NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

TRANSFORMING FLEET NETWORK OPERATIONS WITH COLLABORATIVE DECISION SUPPORT AND AUGMENTED REALITY TECHNOLOGIES

by

John J. Fay

March 2004

Thesis Advisor:	Alex Bordetsky
Second Reader:	Gurminder Singh

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** March 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Transforming Fleet Network Operations with Collaborative Decision Support and Augmented Reality Technologies			**5. FUNDING NUMBERS**
6. AUTHOR(S) John J Fay			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT

Current network administrators use network management software to monitor and control elements within a network. This is largely a manual process since managers must interrogate devices individually and evaluate performance statistics manually. The systems provide multiple views on network data but lack capabilities that allow operators to visualize network performance. Since personnel are required to identify problems, interpret potential solutions, and decide on appropriate corrective measures without automatic assistance, maintaining and solving problems for a network can be time-consuming and complex significantly reducing network efficiency. Since FORCENET is a heterogeneous concept that combines various C4I networks, sensors, weapon systems, and platforms, a new model must be developed for network operations. This paper researches an improved model for fleet network operations management for distributed sea-based forces using existing technologies. Combining a collaborative tool, Decision Support System (DSS), and Augmented Reality (AR) imagery transforms Naval information network management from a "minimum threshold" to an "operations fusion" perspective. Little is known about AR technologies, but the potential exists for virtual network operations centers that can remotely direct networks for sea and shore assets through collaborative efforts. The product of this paper will serve as a baseline for network operations in the network centric environment.

14. SUBJECT TERMS Network Operations, Network Management, Collaboration, Augmented Reality, FORCEnet, Decision Support System			**15. NUMBER OF PAGES** 105
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

TRANSFORMING FLEET NETWORK OPERATIONS WITH DECISION SUPPORT AND COLLABORATIVE TECHNOLOGIES

John J. Fay
Lieutenant, United States Naval Reserve
B.A., University of Maine, 1996

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2004

Author: John J. Fay

Approved by: Alex Bordetsky
Thesis Advisor

Gurminder Singh
Second Reader

Dan C. Boger
Chairman, Department of Information Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Current network administrators use network management software to monitor and control elements within a network. This is largely a manual process since managers must interrogate devices individually and evaluate performance statistics manually[1]. The systems provide multiple views on network data but lack capabilities that allow operators to visualize network performance. Since personnel are required to identify problems, interpret potential solutions, and decide on appropriate corrective measures without automatic assistance, maintaining and solving problems for a network can be time-consuming and complex significantly reducing network efficiency.

Since FORCEnet is a heterogeneous concept that combines various C4I networks, sensors, weapon systems, and platforms, a new model must be developed for network operations. This paper researches an improved model for fleet network operations management for distributed sea-based forces using existing technologies. Combining collaborative tools, a Decision Support System (DSS), and Augmented Reality (AR) imagery transforms Navy information network management from a "minimum threshold" to an "operations fusion" perspective. Little is known about AR technologies, but the potential exists for virtual network operations centers that can remotely direct networks for sea and shore assets through collaborative efforts. The DSS provides models for optimization and a knowledge base of potential actions (corrective and preventative). The product of this paper will serve as a baseline for network operations in the network centric environment. Further research would support the development of heterogeneous virtual command and control environments.

[1] Computer Network and Internets, pp. 562-563, Douglas E. Comer. Prentice Hall Publishing.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Although this paper has a single author, some people deserve recognition because of the tremendous guidance and support they provided throughout the research process. I valued their support, opinions, and suggestions and wish to express my most sincere appreciation for all the help they provided.

Dr. Alex Bordetsky must be mentioned because he provided tremendous support of my efforts from the initial conception of the topic until its completion. He is the best advisor a student could have and this paper would not be completed without him. Dr. LorRaine Duffy and Dr. Cheryl Putnam from SPAWAR Systems Center in San Diego also provided unparalleled support during this research. During multiple informative meetings with them, I was able to maintain my focus and keep the research on track. LT Robert Fannon, the N2 Department Head at NCTAMS Pacific in Hawaii, receives my thanks because of his willingness to put up with my harassing emails and phone calls. By allowing me to visit the Pacific Region NOC and by providing information, he saved me countless hours of effort.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND AND PURPOSE

The Navy recognizes that information can dramatically increase combat effectiveness. Developed by the Chief of Naval Operations Strategic Studies Group, FORCEnet emerged as the enabler of the strategic concept, SEAPOWER 21[2]. FORCEnet seeks to provide "superior knowledge, leading to increased combat power" through "integrated sensors, analysis tools, and decision aids."[3] This concept will have far reaching effects on core and peripheral processes within the Navy. Since FORCEnet will have such an important role, it is essential that it is carefully implemented.

This research seeks to support the FORCEnet initiative by providing a transformed model for fleet network operations. An important distinction must be made because the goal of this research is not to describe the implementation of FORCEnet. This research will address a core function that will apply regardless of how FORCEnet is implemented. It will establish a baseline for the fleet network operations centers that provide critical services related to information system management. Network operations are important because it is an underlying function required to effectively operate the various networks, sensors, devices, and information systems that will be used in the fleet.

Current network administrators use network management software to monitor and control elements within a network. This is largely a manual process since managers must interrogate devices individually and evaluate performance statistics manually[4]. The systems provide multiple views on network data but lack capabilities that allow operators to visualize network performance. Since personnel are required to identify problems, interpret potential solutions, and decide on appropriate corrective measures without automatic assistance, maintaining and solving problems for a network can be time-consuming and complex significantly reducing network efficiency.

---

[2] http://www.usni.org/Proceedings/Articles03/PROmayo02.htm#defining, Feb 04

[3] http://www.usni.org/Proceedings/Articles03/PROmayo02.htm#defining, Feb 04

[4] Computer Network and Internets, pp. 562-563, Douglas E. Comer. Prentice Hall Publishing. 2001

Since FORCENET is a heterogeneous concept that combines various C4I networks, sensors, weapon systems, and platforms, a new model must be developed for network operations. This paper researches an improved model for fleet network operations management for distributed sea-based forces using existing technologies. Combining a collaborative tool, Decision Support System (DSS), and Augmented Reality (AR) imagery transforms Navy information network management from a "minimum threshold" to an "operations fusion" perspective. Little is known about AR technologies, but the potential exists for virtual network operations centers that can remotely direct networks for sea and shore assets through collaborative efforts. The DSS provides models for optimization and a knowledge base of potential actions (corrective and preventative). The product of this paper will serve as a baseline for network operations in the network centric environment. Further research would support the development of heterogeneous virtual command and control environments.

B. GENERAL

This research seeks an improved model for managing fleet information frameworks. It will identify the principal capabilities that must be incorporated for future fleet network operations centers. It will also provide the general design for technologies identified as beneficial to network operations. The processes involved with network operations will certainly change with the introduction of new technologies but this paper does not address those changes.

1. Research Questions

This research was started with the goal of improving network operations. Two questions were identified to maintain the research focus and they are as follows.

a. Establish a collaborative DSS model that improves network operations for distributed sea based forces using existing hardware and software.

b. Incorporate AR technology for real-time collaboration and improved visualization of network performance

2. Network Management

Network management is the core function that will be addressed. Network management permits the effective use of information systems by users. Network management is currently accomplished by three network operations centers (NOC) and serves the entire fleet in excess of 300 ships and submarines. Each NOC is assigned a particular area of responsibility and they are responsible for any number of units located within a vast geographic area. This potentially creates disjointed information management as ships transit between areas of responsibility. There is also the challenge of communicating with ships in other areas depending on operational requirements. There is a cumbersome process involved for the NOC to transfer a fleet unit to another area and this does not suit a dynamic operational environment well. Since each NOC is responsible for a large scale network, it does not have the ability to manage specific devices across the various subnetworks that exist in the fleet.

The role of network management is even more important with the emergence of FORCEnet and its goal to integrate information systems across platforms and systems. This cannot be achieved under the current system of network management. This research will identify the capabilities required to conduct network management. Many of the functions are being used today, but the major difference is that the capabilities identified in this paper can be easily incorporated on each fleet asset. Instead of ships requiring an area NOC to manage networks, they become the managers. These roles can be easily transferred among members of a strike group or operation so the decision-making rights for the network reside at the proper level. For example, who should manage the unmanned aerial vehicles (UAV) that are becoming commonplace in the fleet providing surveillance, targeting, and communication links? An area NOC cannot effectively manage this level of network granularity for users. Instead, network management roles for this device should be placed with the fleet unit.

3. Collaboration Tool Suite

The primary means area NOCs currently use to communicate is telephone or email. There is very little information sharing or coordination accomplished across area

boundaries or with fleet units. Typically, the NOC will only communicate with users if a problem exists. Adding electronic collaborative tools will provide significant rewards to the network operations environment.

Collaboration allows for better communication and improved decision making effectiveness for groups. Integrating collaboration with network operations lets commands get involved with the process. This is where the "operations fusion" change can really take place. A variety of people, each with their own perspective, could share the same real-time network information. Instead of relying on one or two watch standers in a NOC to interpret network performance information, now many people are evaluating the situation. Network performance is enhanced and each individual gains knowledge from the information exchange as the group interacts. Collaboration also allows interactive training and information dissemination to easily occur within the network operations environment.

