figure 16. The Focus of RMON1 and RMON2 on OSI Layers (From “RMON,” n.d.)

The RMON management and agent relationship is comprised of an agent or monitor and a management station (“RMON,” n.d.). The agent or monitor can also be described as a probe while the management station may be recognized as a client (“RMON,” n.d.). “Agents store network information within their RMON MIB and are normally found as embedded software on network hardware such as routers and switches although they can be a program running on a PC” (“RMON,” n.d.). Because “agents can only see the traffic that flows through them” they could be used on SATCOM terminals for monitoring data throughput (“RMON,” n.d.). The RMON client would then be placed within the ADNS network monitoring station “using SNMP to obtain and correlate RMON data” (“RMON,” n.d.).

E. NETWORK MONITORING TOOLS

1. Sensors

Satellite terminals do not have the ability to monitor their environment. While RFI sensors do accomplish this task, they are not part of the routable network or used by communication systems to monitor the operational environment. Most U.S. Navy ships have an Electronics Warfare suite that can perform environmental sensing. In addition, there are several commercial sensors available for satellite environmental monitoring. The following military and commercial systems represent the capabilities available for monitoring the RF spectrum and for supporting satellite communication systems.

a. Military Example

In the early 1970s, the Navy considered the development of an electronic warfare suite for the replacement of existing shipboard surveillance sensors ("AN/SLQ-32 system," n.d.). The Chief of Naval Operations' (CNO) decision for the development of a new capability was in response to the Anti-Ship Cruise Missile (ASCM) threat made evident by the 1967 sinking of the ELATH, an Israeli destroyer, where Egypt had used a Soviet made SS-N-2 STYX ("AN/SLQ-32 system," n.d.). The capability of U.S. Navy installed shipboard surveillance sensors AN/WLR-1 and AN/ULQ-6 systems were determined to be incapable of countering a missile strike through the analysis of the ASCMs under development at the time ("AN/SLQ-32 system," n.d.). The early warning systems were simply not effective against ASCM characteristics ("AN/SLQ-32 system," n.d.). As a result, the AN/SLQ-32(V) was developed to provide powerful countermeasures and effective early warning capability related to targeting emitters and threat weapon systems ("AN/SLQ-32 system," n.d.). Although the AN/SLQ-32(V) was designed with Electronic Attack (EA) features which provides active jamming and able to launch infrared (IR) decoys and short-range Super Rapid Blooming Off-board Chaff (SRBOC), the system has an integrated on-line database for the identification of threats that complements the early warning capability ("AN/SLQ-32 Suite," n.d.). This early warning capability is an effective RF Interference (RFI) detector. As a standalone system,

the AN/SLQ-32(V) suite is not SNMP enabled nor does it provide an input to the routable network for monitoring the operational environment by other systems.

b. Commercial Examples

In addition to the AN/SLQ-32(V) Electronic Warfare Suite, there have been several commercial RFI monitoring capabilities developed. For example, SAT Corporation has marketed the "Monics® Satellite Carrier Monitoring System" for monitoring satellite uplinks and downlinks and Antenna Technology Communications Incorporated introduced the "Warrior Satellite Monitoring System," which allows governments and militaries full satellite monitoring and RF jamming capabilities. These two SATCOM monitoring capabilities are briefly discussed in the following paragraphs.

i. Monics®. "Monics is a distributed Satellite Communications Monitoring system" that "automatically monitors thousands of carriers and provides alerts for abnormal conditions" ("Monics," n.d.*a*). "From a central Network Operations Center, operators can monitor data & spectrum from an unlimited number of remote monitoring sites. Each Local Network Server allows the local (remote) site to function as a part of the network or autonomously Measurement data and spectral traces are stored for viewing of historical information" ("Monics," n.d.*b*). "With digital signal processing, Monics provides a digital carrier's modulation type, symbol rate, BER, and Carrier under Carrier Interference Detection" ("Monics," n.d.*b*).

ii. Warrior. Warrior is a packaged system that "allows government and military entities complete satellite monitoring, transmission and RF jamming capabilities" ("ATCi," n.d.). "Warrior was designed with the ability "to simultaneously process thousands of RF carriers—X-Band, C-Band, Ka-Band and Ku-Band" ("ATCi," n.d.).

2. Monitors

There is a variety of commercially available network management tools offering an assortment of performance monitoring options and network management capabilities. Although these network monitoring tools are available for ship and shore facilities alike,

these tools are not normally deployed to monitor the satellite terminal throughput or status of the router data port connected to the input of the terminal's modem. While supporting several Tactical Network Topology (TNT) Field Experimentation exercises using mobile satellite subscriber stations, this researcher has used both DopplerVUE and Orion Network Performance Monitor (NPM). These performance monitoring tools are discussed to provide a basic understanding of available network monitoring capabilities.

a. Terminal Equipment Fault Monitor

Satellite terminals have associated fault monitoring systems that allow technicians to check the operational status of the terminal. For example, Figure 17 illustrates that a technician of a SWE-Dish IPT-i Mil Suitcase 2.4 can access the Alarm Page using a GUI Interface. Using this view, the technician can observe the terminals status, which includes but is not limited to the modem, GPS input, the transmitter's Solid-State Power Amplifies (SSPA), the Receiver end Low Noise Block (LNB) and system temperature ("Instructions for Use," 2007, p. 85). The technician is provided a color coded display indicating the following statuses ("Instructions for Use," 2007, p. 85):

- Green color–functioning unit
- Yellow color–a warning is present
- Red color–an alarm is present

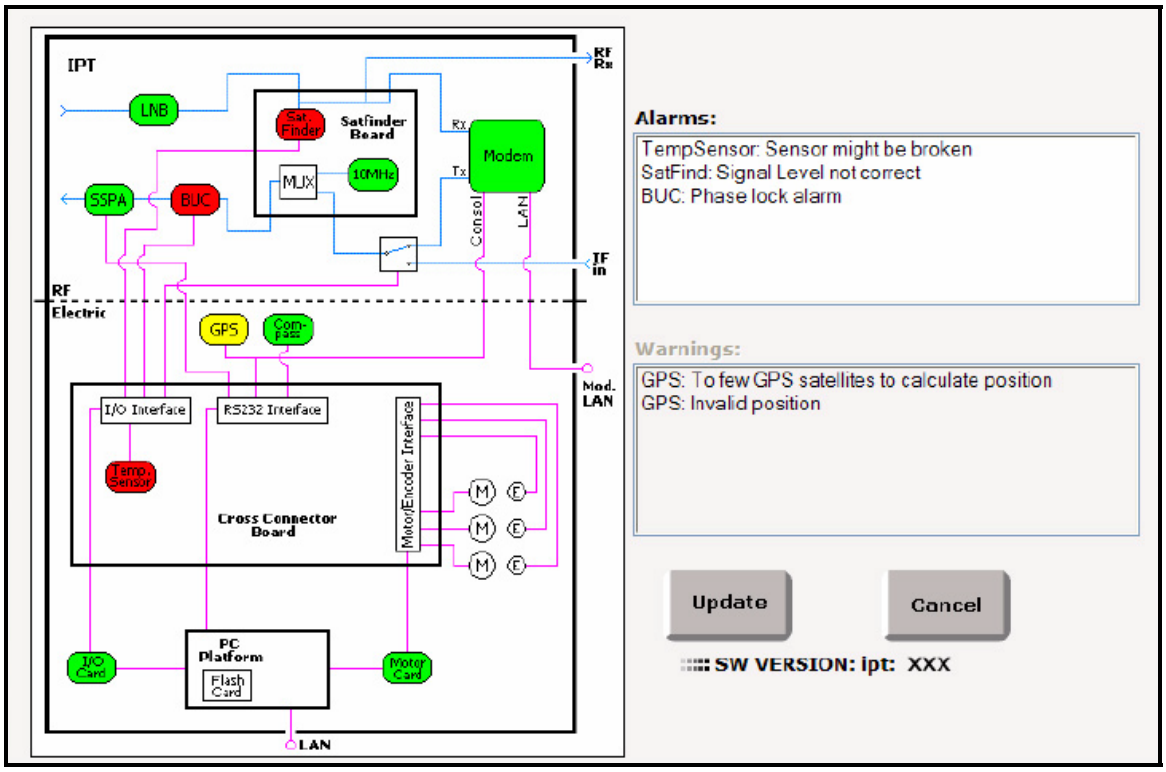

Figure 17. SWE-Dish IPT-i Mil Suitcase 2.4 GUI Alarm Page (From "Instructions for Use," 2007, p. 85)

This monitoring capability is built into all SATCOM terminals that the thesis researcher has come into contact with. The ability to monitor the terminals RF environment for interference that may affect the performance of the network connection is essential to determining the complete status of the SATCOM system. Environmental monitoring is something the SATCOM terminal is not capable of doing. This can be accomplished via alternative means through specialized environmental sensors, such as those previously discussed.

In conclusion, the type of alarm capability discussed above provides a good example of what monitoring capabilities could be made available to a network management console if the SATCOM terminal were SNMP enabled. With an SNMP enabled system and SNMP enable sensors, the network monitoring station would be able to receive status notifications for immediate action and potentially dispatch technicians if needed or respond automatically.

b. Orion NPM

SolarWinds' Orion Network Performance Monitor (NPM) is a fault monitoring and network performance management platform that "delivers detailed monitoring and analysis of performance data from routers, switches, servers, and other SNMP-enabled devices" ("ORION NPM," n.d.). This software performs automatic network discovery of devices and gives performance statistics in real time ("ORION NPM," n.d.). NPM provides the network manager the ability to perform quick detection, diagnosis, and resolution of network issues ("ORION NPM," n.d.). This application "monitors, tracks the up/down status, and analyzes real-time, in-depth, network performance statistics for routers, switches, wireless access points, servers, and any other SNMP-enabled device" ("ORION NPM," n.d.). Orion NPM can provide "NetFlow traffic analysis, IP SLA WAN monitoring, IP address management, network configuration management, user device tracking, and application and server performance" ("ORION NPM," n.d.).

c. DopplerVUE

DopplerVUE is a network management and performance tool produced by Kratos Defense & Security Solutions, Inc. that "integrates fault, performance and discovery into a single, unified dashboard across devices, applications and services" ("dopplerVUE: TNM," n.d.). This product is IPv6 ready and can "provide connectivity to all IP-enabled elements through ICMP, SNMP (including custom MIBs), Syslog, Windows Event Log, NetFlow and WMI to provide fully-integrated fault and performance monitoring" ("dopplerVUE: TNM," n.d.). DopplerVUE delivers a real-time network fault and performance monitoring "statistics for routers, switches, wireless access points, servers, and any other SNMP-enabled devices" ("dopplerVUE: INPM," n.d.).

Therefore, these network monitoring tools could be used to monitor the satellite connection for up and down status as well as the throughput of the data port from the ADNS router.

F. THE 8TH LAYER

When looking at the 8th Layer, man is portrayed as the manager of the network. Unfortunately, people are not responsive enough to address the multiple minute-by-minute network requirements of today's routable networks. In this researcher's experience, as a prior Navy Electronics Technician Chief and Electronics Material Officer, human beings cannot monitor all aspects of the operational environment and all system indicators simultaneously. Dr. Sarah Stein of North Carolina State University, writes in her white paper on the 8th Layer that, "There are seven layers in the networking architecture that define how systems communicate. This architecture is the foundation on which all information technology (IT) is built. Insiders frequently refer to the human factor in IT as the 8th Layer. The title is the message; our greatest challenge is not the technology" (Stein, 2004, p. 3). Agreed, Man needs assistance from the network devices to make the overall system more effective. The 8th Layer can provide that assistance.

In the paper, "Extending the OSI model for wireless battlefield networks: a design approach to the 8th Layer for tactical hyper-nodes," authors Alex Bordetsky and Rick Hayes-Roth introduce the idea of "the architecture and functionality of a new 8th Layer" that expands the current OSI model (Bordetsky & Hayes-Roth, 2007). The paper argues that "mapping NOC capabilities in Layer 8 functionality is critical for emerging Command and Control network-centric environments based on unmanned vehicle-decision maker adaptive self-forming networks" (Bordetsky & Hayes-Roth, 2007). Their concept is to make adaptive networking available by providing each critical node of a C4I network a dedicated Network Operation Center (NOC) capability (Bordetsky & Hayes-Roth, 2007). These critical nodes are identified as "'intelligent nodes" due to being able to adapt to their environment through the integration of the "8th Layer hyper-nodes" (Bordetsky & Hayes-Roth, 2007). These hyper-nodes obtain the sought adaptive behaviors through meeting specified constraints such as Service Level agreements. The hyper-nodes poll SNMP MIB data from each NOC's network equipment for status information in order to provide a full status picture, which describes the NOCs overall health (Bordetsky & Hayes-Roth, 2007). By relating the 8th Layer concept provided by Bordetsky & Hayes-Roth to the SATCOM / routable network relationship, it clearly

indicates that having an SNMP Agent to perform 8th Layer functions is the proper method to monitor the operational environment of satellite communications systems.

G. SUMMARY

The purpose of this chapter was to present the information necessary to gain a better understanding of routable networks, ADNS, environmental sensors, network monitoring tools, an SNMP agent available for supporting satellite communications systems, RMON, and the concept of the 8th Layer. A clear understanding of these available capabilities and tools pave the way to finding a solution for monitoring the operational environment of Navy SATCOM. Through providing a solid foundation of the available technologies in Chapters II and III, this thesis will now focus on identifying the essential elements necessary to improve the overall monitoring capability of the extended Internet.

In Chapter IV, this thesis will discuss a Tactical Network Topology (TNT) extended network case-study focused on how to monitor an SHF satellite link and extended network using SNMP means.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS OF MANAGEMENT CAPABILITIES

When looking at an overview of the entire satellite communications system it can be difficult to identify the keys to monitoring the operational status of the SATCOM link that provides the extended Internet connection. In Chapter II, a basic satellite system was broken down into pieces in order to understand what the operational function of each unit was. Doing so made it possible to isolate each element and assist in eliminating those parts of the system that had could not be used for making an effective change for monitoring the system and gave light to those system parts that were affected or could be used to improve the overall operation picture of the extended Internet conduit. In Chapter III, this thesis presented information necessary to gain a better understanding of routable networks, ADNS, environmental sensors, network monitoring tools, an Simple Network Management Protocol (SNMP) agent available for supporting satellite communications systems, and the concept of the 8th Layer. By making use of the technologies discussed in this chapter, a solution for monitoring the operational environment of Navy SATCOM can be found. In Chapter IV, a TNT case-study was presented for a quick look as to how to monitor a satellite link and extended network using SNMP means. This thesis will now focus on identifying the essential elements necessary to improve the overall monitoring capability of the SATCOM connection from an SNMP enabled routable network point of view.

A. SATCOM EQUIPMENT

1. Satellites

Satellites simply act as a repeater that uses a medium of for sending a received data stream back to the Earth. Using a capability similar to that of NASA's ACTS program, it would be possible for the base station to manage and monitor the satellite channels using SNMP. With an SNMP agent embedded on satellites the base station would have the capability to monitor and manage the satellite and satellite channels.

2. Terminal Equipment

Satellite terminals, fixed or mobile, are standalone systems that are not SNMP enabled. They are isolated from the routable network and environmental sensors. This segment of the system has an internal monitoring capability that is locally accessed by a technician. Through the use of a GUI the technician can observe a fault monitoring display to identify transmit, receive, and various other alarms and warnings. By embedding an SNMP agent in the SATCOM terminal and providing either a back channel or an Ethernet connection, it would be possible for this device to be remotely monitored from the routable network at a network monitoring console.

3. Modems

Modems simply convert an incoming signal for transmission or reception of an RF signal. The modem can be part of the SATCOM terminal equipment but, if the modem is external to the terminal equipment then the modem should be SNMP enabled through the use of an embedded SNMP agent.

a. MD-1366 Enhanced Bandwidth Efficient Modem (EBEM)

The Navy's standard modem, the MD-1366 Enhanced Bandwidth Efficient Modem (EBEM), can accommodate an Ethernet Service Expansion Module (ESEM) that provides accessibility through a GUI interface. This feature is not used by the U.S. Navy. If the Navy were to purchase this module and connect the Ethernet port to the routable network, the modem could be enabled to support a remote monitor.

b. MIL-STD-188-165B

MIL-STD-188-165B is the new standard that the MD-1366 EBEM was designed after. But, although MIL-STD-188-165B is the new standard, it makes no mention of SNMP agents or a network interface (back channel) requirement. The absence of standards defining SNMP agents and a network interface requirement means that the modem and SATCOM systems remain removed from the routable network. The Navy's standard SATCOM modem has the potential for handling the SMNP protocol for

monitoring the operational status of the terminal, however; the Navy has made a decision not to implement the ESEM capability or address the need for an SNMP capability in the MIL STD.

B. ADNS

ADNS uses SNMP enabled Cisco routers, which support other devices on the network that have enabled SNMP agents. ADNS has the ability to perform the function of remote network monitoring through the use of the Integrated Network Manager (INM). Therefore, INM provides the necessary management and monitoring capabilities needed to monitor satellite terminals and obtain environmental information from shipboard sensors to obtain a clear operational picture of the satellite connection. As a result, the monitor console could obtain SNMP statistics and information from the SATCOM terminal and modem if these devices were SNMP enabled.

C. SNMP AND RMON

1. RFC 1213: SNMP MIB-II

The MIB for Network Management of TCP/IP-based internets, RFC 1213 MIB-II, was the primary MIB used for monitoring the satellite link of extended network connections during both the TNT exercise at Avon Park, Florida and the TNT Maritime Interdiction Operations (MIO) 11-2 exercise at Souda Bay, Greece. RFC 1213 was used to monitor the VPN interface, which was the last node prior to the satellite link.

The network performance monitoring tools used during the experiments could only monitor the status of the extended network. Due to the lack of an embedded SNMP agent on the terminals, these tools could not be used to remotely monitor or capture detailed status information about the operational condition of the satellite terminals (i.e., System up/down status, transmitter fault indication, low transmitter power, receiver fault indication, poor receiver SNR, and loss of satellite tracking).