This research will identify the collaboration features that can be used within network operations. A specific solution can be determined once the individual capabilities are identified. Once the solution is identified, it must obtain the DOD Collaborative Tool Suite interoperability certification also discussed in this paper.

4. Decision Support System

Decision Support Systems (DSS) are already part of network management suites in a limited capacity. For example, most network management suites maintain a database to store performance statistics, which provide SNMP support including a knowledge base of Management Information Bases (MIBs).

Although certain DSS components are included in existing network management suites, these tools do not provide the necessary level of support to the decision maker. The Fleet network environment is dynamic and complex and already takes significant effort to effectively manage. The current level of complexity will pale in comparison to networks of the future. Network research is ongoing regarding peer-to-peer, self-aware, and self-healing networks. Those systems require new distributed DSS solutions that reach back to self-organizing networking clusters. An improved system must be developed to provide improved support to network managers to manage this complexity

and this can be found in DSS technology. This research will identify the basic DSS functions that will give future network managers the ability to properly manage increasingly complex networks.

C. MEASURES

The purpose of this research is to transform current fleet network operations with multiple technologies. This is more than a collection of individual tools however. This research is an innovative combination that considers the users, the technologies, the software, and the environment in which operations will occur. There is also multi-dimensional approach to this research since analytical and experimental methods are used together.

1. Evaluate Current Fleet Network Operations Model

Once the research questions were identified, the next logical step was to establish the current means the Fleet uses to accomplish network operations. This was accomplished by visiting the Pacific Region NOC in Hawaii and several surface combatants. Each site provided a wealth of information regarding the state of network operations.

There are other entities involved with Fleet network operations that needed to be contacted. Specifically, the Space and Naval Warfare Systems Command (SPAWAR). SPAWAR is responsible for a variety of Fleet activities but this research was interested in the configuration management accomplished by its system center in Charleston, SC. SPAWAR also maintains a technical website that provided significant insight for network operations.

2. Identify the Network Management Functions Required for the Transformed Network Operations Environment

This section is the core function of the transformed network operations model. The overall purpose of this research is to create a better way to manage fleet information networks. Many of the functions that are currently performed will continue to be valid. Other functions that are not currently in place may be added to further the ability of

future network operations for the fleet. This research seeks to identify the baseline network management functions that should be incorporated into the transformed network operations model.

3. Apply the Department of Defense Collaborative Tool Suite (DCTS) to the Transformed Network Operations Environment

DCTS is an important consideration since collaborative tools play a part in the transformed network operations model. Any collaborative tool that will be installed on DOD networks must earn a DCTS certification. This research identified the DCTS program, its requirements, and the various testing procedures to facilitate implementation of the improved model.

4. Determine DSS Architecture for Network Operations

The next step in establishing a transformed network operations model called for the development of the DSS architecture. The DSS architecture is the framework that will ease the burden for users conducting network management. DSS is intended to "support the decision-making process"[5] performed by humans. This is a critical aspect to the transformed network operations model because people will make key decisions regarding network performance and set-up. Some of the more routine tasks may be automated but these are only intended to alleviate the burden provide for the human in the loop. This research will identify the underlying structure for DSS functions.

5. Ascertain the viability of Augmented Reality Technology for Improving Network Visualizations

Applying augmented reality (AR) technology is the most innovation addition to network operations. In fact, there are very few AR applications that have gone beyond the prototype stage. This technology provides computer generated text, graphics, or images and overlays them onto the user's real-world sensory inputs. This may potentially bring a tremendous capability jump for collaboration and visualization for network managers. This research will determine if AR is appropriate to the network operations environment.

6. Test and Evaluate

In order to correctly identify the network operations model, testing and evaluation must occur. The steps taken here will validate concepts that were discovered while conducting research in other areas. The testing conditions that will be evaluated will vary.

---

[5] *Decision Support Systems in the 21st Century*, George M. Marakas, Prentice Hall, 1999

To illustrate this, the evaluation of network management packages will be very close to the actual measures taken later. In the case of AR technology, the evaluation is based on simulated factors since AR programs development is outside the scope of this paper. The end goal of this portion is to corroborate the ideas discovered during research. The tests here seek to verify valid concepts with future testing providing specific implementation guidance.

THIS PAGE INTENTIONALLY LEFT BLANK

II. EVALUATE CURRENT FLEET NETWORK OPERATIONS METHODS

A. DETERMINE CURRENT STATUS OF FLEET NETWORK OPERATIONS

Before considering what functions must be incorporated into a transformed network operations center, the existing capabilities must be identified. The Fleet NOCs provide a variety of services for fleet units including basic connectivity, email, Internet access, bandwidth monitoring, and security functions. The FCAPS model was selected as the framework in order to effectively evaluate and categorize the methods in use at the Fleet NOCs.

1. FCAPS Model

FCAPS is actually an acronym for Fault, Configuration, Accounting, Performance, and Security management[6]. The model was developed by the International Telecommunications Union (ITU) as recommendation M.3400 to provide a structure for network operations. The FCAPS model is organized by function and describes the five types of information handled by management systems[7]. It is the current model that industry and researchers use to evaluate network functions. Since the FCAPS model is so relevant to information networks, it will be used to identify the methods used for current fleet network operations.

a. Fault Management

Fault management is defined as the "functions which enable the detection, isolation, and correction of abnormal operation of the telecommunications network and its environment"[8]. The categories included within fault management are quality assurance for RAS (reliability, availability, and survivability), alarm surveillance, localization, correction, testing, and administration (ex trouble ticket). In brief, this section of the model is concerned with discovering, correcting, and correcting network problems.

---

6 ITU-T Recommendation M.3400 (02/2000), TMN Management Functions

7 http://www.iec.org/online/tutorials/ems/topic3.html, Feb 04

8 ITU-T Recommendation M.3400 (02/2000), TMN Management Functions

Since the fleet NOCs serve a highly mobile and distributed fleet, the fault management functions are extremely important. When considering fault management, the fleet NOCs are most concerned with maintaining network connectivity between various nodes. The NOCs use multiple software packages to monitor fleet connectivity. IPSWITCH'S *What's Up Gold* (WUG) is the primary network management suite and provides a variety of information about network performance using SNMP and ICMP management tools. NOC personnel view status about connections and equipment (ex., servers) for the overall network and the software packages are configured so NOC personnel may quickly recognize a problem when it occurs. If the problem is significant enough (according to established NOC policies) personnel may be automatically notified with an email or pager message by the software. Periodically NOC watch standers check the status of their end-users but the primary focus is on overall network connectivity. The NOC does not generally look at the situation for individual users unless they are notified of a problem. This usually occurs when a user reports a loss of access to the network or experiences an inability to perform network related tasks (ex., send email). The NOC does have a capability to view certain parameters for the user through the embedded. Although WUG incorporates SNMP, the two main methods used by the NOC to quickly determine network connectivity are ICMP (ex., PING functions) and TELNET. These methods are also used to determine what services are in use and to discover problems.

Part of the fault management function is accomplished by the dual path fleet network architecture. Since there is more than one path in the fleet network, the impact of a casualty is greatly reduced. At any given time, all network paths are used to maximize the effective bandwidth. If a path failure occurs, the network bandwidth is reduced by fifty percent. Users will maintain access to services but at a reduced capacity. When a path failure does occur, the NOC sends a radio traffic message to the affected users notifying of the problem.

Another concern for the NOC is the status of the fleet router. The fleet router is an enterprise level COTS router that manages network traffic flow for fleet users. This is a critical device in the fleet network and a problem with this equipment could cause fleet users a complete loss of network availability. If problems are discovered

with the fleet router, the NOC will attempt to reconnect to the router. If this fails, the NOC attempt to resolve the problem using ICMP and TELNET functions.

b. Configuration Management

Configuration management is defined as the "functions to exercise control over, identify, collect data from and provide data to network elements"[9]. The areas residing within configuration management are network planning and engineering, installation, service planning and negotiation, provisioning, and status and control.

The Fleet NOCs do not currently manage the configuration of software of hardware or software that reside at each location. The program executive office (PEO) for Command, Control, Communications, Computers, and Intelligence (C4I) is responsible for establishing the configuration policy for the network operations centers. Ideally, the PEO C4I office sets the policy that determines the appropriate hardware and software. After policy is set, the necessary systems are acquired, and finally they are accounted for and tracked. Only those systems identified by the PEO C4I staff should be installed into the NOC. The activity responsible for maintaining configuration information for the NOCs is the Naval Space and Naval Warfare Command (SPAWAR). More specifically, the SPAWAR center responsible is located in Charleston, South Carolina and has a database that includes serialized hardware, software, and the appropriate network topologies. Each piece of equipment may have a variety of information associated with it including trouble tickets, casualty reports (CASREPS), and other pertinent information so that a history is collected.

Unfortunately this database has not been maintained properly because of budgeting constraints. As a result, the current NOC configuration is a combination of authorized (and documented) systems in addition to systems developed in-house by NOC personnel. SPAWAR SYSCEN Charleston does not have functional system to accomplish configuration management. Each NOC maintains there own set of hardware and software but there is little coordination between the area NOCs.

c. Accounting Management

Accounting measurement is defined as "the measurement of the use of network services and the determination of costs to the service provider and charges to the

[9] ITU-T Recommendation M.3400 (02/2000), TMN Management Functions

customer for such use"[10]. Accounting management includes usage measurement, tariffing and pricing, collection and finance, and enterprise control. This part of the FCAPS model is normally concerned with ensuring the customer is appropriately billed for the services delivered. The typical functions associated with accounting management do not apply to fleet assets as in the commercial sector.