The satellite terminal status information just described is essential for monitoring the performance of the terminal device providing the network connection for the

extended network and this information provides details for real-time system troubleshooting and analysis. Therefore, a satellite terminal embedded with an SNMP agent and the use of remote monitoring (RMON) MIB such as RFC 1757, which has replaced RFC 1271, would improve the monitoring capability of the network manager and monitoring console operators.

2. RFC 1757: RMON MIB

Using the RMON MIB in concert with SNMP MIB 1213 would be beneficial to monitoring satellite terminals from a network monitoring console. The added monitoring capabilities that MIB 1757 provides could be used to provide satellite terminal status information such as fault alarms and system events based on predetermined values. Of the available groups, three statistic groups provide desirable information that could be used for remotely monitoring satellite terminals. These groups are the:

- Alarm Group (3): "The Alarm group periodically takes statistical samples from variables in the probe and compares them to previously configured thresholds. If the monitored variable crosses a threshold, an event is generated. A hysteresis mechanism is implemented to limit the generation of alarms. This group consists of the alarmTable and requires the implementation of the event group" (Teare, 2008).
- Packet Capture Group (8): "The Packet Capture group allows packets to be captured after they flow through a channel. This group consists of the bufferControlTable and the captureBufferTable, and requires the implementation of the filter group" (Teare, 2008).
- Event Group (9): "The Event group controls the generation and notification of events from this device. This group consists of the eventTable and the logTable" (Teare, 2008).

3. Conceptual SNMP Enabled SATCOM System Using RMON

Having an SNMP enabled device on a routable network, the SNMP manager is capable of collecting the RF interference level from the enabled device's agent, which could be an embedded RMON agent. This concept is illustrated in Figure 18 as an SNMP enabled SATCOM monitoring capability. In order to perform this task, the SNMP manager is configured to send a GET Request, at pre-determined intervals, to the SNMP agent on the enabled device. The GET Request defines the parameters needed by the

agent to identify the appropriate information to be obtained. The SNMP RMON agent issues a Response to the SNMP manager with the requested parameters. In this case, if RF interference was detected in the SATCOM's operating frequencies the network monitor console would indicate an alarm. The network manager would then contact the technician to check the system. Having SNMP and RMON capabilities incorporated in SATCOM equipment is essential to being able to monitor the status of the link from a remote console located at either the Master Station or a routable network.

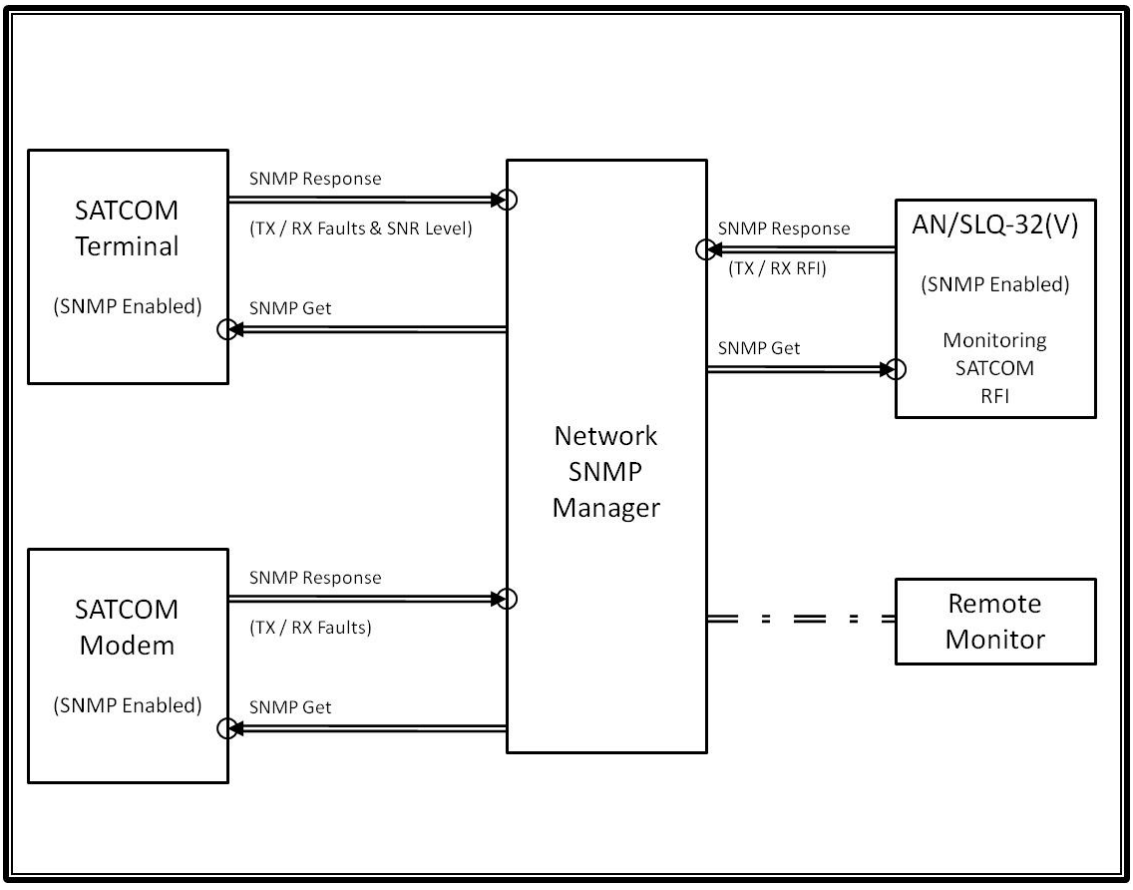

Figure 18. Conceptual SNMP Enabled SATCOM Monitoring Capability

D. SENSORS AND MONITORS

1. Sensors

Shipboard RFI sensors perform the task of monitoring the RF environment. These systems are isolated from the routable network and SATCOM terminal fault monitoring systems. The AN/SLQ-32 EW system previously discussed in this thesis performs the RF monitoring task needed but, is not SNMP enabled or connected to the routable network. This means that the EW system's capabilities cannot be fully exploited to assist in determining the SATCOM system's operational status.

2. Monitors

With ADNS having the ability to perform network monitoring, Orion and DopplerVUE network performance monitoring tools could be used on the ADNS system for obtaining SNMP statistics and the information from the SATCOM terminal and modem if these devices were SNMP enabled.

E. DE-COUPLE DATA FROM A RFI SENSOR

The AN/SLQ-32 Electronics Warfare Suite monitors the RF environment for identifying threats. Raw data is collected for identification, which contains RF environmental parameters that can be used by an SNMP enable device. An SMNP manager requesting RF environmental parameters from the Electronics Warfare suite would receive a Response message with the desired parameters. Through the development of an SNMP MIB this data stream can be made available for use in a SATCOM monitoring framework.

F. INTEROPERABILITY ARCHITECTURE

In his paper, "Toward an Interoperability Architecture," Professor Rex Buddenberg at the Naval Postgraduate School, Monterey, writes about modularization and that part of the interoperability problem is due to the tradeoffs between conformity and desired characteristics (Buddenberg, n.d.). He states that "The objective is that

modules become inherently interoperable so we have components delivered by multiple programs that can be assembled for particular tasks" (Buddenberg, n.d.).

As I see it, the core of the satellite communications architecture has been welded together so that things fit together for the special purpose of providing an extended internet connection over satellite communications systems. The satellite communications architecture currently in place is isolated from the routable network it supports. The architecture does not afford the flexibility of monitoring SATCOM terminals and modems from the routable networks due to the lack of SNMP enabled devices implemented in SATCOM and an available back channel or Ethernet connection to the routable network.

G. POTENTIAL AUTOMATION

Satellite terminals have no environmental inputs, no method for network remote monitoring, and no automated access management. As an example; even though a smartphone must be set up by the user, once programmed these devices can monitor connectivity in order to adapt to a changing environment. The smartphone is able to perform this task by monitoring the status of all available connections.

Satellite communications terminals lack the ability to adapt to a changing environment. SATCOM connections are standalone, singular point-to-point terminations with no alternative means for monitoring or management of the connection. As independent systems isolated from the routable network, satellite terminals do not have the ability to monitor or adapt to their environment like a smartphone does.

In order to improve our satellite capability, we must consider the development of adaptive capabilities such as the 8th Layer concept provided by Bordetsky and Hayes-Roth. Implementing an agent to manager relationship that currently does not exist in the SATCOM to routable network relationship, SNMP enabled environmental sensors and SATCOM terminal equipment would provide the path for automation. If the SATCOM terminals and modems were enabled with SNMP agents, the U.S. Navy could automate SATCOM systems to provide status updates to the network monitoring console. Automate environmental monitoring functions.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CASE STUDIES

A. INTRODUCTION

The thesis author participated in two field experiments as part of the network management team. The field experiments were performed during the weeks of 21 February and 06 June 2011, for the Tactical Network Topology (TNT) extended network at Avon Park, Florida and the TNT Maritime Interdiction Operations (MIO) 11-2 extended network at Souda Bay, Greece, respectively. These case-studies focused on how to monitor an SHF satellite link and extended network using Simple Network Management Protocol (SNMP) means.

B. TNT AT AVON PARK, FL

1. Purpose

The goal of this case study was to attempt to monitor two SHF satellite links utilizing SNMP MIB objects on Cheetah and Wintec Very Small Aperture Terminals (VSAT) illustrated by the TNT extended network basic diagram in Figure 19. These terminals were provided by L-3 Communications CyTerra Corporation (L-3) and Waikato Institute of Technology (Wintec), respectively.

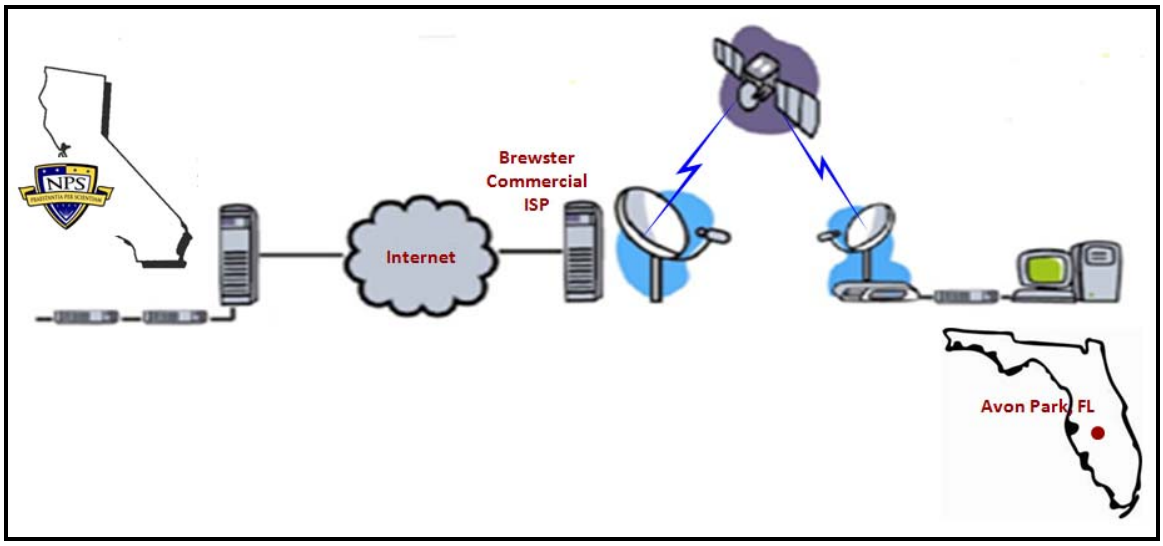

Figure 19. TNT Extended Network Basic Diagram

2. Network Extended by the Satellite Reachback

The extended network at Avon Park, FL was setup with two services working together for providing reachback connectivity. The Wintec terminal was setup to provide the primary internet access to the clients. The Cheetah terminal was setup to support the virtual link directly between the TNT and Center for Network Innovation and Experimentation (CENETIX) lab located at the Naval Postgraduate School (NPS). The computers linked to the Virtual Private Network (VPN) from the NOC, located at NPS, accessed the Cheetah satellite connection and all other clients, external to the NOC, were given access to the Wintec satellite connection. The detailed diagram provided in Figure 20 illustrates the internal network setup of the extended TNT network.

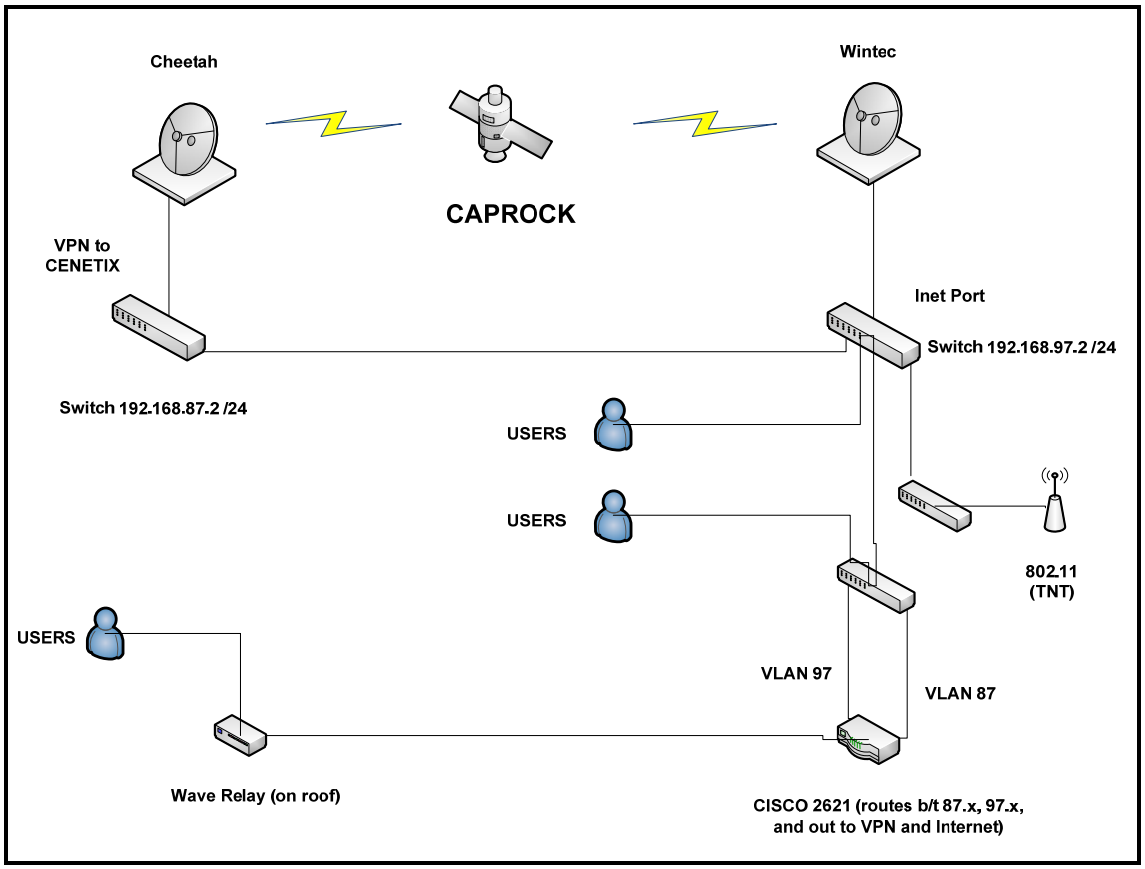

Figure 20. Detailed Diagram of Internal Network at Avon Park, FL

A secured connection was formed from Avon Park to Naval Postgraduate School through the use of a VPN, illustrated in Figure 21. The VPN protocol used to facilitate security was IP Security (IPSEC) and Encapsulating Security Payload (ESP). These protocols allow for a TCP/UDP connection to be established.

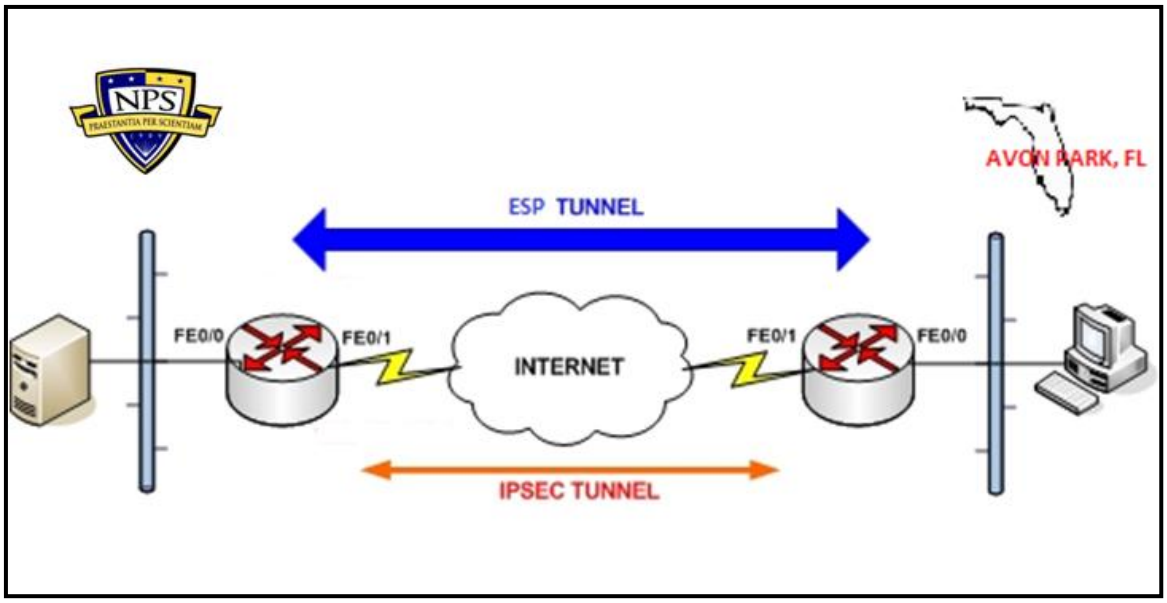

Figure 21. VPN using Secure IPSEC Tunnel

3. Network Management Environment

DopplerVUE and Orion NPM network management tools were used to identify, monitor, and manage the network utilizing the 1213 MIB. Management of the network utilizing two different nodes with two different software platforms proved to be challenging. DopplerVUE was leveraged to access remote devices, monitor bandwidth utilization and view other pertinent information available via SNMP. The Orion NPM network management software was used for performing network discovery and monitoring for determining degradation and outages.