Electronic mail (email) had evolved into a requirement onboard ships to conduct a variety of business. Email has emerged as a mission essential tool for ships because it provides the capability to coordinate and communicate and each ship has their own domain email server. To facilitate this, NOCs can create and delete email accounts from mail servers for individual ships and also monitor email usage through custom scripts developed by NOC personnel. As a backup to this, the NOCs maintain an alternate email capability for ships using the Internet Message Address Protocol (IMAP). IMAP allows ships to dial-up to a mail server located at the NOC and access mail messages if the primary method is unavailable.

Unlike fixed network installations at stationary sites, Navy ships transit around the world to accomplish missions. This further complicates the role of the NOC because as ships move from one area of responsibility to another, the appropriate NOC must assume the responsibility for ship's network connectivity. There are procedures in place to allow the transfer of responsibility between NOCs as dictated by operational requirements.

The accounting management functions for fleet assets are limited mostly to bandwidth allocation issues. Ships are provided connectivity through several means. These include military specific network to commercial satellite networks with pre-negotiated leases appropriate for the operational environment for each unit or group. For example, a ship that is deployed overseas likely has a steady amount of bandwidth allocated. For ships that are not deployed and are only conducting local training evolutions at sea, the bandwidth allocation may be limited to certain times of day so that unit may conduct routine business like email or web services. Regardless of the amount allocated, ships are not responsible for the bill associated with network connectivity. The

[10] ITU-T Recommendation M.3400 (02/2000), TMN Management Functions

NOC'S manage the resource allocation to fleet units according to the operational context using a variety of tools. They use PacketShaper (from Packeteer) software and routers to monitor and manage the bandwidth used by ships.

d. Performance Management

Performance management is defined as the "functions to evaluate and report upon the behavior of telecommunication equipment and the effectiveness of the network or network element"[11]. Several categories of functions occur within the performance management domain including Quality of Service (QoS), quality assurance, monitoring, control, analysis, and testing.

Industry research results suggest that IT Managers spend thirty percent of their time attempting to discover what is causing network performance degradations[12]. This indicates the importance performance management plays for network operations. The addition of performance management software in the NOCs is an indication that this concern is reflected in the Fleet NOCs. The primary software the NOCs use is called PacketShaper and is focused on four areas of performance management. The software provides increased application visibility because it can see different types of traffic based on common networking standards. For example, the software can differentiate between HTTP used in web browsing or Voice Over Internet Protocol (VoIP) packets. It lets network managers control the types of information flowing across the network according to organizational goals because the software can restrict protocols and packet types completely or to a percentage of the available information capacity. The software also uses compression to improve the use of bandwidth and provides centralized management of reports, analysis, and administration. This software looks at higher network layers than standard network management suites which grants network administrators tremendous capabilities. The NOCs use Sitescope software (from Mercury Interactive) to determine system health for hardware, and "link" status to monitor the connection to ships.

An important function that occurs in fleet network operation centers (NOC) is maintenance of data logs. The logs contain a record of center activities and include real-time information about network events and performance. User generated log

[11] ITU-T Recommendation M.3400 (02/2000), TMN Management Functions

[12] http://www.nwfusion.com/news/2003/1201apm.html, Feb 04

entries must be pertinent and accurate to properly describe the operational history of information networks. Automatic log entries are also generated by network management software packages. The subject matter of the logs may include situation reports, significant events, system faults (or casualties), troubleshooting efforts, trouble tickets, circuit activation and deactivation, personnel matters, and other information.

e. Security Management

Security management is defined as "the management of security" and includes prevention, detection, containment, recovery, administration functional categories. The Department of Defense is a highly visible target for malicious network activities and as such security management is an area that must be properly addressed. The DOD is very concerned with security because of the importance information networks. Although a very important subject area, this paper will only address a narrow portion of network security.

The policies for the Navy's network security are established by the Chief of Naval Operations (CNO) for the entire department, which fleet networks are a component. The Naval Network Warfare Command (NETWARCOM) and its subordinate commands serve as the CNO'S primary advisors for network security policies. These policies and instructions are in addition to those promulgated by the DOD.

Network operations centers are involved with several aspects of network security. The broad areas of interest include ensuring only authorized users gain access, information confidentiality and integrity is maintained on the network, and network services are available to the appropriate users.

Information logs were mentioned under performance management but they also play a role with security management. Manual and automatic logs indicate the aggregate network activity history and trend information for NOC personnel that real-time displays cannot easily present. Once the data is analyzed, a determination can be made to see if network attacks or other unusual behavior. Access logs are also maintained

to provide a layer for physical security since visitors may enter NOC spaces. The information included in these logs often includes the visitor badge number and name of the appropriate escort.

Fleet firewall management is a big part of the security function performed by the regional NOCs. A firewall is a "device that has a set of rules specifying what traffic it will allow or deny"[13]. As previously mentioned, the NOCs are responsible for enacting the policies set forth by upper level commands. Firewall policies are established by senior members of the NOC chain of command and the NOC implements those policy decisions. To preserve the security of fleet networks, specific settings will not be discussed. Instead, the concepts most relevant to the NOCs will be discussed in generic way. First, only authorizes users can communicate through fleet firewalls with trusted systems. The NOCs maintain the authority to authorize or restrict access to the Firewall for communication. This does not include the delegation of administrator privileges as they are reserved for the NOC. Another part of the NOC'S responsibility for firewall management includes managing telnet, FTP, and other protocols that may cross the firewall. Often these protocols are used to infiltrate systems because of security flaws in the standard. The NOC'S implement and maintain the specific criteria (ex., port numbers and device settings) so only authorized entities use these protocols for legitimate purposes.

Lastly, the NOC'S maintain virus scanning software for the entire network in another attempt to prevent malicious attacks. These systems exist for individual devices and for overall network traffic.

B. USER-INTERFACE BETWEEN HARDWARE AND SOFTWARE

1. Shore Assets

The three Fleet NOCs are the shore assets we address here. Each NOC uses the network management suite What's Up Gold and a performance management solution called PacketShaper, and Sitescope.

[13] Inside Network Perimeter Security, Northcutt et al, New Riders Publishing, 2003

The What's Up Gold interface combines graphical and textual information to provide network status information. It provides a "network map" display so at a quick glance users can see the status of network devices. There are also more detailed presentations that give specific performance criteria. It is a commercial network management solution used in each NOC. PacketShaper uses software and hardware and allows network managers to view network performance information at higher levels than typical network management suites. It provides network managers the ability to monitor specific types of applications and protocols, control traffic flow, and compress traffic for more efficient use of bandwidth. The NOCs also use applications that are developed by on-site personnel. These are unique to each NOC and maintained by their developers.

2. Sea-based Commands

Fleet users are all sea based commands. With few exceptions, Navy ships and submarines have local area networks installed at part of the Information Technology for the 21st Century (IT21) initiative. After visiting different platform types, there is no existing capability for ships or submarines to act as a network operations center. The primary role for personnel onboard ships is to conduct server administration, establish connectivity with the fleet network, and perform the necessary maintenance actions to keep the shipboard network functional. Shipboard personnel are able to determine if connectivity exists but they cannot manage it. There is also no ability for shipboard personnel to gather information about connections from other nodes within the network.

C. IDENTIFY NOC COORDINATING MECHANISMS

The chain of command for the network operations centers must be explained in order to properly identify the procedures and coordination mechanisms for the fleet NOCs. There are three network operations centers located in Hawaii and Virginia that perform network operations management for the fleet. They are an internal part of the Naval Computer and Telecommunication Area Master Station (NCTAMS) Atlantic and Pacific commands.

Administratively, the NCTAMS immediate superior in the chain of command (COC) is the Naval Computers and Telecommunications Command (NCTC). The NCTC in turn reports to the head of the navy for communications and computer policies, the

CNO N6 office. This organizational chain of command is mainly concerned with identifying the requirements, plans, systems, policies and manpower related to Joint (multiple DOD services) communications for the Navy. A significant portion of the work accomplished here is the generation of funding priorities so the Navy can accomplish its mission. The operational COC has more impact on day-to-day NCTAMS operations than the administrative COC. Operationally, the NCTAMS receive direction from the fleet commanders (Atlantic and Pacific Fleets). The Fleet commanders serve as the Navy element to US Component Commanders (ex., USPACOM). The component commanders report to the President and Secretary of Defense through the Joint Chiefs of Staff.

The fleet unit (ex., destroyer) unfortunately doesn't necessarily realize the effect the senior COC has on network operations because it may not be visible. Individual fleet assets are the apparatus of policies set by the upper echelon commands and do not always perceive the various issues involved considering the scope of the entire fleet. The fleet is participating in real-world operations and exercises at any given time. NCTAMS receive prioritization direction about network resource allocation from the Fleet commanders. NCTAMS can then establish which units are most relevant to the current mission requirements and provide network services accordingly. The NOCs act as the intermediaries between the upper echelon commands and the fleet units because they enact policies manage network resources accordingly. As a result, the fleet assets are the end user in the process since they receive the network resource and services.