The Orion NPM IP Network Browser function was used to scan for all IP addresses being used within the subnet address of 192.168.87.0 and subnet mask of 255.255.255.0. In this case, it was found that only two of all IP addresses being used identified equipment capable of supporting SNMP information capture (MIB 1213). The snapshot illustrated in Figure 22 indicates the SNMP IP Addresses and System Name of the SNMP capable equipment by a plus sign (+) prior to the IP Address. Selecting the plus sign (+) expands the selection in order to observe greater detail of the item.

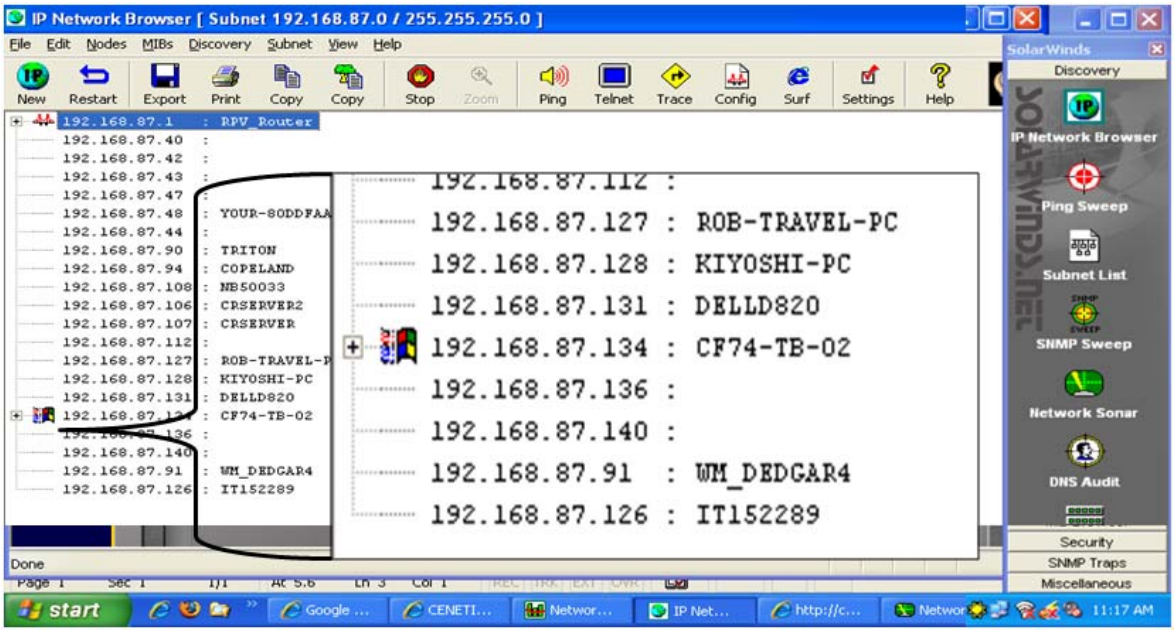

Figure 22. Orion NPM IP Network Browser Function Snap Shot

Orion NPM was used to perform various discoveries to include all subnets, nodes, routers, and MAC addresses on a network. The Network Sonar Discovery Wizard was used to provide a subnet list of our network as illustrated in Figure 23.

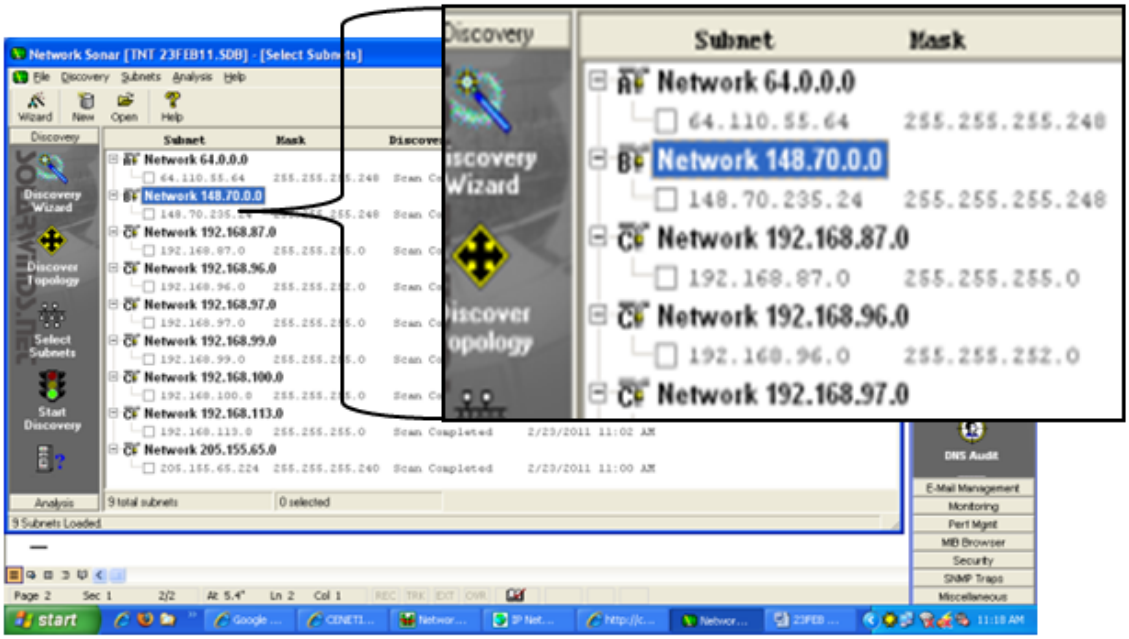

Figure 23. Subnet List provided by Orion NPM Network Sonar Discovery Wizard

Then, a subnet address is selected to perform a discovery of all nodes on all networks by network address. This function provided additional information such as the Mask, the Class of the network, the Subnet Mask, the Broadcast Address, the Subnet Type, the IP Address and the if description (ifDiscr).

The snapshot in Figure 24 illustrates a subnet discovery query provided by Orion NPM Network Sonar. The SNMP Sweep function of the Network Sonar tool lets the network manager select a range of IP Addresses to be scanned, the information obtained by this Sweep function provides similar results and provides the same detailed information as performing the Network Sonar Subnet discovery query.

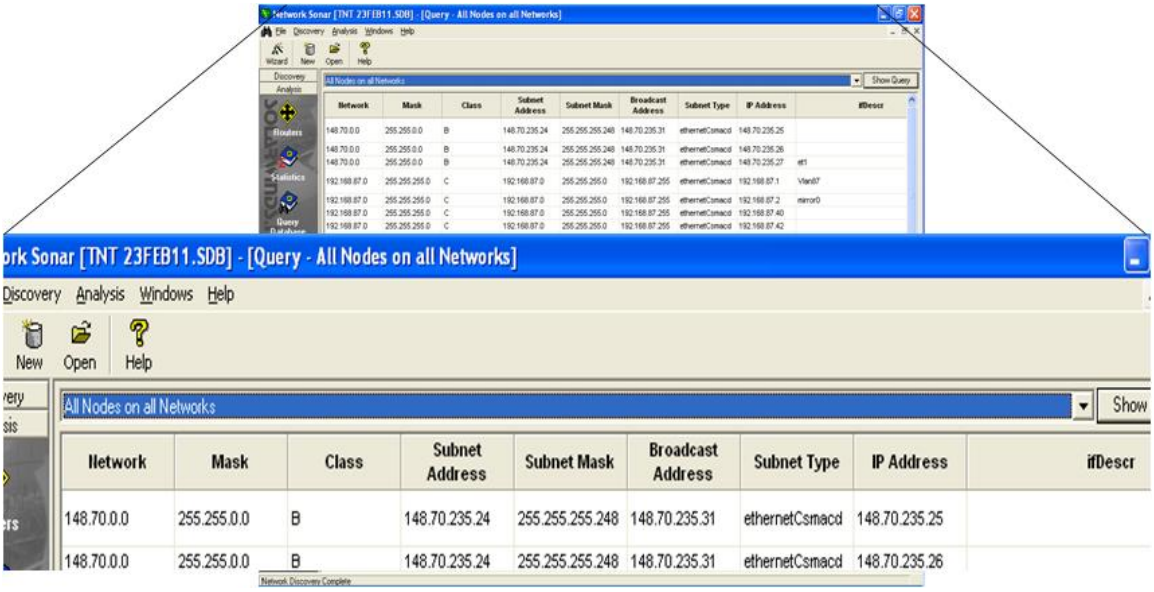

Figure 24. Orion NPM Network Sonar Subnet Discovery Query

Routers on the network were able to be identified using the Router Query and used the MAC Addresses Discovery tool to identify equipment such as routers, switches, and Virtual Private Networks on the network. Both queries provided detailed information about the queried items to include key elements such as Agent IP Addresses, Domain Name Server (DNS), Response Times, System Descriptions, Physical Addresses and IP Addresses, as shown in the Router and MAC Address Query snapshots illustrated in Figure 25.

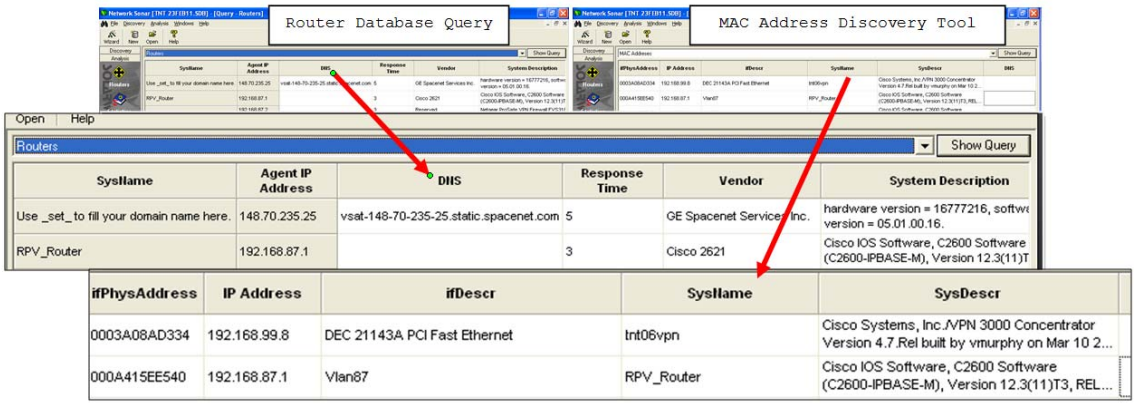

Figure 25. Orion NPM Router Query and MAC Addresses Discovery Tools

The Orion NPM was used to observe the up/down status of nodes, with special interest in monitoring the DNS nodes, the Virtual Private Network (VPN) node and the Default Gateway. The snapshot illustrated in Figure 26 was taken at a time when the network had just recovered from a hit (degraded connection) where the network experienced an approximate 20% packet loss at the Default Gateway, indicated by the Red peak in the lower right quadrant. By examining the details shown in Figure 26 more closely, the NPM also indicates a reduction in the Average Response Times from approximately 1500 to 1250 milliseconds, showing an improvement in the network response times as the network recovers. The Default Gateway (64.110.55.65) has an up status (shown in green at the far left of the illustration) yet some nodes are still down (Red status indicator) while the network is going through the recovery stage.

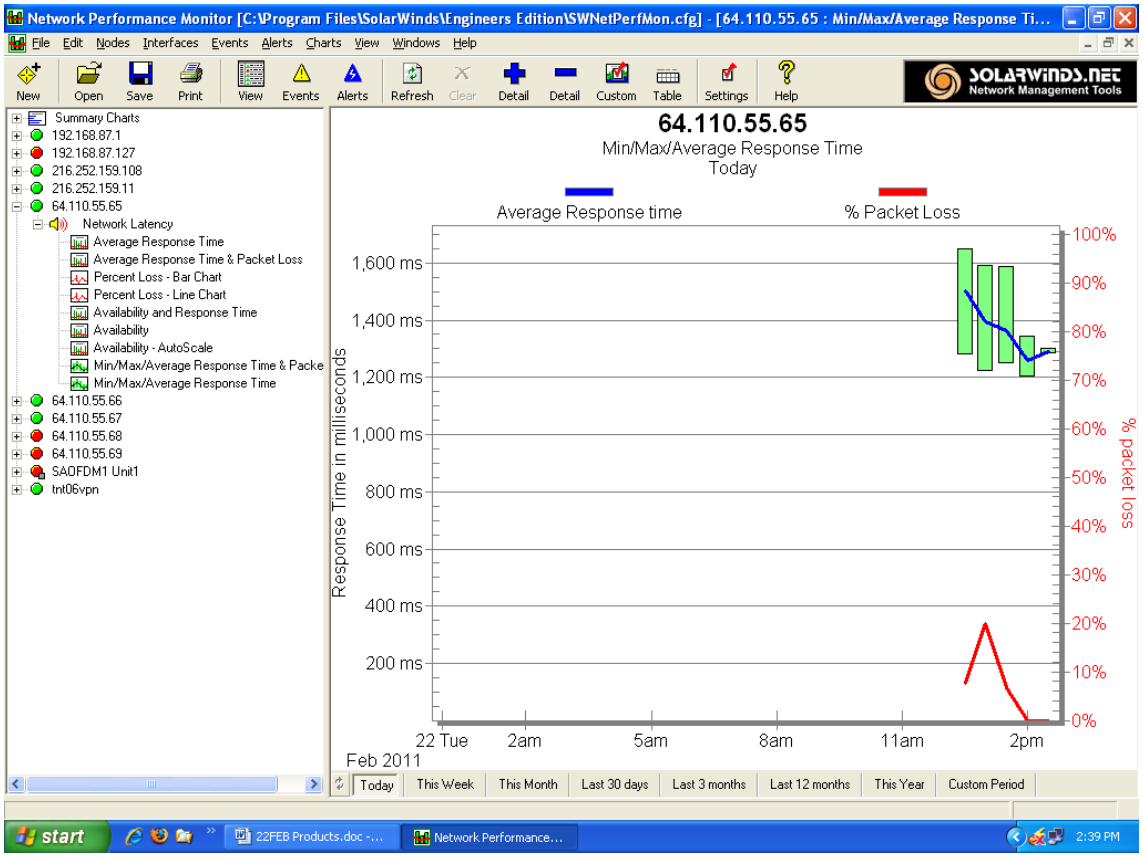

Figure 26. Orion Network Performance Monitor Indicating Degraded Network Connection in Recovery

C. TNT MIO 11-2 AT SOUDA BAY, GREECE

1. Purpose

As stated in the TNT MIO 11-2 Experiment Report; "Networking And Interagency Collaboration On Maritime-Sourced Nuclear Radiological Threat Detection and Interdiction," the "experiment was the latest in a campaign of experimentation (Alberts, 2002) events in which we continue to explore Maritime Interdiction Operations (MIO). The spotlight of experiment was on "the use of networks, advanced sensors, and collaborative technology to support integrated detection and interagency collaboration to counter nuclear and radiological threats aboard maritime craft" (TNT MIO, 2011, p. 5).

For the purposes of this thesis, the author's goal of this case-study was to attempt to monitor a single SHF satellite link utilizing SNMP MIB objects on a Cheetah VSAT terminal, shown in Figure 27, by the MIO Testbed Reachback and Detection extended network basic diagram illustrated in Figure 28. This terminal and the Internet gateway access were provided by L-3 Communications CyTerra Corporation (L-3).

Figure 27. Cheetah Terminal provided by L-3 (TNT MIO, 2011, p. 37)

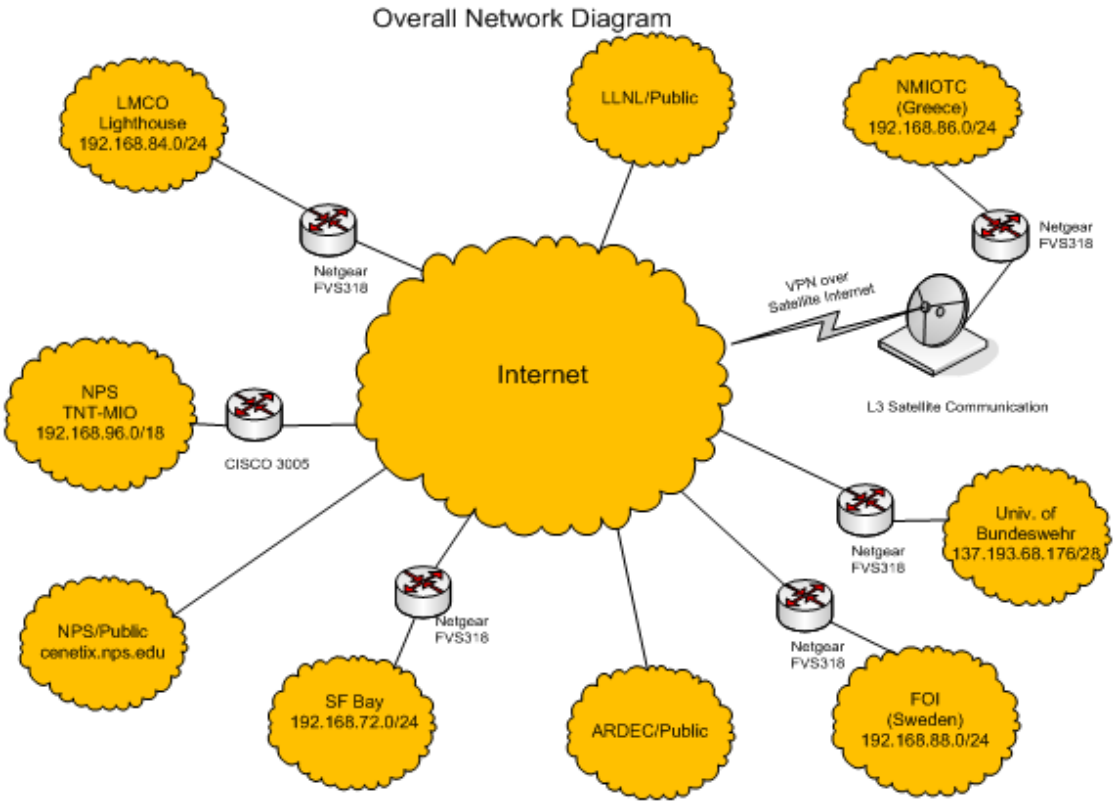

Figure 28. MIO Testbed Reachback and Detection Extended Network Basic Diagram (From TNT MIO, 2011, p. 50)

2. Network Extended by the Satellite Reachback

The Cheetah terminal was setup to support a secure connection from the North Atlantic Treaty Organization (NATO) Maritime Interdiction Operational Training Center (NMIOTC) at Souda Bay, Greece to the CENETIX Lab at the Naval Postgraduate School (NPS), Monterey, California. The secure connection (VPN) used IPSEC and ESP security protocols, which allowed for TCP/UDP data packet transfer. The VPN was established through the use of a Netgear FVS318 VPN Firewall, just like the VPN illustrated in Figure 21. This connection is also illustrated in Figure 28 as the node between the L-3 satellite terminal and NMIOTC (Greece). In addition, network routing was configured to provide services for all reachback connectivity to various sites and internet access to the clients through an Internet gateway router located at the supporting STEP site.

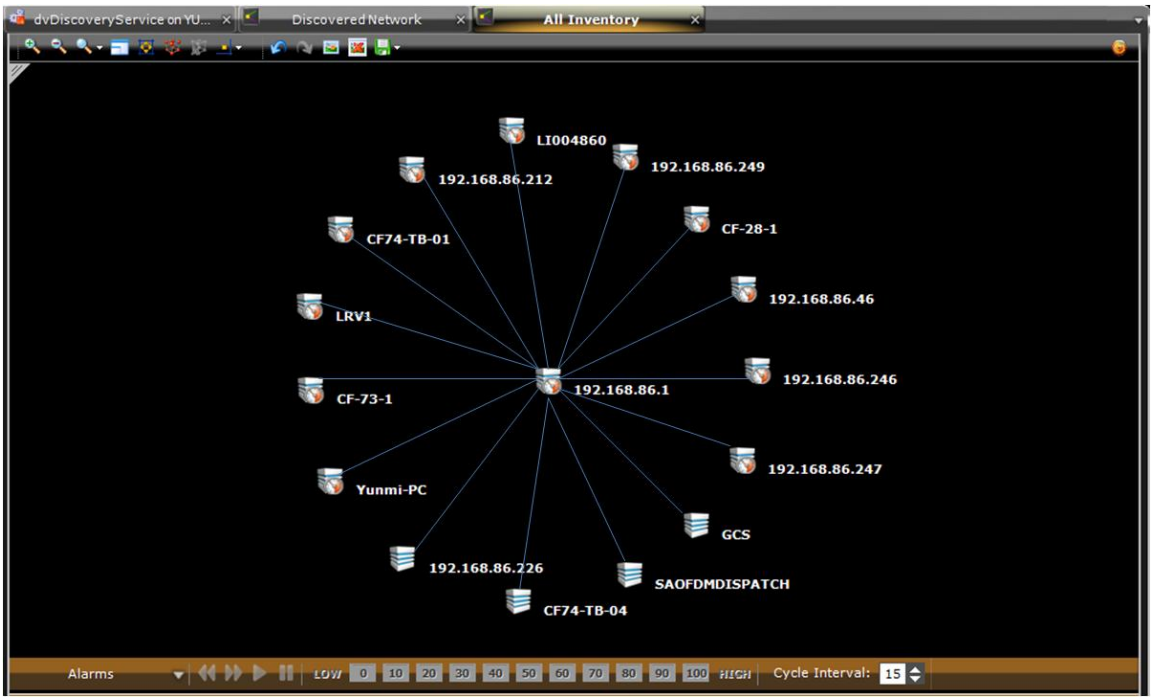

Figure 29. TNT MIO 11-2 Extended Network at Souda Bay, Greece

The internal network setup for the TNT MIO 11-2 at Souda Bay, Greece illustrated in Figure 29 consisted of 16 nodes plus a local relay site. The MIO network was extended for searching both large and small vessels during the experiment. The network was extended through the use of the shore-based relay site, which supported extended wireless mesh network connections as illustrated in Figures 30 and 31 (TNT MIO, 2011, pp. 50–52).

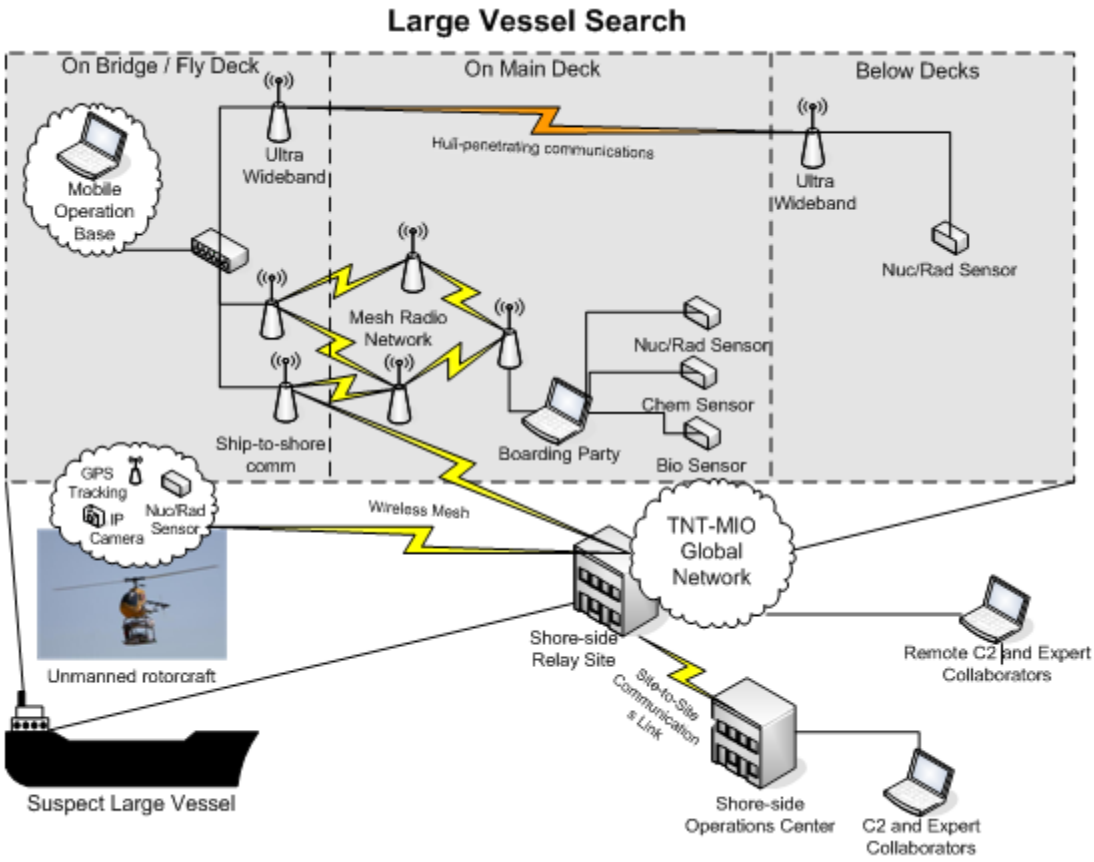

Figure 30. Large Vessel Wireless Mesh Connection (From TNT MIO, 2011, p. 51)

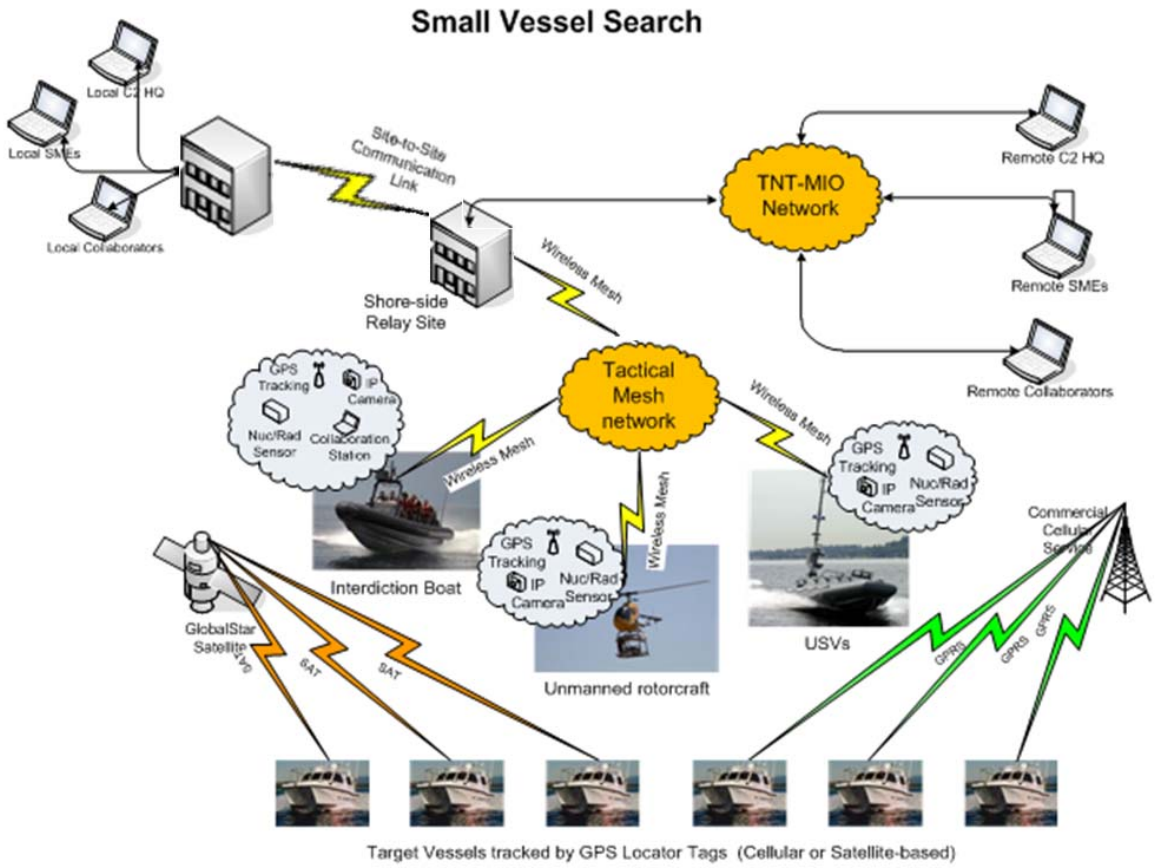

Figure 31. Small Vessel Wireless Mesh Connection (From TNT MIO, 2011, p. 52)

During the large and small vessel search portions of the experiment, the mesh network provided the capability for voice communications, audio and video recording for sensor data collection, and posting verbal surveillance descriptions to the MIO collaborative site (TNT MIO, 2011, p. 25, 30). Swimmer and boarding crew position tracking and sensor data was sent to the NMIOTC for situational awareness and transmitted rad/nuc detection files (Identifinder postings) were sent to the shared event log (TNT MIO, 2011, p. 28).

3. Network Management Environment

The network monitoring tools and MIBs utilized for the TNT MIO case-study were the same as those previously discussed in the TNT case-study at Avon Park, FL.: DopplerVUE and Orion NPM network management tools utilizing MIBs 1213 and 3418.

The lack of tools for MIB 3418 precluded the use of MIB 3418. Therefore, only significant examples where monitoring the satellite terminal equipment shows the importance of identifying, monitoring, and managing the network will be provided.

The Orion NPM IP Network Browser function was used to scan for all IP addresses within the subnet address of 192.168.86.1 and subnet mask of 255.255.255.0. The results of the IP Network Browser illustrated in Figure 32 found that only eight of all IP addresses accessing the network identified equipment capable of supporting SNMP information capture (MIB 1213). While the IP Network Browser was performing the network scan, the snapshot illustrated in Figure 32 was also taken of the Orion Bandwidth Gauge tool performing transmit and receive bandwidth usage. By capturing IP Address 192.168.86.1 transmit and receive bandwidth, it was possible to capture the usage of the nodes actually connected to the extended network and visually monitor the satellite uplink and downlink status indirectly.

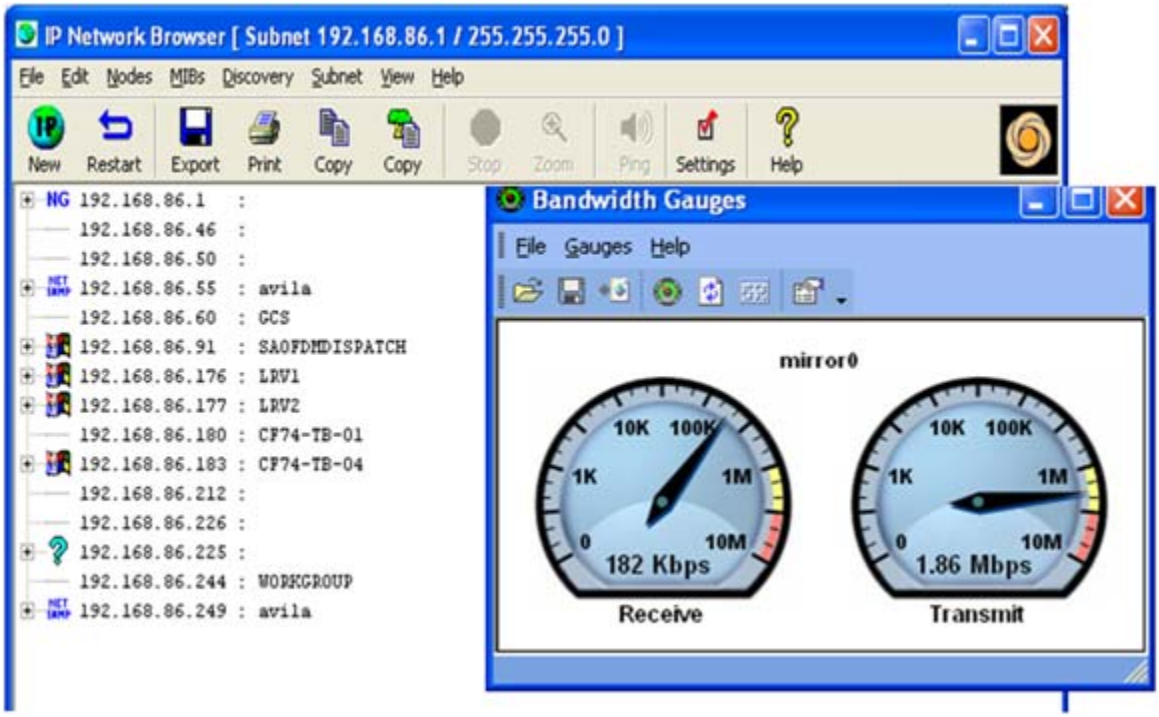

Figure 32. Transmit and Receive Bandwidth Monitoring with associated Subnet IP Address User List

The Orion NPM was used to observe the performance of nodes, with special interest in monitoring the VPN node (IP Address 192.168.86.1). The NPM tool illustrated in Figure 33 was configured to monitor the VPN node 24 hours per day in order to capture continuous network Average Response Time (**Blue**), % Packet Loss (**Red**), and Peak Minimum and Maximum Response Times (**Green**). The snapshot illustrated in Figure 33 indicates a network connection outage.

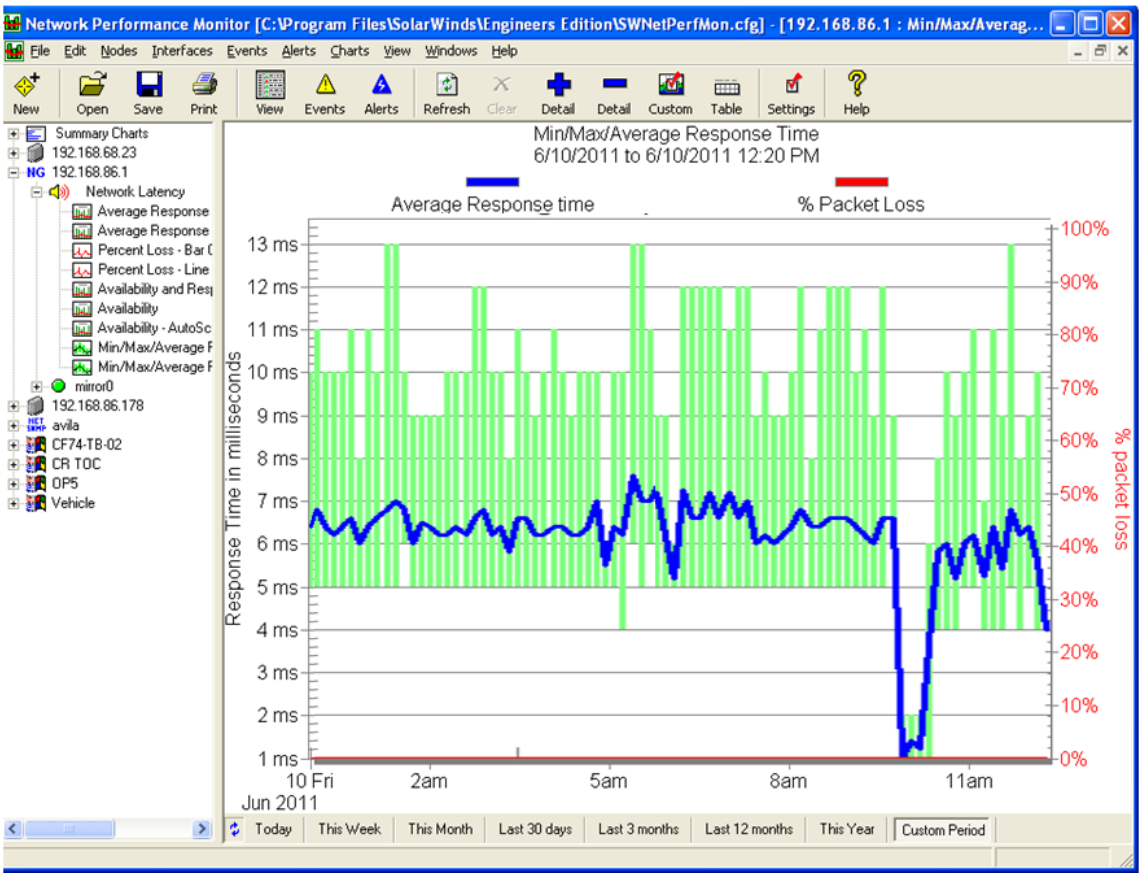

Figure 33. Orion NPM Indicating Reachback Outage

The Orion SNMP Real-Time Graph was used to observe the up/down status of nodes through the use of ifinOctets (receive link) and ifoutOctets (transmit link), which is performing a bit counter function of the data streams (MIB 1213). This network monitoring tool was configured to capture continuous bit flow in and out of the VPN node 24 hours per day in order to monitor the satellite terminal's uplink/downlink status.