For example, assume two ships are underway and require satellite connectivity. Ship "A" is part of a deployed Carrier Strike Group while Ship "B" is conducting local training operations. Since this operational context is provided by the Fleet Commander staff, the NOC can allocate resources accordingly. In this case, Ship "A" receives the necessary resources based on the approved set of priorities provided to NCTAMS. On the other hand, Ship "B" is allocated resources by the NOC from the remaining network capacity since they are only conducting local training operations.

The situation also illustrates the need to increase the situational awareness for future network operations centers. The awareness between the NOC and individual fleet units is typically low since there is limited organizational coordination. Each regional

NOC has approximately five personnel on duty including a supervisor at any given time. This will vary depending on the operational requirements (and region) but this makes it very difficult to maintain an overall picture of network performance. The personnel in the NOC will float among tasks as needed and there is no regular communication occurring between entities (ex., NOC to ship) unless a problem develops with the network. This does not lend itself to fully effective network operations. Future network operations will require all network participants to share a common picture. The methods to accomplish this are addressed later in this research but increasing communication and network visualization among all participants greatly increases the effectiveness of the network.

III. APPLYING THE DEFENSE COLLABORATIVE TOOL SUITE TO THE NETWORK OPERATIONS ENVIRONMENT

A. WHAT IS DCTS?

1. Background

Historically, the individual components within the United States Department of Defense (DOD) acquired systems individually without respect to the other services. For example, if the Army and Navy were trying to purchase tactical two-way radio systems, there was probably no discussion between the two services about system requirements. There would also be no discussion between the services regarding the interoperability of those radio systems.

A major DOD restructuring took place as a result of the Goldwater-Nichols Department of Defense Reorganization Act of 1986. The new law affected the highest levels of the military through centralization of operational authority and a streamlined military chain of command[14]. The most notable result of the Goldwater-Nichols Act was to require the DOD to operate in a joint manner. In other words, the Act required the services to be able to work together and have interoperable systems. Even though the Goldwater-Nichols Act was passed in 1986, the DOD was very slow to respond to the requirement to work jointly. The Government Accounting Office (GAO) strongly criticized the DOD for its efforts as recently as 1998[15]. The United States Congress (Congress) specifically instructed the DOD to address the lack of collaborative tool interoperability in 1999.

In response to Congressional pressure, the Office of the Secretary of Defense (OSD) and the Joint Staff created the Collaboration Tiger Team (CTT)[16]. The members of the team included Combatant Commanders (formerly known as CINCs), Service representatives, and other federal agencies. The CTT received a two part mission. The first requirement was to establish the strategic guidance for the DOD to employ collaborative tools. Based on the strategy it created, the next step was to define and

14 http://www.ndu.edu/library/goldnich/goldnich.html

15 GAO Letter 1993, 1998

16 http://www.jitcwashops.disa.mil/projects/jtcb_dcts.htm

validate the functional requirements for DOD collaborative tools. The functional requirements list was instituted so the more important aspects were given a higher priority.

With a mission in place, the CTT obtained support from the Joint Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) Battle Center (JBC) to conduct assessments of DOD collaborative tools with a Joint Task Force (JTF). The results of these assessments became the Collaboration Tool Suite (CTS) and were submitted in September 2000 as the CTT recommendation for an interim standard for the DOD. The CTS was approved in January 2001[17] and became the Defense Collaboration Tool Suite (DCTS). DCTS is a baseline that the Collaboration Management Office (CMO) uses to ensure interoperability between products originating from different vendors. CMO is part of the Defense Information Systems Agency (DISA) and will partially subsidize DCTS testing under a program called the Collaboration Interoperability Partnership Testing Program (CIPTP).

2. The Scope of DCTS Requirements

The following tables indicate the requirements for DCTS certification[18].

Table 1. Collaborative Functions Requiring DCTS Certification

Voice Conferencing
Video Conferencing
File Sharing
Application Sharing
Awareness
Instant Messaging
Whiteboarding

Table 2. Case by Case DCTS Determination

Websites
Webportals
Office Automation Packages

[17] SECDEF MSG DTG 291130 Jan 01

[18] http://www.jitcwashops.disa.mil/download/Who%20Must%20Be%20Tested%20for%20Collaboration%20Interoperability.doc

Table 3. Generic Exceptions to DCTS Certification Requirement

Email
Studio-Type VTC (H.320)
Operating Systems

Table 4. Other Exemptions

Appian Enterprise (versions 2 and 3)
ECATS
GroupSystems for Windows, Workgroup Edition, Version 3.4
GroupSystems MeetingRoom , Version 4.0
GroupSystems Online, Version 3.4
Oracle Collaboration Suite
Plumtree Collaboration Server, Version 3.0
Sitescape Enterprise Forum, V.7
ARNG Snitz Forums 2000 V.3.4.03
USO Videophone – Operation: In Sight
Tomoye Simplify 3.1
Facilitate.com Version 7.5
Facilitate.com Version 8.0
Ultimus Workflow Suite Version 5
Hummingbird DM, RM, Imaging, DM Workflow, Web Publishing (versions 5.0 and 5.1)
Zaplet Version 3.0
Frontier Technology, Inc Integrated Desktop Analysis and Planning System (IDAPS)

3. Impact

The DOD Chief Information Officer (CIO) published a memorandum on November 1, 2002 concerning collaboration interoperability standards. The memo states that "all collaboration products used by the Department must demonstrate interoperability and compliance with DOD collaboration criteria." In that memo, the DOD CIO also states that systems already installed on DOD networks must demonstrate interoperability.

Since DCTS is a Department of Defense program, each service (ex., US Navy) seeking to install collaborative tools onto their networks must ensure each product successfully obtains the DCTS certification. The completed certification requires products to be interoperable "off-the-shelf" meaning that products must not interfere with other approved DCTS products without special configuration or set-up ahead of time.

To achieve the interoperability certification, or DCTS approved, vendors must submit their products through the CMO to the Joint Interoperability Test Command (JITC) in Indian Head, Maryland for testing.

DCTS v1.1.12 began employment in April 2002 and within six months had sixty-two sites located throughout the world. In 2003 DCTS was fielded in another 62 sites including DOD Combatant Commands. An enhanced version of DCTS, v2.0, was scheduled for release in 2003[19].

B. DCTS REQUIREMENTS

1. Vendor Awareness

The first step for a vendor to reach a DCTS certification is to solicit from the Federal Government. This is primarily accomplished through the FedBizOpps website (http://fedbizops.gov), which serves as the sole entry point for Federal Government solicitations for procurement over $25,000. Vendors seeking to add collaborative components, tool sets, or services should look to this site for Federal Agency postings for business opportunities.

Once the vendor is aware of the DCTS program, CMO is contacted to continue the process. CMO will send a response letter to the vendor with important DCTS documentation. The documents included provide information about the DCTS baseline, testing procedures, entrance criteria, test requirements, fee schedule, and required application/testing agreement. The letter also contains the contact information for JITC since they will actually schedule and conduct the interoperability testing for the product(s).

[19] http://www.fvc.com/eng/usgov/dcts.htm,

2. Vendor Self-Assessment

The second action for the vendor is to conduct a self-assessment of the product that will be tested by JITC. This is required because there are three types of interoperability tests and each has a different cost. The vendor conducts the self-assessment because any combination of the tests is possible depending on the product. The product is tested based on the choice made by the submitting vendor.

The Augmented Capability test is the first type and is the lowest level of testing available. If a product adds capability to an existing DCTS baseline, it is characterized as an Augmented Capability. This added functions may be described by "plugging in" new features or replacing an existing capability with an improved one. The fee associated with this test is $5,000.

The middle level is called Equivalent Component Functionality. Products to be tested at this level seek to replace quantifiable functionality already existing in DCTS products. In other words, a product designed to replace a DCTS function must be interoperable with other DCTS functions. The normal fee for this test is $8,000. If the product to be tested is a multipoint control unit (MCU), the fee is $10,000.

The highest level of interoperability is System Level. This is the most extensive set of tests because the vendor is attempting to certify a full-featured collaboration suite for use in the DOD. The test covers all modes and functions of the candidate system and costs $20,000.

Table 5. Types of DCTS Interoperability Testing[20]

Test Type	**Fee**
Augmented Capability	$5,000
Equivalent Component Functionality	$8,000 ($10,000 if MCU)
System Level Testing	$20,000

Once the vendor considers what type of testing is desired, the product needs to be evaluated against the DCTS Entrance Criteria Checklist. This checklist is broken down into individual criterion by type. Each type is listed with the standards for each capability

[20] Testing Fee Schedule v2

residing within the product to be tested. These standards represent the minimum standard that the product must comply with to enter the testing phase.

3. Vendor Initiates Test

Once the self-assessment is completed, the Vendor can initiate the test process by submitting the required documents to JITC.

The first document is the 'Testing Application and Agreement'. In this document the vendor acknowledges various government conditions that apply to the product submission. Most importantly, the vendor indicated the product(s) to be tested and what interoperability test type(s) it will be evaluated against. The choices selected by the vendor establish the fee schedule. Once both sides agree and the application is completed, it is signed by Federal Government and vendor representatives and becomes part of the product file.