The snapshot illustrated in Figure 34 shows the real-time monitoring of the VPN node (IP Address 192.168.86.1) with ifinOctets in **Blue** and ifoutOctets in **Red**.

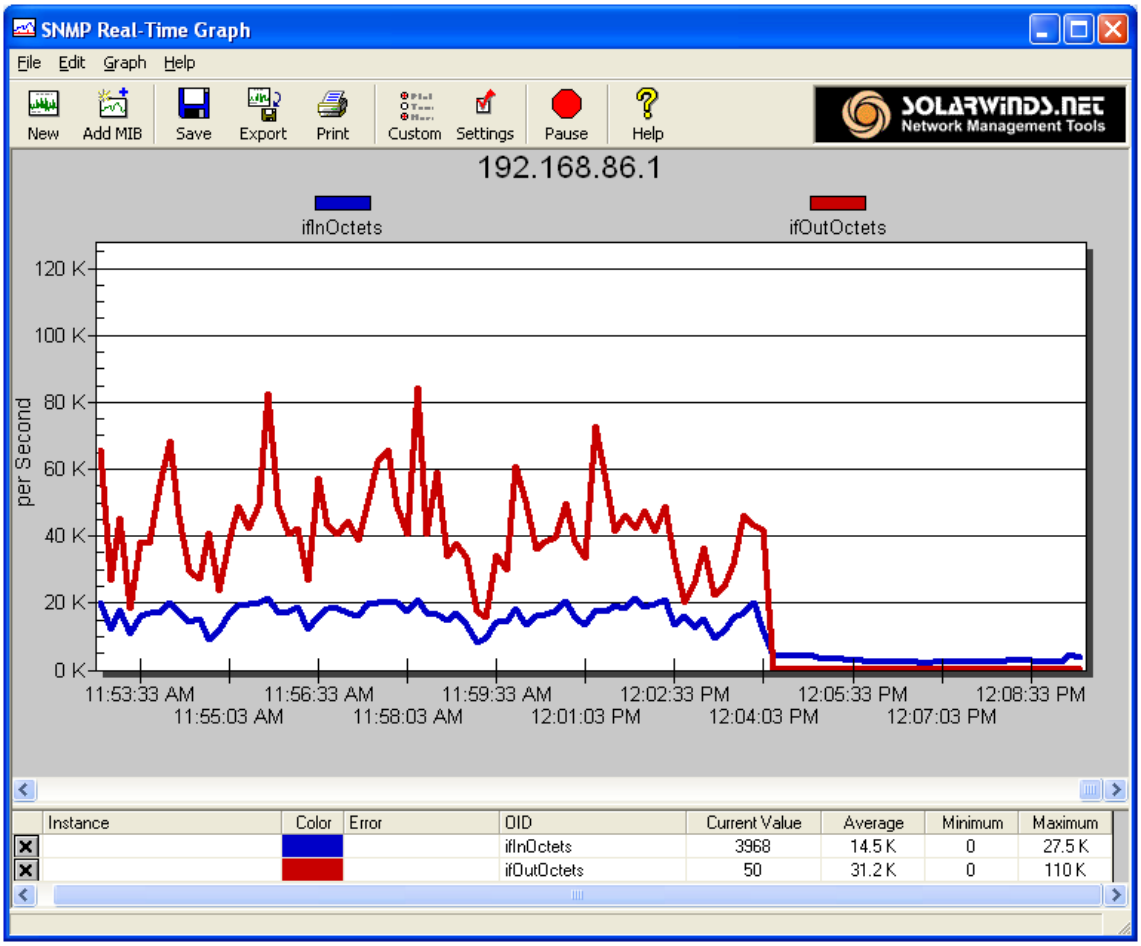

Figure 34. SNMP Real-Time Graph Indicating Reachback Outage

The snapshot illustrated in Figures 33 and 34 were taken show the importance of monitoring the network's performance. The snapshot in Figures 33 illustrates a loss of network connectivity between approximately 9:30 and 10:30 in the morning on 10 June 2011. The snapshot in Figures 34 illustrates a loss of network connectivity at approximately 12:04 in the afternoon on the last day of the exercise. Real-time network performance monitoring should not be restricted to just monitoring the nodes of the network, but also the satellite terminals that provide the extended network connectivity and their system fault monitoring capability as well.

D. MONITORING WITH RFC 1213: SNMP MIB-II

The MIB for Network Management of TCP/IP-based internets, RFC 1213 MIB-II, was the primary MIB used for monitoring the satellite link of extended network connections during both exercise.

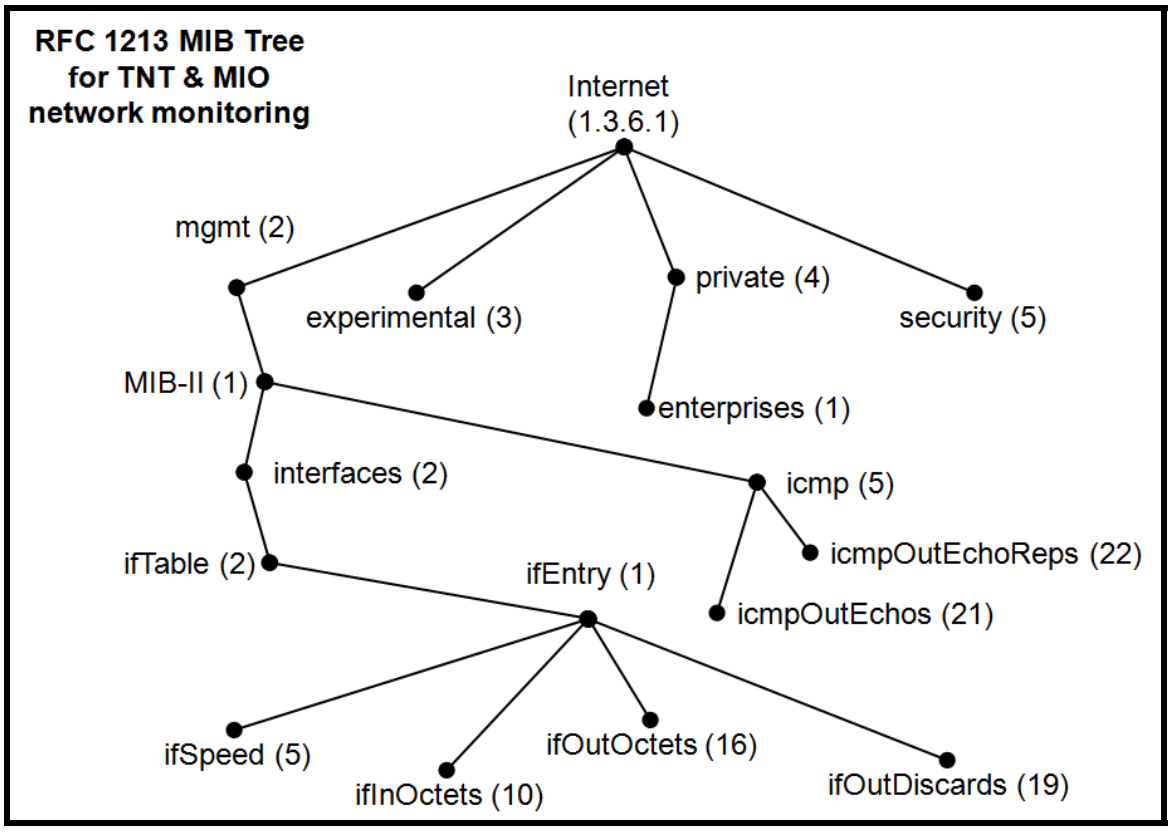

Figure 35. RFC 1213 MIB Tree for TNT & MIO Network Monitoring

RFC 1213 was used to monitor the interface of the last node (Netgear FVS318 VPN Firewall) prior to the data link. Figure 35 illustrates the RFC 1213 MIB Tree structure utilized for some of the interface details captured while monitoring the extended network. A complete list of FRC 1213 interface details is provided in Tables 4 and 5 of Appendix D. Specific node interface details were observed by selecting various tools provided by the DopplerVUE and Orion NPM software (i.e., NPM tool using ifOutDiscards for %Packet Loss and using both icmpOutEchos and icmpOutEchoReps for Average Response Time, Bandwidth Gauge tool using the ifSpeed for bandwidth

capacity, and the SNMP Real-Time Graph tool using ifInOctets and ifOutOctets for counting the bits of sent and received data for bandwidth usage).

The tools previously described helped monitor the status of the extended network connections but, could not be used to monitor the status of the actual satellite terminals.

E. RFC 1757: RMON MIB STRUCTURE

The ability to monitor satellite terminals from a network monitoring console also lends itself towards the use of the RMON, MIB 1757. Although MIB 1757 extends the SNMP MIB, it could be used to provide added monitoring capabilities that MIB 1213 cannot perform by itself. RFC 1757 RMON MIB structure is illustrated in Figure 36.

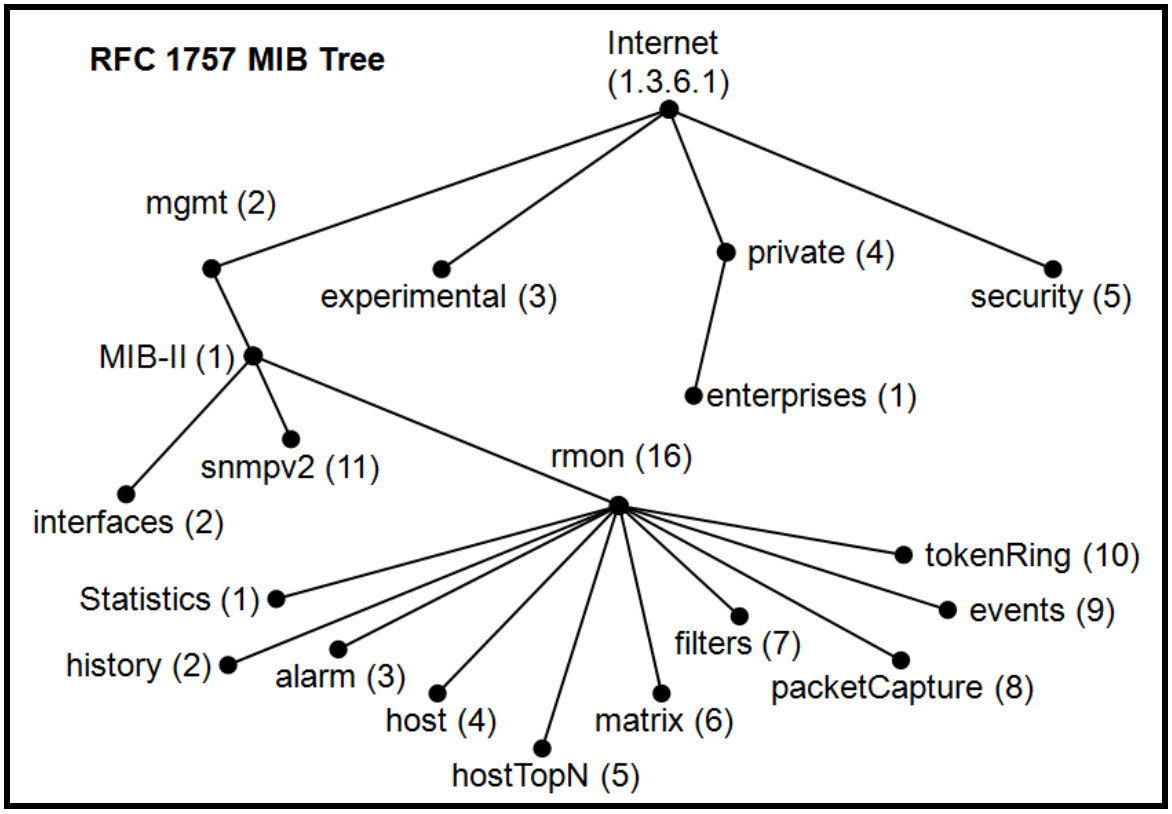

Figure 36. RFC 1757: RMON MIB Tree

RFC 1757 RMON MIB has 10 statistic groups that conform in such a way that if a remote monitoring device applies a group, then all objects in that group must be applied (From Teare, 2008). “All groups in this MIB are optional. Implementations of this MIB

must also implement the system and interfaces group of MIB-II [6]. MIB-II may also mandate the implementation of additional groups" (Teare, 2008). "These groups are defined to provide a means of assigning object identifiers, and to provide a method for managed agents to know which objects they must implement" (Teare, 2008). Each of the 10 statistic groups is defined in Table 6 of Appendix D.

F. CONCLUSION

Both TNT and MIO extended networks were monitored through the use of DopplerVUE and Orion network performance monitoring and management tools. Best effort was made to monitor the network using the tools available. Although SNMP MIB 3418 statistics and MIB 1213 information were used, MIB 1213 was the primary MIB used for capturing SNMP enabled node interface and response time details.

As a reminder, all of the monitoring during the TNT and MIO exercises was performed manually. There are no alarms to alert the person monitoring the network. Had there been an SNMP agent embedded in the satellite terminals and a SNMP monitoring console, these scenarios would have provided an alarm indication to the network operator at the network monitoring console so that steps could be taken to resolve the problem more quickly. As a result of not having an automated SNMP enabled satellite terminal, outages were not noticed until network users verbally indicated that no data was being received.

For future TNT and MIO exercises, the explicit use of SNMP enabled devices must be emphasized at the highest level. Until exercise planners recognize the value of MIB 1213, these exercises will not produce the valuable information the Naval Postgraduate School needs to generate scholarly observations and recommendations concerning the management of DoD tactical networks.

In Chapter V, this thesis will analyze the Navy's current sensing and monitoring capabilities for the use in developing environmental monitoring methods. This equipment already captures useful data, which can be used for triggers and indicators of networking maladies. Using the concept of MIB Get/Response queries, Chapter IV discusses the development of a SATCOM SNMP protocol and feasible MIB structure. This protocol

will define how environmental monitoring will be accomplished. The chapter will conclude with introducing potential automation capabilities through an SNMP enabled SATCOM monitoring system and its benefits to the U.S. Navy.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

In the past, satellite communication systems provided a large portion of the commercial long distance connectivity. Today they are primarily used to extend the reach of networks to mobile platforms and satisfy the need for ad hoc connectivity. They provide the necessary physical medium for making the connection between two access points possible.

NASA is headed in the right direction, as it has been moving towards the development of the Advanced Communications Technology Satellite (ACTS). The Department of Defense and the U.S. Navy need to move in the same direction and plan for improved network monitoring and management functions of SATCOM systems through the use of the Simple Network Management Protocols (SNMP). SATCOM stations must be remotely accessible by network monitoring and management functions through the routable network.

The ideal solution would be for the satellite communications network to act as segments in a routable network just like the internet. If this could be accomplished, then satellite links would work the same as terrestrial links. At a minimum, the U.S. Navy should be looking into providing an improved system status monitoring capability. These systems must be able to adapt to the environment as it changes by means of sensing Radio Frequency Interference (RFI) and SATCOM terminal faults. This capability would provide degraded system function recognition of vital links.

This research has provided a theoretical network monitoring capability that can sense an adverse environment, provide the appropriate SNMP responses to the SNMP manager’s queries, and alert the network monitor in the routable network.

A. RECOMMENDATIONS

1. Provide SATCOM Systems with a Routable Network Monitoring Capability

Embed a SNMP agent in the satellite communication system terminal or terminal based equipment for the purpose of monitoring the satellite stations' Signal to Noise Ratio (SNR) and fault monitoring alarms. Then, enable the SNMP capability and provide an Ethernet connection to the ships routable network.

Detection of any faulty condition or poor SNR level would result in sending a trigger or response to the shipboard SNMP management console to alert the network monitoring console operator of the faulty condition. Therefore, the technician associated to the equipment could be notified, to provide rapid response for the malicious environmental condition.

2. Provide an SNMP Enabled RF Environmental Sensor to Enhance Shipboard Satellite Communications Systems and Network Monitoring

There is a need for the subscriber satellite stations and associated networks to be able to monitor the RF environment. Although most U.S. Naval ships have some version of the AN/SLQ-32 Electronics Warfare (EW) system, this system has not been integrated to provide an input to satellite communications systems or the routable network aboard ships. Therefore, a phased approach should be taken to remedy this situation.

a. Phase 1

Have the AN/SLQ-32 EW System Operator monitor the RF spectrum and set an alarm for all satellite communications systems transmit and receive operating frequencies. Should any RF interference be detected the EW system operator would notify the Tactical Action Officer (TAO) in the Combat Information Center (CIC) and the Network Monitoring Console operator for further action. The result would be that the technician for the affected satellite system would take corrective action with the Channel

Access Control Operator and the DISA Gateway Service Desk; taking additional steps to sustain the connection and data flow to the subscribers' receive / down link, should that link not be affected by the interference.

b. Phase 2

Integrate the AN/SLQ-32(V) EW System by embedding a SNMP agent in the EW system. Then, enable the SNMP capability and provide an Ethernet connection to the ships routable network. Upon detection of interference in the SATCOM terminals uplink or downlink operational frequency band, the EW system would provide the necessary trigger or response to the shipboard SNMP enable network monitoring console to alert the operator of the malicious environmental condition.

c. Phase 3

Identify and integrate an SNMP enabled RF environmental sensor specifically designed for supporting all fixed and mobile satellite communications systems. This new sensor should have the ability to be programmed with set tolerance levels that reflect the point at which RF interference causes high and infinite congestion on both the uplink and downlink frequencies of all communications systems. This system should be integrated into the shipboard routable network so that the shipboard network monitoring console receives alerts as described in Phase 2.