The second document submitted is the 'Entrance Criteria Checklist/Verification'. This indicates to the government (JITC) that the product(s) meet the preliminary interoperability testing criteria and the testing process can continue. The following table is a summary of the entrance criteria.

In addition the vendor must include the product(s) documentation for JITC review. Lastly, the vendor includes a company check for the amount established in the submitted Testing Application and Agreement'. Once the vendor supplies the necessary documentation, JITC will schedule interoperability testing.

Table 6. Entrance Criteria.

	Criterion	Applicable Standard (or Reference Implementation) for DOD Collaboration	Required For Certification	Product Supports this Standard? (Circle applicable response)
1.	Coexistence	DODD 4630.5 (COE Level 5 Compliance)	Yes	Y / N / NA
2.	Collaborator Status	HTTP, XML, SOAP, via published API	Yes	Y / N / NA
3.	Conference Discovery	HTTP, XML, SOAP, via published API	Yes	Y / N / NA
4.	Virtual Space Discovery	HTTP, XML, SOAP, via published API	Yes	Y / N / NA
5.	Text conference Text (IM)	NetMeeting, SunForum Envoke, Envoke published API	Yes	Y / N / NA
6.	Access Virtual Spaces	None – Done by demonstration with reference	Yes	Y / N / NA
7.	Join conference	- H.323 (Audio/Video) - T.120 (Data)	Yes	Y / N / NA
8.	Share applications	ITU T.128	Yes	Y / N / NA
9.	Whiteboards	T.126	Yes	Y / N / NA
10.	Audio	ITU H.323/G.711	Yes	Y / N / NA
11.	Video	H.323/H.261	Yes	Y / N / NA
12.	File transfer	ITU T.127 FTP, http & XML	Yes	Y / N / NA
13.	Authentication, Encryption, Lockdown	Authentication by password or certificate (PKI), Encryption by SSL or VPN; workstations & servers locked down according to type accreditation requirements	Yes	Y / N / NA
14.	Usability		Yes	Y / N / NA
15.	Directory Services	LDAP V3	Future	Y / N / NA

4. Interoperability Testing Process

The testing process used by JITC covers each functional area within the DCTS program. Each collaborative function within DCTS has its own test process and set of criteria. This section will address the test criteria applicable to each collaborative capability. Each criterion consists of a series of steps evaluated on a pass-fail basis.

a. Coexistence

The purpose of this test criterion is to verify the product being tested will not interfere with or disrupt existing DCTS functions. This test applies to all collaborative functions except Authentication/Encryption/Lockdown, Usability, or Directory Services.

The coexistence test is initiated with a fresh Operating System (OS) load and with no special configurations for the product being tested or the DCTS system. JITC will first evaluate the vendor's documentation for the DOD Common Operating Environment (COE) compliance (level 5). This is the minimum level for DOD interoperability compliance and ensures that "applications appear integrated to the user."[21] Once the documentation review is complete, the candidate system is installed. Once properly installed, the candidate system is checked for normal operation. The next phase of this test calls for a system security lockdown. This condition remains in place for the duration of the test. At this point the vendor's licensing requirements are checked to make sure that any user DOD can use the system on a complaint network without having to exchange license information. Lastly, the product must successfully complete operation with the existing DCTS system.

b. Collaborator Status

This criterion evaluates the ability of a candidate system to display collaboration status to other involved parties. The DOD requires collaborative tools to publish the logon status of system users and so users can view all possible users listed in the Global Discovery Server (GDS) when logged on.

To start this test, a reference user is created on the GDS and establishes on online presence. The DCTS global discovery client or Candidate's client is then activated on the system being tested. Once launched the client must discover the presence and awareness of the reference user. To set up the final test of this criterion, the candidate system must pass the information to the GDS. Once this occurs, the collaboration status of the reference user is verified on the client system within the DCTS.

c. Conference Discovery

In this criterion, the user must be able to show the availability and location of all published conferences (also called meetings) conforming with the ITU H.323/T.120 standards. The reference or location may be in the form of an Internet Protocol (IP)

[21] *Delivering on the promise of 'plug and play'*, Daniel Verton, Dec 6, 1999, Federal Computer Week

address or a Uniform Resource Locator (URL). Once the information is gathered, it must to published to the GDS. Furthermore the system must allow the user to access information about published meeting schedules.

This test is initiated once a reference user is logged in to DCTS and a conference is established on the DCTS conference server. As in the previous test, the discovery agent is launched either from the DCTS or candidate client. The client will attempt to discover the meeting on the DCTS Multipoint Control Unit (MCU). If the client is hosting the meeting then the information about it must be published on the GDS. Once this is complete, the conference is verified on the parent DCTS system.

d. Virtual Space Discovery

The purpose of this criterion is for the candidate to poll the GDS and the occupants of virtual spaces so the results can be published to end users.

The test is started once the reference user is logged on and publishes an online workspace. The discovery agent is launched on the candidate system and is used to find any public virtual space (including occupants) located on the GDS. If the system is hosting the virtual space it must be able to publish the appropriate information to the GDS. Once these parts are completed, the virtual space and occupants are verified from the candidate on DCTS.

e. Text Conference

In this criterion the candidate supports text based conferences. To start the test a reference user logs in to DCTS and establishes its presence. Once logged in a text based message exchange is coduct4ed with single DCTS user. If successful the test is expanded so the candidate must conduct a text conference with multiple DCTS users simultaneously in individual sessions. The last part of this test is for a multiple user text conference in a group chat environment.

f. Virtual Space Access

This criterion is intended to determine if the candidate can access any virtual space that exists on the GDS and follows the requirement to discover virtual spaces. In this test, there is a provision that allows a system to use an alternate virtual

space access method if it is not an integral part of the system being tested. This test also looks at the system's ability to host a virtual space and grant access to others

The test is started once the DCTS discovery agent or candidate client is activated. The client must discover a public virtual space on the GDS, access and verify proper virtual space operation on the candidate system. Once a single space is verified the system must demonstrate the ability to access multiple virtual spaces. The ability to host virtual spaces must also be demonstrated if this capability exists on the candidate system. The last phase of this criterion testing calls for a test of these capabilities on the DCTS system.

g. Conference Join

Since the candidate system already demonstrated the ability to discover conferences, this test establishes the candidate system's ability to join them.

The test is started once a reference user is logged in to DCTS, a conference is established, and the conference is joined by a DCTS client. Then the candidate conference client or DCTS conference client is launched on the candidate system. The candidate system must successfully join the conference and operate properly using conference functions with the reference user. Once the candidate demonstrates the success in the single meeting environment, it must demonstrate the ability to exit and reenter meetings. The next step is for the candidate to exit the meeting, join another, and then rejoin the original meeting. The candidate must then schedule a meeting and publish the information on the GDS. Once scheduled, its creation is verified from the DCTS reference user and the candidate's conference is joined. At this point the reference user and the candidate client interact to verify meeting functionality. The last step is for the reference user to exit this meeting, join another meeting, and then return to the candidate conference.

h. Application Sharing

In this criterion, the candidate system is evaluated for its application sharing capability using a graphically intensive program.

The start condition exists when a reference user joins a conference on DCTS. The conferencing client is activated on the candidate system and participates with

the reference user in the meeting. Once this happens the application sharing functionality is tested. The testing process looks at the ability of the candidate system to handle a graphically intense program, the ability to relinquish control of the application, and the ability to regain control of the application. If applicable, the next part looks at the ability of the candidate system to host application sharing meetings. The system is required to publish the conference information onto the GDS and allow other clients to discover and join the meeting. Once joined, the meeting functionality to verified in the same manner as this initial application sharing.

i. Whiteboard

This section evaluates the candidate system's ability to join a whiteboard session on DCTS and interact with others.

The test is started with a reference user logging on to DCTS and joining a meeting. From there, a conferencing client is launched on the candidate system and joins the reference user in the applicable meeting. The whiteboard functionality is tested within the meeting by viewing and modifying a still image with other users. If the system still hosts meetings, the information is posted to the GDS and the candidate launches the conference. The session is checked from the reference user on DCTS.

j. Audio

This part of the testing checks the ability of a candidate system to exchange audio information between users.

As with other tests, a reference user joins a DCTS based conference and the candidate system does the same. Once the reference and candidate user are participating in the meeting, the ability to conduct a point-to-point audio exchange is conducted. Next the system's ability to exchange multi-point audio is tested. The testing then evaluates to the candidate system's ability to host conferencing with an audio. As in other tests, the candidate establishes a conference and is joined by the reference user. The point-to-point and multi-point audio exchange capabilities are then tested while being hosted by the candidate system.

k. Video

In this criterion the candidate system is tested to see if it can exchange video with other users on DCTS.

The reference user and candidate client join a published DCTS conference. A point-to-point video session is established between the users and a multi-point session subsequent to that. Once each video transfer is in progress, the features are tested for full operational capability. After this is complete the system's ability to host video sessions is checked similar to the audio test.

l. File Transfer

This criterion investigates the candidate system's ability to import and export documents within DCTS.

A reference user logs on to a published DCTS meeting with the candidate client. The candidate client will export a file (document) to the DCTS virtual space. Once accomplished, the reference user activates the DCTS discovery client to import the document to the DCTS machine. Once downloaded, the document is opened to see if it works as expected. Next the DCTS user exports a file to the virtual space and is imported by the candidate client. The downloaded file is then checked for the appropriate functionality.

m. Authentication, Encryption, Lockdown

This criterion focuses on functionality that will appear transparent to the user after initial connections are established. The goal of this test is to verify that systems used in a Command and Control Environment are interoperable with DCTS security criteria. The specific requirements are listed in the DCTS SSAA Version 1.1 (30 Jan 2002) and DOD Directive 5200.28.