3. Establish Custom RMON MIB Variables that specifically meet SATCOM Terminal Monitoring Requirements

The ability to monitor a SATCOM terminal is essential to determining the complete status of the network connection. This could be accomplished via remote monitoring of the satellite terminal given the proper MIB and MIB variables. Through the use of RMON RFC 1757 group statistics and SNMP RFC 1213 interface and ICMP variables the monitoring console could provide some details for monitoring the status of the network extension if the terminal were SNMP enabled. But, it is the opinion of the thesis author that these MIBs do not have a complete set of variables needed for

monitoring satellite terminals. Therefore, it is important to identify and define the appropriate MIB variables desired in an effective satellite terminal monitoring capability.

a. Desired MIB Variables

Using the alarm page previously introduced in Figure 17 on page 34, the thesis author has developed the custom RMON MIB variables provided in Table 7 of Appendix D. These variables consist of monitoring the functions of the terminal's transmitter for low output power and fault indicators, receiver for fault indicators and signal to noise ratio statistics, and the antenna subsystems ability to track the satellite, to include the loss of the received Global Positioning System (GPS) navigational data.

- **txEvent**: Transmitter Faults– Reaction to Predetermined Condition. This variable would provide various transmitter fault indications (i.e., faulty SSPA, klystron or magnetron fault, or no modulation).
- **txPwrOutAlarm**: Transmitter Power Low – Predetermined Threshold Watch. This variable would provide an alarm at a predetermined value (i.e., the alarm would indicate that the transmitter is not operating at the minimum output power).
- **rxEvent**: Receiver Faults – Reaction to Predetermined Condition. This variable would provide various receiver fault indications (i.e., high noise level in receive path, faulty LNA, no receive signal).
- **snrInStatistics**: Real Time Receiver Signal to Noise Ratio – Current Statistics. This variable would provide continuous signal to noise values for monitoring the RF environment.
- **trackSatEvent**: Antenna Satellite Tracking – Reaction to Predetermined Condition to include loss of GPS input. This variable would provide various antenna subsystem fault indications (i.e., faulty antenna actuator, antenna limit position attained, or no GPS signal).

b. Proposed Custom RMON MIB Structure

Using the RMON MIB 1757 in concert with SNMP MIB 1213 would be beneficial to monitoring SNMP enabled satellite terminals from a network monitoring console. To enhance the monitoring capability of these MIBs, the thesis author proposes that the custom RMON MIB structure illustrated in Figure 37. This MIB structure

includes the use of SNMP interface and ICMP variables, as well as the standard RMON group variables. The recommended RMON variables for monitoring specific functions of a satellite terminal have been highlighted.

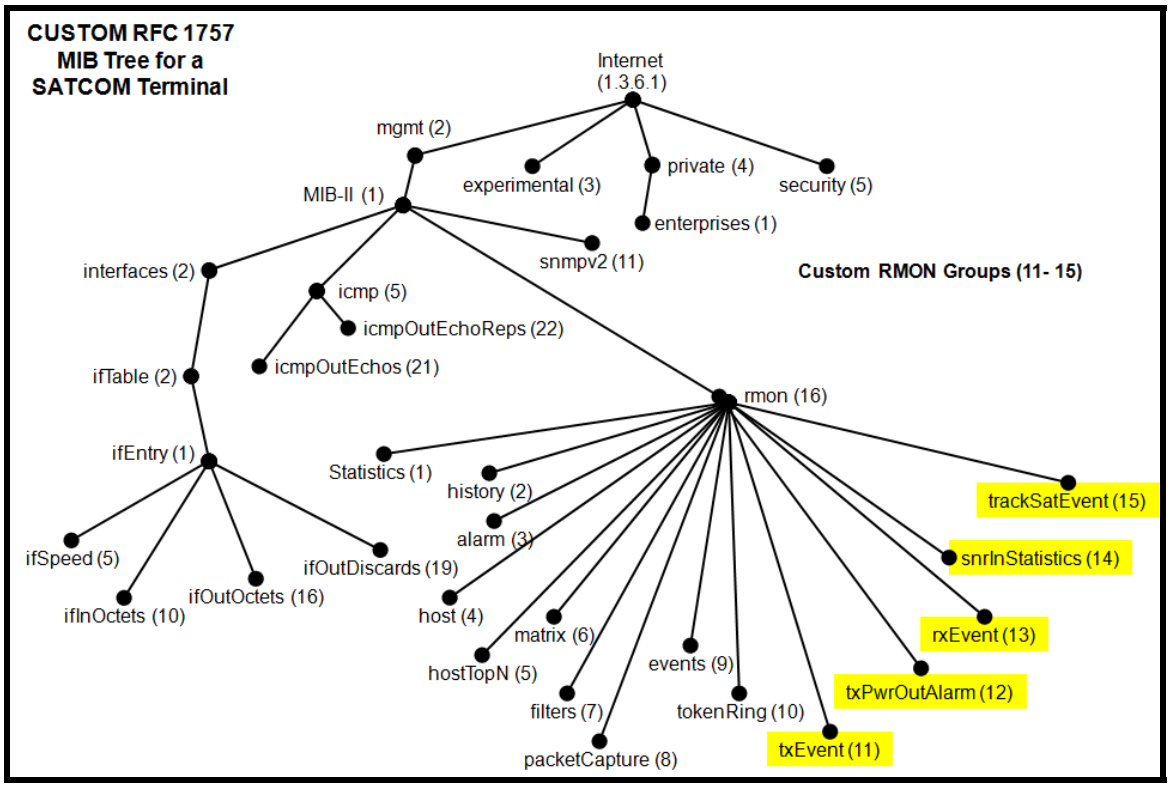

Figure 37. Proposed Custom RMON MIB Structure

The variables mentioned should not be considered as exhaustive. They provide only a starting point for future capabilities that could be incorporated into satellite terminals for improving the current monitoring capability of the extended network. With these variables and the proper NPM tools in place the network monitor console would have the detailed status information about the operational condition of the satellite terminal. This would also provide a more complete picture of the network's connectivity and how the network is affected by the condition of the satellite terminal.

B. FUTURE WORK

This thesis is only an initial effort for developing an adaptive access control capability for subscriber and base stations to sustain the extended Internet over a satellite connection. Additional efforts should be considered in the areas described below.

1. Encryption Requirements

Both individual circuits (circuit encryption) and the channel (bulk encryption) are used at each end of the satellite connection. Although a portion of the connection can be sustained through this thesis' recommendations, further research will be required to determine how, if at all, the data encryption can be sustained due to synchronization requirements of encryption, during periods when there is only a usable uplink or downlink.

2. Providing Satellite Communications Stations with an RFI Monitoring Capability

There is a need for satellite stations to be able to monitor the RF environment. Although most U.S. Naval ships have some version of the AN/SLQ-32 Information Warfare system, not all ships have it and it is not used for monitoring the satellite communications systems' RF environment. Therefore, further research is needed for providing an RF environmental monitoring capability for improved connectivity of satellite communications stations. Such a capability could be used to alert the subscriber of RF Interference (RFI) and assist the satellite station in making changes that overcome the RFI.

3. The Capability for a Subscriber Station to Change Bands (Ka, Ku, X)

In order to sustain a mobile users connection, it may be found advantageous to have the ability to change RF bands (i.e., Ka, Ku, X) and operate in an RF interference free environment in times when the RF environment adversely impacts the satellite connectivity. Further research would be required to determine the requirements of a

multiple RF band terminal and how it could switch from one band to another in order to sustain connectivity and continue using the same services.

4. Sustaining the Subscriber Station's Receive Capability

Once a subscriber's transmit RF signal degrades, or no longer appears at the satellite, the satellite access is discontinued resulting in a loss of both transmit and receive of all data through the affected satellite terminal. With an embedded SNMP agent in the SATCOM terminal equipment, the terminal would not only be capable of providing fault monitoring, but could also provide the proper "keep-alive" response to the based station access controller to prevent a system disconnect. This would give the U.S. Navy an adaptive capability for bidirectional SATCOM systems and sustain a receive capability that is currently not available. Therefore, further research is required for sustaining the receive portion of a SATCOM connection during times when the subscriber's transmitter experiences degradation or complete loss of transmit capability and there is a need to continue receiving data.

5. Software Coding/Programming for Creating an SNMPv3 Keep-Alive Message

The satellite channel access control system monitors the RF connection of the subscriber station's access. Should the subscriber's RF signal degrade or no longer appear at the satellite, an alarm notifies the satellite channel access control operator. The access control operator will direct the STEP Site to disconnect the subscriber's services, if the subscriber does not respond to the control operator's requests. The access control operator only needs to receive a keep-alive notice from the subscriber station in order to sustain the connectivity of a satellite communications system. This notice cannot be sent at times when the subscriber station cannot transmit. Through the use of a backchannel, a keep-alive notice could be sent by SNMPv3 message via the routable network behind the terminal equipment of the station. Therefore, further research is required for creating the programming code necessary for obtaining and inserting the proper information (IP addresses, payload, and additional information) to create a SNMPv3 keep-alive message destined for the Channel Access Control system.

6. Automation of the Satellite Access Control Process

Gaining access to the satellite and supporting STEP Site resources is performed manually. This is one reason why the subscriber must submit a SAR. Once approved for access, the subscriber must make a telephone call to the access control operator to make the initial connection (see satellite access procedures in NTP 2). This access process is inefficient and inflexible. Therefore, further research is required for establishing an automated satellite access process. Through an automated satellite access control process subscribers would be able to gain initial access and sustain access to the satellite improving subscriber accessibility and adaptability. This capability could be provided through SNMPv3 messages via a backchannel to the routable network behind the subscriber's terminal equipment.

7. Sustaining the DISA Gateway Router Connection

If a subscriber's RF signal degrades or no longer appears at the satellite there is not only a satellite access issue but in addition, the DISA Gateway router no longer receives responses from the subscriber's router, indicating a line failure. When this happens the DISA Gateway Desk receives an alarm. The DISA Gateway Desk will have the subscriber disconnected from the DISA Gateway router if the subscriber does not take corrective action or cannot be contacted in a reasonable time. Therefore, further research is required for sustaining the router to router connection (i.e., subscriber router to DISA Gateway router) during times when the subscriber's transmitter experiences degradation or complete loss of transmit capability and there is a need to continue receiving data.

APPENDIX A: SELECTIVE COMMERCIAL COMMUNICATIONS SATELLITE CHRONOLOGY

The following Selective Communications Satellite Chronology was provided by the National Aeronautics and Space Administration (NASA), History Division, COMMUNICATIONS SATELLITES SHORT HISTORY web page in the article "Communications Satellites: Making the Global Village Possible" by David J. Whalen unless otherwise referenced (Whalen, n.d.):

- 1945 Arthur C. Clarke Article: "Extra-Terrestrial Relays"
- 1955 John R. Pierce Article: "Orbital Radio Relays"
- 1956 First Trans-Atlantic Telephone Cable: TAT-1
- 1957 Sputnik: Russia launches the first earth satellite.
- 1960 1st Successful DELTA Launch Vehicle
- 1960 AT&T applies to FCC for experimental satellite communications license
- 1961 Formal start of TELSTAR, RELAY, and SYNCOM Programs
- 1962 TELSTAR and RELAY launched
- 1962 Communications Satellite Act (U.S.)
- 1963 SYNCOM launched
- 1964 INTELSAT formed
- 1965 COMSAT's EARLY BIRD: 1st commercial communications satellite
- 1969 INTELSAT-III series provides global coverage
- 1972 ANIK: 1st Domestic Communications Satellite (Canada)
- 1974 WESTAR: 1st U.S. Domestic Communications Satellite
- 1975 INTELSAT-IVA: 1st use of dual-polarization
- 1975 RCA SATCOM: 1st operational body-stabilized comm. satellite
- 1976 MARISAT: 1st mobile communications satellite
- 1976 PALAPA: 3rd country (Indonesia) to launch domestic comm. satellite
- 1979 INMARSAT formed

- 1981 third and fourth Ariane rockets launched by the European Space Agency (Marson, 1997)
- 1983 Venera 15 returns first photos of Venus polar region- USSR
- 1983 Inferred Astronomical satellite discovers new comets, asteroids, galaxies and a dusting around the star vega that may be new planets (Marson, 1997)
- 1984 Vega 1 and 2 launched, drops probes into Venus's atmosphere- Soviet/ international (Marson, 1997)
- 1985 Skigate launched by Japan's institute space and aeronautical science first to rendezvous with Haley's comet (Marson, 1997)
- 1989 Phobous 2 orbits Mars studying atmosphere and magnetic field- Soviet/ international (Marson, 1997)
- 1989 Galileo launched from shuttle Atlantis took pictures of Venus and asteroid Ida then continues to Jupiter- US (Marson, 1997)
- 1991 Globalstar project launched in as a joint venture of Loral Corporation and Qualcomm ("Globalstar," n.d.)
- 1993 (September) NASA launched an experimental Advanced Communications Technology Satellite (ACTS) with imbedded SNMP capability (Bergamo & Hoder, n.d.)
- 1995 Globalstar received its U.S. spectrum allocation from the FCC ("Globalstar," n.d.)
- May 5, 1997 through May 17, 1998 72 Iridium satellites put into the intended orbits ("Iridium," n.d.)
- 1998 First Globalstar satellites launched ("Globalstar," n.d.)
- 1998 (November 1) First call on the original Globalstar system was placed ("Globalstar," n.d.)
- 1999 RFC 2488 Enhancing TCP Over Satellite Channels using Standard Mechanisms
- 2000, Last of 52 Globalstar satellites launched ("Globalstar," n.d.)
- IP MultiMedia Over Satellite (IMMSAT) RFC 2327 is a session description protocol for long delays over satellite
- 2002 Iridium spare satellites launched for a total of 7 spares ("Iridium," n.d.)
- 2004 Restructuring of old Globalstar completed ("Globalstar," n.d.)
- 2007 Globalstar launched eight additional first-generation spare satellites into space ("Globalstar," n.d.)

APPENDIX B: SELECTIVE MILITARY COMMUNICATIONS SATELLITE CHRONOLOGY

The following Selective Military Communications Satellite Chronology was obtained from information in the article "A History of U.S. Military Satellite Communications Systems" by Donald H. Martin unless otherwise referenced (Martin, n.d.*a*):

- In 1958, The first artificial communication satellite, Project SCORE (Signal Communication by Orbiting Relay Equipment) was launched
  - Primarily to show that an Atlas missile could be put into orbit and
  - To demonstrate a communications repeater built into the missile
- In October 1960, the launch of the Courier program satellite was successful
  - The goal was to develop a satellite of higher capacity and longer life than SCORE
- In 1960, Advanced Research Projects Agency undertook the Advent program, concurrent with the Courier program
  - The goal was to provide an operational military communication satellite
  - This program was cancelled in 1962 due to lacking the available technology to meet the sophisticated program concept
- In 1962, the West Ford "satellite" project resulted from a Lincoln Laboratory study on secure, survivable, reliable communications
  - During the first few weeks after launch, voice and data were transmitted from Pleasanton, California, reflected by wires hanging from the satellite, and received at Westford, Massachusetts
- In 1962, the Advent program was canceled and the Initial Defense Communication Satellite Program (IDCSP) was created
  - The IDCSP satellites were the DSCS Phase I space segment
  - Seven IDCSP satellites were launched in 1966
  - Additional groups of three to eight satellites launched in 1967 and 1968
  - Increasing military activity in Vietnam led to the establishment of an operational communication link using IDCSP where digital data

were transmitted from Vietnam to Hawaii through one satellite and on to Washington, D.C.

- In 1968, the system was declared operational, and its name was changed to Initial Defense Satellite Communication System

- The Lincoln Experimental Satellites (LES) series resulted from continued studies in space technology by Lincoln Laboratory after the West Ford program
  - Launched in 1965, LES-1 through LES-4 carried equipment for communication and propagation experiments
  - The LES-5 and -6 satellites, launched in 1967 and 1968, respectively, had communications equipment that operated in the UHF band
- In 1969, TACSAT (Tactical Satellite) was launched
  - Testing was done with a variety of terminals, including large ground stations, mobile ground stations, aircraft, and ships
  - TACSAT was used for operational support of Apollo recovery operations
  - Military use, especially of the UHF band, was extensive
  - Operations continued until an attitude-control failure in 1972
- In 1973, the Defense Communications Agency (DCA), now the Defense Information Systems Agency, was assigned responsibility for developing the MILSATCOM architecture for the Department of Defense
- In 1976, the first comprehensive Military Satellite (MILSATCOM) architecture was published
- With the DSCS Phase I space segment starting with IDCSP satellites in 1968, the DoD decided to proceed with the development of satellites for DSCS Phase II of the wideband satellite systems
- The wideband systems are the Defense Satellite Communication Systems (DSCS) II and III and the Global Broadcast Service (GBS) payload on the UHF Follow-On (UFO) satellite
- In 1971, the DSCS II program began with the first of six satellites launched in pairs
  - By 1989 a total of 16 satellites were launched to establish and maintain an orbital constellation with at least four active and two spare satellites
  - All are now out of service
- In 1977, program development of the DSCS III began

- The first satellite was launched in 1982
- 11 additional satellites have been launched since then
- All are currently operational

- Global Broadcast Service (GBS) is part of the wideband MILSATCOM program
  - Phase I of GBS used a commercial satellite and a limited number of commercial receive terminals
  - Phase II uses the GBS payload on UFO satellites 8 through 10 with 30-gigahertz uplink and 20-gigahertz downlink frequencies, often called Ka-band
  - Phase III will be developed in the future
- In 1978, the first Fleet Satellite Communications (FLTSATCOM), the last in 1989
  - Served Navy surface ships, submarines, aircraft, and shore stations
- In 1976 and 1977 Congress directed DoD to increase its use of leased commercial satellite services, and specifically applied this direction to the tactical satellite system that would follow FLTSATCOM
  - As a result, the LEASAT program, primarily served the Navy, plus Air Force and ground forces mobile users
  - The first two launches took place in 1984, the last in 1990
  - Leases on satellites 2, 3, and 5 were extended into 1996
  - LEASATs have been removed from service and replaced by UFO satellites
- In 1988, the UFO contract was awarded. UFO satellites replaced the Navy's FLTSATCOM and LEASAT satellites: a constellation of eight UFOs, plus one spare
  - A contract for an eleventh satellite was signed in 1999
  - Nine of ten were successfully launched between 1993 and 1999 with satellite 11 launched in 2003
- FLTSATCOM satellites 7 and 8 contained an EHF payload (44-gigahertz uplink and 20-gigahertz downlink) called the FEP (FLTSATCOM EHF Package)
  - Developed to demonstrate operational capabilities of EHF terminals and prove key functions of the MILSTAR system

- In 1988, the UFO contract was awarded. UFO satellites replaced the Navy's FLTSATCOM and LEASAT satellites: a constellation of eight UFOs, plus one spare
    - A contract for an eleventh satellite was signed in 1999
    - Nine of ten were successfully launched between 1993 and 1999 with satellite 11 launched in 2003
- The MILSTAR program includes two Block I and four Block II satellites. These blocks are also known as LDR (low data rate) or MILSTAR I, and MDR (medium data rate) or MILSTAR II
    - The block change resulted from a 1990 program restructure in response to global political changes
    - The Block I satellites were launched in 1994 and 1995
    - The second was launched in 2001
    - The third was launched in January, 2002
    - The last one is scheduled for launch in November, 2002
- The Interim Polar Program adapted the UFO/EHF payload for use on host satellites in high-inclination orbits
    - These payloads support military forces operating above 65 degrees north latitude
    - The first launch with an interim polar payload was in 1997
    - Two additional launches occurred in 2003 and 2005

APPENDIX C: SELECTIVE INTERNET CHRONOLOGY

The following Selective Internet chronology was obtained from information in the article "History of the Internet: Timeline" By Dave Marshall unless otherwise referenced (Marshall, n.d.):

- 1969- Birth of Internet
  - ARPANET commissioned by DoD for research into networking
  - First node at UCLA (Los Angeles) closely followed by nodes at Stanford Research Institute, UCSB (Santa Barbara) and U of Utah (4 Nodes).
- 1971- People communicate over a network
  - 15 nodes (23 hosts) on ARPANET.
  - E-mail invented—a program to send messages across a distributed network.
- 1972- Computers can connect more freely and easily
  - First public demonstration of ARPANET between 40 machines.
  - Internetworking Working Group (INWG) created to address need for establishing agreed upon protocols.
  - Telnet specification
- 1973- Global Networking becomes a reality
  - First international connections to the ARPANET: University College of London (England) and Royal Radar Establishment (Norway)
  - Ethernet outlined—this how local networks are basically connected today.
  - Gateway architecture sketched on back of envelope in hotel lobby in San Francisco. Gateways define how large networks (maybe of different architecture) can be connected together.
  - File Transfer protocol specified—how computers send and receive data.
- 1974- Packets become mode of transfer
  - Transmission Control Program (TCP) specified. Packet network Intercommunication—the basis of Internet Communication.

- Telenet, a commercial version of ARPANET, opened—the first public packet data service.

- 1976- Networking comes to many
  - Queen Elizabeth sends out an e-mail.
  - UUCP (Unix-to-Unix CoPy) developed at AT&T Bell Labs and distributed with UNIX.
  - UNIX the main operating system used by universities and research establishments could now "talk" over a network.
- 1977- E-mail takes off, Internet becomes a reality
  - Number of hosts breaks 100.
  - THEORYNET provides electronic mail to over 100 researchers in computer science (using a locally developed E-mail system and TELENET for access to server).
  - Mail specification
  - First demonstration of ARPANET/Packet Radio Net/SATNET operation of Internet protocols over gateways.
- 1979- News Groups born
  - Computer Science Department research computer network established in USA.
  - USENET (A collection of discussions groups, news groups established) using UUCP.
  - First MUD (Multiuser Dungeon)—interactive multiuser sites. Interactive adventure games, board games, rich and detailed databases.
  - ARPA establishes the Internet Configuration Control Board (ICCB).
  - Packet Radio Network (PRNET) experiment starts with ARPA funding. Most communications take place between mobile vans.
- 1981- Things start to come together

  BITNET, the "Because It's Time NETwork" Started as a cooperative network at the City University of New York, with the first connection to Yale
  - CSNET (Computer Science NETwork) established to provide networking services (especially E-mail) to university scientists with no access to ARPANET. CSNET later becomes known as the Computer and Science Network.

- 1982- TCP/IP defines future communication
    - DCA and ARPA establishes the Transmission Control Protocol (TCP) and Internet Protocol (IP), as the protocol suite, commonly known as TCP/IP, for ARPANET.
    - External Gateway Protocol specification—EGP is used for gateways between (different architecture) networks.
- 1983- Internet gets bigger
    - Name server developed with large number of nodes.
    - Desktop workstations come into being.
    - Internet Activities Board (IAB) established, replacing ICCB
    - Berkeley releases new version of UNIX 4.2BSD incorporating TCP/IP.
    - EARN (European Academic and Research Network) established on similar lines to BITNET
- 1984- Growth of Internet Continues
    - Number of hosts breaks 1,000.
    - Domain Name Server (DNS) introduced (e.g., www.cs.cf.ac.uk).
    - JANET (Joint Academic Network) established in the UK
- 1986- Power of Internet Realized
    - 5, 000 Hosts. 241 News groups.
    - NSFNET created (backbone speed of 56 Kbps)
    - NSF establishes 5 super-computing centers to provide high-computing power for all—This allows an explosion of connections, especially from universities.
    - Network News Transfer Protocol (NNTP) designed to enhance Usenet news performance over TCP/IP.
- 1987- Commercialization of Internet Born
    - Number of hosts 28,000.
    - UUNET is founded with Usenix funds to provide commercial UUCP and Usenet access.
- 1988
    - NSFNET backbone upgraded to T1 (1.544 Mbps)
    - Internet Relay Chat (IRC) developed

- 1989- Large growth in Internet
  - Number of hosts breaks 100,000
  - First relays between a commercial electronic mail carrier and the Internet
  - Internet Engineering Task Force (IETF) and Internet Research Task Force (IRTF) comes into existence under the IAB
- 1990- Expansion of Internet continues
  - 300,000 Hosts. 1,000 News groups
  - ARPANET ceases to exist
  - Archie released files can be searched and retrieved (FTP) by name.
  - The World comes on-line (world.std.com), becoming the first commercial provider of Internet dial-up access.
- 1991- Modernization Begins
  - Commercial Internet eXchange (CIX) Association, Inc. formed after NSF lifts restrictions on the commercial use of the Net.
  - Wide Area Information Servers (WAIS)
  - Large bodies of knowledge available: E-mail messages, text, electronic books, Usenet articles, computer code, image, graphics, sound files, databases etc.
  - Powerful search techniques implemented. Keyword search.
- 1991- Friendly User Interface to WWW established
  - Gopher released by Paul Lindner and Mark P. McCahill from the U of Minnesota.
  - World-Wide Web (WWW) released by CERN; Tim Berners-Lee developer (Initially non-graphic, see MOSAIC, 1993).
  - NSFNET backbone upgraded to T3 (44.736 Mbps). NSFNET traffic passes 1 trillion bytes/month and 10 billion packets/month
  - Start of JANET IP Service (JIPS) using TCP/IP within the UK academic network.
- 1992- Multimedia changes the face of the Internet
  - Number of hosts breaks 1 Million. News groups 4,000
  - Internet Society (ISOC) is chartered.
  - First MBONE audio multicast (March) and video multicast (November).

    - The term “Surfing the Internet” is coined by Jean Armour Polly.
- 1993- The WWW Revolution truly begins
    - Number of Hosts 2 Million. 600 WWW sites.
    - InterNIC created by NSF to provide specific Internet services
    - Business and Media really take notice of the Internet.
    - US White House and United Nations (UN) comes on-line.
    - MOSIAC (User Friendly Graphical Front End to the World Wide Web) takes the Internet by storm (Develops into Netscape)
- 1994- Commercialization begins
    - Number of Hosts 3 Million. 10,000 WWW sites. 10,000 News groups.
    - ARPANET/Internet celebrates 25th anniversary
    - Local communities begin to be wired up directly to the Internet (Lexington and Cambridge, Mass., USA)
    - US Senate and House provide information servers
    - Shopping malls, banks arrive on the Internet
    - NSFNET traffic passes 10 trillion bytes/month
    - WWW edges out telnet to become 2nd most popular service on the Net (behind ftp-data) based on % of packets and bytes traffic distribution on NSFNET
- 1995- Commercialization continues apace
    - 6.5 Million Hosts, 100,000 WWW Sites.
    - NSFNET reverts back to a research network. Main US backbone traffic now routed through interconnected network providers
    - WWW surpasses ftp-data in March as the service with greatest traffic on NSFNet based on packet count, and in April based on byte count
    - Traditional online dial-up systems (Compuserve, America Online, Prodigy) begin to provide Internet access
    - A number of Net related companies go public, with Netscape leading the pack.
    - Registration of domain names is no longer free.

- New WWW technologies Emerge Technologies with mobile code (JAVA, JAVAscript, ActiveX), Virtual environments (VRML), and Collaborative tools (CU-SeeMe)

- 1996- Microsoft enters
  - 12.8 Million Hosts, 0.5 Million WWW Sites.
  - Internet phones catch the attention of US telecommunication companies who ask the US Congress to ban the technology (which has been around for years)
  - The WWW browser war begins, fought primarily between Netscape and Microsoft, has rushed in a new age in software development, whereby new releases are made quarterly with the help of Internet users eager to test upcoming (beta) versions.

The following Selective Internet chronology was obtained from information in the article "Hobbes' Internet Timeline 10.1" By Robert H. Zakon unless otherwise referenced (Zakon, 2010):

- 2000's Internet technology continues improvement
  - A massive denial of service attack is launched against major web sites, including Yahoo, Amazon, and eBay in early February
  - Web size estimates by NEC-RI and Inktomi surpass 1 billion indexable pages
  - Internet2 backbone network deploys IPv6 (16 May)
  - Mexico's connection to Internet2 becomes fully operational as the California research network (CalREN-2) is connected with Mexico's Corporación Universitaria para el Desarrollo de Internet (CUDI) network.
  - RFC 2795: The Infinite Monkey Protocol Suite
  - Emerging Technologies: Wireless devices, IPv6
- 2001
  - High schools in five states (Michigan, Missouri, Oregon, Virginia, and Washington) become the first to gain Internet2 access
  - European Council finalizes an international cybercrime treaty on 22 June and adopts it on 9 November. This is the first treaty addressing criminal offenses committed over the Internet.
  - Afghanistan's Taliban bans Internet access country-wide, including from Government offices, in an attempt to control content (13 Jul)

- Brazil RNP2 is connected to Internet2's Abilene over 45Mbps line (21 Aug)
- First uncompressed real-time gigabit HDTV transmission across a wide-area IP network takes place on Internet2 (12 Nov).
- RFC 3091: Pi Digit Generation Protocol
- RFC 3092: Etymology of "Foo"
- RFC 3093: Firewall Enhancement Protocol (FEP)
- Emerging Technologies: Grid Computing, P2P

- 2002
  - US ISP Association (USISPA) is created from the former CIX (11 Jan)
  - Global Terabit Research Network (GTRN) is formed composed of two OC-48 2.4GB circuits connecting Internet2 Abiline, CANARIE CA*net3, and GÉANT (18 Feb)
  - The highest Wi-Fi network in the northeast US is deployed by this Timeline's author. The solar-powered network bridges Mounts Washington and Wildcat in New Hampshire
  - Abilene (Internet2) backbone deploys native IPv6 (5 Aug)
  - Internet2 now has 200 university, 60 corporate, and 40 affiliate members (2 Sep)
  - Having your own Blog becomes hip
  - The FBI teams up with Terras Lycos to disseminate virtual wanted posts across the Web portal's properties (11 Dec)
  - RFC 3251: Electricity over IP
  - RFC 3252: Binary Lexical Octet Ad-hoc Transport
- 2003
  - Public Interest Registry (PIR) takes over as .org registry operator on 1 Jan. Transition is completed on 27 Jan. By giving up .org, VeriSign is able to retain control over .com domains
  - The SQL Slammer worm causes one of the largest and fastest spreading DDoS attacks ever.
  - Flash mobs, organized over the Net, start in New York and quickly form in cities worldwide
  - Last Abilene segment upgraded to 10Gbps (5 Nov)

- Little GLORIAD (Global Ring Network for Advanced Application Development) starts operations (22 Dec), consisting of a networked ring across the northern hemisphere with connections in Chicago, Amsterdam, Moscow, Novosibirsk, Zabajkal'sk, Manzhouli, Beijing, and Hong Kong. This is the first-ever fiber network connections across the Russia-China border
- RFC 3514: The Security Flag in the IPv4 Header (The Evil Bit)

- 2004
  - For the first time, there are more instances of DNS root servers outside the US with the launch of an anycast instance of the RIPE NCC operated K-root server
  - Abiline, the Internet2 backbone, upgrade from 2.5Gbps to 10Gbps is completed (4 Feb)
  - CERNET2, the first backbone IPv6 network in China, is launched by the China Education and Research Network (CERN) connecting 25 universities in 20 cities at speeds of 1-10Gbps (27 Dec)
  - Emerging Technologies: Social networking, Web mashups
  - RFC 3751: Omniscience Protocol Requirements
- 2005
  - Pakistan suffers a near complete Internet outage as a submarine cable becomes defective (Jun)
  - RFC 4041: Requirements for Morality Sections in Routing Area Drafts
  - RFC 4042: UTF-9 and UTF-18 Efficient Transformation Formats of Unicode
- 2006
  - US Government prohibits private (anonymized) domain registrations for .us after 26 Jan
  - ICANN board votes against .xxx TLD (10 May)
  - Internet connectivity to southeast Asia is severely limited after major fiber optic lines are severely damaged by an earthquake in Taiwan and subsequent underwater mudslides (Dec)
  - Emerging Technologies: Cloud computing
- 2007

- ICANN drops .um domain name (US minor outlying islands) for lack of use (Jan) and terminates RegisterFly.com's registrar status on 16 Mar (effective 31 Mar)
- Internet2 completes US East to West coast span of its 100GB/s network on 13 Oct
- RFC 4824: The Transmission of IP Datagrams over the Semaphore Flag Signaling System (SFSS)

- 2008
  - NASA successfully tests the first deep space communications network modeled on the Internet, using the Disruption-Tolerant Networking (DTN) software
  - Google's crawler reaches 1 trillion pages, although only a fraction are indexed by the search engine. For comparison, Google's original index had 26 million pages in 1998, and reached 1 billion in 2000
  - IPv6 addresses are added for the first time to 6 of the root zone servers (4 Feb)
  - RFC 5241: Naming Rights in IETF Protocols
  - RFC 5242: A Generalized Unified Character Code: Western European and CJK Sections
- 2009
  - DNSSEC becomes operational on .gov (28 Feb), .org (2 Jun), .us (15 Dec)
  - US Department of Commerce relaxes control over ICANN, in favor of a multi-national oversight group
  - Twitter is asked by the US Government to delay planned maintenance of its service on 15 June as a result of heavy use by Iranian users during unrest in that country
  - RFC 5513: IANA Considerations for Three Letter Acronyms
  - RFC 5514: IPv6 over Social Networks

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D: TABLES

RFC	Definition
1155	Structure and identification of management information for TCP/IP-based Internets
1156	Management Information Base for network management of TCP/IP-based Internets
1157	Simple Network Management Protocol (SNMP)
1158	Management Information Base for network management of TCP/IP-based Internets: MIB-II
1159	Message Send Protocol
1160	Internet Activities Board
1161	SNMP over OSI
1270	SNMP communications services
1271	Remote network monitoring Management Information Base
1900	Renumbering needs work
1901	Introduction to community-based SNMPv2
1902	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
1903	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
1904	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
1905	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
1906	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)
1908	Coexistence between Version 1 and Version 2 of the Internet-standard Network Management Framework
1909	An Administrative Infrastructure for SNMPv2

Table 1. List of Relevant SNMP MIBs (From Bates, 2002, p. 582)

RMON 1 MIB Group	Function	Elements
Statistics	Contains statistics measured by the probe for each monitored interface on this device.	Packets dropped, packets sent, bytes sent (octets), broadcast packets, multicast packets, CRC errors, runts, giants, fragments, jabbers, collisions, and counters for packets ranging from 64 to 128, 128 to 256, 256 to 512, 512 to 1024, and 1024 to 1518 bytes.
History	Records periodic statistical samples from a network and stores for retrieval.	Sample period, number of samples, items sampled.
Alarm	Periodically takes statistical samples and compares them with set thresholds for events generation.	Includes the alarm table and requires the implementation of the event group. Alarm type, interval, starting threshold, stop threshold.
Host	Contains statistics associated with each host discovered on the network.	Host address, packets, and bytes received and transmitted, as well as broadcast, multicast, and error packets.
HostTopN	Prepares tables that describe the top hosts.	Statistics, host(s), sample start and stop periods, rate base, duration.
Matrix	Stores and retrieves statistics for conversations between sets of two addresses.	Source and destination address pairs and packets, bytes, and errors for each pair.
Filters	Enables packets to be matched by a filter equation for capturing or events.	Bit-filter type (mask or not mask), filter expression (bit level), conditional expression (and, or not) to other filters.
Packet Capture	Enables packets to be captured after they flow through a channel.	Size of buffer for captured packets, full status (alarm), number of captured packets.

Table 2. RMON1 MIB Group Functions (From RMON, n.d.)