The test is started with a reference user logged on to DCTS. The first test checks to see that proper authentication with a user name and password occurs before the candidate's client is allowed access to spaces, collaborators, or conferences. If successful, the next step verifies the end-to-end encryption using the Secure Socket Layer (SSL), Virtual Private Network (VPN), or other equivalent technology. Lastly, the test will evaluate the ability of the candidate workstations to be locked as determined by the appropriate accreditation requirements.

n. Usability, Stability, Performance

The usability testing items are still being developed however the goal of these tests is to verify that candidate systems can operate over time with an acceptable level of reliability, or "up time".

The test starts with a reference user inviting the candidate to a DCTS conference room. The candidate selects the conference room link and enters the meeting. At this point the candidate enables text chat, whiteboard, application sharing, and file sharing for 30 minutes. The candidate succeeds if the conference is held successfully and can be closed when finished. This test is repeated two additional times with success determined based on the availability and proper operation of the candidate system.

o. Directory Services

Currently this capability is not tested because it does not exist for the DOD yet. Although the capability is does not currently exist, this capability is identified as a future DOD requirement for DCTS certification.

5. Post Testing Phase

With testing complete JITC will now take one of two actions. The first possible action results when the product successfully passes the certification tests. JITC will forward the results to CMO who approves the logo agreement. The logo agreement establishes the label the product may carry as appropriate to the testing accomplished. There are three logos (or approved language sets and Table 7 lists the three label types.

Table 7. DCTS Logo Requirements

Approved Language	**Requirements**
DoD Certified Interoperable Collaboration System – v.2 Phase 1	Pass all procedures
DoD Certified Interoperable Collaboration Component – v.2 Phase 1	Pass all procedures for criteria 1, 2, 3, 4, 13, and 14. Pass all procedures for one or more of criteria 5, 6, 7, 8, 9, 10
DoD Certified Interoperable Collaboration Enhancement – v.2 Phase 1	Pass all procedures for criteria 1, 2, 3, 4, 13, and 14 + CMO certification as a collaboration enhancement

A slightly more complicated process follows when the product fails the certification test process. If the product fails, the vendor is notified and has the option to reclama to CMO. This is essentially an appeal to the next level in the chain of command. If the CMO denies the reclama, no logo is awarded for the vendor's product. If the reclama is approved by the CMO product retesting will occur. The important question that arises at this point is whether the retest will occur at no cost to the vendor. If it is determined that a no-cost retest will occur, JITC schedules the test and notifies and vendor and CMO. If the vendor will pay for the retest, then a complete resubmission of the testing application is required.

C. IMPLICATIONS FOR A TRANSFORMED NETWORK OPERATIONS MODEL

The implication for a transformed network operations model is straightforward. Any collaborative tool set that will be used on DOD networks must be tested for interoperability with DCTS. If the solution for the new network operations model includes collaborative tools, it must undergo interoperability testing. Once a product passes the interoperability testing, it is allowed to be installed on the appropriate level of DOD information system.

The interoperability testing requirement creates additional cost for the any collaborative product. The vendor must pay the required fees to have the testing accomplished and those costs are likely to be passed on to the government customer. Although the certification costs are nonrecurring, they should be accounted for during initial budget estimation.

IV. ARCHITECTURE FOR TRANSFORMED NETWORK OPERATIONS

A. TRANSFORMED NETWORK OPERATIONS VISION

1. Goals and Objectives

FORCEnet is the enabler for the US Navy's strategic initiative, *Seapower 21*. FORCEnet will create a fully networked force through existing initiatives and programs to support assured access, power projection, and expeditionary maneuver warfare[22]. It will connect tactical and non-tactical information networks in a streamlined package as opposed to the stove piped information networks of today. This paper seeks to support FORCEnet by creating a model for future network operations. The new network operations model will apply existing concepts to the network operations domain.

2. Core Capabilities

a. Provide Shipboard Network Operations Capability

The primary goal of this research is to provide ships with a capability to perform network operations at sea. The existing capability is very limited for ships to manage their internal LANs and there is no capability onboard ship to accomplish network operations for external networks. Providing this capability to fleet assets increases the possibility that FORCEnet will "transform situational awareness, accelerate speed of decision, and allow [the Navy] to greatly distribute combat power."[23]

Providing these capabilities onboard ships removes a major single point of failure in the fleet network architecture. Fleet assets are completely reliant on the regional NOCs for network connectivity because the regional NOCs are the central hub for network information flow for the fleet (for non-tactical networks). The NOCs are responsible for all network management functions leaving fleet units in a passive role in maintaining network connectivity. Problems as experienced by fleet assets are reported to the NOC but after that point the ship plays little to no role in fixing problems.

This causes two possible consequences. First, although certain redundancies exist, a failure at the NOC may potentially disrupt fleet network

[22] FORCEnet IOC Brief, CNO N7 (Warfare Requirements and Programs), 22 March 2002

[23] http://www.chinfo.navy.mil/navpalib/cno/proceedings.html, Jan 2004

connectivity. As information networks become essential to combat operations, failures become increasingly critical to mission success. Second, due to the nature of the NOC'S mission as a supporting entity, they are not necessarily aware of immediate operational requirements. Fleet assets can provide invaluable perspective when correcting outages or allocating resources since are intricately involved with operations and exercises. With fleet involvement, the effects of problems can be minimized and planning efforts can be maximized.

b. Support Dynamic and Distributed Force

Since its inception, the Navy has operated overseas. What has changed over time is the nature of how ships operate together. Today's fleet assets may operate hundreds of miles from one another but still need to maintain data and voice communications to accomplish a mission. The Navy continues to evolve the way forces are employed but the need to maintain the flow of information to decision-makers remains critical.

The fleet network is used in a much more complex environment than a typical shore based network. In fact, the CNO'S Sea Power 21 strategy calls for the fleet to be even more flexible and responsive than today standards[24]. The level of complexity continues to increase with the introduction of remotely operated and fully networked unmanned vehicles into the fleet. With this in mind, personnel are required to address many additional network considerations beyond that of the typical shore based network.

Unlike networks residing in facilities that are geographically fixed, fleet networks are located on highly mobile platforms. Ships and submarines travel around the world supporting a wide range of operations. Fleet assets may move between satellite coverage areas or between fleet NOC areas of responsibility. Depending on whether a command is operating overseas or in the United States, at sea or in-port, the network connection may be through a land line or satellite connection. Different types of fleet commands require different network services. For example, a command ship uses significantly more bandwidth and network services than a destroyer because of a greater need for communications. The transformed network operation model must be able to

[24] http://www.chinfo.navy.mil/navpalib/cno/clark-guidance2004.html, Jan 2004

manage the different connection types and the potential for status changes for individual assets and groups of assets regardless of geographic location.

c. Collaborative

Collaboration is simply defined as "the act of working together"[25] and is not a new concept. Electronic collaboration emerged in the last decade as computer networks proliferated around the world. In 1995, the World Wide Web Consortium (W3C) held a workshop to explore collaboration protocols and since then collaboration technologies continued to expand and gained increased value across a variety of organizations.

The goal of this paper is to introduce groupware, or collaborative support technologies[26], into the transformed network operations model because of the many benefits offered. Adding collaboration to the network operations process may be the single biggest improvement compared with other individual technologies. There is much more knowledge in a collaborative group than any single person possesses. The individuals involved gain tremendous knowledge by interacting with other members of the group. This knowledge translates into better individual performance in the future. The group as a whole benefits because collaborative tools allow for increased innovation in terms of problem solving because of the communication among group members. As a group shares information and seeks solutions, a wider variety of possibilities emerges as a result of collaboration. Collaboration also allows the decision process to be evaluated by all the involved group members[27].

In the context of fleet network operations, collaboration brings multiple benefits. Collaboration allows group members to work towards a single objective (ex., during troubleshooting) to avoid "re-inventing the wheel"[28]. This results in reducing the time needed for individual issues because communication is increased[29]. Group efficiency is also positively impacted because of the potential for synchronous and

---

25 http://www.hyperdictionary.com/dictionary/collaboration, Dec 2003

26 *Decision Support Systems in the 21st Century*, George M. Marakas, Prentice Hall, 1999

27 *Decision Support Systems in the 21st Century*, George M. Marakas, Prentice Hall, 1999

28 http://www.e-government.govt.nz/docs/govis2002-procurement/chapter10.html, Jan 2004

29 http://www.kjmassoc.com/e_onlinecollaboration.asp. Jan 2004

asynchronous operations. As an example, asynchronous collaboration can allow individuals to accomplish routine maintenance with procedures posted to a common file space. Synchronous collaboration facilitates planning for operations since all participants can discuss the relevant issues at one time instead of requiring additional time for feedback or reporting. A major benefit for the Navy is the ability of electronic collaborative tools to remove geographic barriers[30] since participants may be located anywhere in the world. The intent of this paper is not to examine the benefits of collaboration. Instead, it is assumed that collaboration adds great benefits to the efficiency and effectiveness of group processes based on existing research. The intent here is to create a collaborative model applicable to the network operations environment and is discussed in the next section.

d. "Reach Back"

The reach back capability refers to the ability for deployed forces to contact the appropriate support activities through long-haul network connectivity. This capability currently exists in a limited capacity through naval message traffic, radio-telephone (R/T) circuits, telephone, and email.

Fleet assets used radio message traffic to communicate with distant commands for decades. In terms of correspondence, it is still the only "official" method to communicate with other commands despite being based on very old technology. Although still used, it is ill equipped to effectively function in a network operations environment. The information systems used to send this information have improved over time but sending messages is slow, cumbersome, and often incurs significant message backlogs due to system capacity limitations. Sending these messages is also manpower intensive compared with other means (ex., email). Radio message traffic is simply inadequate for the network operations environment.

R/T circuits, or voice circuits, are commonly used in operational environments. These allow operators to easily pick up a handset, press a button, and synchronously communicate with one or more entities on the circuit. Ships and aircraft have communications equipment limitations because a limited amount of transmitters and

30 http://www.ltscotland.org.uk/connectingcommunities/benefits_collaboration_on_the_Net.asp, Jan 2004

receivers are available in comparison to the many tactical circuits that must be monitored. Dedicating a circuit to network operations would reduce the capability for another mission area. A second reason this is not appropriate for network operations is the lack of ability to maintain a record of events. It is possible to record these circuits, but retrieving and storing the information so it may be used later is very difficult to accomplish with existing systems. Another problem with voice circuits is the challenge to operators in describing problems and situations. Difficult issues can take a long time to resolve because of the limited ability of users to provide situational awareness to the support activities. This causes a needless increase in the amount of time required to fix problems. Efforts should be directed more towards correcting problems rather than determining them. Lastly, acquiring additional voice communications equipment to increase the reach back capability does not provide enough return on investment. The conclusion to be drawn is that voice circuits as currently implemented aboard fleet units are inappropriate in network operations. Telephones are another tool that the fleet uses to communicate with support activities either through land lines or satellites. The telephone has comparable problems to voice circuits so they will not be discussed further.

Electronic mail (email) is the last type of capability applicable in this discussion. While still considered an unofficial means of communication, email use has rapidly expanded in the Navy since the IT21 program was initiated in the early 1990s. Email is fast, can be sent to multiple recipients at one time, provides limited file sharing capabilities (through attachments), and produces a record of communication between parties[31] [32]. Email does have certain disadvantages though. Email only allows asynchronous communication, meaning that the recipient won't be able to communicate in real-time. There will always be a delay between the time of the original transmission and receipt of a response. The biggest disadvantage may be that communicating among a group of people is cumbersome. It was intended to be a "one-to-one medium" and requires active participation by users[33]. As an example, imagine that an email requiring reply is sent to a group of people. Each recipient will receive the message and send a

[31] http://www.buffalolib.org/ComputerTraining/training.email.pros.html, Jan 04

[32] HTTP://WWW.HOMEBUSINESSMANUAL.COM.AU/TECHNOLOGY/EMAIL.HTML, JAN 04

[33] http://klingon.cs.iupui.edu/~aharris/mmcc/mod8/abip23.html#@l123, Jan 04

response to the original sender and possibly the entire group. The original sender must then read each the response to gather the applicable feedback. In a large group, this takes a tremendous amount of time and can be made worse if all users see all replies. Lastly, email is not the most reliable means to communicate. There is no guarantee that an email will be received and the sender may not be aware that a message was lost.

3. Technologies

a. COTS

Commercial-Off-The-Shelf (COTS) may also be called a Non-Developmental Item (NDI) within the DOD. A COTS-based approach is used to acquire a technology or system that already exists in the marketplace, thus reducing the need to develop a product from scratch saving money and deployment time and accomplishing performance requirements. To successfully apply the COTS principle, organizations must consider the context where the system will be used, evaluate the existing marketplace, the system architecture, design, and other considerations[34].

There are a couple of benefits to this type of effort for network operations. First, there is a great cost savings potential when purchasing a product that already exists. The research, development, testing, and evaluation (RDT&E) of a product is already accomplished for a given set of capabilities saving the customer tremendous amount of time and money. Since information networks operate on common protocols and standards, the performance requirements can also be met for the network operations model. Additional COTS benefits include increased system capabilities, greater system quality, and reduced downstream maintenance.[35]

b. Network Management Suite

The core functions for fleet network operations reside in the network management suite. This paper will evaluate existing network management tools to establish the baseline set of capabilities to be included for use in the fleet. The primary software bundles that will be examined are "What's Up Gold" (WUG) from Ipswitch and "Solarwinds Engineer Edition" (SLR) from Solarwinds. These software packages were selected for evaluation because they are both being already being used by the Navy in

[34] http://www.sei.cmu.edu/cbs/overview.html, Feb 04

[35] http://www.sei.cmu.edu/cbs/lessons/program-management/rec3.htm, Feb 04

different capacities. Secondly, the manner in which these tools accomplish network management is accomplished is sufficiently different to effectively compare and contrast software functions. The use of these software tools does not serve to endorse either product. The goal of examining these software packages is to create a generic model for a transformed fleet network operations model. Once completed the transformed network operations model will provide "data gathering, dynamic topological awareness, advanced analytics"[36]

The first important consideration for a network management suite is that it must be able to manage common network standards like SNMP. Using a standards based approach for network management software allows the various network management nodes to share the same relevant information from a variety of hardware platforms. Proprietary solutions that only handle a single product line are not suited to the needs of the Navy. Since the Navy does not use a single vendor's hardware, these products add needless expense and provide very little gain.

Any network management suite must have the ability to conduct network discovery or mapping. This capability allows the software to locate the devices that are present on the network. Once the software recognizes the devices on the network, it can then provide information about device performance. WUG and SLR use two different approaches for this function. WUG uses a windows based discovery wizard that takes the user through the discovery. SLR presents the user with a window that resembles a common web browser. Although both packages use familiar graphic-user-interfaces (GUI) common in other applications, the final display of these packages differ significantly. The WUG output is a color picture that shows nodes and their connections while the SLR output is a window with text based information. In both cases, the tools use color variations to present a quick information summary for the user. Both packages require the operator to enter certain information such as the IP address range for a given subnet. This capability allows administrators to easily recognize what devices are connected on the network and is essential because network monitoring cannot occur until this is done. The ease of discovery in both packages allows administrators to rapidly

[36] *Network Management Tools and Trends*, Mike Jude, Business Communications Review, May 2002

adjust the software suite to handle the dynamic fleet network environment. Additionally, the WUG package allows the user to select the type of service to seek in addition to IP addresses. The specific function allows administrators to tailor the network by traffic type monitoring as needed.

The next capability to discuss is network monitoring. This is the most important function required in any network operations center. This capability provides a view of network status so an operator can determine the health of the network as a whole or for individual nodes. The primary method of SLR is through a multicolor window containing tabular information that provides network performance information. Each device is listed with the respective status and associated graphic. SLR can also display each interface as separate node. For example, this proves helpful to network managers when devices have more than one IP address because the software can monitor each address separately. As conditions change, the textual information is updated and the graphic is changed to indicate the appropriate status. The WUG monitor solution is very different in that it provides a graphic for a particular network device to indicate status. The graphic is augmented with text alerts located at the bottom of the window. The WUG network map shows nodes and connections along in color to show status. As events occur, the WUG software updates the color of the graphic and the text-based data as appropriate to indicate status. For example, a node that loses connectivity will change from a green status to red indicating a major event. The goal is the same for each product even though the implementations are dissimilar. In both cases, the information generated by the software allows the network administrator to quickly determine the status of the network and its devices. It is obvious why this capability is vital to the network operations center. Users must have the ability to rapidly determine network status to effectively manage the situation. Any solution implemented in a transformed network operations model must be reasonably intuitive to NOC personnel so network performance can be properly and easily identified. The user should not have to conduct extensive searches through multiple windows to establish the overall performance of the network. Since the displays that present the overall network situation are typically high-level, the software must be capable of delivering the detailed information to users in addition to the

rapid overall status presentation. This ability provides NOC personnel to correctly determine the cause of problems or identify symptoms of impending problems.