RMON 2 MIB Group	Functions
Protocol Directory	The Protocol Directory is a simple and interoperable way for an RMON2 application to establish which protocols a particular RMON2 agent implements. This is especially important when the application and the agent are from different vendors
Protocol Distribution	Mapping the data collected by a probe to the correct protocol name that can then be displayed to the network manager.
Address mapping	Address translation between MAC-layer addresses and network-layer addresses which are much easier to read and remember. Address translation not only helps the network manager, it supports the SNMP management platform and will lead to improved topology maps.
Network Layer host	Network host (IP layer) statistics
Network layer matrix	Stores and retrieves network layer (IP layer) statistics for conversations between sets of two addresses.
Application layer host	Application host statistic
Application layer matrix	Stores and retrieves application layer statistics for conversations between sets of two addresses.
User history	This feature enables the network manager to configure history studies of any counter in the system, such as a specific history on a particular file server or a router-to-router connection
Probe configuration	This RMON2, feature enable one vendor's RMON application to remotely configure another vendor's RMON probe.

Table 3. RMON2 MIB Group Functions (From RMON, n.d.)

S.No	Interface Details	Description
1.	ifNumber	Specifies the number of network interfaces (regardless of their current state) present on this system.
2.	ifDescr	Specifies a description about the interface. This string should include the name of the manufacturer, the product name, and the version of the hardware interface.
3.	ifType	Specifies the type of interface. This indicates the physical/link protocol(s) below the network layer in the protocol stack.
4.	ifMtu	Specifies the size of the largest datagram that can be sent or received on the interface, specified in octets. For interfaces that transmit network datagrams, this is the size of the largest network datagram that can be sent on the interface.
5.	ifSpeed	Specifies an estimate of the interface's current bandwidth in bits per second. For interfaces that do not vary in bandwidth or for those where no accurate estimation can be made, this object should contain the nominal bandwidth.
6.	ifPhysAddress	Specifies the interface's address at the protocol layer immediately below the network layer in the protocol stack. For interfaces that do not have such an address (for example, a serial line), this object should contain an octet string of zero length.
7.	ifAdminStatus	Specifies the desired state of the interface. The testing(3) state indicates that no operational packets can be passed.
8.	ifOperStatus	Specifies the current operational state of the interface. The testing(3) state indicates that no operational packets can be passed.
9.	ifLastChange	Specifies the value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then this object indicates zero.
10.	ifInOctets	Specifies the total number of octets received on the interface, including framing characters.
11.	ifInUcastPkts	Specifies the number of subnetwork unicast packets delivered to a higher-layer protocol.
12.	ifInNUcastPkts	Specifies the number of non-unicast (for example, subnetwork broadcast or subnetwork Multicast) packets delivered to a higher-layer protocol.

Table 4. RFC 1213 Interface Details (From STRM: SNMP Agent Guide, 2008)

S.No	Interface Details	Description
13.	ifInDiscards	Specifies the number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
14.	ifInErrors	Specifies the number of inbound packets that contained errors preventing them from being deliverable to a higher layer protocol.
15.	ifInUnknownProtos	Specifies the number of packets received through the interface that were discarded because of an unknown or unsupported protocol.
16.	ifOutOctets	Specifies the total number of octets transmitted out of the interface, including framing characters.
17	ifOutUcastPkts	Specifies the total number of packets that higher level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
18.	ifOutNUcastPkts	Specifies the total number of packets that higher level protocols requested be transmitted to a non-unicast (for example, a subnetwork broadcast or subnetwork Multicast) address, including those that were discarded or not sent.
19	ifOutDiscards	Specifies the number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
20.	ifOutErrors	Specifies the number of outbound packets that could not be transmitted because of errors.
21.	ifOutQLen	Specifies the length of the output packet queue (in packets).
22.	ifSpecific	Specifies the reference to MIB definitions specific to the particular media being used for the interface. For example, if the interface is Ethernet, then the value of this object refers to a document defining objects specific to Ethernet. If this information is not present, its value should be set to the OBJECT IDENTIFIER { 0 0 }, which is a valid object identifier, and any valid implementation of ASN.1 and BER must be able to generate and recognize this value.

Table 5. RFC 1213 Interface Details (Continued) (From STRM: SNMP Agent Guide, 2008)

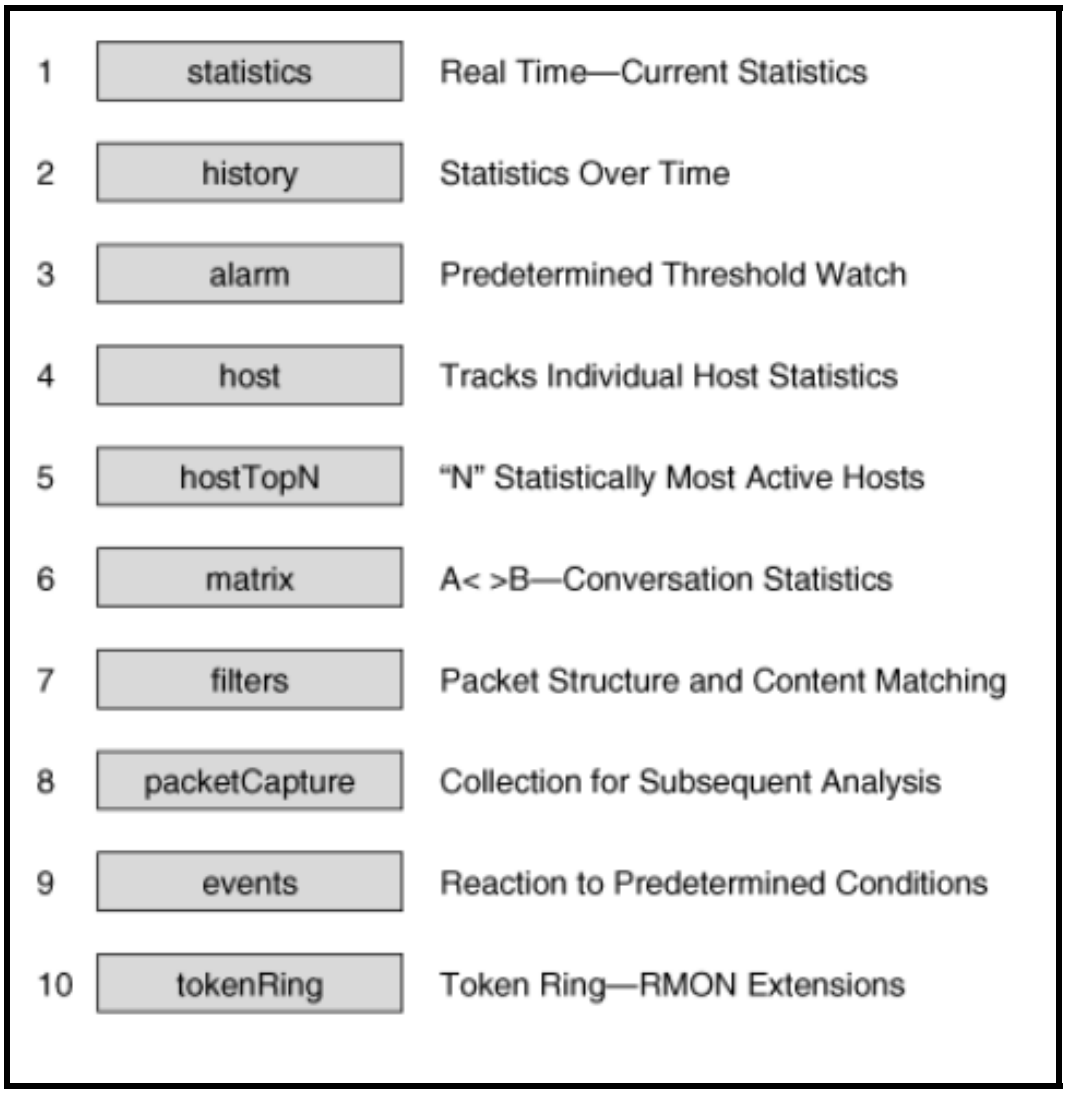

Table 6. RFC 1757: RMON Groups (From Teare, 2008)

CUSTOM SATCOM TERMINAL RMON STATISTIC GROUPS		
1	txEvent	Transmitter Faults– Reaction to Predetermined Condition
2	txPwrOutAlarm	Transmitter Power Low – Predetermined Threshold Watch
3	rxEvent	Receiver Faults – Reaction to Predetermined Condition
4	snrInStatistics	Real Time Receiver Signal to Noise Ratio – Current Statistics
5	trackSatEvent	Antenna Satellite Tracking – Reaction to Predetermined Condition to include loss of GPS input

Table 7. Custom RMON Statistic Groups for SATC Terminals

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alberts, D. S. & Hayes, R. E. (2002). Code of Best Practice for Experimentation, Washington, DC: CCRP Publication Series, DODCCRP, Retrieved on 23 September 2011 from http://www.dodccrp.org/files/Alberts_Experimentation.pdf

"AN/SLQ-32 Electronic Warfare (EW) system," (n.d.). FAS, Retrieved on 28 August 2011 from http://www.fas.org/man/dod-101/sys/ship/weaps/an-slq-32.htm

"AN/SLQ-32 Electronic Warfare Suite," (n.d.). Wikipedia, Retrieved on 28 August 2011 from http://en.wikipedia.org/wiki/AN/SLQ-32_Electronic_Warfare_Suite

"ATCi Introduces Warrior Satellite Monitoring System: Packaged System Allows Government and Military Entities Complete Satellite Monitoring, Transmission and RF Jamming Capabilities," (n.d.). ATCi, Retrieved on 27 August 2011 from http://www.atci.com/presswarrior.php

"Automated Digital Network System (ADNS)," (n.d.). GlobalSecurity, Retrieved on 4 February 2011 from http://www.globalsecurity.org/military/systems/ship/systems/adns.htm

Bao, L. & Garcia-Luna-Aceves, J.J. (n.d.). Link-State Routing in Networks with Unidirectional Links, UCSC, Retrieved on 25 June 2011 from http://ccrg.soe.ucsc.edu/publications/bao.ic3n99.pdf

Bates, R. J. (2002). Network Management SNMP. In *Broadband Telecommunications Handbook, Second Edition*. (pp. 575–595). Blacklick, OH: McGraw-Hill Professional Publishing, Retrieved on 06 August 2011 from http://www.scribd.com/doc/60856133/Network-Management-SNMP

Bergamo, M. A. & Hoder, D. (n.d.). Gigabit Satellite Network Using NASA's Advanced Communications Technology Satellite (ACTS): Features, Capabilities, and Operations, PSU, Retrieved on 25 June 2011 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.52.792&rep=rep1&type=pdf

Bordetsky, A. & Hayes-Roth, R. (2007). Extending the OSI model for wireless battlefield networks: a design approach to the 8th Layer for tactical hyper-nodes. *International Journal of Mobile Network Design and Innovation Archive*, *2*(2), pp. 81–91.

Buddenberg, R. (n.d.). Toward an interoperability architecture, DoDCCRP, Retrieved on 31 May 2011 from http://www.dodccrp.org/events/6th_ICCRTS/Tracks/Papers/Track1/020_tr1.pdf

"Cisco 3600 Series Multiservice Platforms," (n.d.). Cisco, Retrieved on 5 August 2011 from http://www.cisco.com/en/US/products/hw/routers/ps274/products_data_sheet09186a0080091f6f.html

"dopplerVUE: Integrated Network Performance Monitoring," (n.d.). Kratos Network Solutions, Retrieved on 28 August 2011 from http://www.kratosnetworks.com/products/dopplervue/integrated_network_performance_monitoring/

"dopplerVUE: Total Network Management," (n.d.). Kratos Network Solutions, Retrieved on 28 August 2011 from http://www.kratosnetworks.com/products/dopplervue/total_network_management

"Earth Station" (Card00742_fr.jpg). (n.d.). CardCow, Retrieved on 06 August 2011 from http://www.cardcow.com/images/set228/card00742_fr.jpg

Freeman, M. (28 December 2009). ViaSat CEO Aiming for the Sky [San Diego Union-Tribune], TMCNet, Retrieved on 06 August 2011from http://www.tmcnet.com/usubmit/2009/12/28/4550731.htm

"Globalstar," (n.d.). Wikipedia, Retrieved on 17 August 2011 from http://en.wikipedia.org/wiki/Globalstar

"High Speed Modems for C4I Satcom," (2011). ViaSat, Retrieved on 25 July 2011 from http://www.viasat.com/government-communications/high-speed-modems

"Information Professional Basic Course," (July 2008), Center for Information Dominance, Corry Station, CIN: A-202-0006, pp. 5-32–9-21.

"Information Warfare and Information Professional Basic Officer Course (CORE Material)," (October 2008), Center for Information Dominance, Corry Station, CIN: A-3B-0027 / A-202-0006, p. 2-23.

"Instructions for Use: IPT-i Mil Suitcase 2.4, Satellite Communications Terminal featuring iDirect," (15 March 2007), SWE-DISH Satellite Systems AB, Document Number: IMIL-Instr-033, p. 85.

"Iridium satellite constellation," (n.d.). Wikipedia, Retrieved on 17 August 2011 from http://en.wikipedia.org/wiki/Iridium_(satellite)#Satellites

Johnston, E. (25 April 2007). "Low Noise Block Downconverter (LNB)," Satellite Signals, Retrieved on 06 August 2011 from http://www.satsig.net/lnb/explanation-description-lnb.htm

Marshall, D. (n.d.). History of the Internet: Timeline, NetValley, Retrieved on 09 September 2011 from http://www.netvalley.com/archives/mirrors/davemarsh-timeline-1.htm

Marson, P. (1997). Satellite Timeline, Saint Mary's, Retrieved on 17 August 2011 from http://www.stmary.ws/highschool/physics/97/PMARSON.HTM

Martin, D. H. (n.d. *a*). A History of U.S. Military Satellite Communication Systems, AEROSPACE, Retrieved on 12 August 2011 from http://www.aero.org/publications/crosslink/winter2002/01.html

Martin, D. H. (n.d. *b*). Milsatcom Timeline, AEROSPACE, Retrieved on 12 August 2011 from http://www.aero.org/publications/crosslink/winter2002/backpage_sidebar1.html

"MD-1366 DISA Certified EBEM SATCOM Modem Establishes New High Throughput Exceeding 200 Mbps On XTAR Satellite," (2011). ViaSat, Retrieved on 06 August 2011 from http://www.viasat.com/news/md1366-disa-certified-ebem-satcom-modem-establishes-new-high-throughput-exceeding-200-mbps-xtar

"MD-1366 EBEM: Enhanced Bandwidth Efficient Modem, Strategic MD-1366/U or Tactical MD-1366A/U," (2008–2011). ViaSat, Retrieved on 06 August 2011 from http://www.viasat.com/files/assets/web/datasheets/EBEM_MD-1366_030.pdf

"Modem," (n.d.). Wikipedia, Retrieved on 10 July 2011from http://en.wikipedia.org/wiki/Modem

"Monics® Satellite Carrier Monitoring System," (n.d.*a*). SAT Corporation, Retrieved on 27 August 2011 from http://www.sat.com/products/satellite/satellite.php

"Monics® Satellite Carrier Monitoring System," (n.d.*b*). SAT Corporation, Retrieved on 27 August 2011 from http://www.sat.com/products/satellite/monics.php

Naval Network Warfare Command. (2008, January 18), *Naval Telecommunications Procedures: NTP 4 (E).* Retrieved on 14 June 2011 from http://judgebusters.com/sitebuildercontent/sitebuilderfiles/navaltelecommunications.pdf

"ORION NPM: Powerful & Affordable Network Performance Monitoring," (n.d.). SolarWinds, Retrieved on 28 August 2011 from http://www.solarwinds.com/products/network-management/network-performance-monitor.aspx

"RMON: Remote Monitoring MIBs (RMON1 and RMON2)," (n.d.). Javvin, Retrieved on 04 September 2011 from http://www.javvin.com/protocolRMON.html

"SatCom Tutorial: an Introduction to Satellite Communications," (25 January 2007), SWE-DISH Satellite Systems AB, Document Number: COM-Tutorial-011, pp. 1–13.

"Satellite communications basics tutorial," (n.d.), Radio-Electronics, Retrieved on 06 August 2011 from http://www.radio-electronics.com/info/satellite/communications_satellite/satellite-communications-basics-tutorial.php

"Satellite Terminal Station Law & Legal Definition," (n.d.). USLEGAL, Retrieved on 18 July 2011 from http://definitions.uslegal.com/s/satellite-terminal-station/

"Satellite Modem," (n.d.). Wikipedia, Retrieved on 10 July 2011 from http://en.wikipedia.org/wiki/Satellite_modem

"Security Threat Response Manager: SNMP Agent Guide," (2008), Release 2008.2, Juniper Networks, Retrieved on 05 September 2011 from http://www.juniper.net/techpubs/software/management/strm/2008_2/SNMP_Agent.pdf#search=%22strm%20snmp%20agent%20guide%22

"Simple Network Management Protocol," (n.d.). Wikipedia, Retrieved on 28 August 2011 from http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

"Simple Network Management Protocol," (2005). Interpeak, *Version 1.22-r5*, Retrieved on 4 August 2011 from http://www.interpeak.com/files/snmp.pdf

Stein, S. (n.d.). LAYER 8: A White Paper on Managing Information Technology Investments to Advance NC State's Mission, (p. 3). North Carolina State University, Retrieved on 12 June 2011 from http://www.ncsu.edu/itd/cmptplans/layer8/whitepaper.pdf

Teare, D. (12 Jun 2008). Structuring and Modularizing the Network with Cisco Enterprise Architecture, informIT, Retrieved on 26 September 2011 from http://www.informit.com/articles/article.aspx?p=1073230&seqNum=4

TNT MIO 11-2 Experiment Report, "Networking and Interagency Collaboration On Maritime-Sourced Nuclear Radiological Threat Detection and Interdiction, (June 7-10, 2011)" (21 September 2011), Provided by Dr. Alexander B. Bordetsky, TNT MIO Principle Investigator, Naval Postgraduates School, Monterey, California

Whalen, D. J. (n.d.). Communications Satellites: making the Global Village possible, NASA, Retrieved on 17 July 2011 from http://history.nasa.gov/satcomhistory.html

Zakon, R. H. (2010). Hobbes' Internet Timeline 10.1, Zakon, Retrieved on 05 September 2011 from http://www.zakon.org/robert/internet/timeline/

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. Dave Roberts
   Naval Postgraduate School
   Monterey, California

5. Alex Bordetsky
   Naval Postgraduate School
   Monterey, California

6. Glenn Cook
   Naval Postgraduate School
   Monterey, California