Information capacity[37] or information throughput monitoring is the next function that must be included within the network operations model. The term is often confused with bandwidth monitoring in the context of network operations because according to Hartley's Law, information capacity is a function of bandwidth and transmission time.[38] The important concept here is that information flow between nodes is measured and compared with the total capacity for a communications channel. This is an important consideration for network administrators because it is the foundation for data throughput between nodes in a network. There is a finite amount of information capacity available to the fleet and is likely to remain that way in the future. Historical trends suggest that as bandwidth availability has increased, so has the number of applications requiring a piece of it.[39] Since bandwidth is a finite resource, its allocation to fleet units must be accomplished according to operational requirements so that the appropriate capacity exists at all points. Once allocated, network operation centers use monitoring tools to determine the utilization of the various fleet connections. What's Up Gold and Solarwinds both include tools that allow network administrators to monitor information capacity although the implementations are very different. The WUG tool is named Throughput Tool and allows users to test the data speed for a network connection in bits per second. To determine the data speed, the user must manually select the Net Tools window containing numerous functions organized by individual tabs. The software conducts the test by sending a number of data packets across the chosen connection. The user may adjust the number of packets sent, the timeout, packet size, and the time the system will wait for a response. At any point the user can stop the test with a click of a button. The SLR function is called the Bandwidth Monitor and displays data throughput in bits per second (bps). The basic presentation is a tabular view of each node including each interface and the respective throughput. The left side of the window provides point

[37] Electronic Communication Systems Fundamental through Advanced 4th Ed, Wayne Tomasi, 2001, Prentice Hall

[38] Electronic Communication Systems Fundamental through Advanced 4th Ed, Wayne Tomasi, 2001, Prentice Hall

[39] IS4920 Intro to C4I Systems, Prof Rex Buddenberg

and click access to a variety of charts and graphs related to information capacity including network latency, packet loss, utilization rates, and packet transfers while presenting the information in its own panel. The SLR software goes beyond this basic functionality to monitor information capacity using a tool called the "Bandwidth Gauge". Throughput information (bps) information for transmit and receive is displayed in a gauge resembling a car speedometer and shows real time performance levels for individual nodes. The major difference between the two software packages is that WUG software is intended for one-time throughput tests where the SLR version can monitor the status continuously while the software is running is selected. Since information capacity is important in the fleet network environment, the network operations model must be able to perform regular monitoring of information capacity.

An alert function is the next capability that should be included in the network operations model. An alert is a "piece of triggered information" that holds information about a device, contact method, and other conditions associated with network performance events.[40] Alerts provide network administrators an automated method become aware of significant network events. This reduces the time required to fix problems since the user doesn't have to spend time reviewing historical logs or observing performance parameters trying to discover them. Once generated by NOC personnel and entered into the system, event alerts automatically inform the necessary person(s) of a problem, leading to more efficient problem solving. Both WUG and SLR offer options for a variety of performance alerts. Solarwinds provides event alerting through electronic mail or paging. It can alert users to events related to network latency, high percentage utilization, status changes for individual interfaces, abnormal error numbers (totals), and other network performance properties. The What's Up Gold alert functions provide a larger range of notification types. In addition to paging and email, it generates audible alerts at the console, beeper notification, program execution, telephone notification through pre-recorded messages, popup messages for Windows NT systems, recurring alerts, and grouped alerts where more than one alert type can be used for a particular event. Both software alert systems allow the user to edit the alerts presenting administrators with the ability to tailor network monitoring as needed. This functionality

[40] What's Up Gold User's Guide, software version 8

gives increased flexibility to network administrators so they can properly establish key performance parameters in the current operating environment. Furthermore, the ability for network management software to alert users reduces the response time for significant events that can affect network performance.

The capabilities discussed to this point are related to real-time network performance. While real-time monitoring is the primary element to network operations, the story of network performance does not end with a "green" status indication. Network administrators must follow up real-time monitoring efforts with periodic reviews of performance logs and reports. These reports are used to establish historical system performance, trends, and also contribute to increased network security. There are numerous advantages to reviewing logged information. The information can be looked at with an aggregate system view rather than focusing on a single piece of equipment. One report can contain information from "dozens of sensors" that is more convenient than individual devices reports would be[41]. Analyzing significant network events viewed by multiple devices becomes easier as well. As an example, a status indicator may show an interface "up" while a log may report that no traffic is passing through that connection. This may indicate that a configuration was changed without the administrator's knowledge. Analyzing logs also bolsters the security of the network because it allows the user to see unusual traffic patterns, like unauthorized access requests for example. The information may also be presented in the form of a graph giving the user an instant feel for the historical performance trends. Regardless of the specific form used, the network administrator gains considerable insight by reviewing the logs and reports not provided through normal monitoring windows. Both What's Up Gold and Solarwinds includes robust capabilities in this area suggesting that current technology is more than adequate to provide useful audit information. Although not a new technology or method, logs and reports must be part of the transformed network operations model because of the tremendous benefits to network managers.

Used earlier as an example, the transformed network operations model should include Simple Network Management Protocol (SNMP) based capabilities. SNMP

[41] Inside Network Perimeter Security, Stephen Northcutt et al, 2003, New Riders Publishing

has emerged as the model for network management because it can be implemented with little coding and agents can be easily built adding increased functionality[42]. It is a standard but it more importantly defines a methodology for effective network management.

SNMP is used by many platforms to gather performance information for information networks because it is part of the TCP/IP suite[43] and provides remote management functions easing the burden for network managers. SNMP entities use some basic commands (read, write, and trap) and Management Information Bases (MIB) to establish network performance information[44]. The SNMP entities perform certain tasks and exchange messages about network performance in order to build the picture for network performance. The SNMP Manager entity resides in an application and generates requests for information. Once the Manager sends a request, the SNMP Agent will process the request, gather the information (trap), and reply to the manager. SNMP Agents also respond to network events if the user has created a notification process. Another way for the Manager to receive information is through automatic notification by an SNMP Agent about a network event. When an Agent observes a significant network event, it sends an event report to the Manager for processing. The manager then sends a response to the Agent since SNMP incorporates a two message reporting system. SNMP also facilitates the management of multi-domain network environments since entities may take on a "dual-role" where they act as both Managers and Agents. The dual-role entity is also known as the intermediate or proxy manager and is often used when a large domain has sub-domains or sub-networks. In this case, the high level manager sends requests to the dual-role entity, which receives the request and transforms it into a request for the appropriate sub-network Agent. The events that the network administrator can monitor are vast with SNMP. The SNMP MIB list contains thousands of network performance parameters established in a hierarchal manner so user can drill down to incredible detail and select those desired. Most network management bundles incorporate the ability to manage devices using SNMP including WUG and SLR. In addition to having a vast array

[42] http://www2.rad.com/networks/1995/snmp/snmp.htm, Feb 04

[43] Internetworking Technologies Handbook, Cisco

[44] Understanding SNMP MIBs, David Perkins and Evan McGinnis, 1997, Prentice Hall

of information available with SNMP MIB, the protocol allows remote management by users of network devices. This SNMP function allows for distributed management and introduces redundancy to management functions if operating on multiple devices.

c. Collaboration Tool Suite

Adding collaborative technology is the major conceptual change for the fleet network operations environment. Combining a common network management package with instant group communications can greatly improve network performance. The potential of collaborative technology, also known as Groupware, is remarkable because it "positively impacts the way people communicate with each other, resulting in improvements in the way people work and the decisions people make."[45] Collaborative technologies are designed to provide members a virtual environment allowing the exchange of information and ideas[46]. There are several methods to electronic collaboration including email, instant messaging, and file sharing to name a few. Collaborative tool suites allow people to stay connected without regard to a physical location and it also "facilitates group problem solving"[47]. The task here is to identify the collaborative functions applicable to network operations environment since it is known that collaboration greatly adds to an organization's effectiveness and ability to communicate. There are many collaborative products available including Groove, Microsoft's Live Meeting, Blackboard, WorkNet by Avail technologies, and Lotus Notes (to name a few). The market for collaborative tools is seeing tremendous growth as companies seek a competitive edge in the marketplace[48] and research has only begun to identify all the benefits this technology will bring[49]. To conduct the evaluation collaborative tools, Groove software was chosen because of its functionality and the already existing relationship between the US Navy and the Groove Networks Inc.

---

[45] *Decision Support Systems in the 21st Century*, George M. Marakas, Prentice Hall, 1999

[46] http://www.nwfusion.com/reviews/2003/0728bg.html, Jan 2004

[47] http://www.usabilityirst.com/groupware/intro.txl, Jan 04

[48] *Collaborative Technology Takes on More Critical Role*, Dennis Callaghan and John S. Mccright, EWeek, Feb 24, 2003

[49] An Empirical Investigation of the Impact of Electronic Collaboration Tools on the Performance of a Supply Chain, Elisabeth LeFebvre et al, 2002, IEEE Computer Society

Since collaboration primarily impacts the communication methods within groups, this will be the first area addressed. One of the most basic forms of collaboration is electronic chat which is a "synchronous form of communication, closely resembling actual, real-time conversations".[50] This provides network operators the ability to rapidly communicate since all members of a chat discussion instantly see all responses conveniently located in one place. Often chat software allows the discussion thread to be saved so the group can have a record of conversations. Chat is an important feature for network operations because it primarily facilitates synchronous communication. However, it does give group members the ability to communicate asynchronously if there is a record of the conversation kept. Maintaining a chat history in the collaborative environment permits members to see previous discussions and gain knowledge already shared. This lets members who recently joined a conversation catch-up while the other users are allowed to maintain progress in the conversation. In a network operations environment administrators can use chat to establish rapid communications about network performance, troubleshooting faults, or general notifications with ease. Each person is instantly aware of the pertinent information and adding this to the common network. Groove incorporates a chat function in every available tool (file view, web surfing, etc.) so users constantly have the ability to monitor communications with other members of the space without regard to the specific task being performed. Groove also maintains the char history (when offline and online) until it is manually deleted by a user.

Another tool to be included within the collaborative suite for the network operations environment is the ability to send messages to individuals within the group. While chat is a very useful medium, there are also drawbacks that individual messaging can overcome. First, chat rooms often involve many individuals potentially causing confusion if different discussion threads occur simultaneous.[51] A messaging capability allows individual group members to communicate privately so the entire group is not involved. This single capability enhances the potential for effective communication and reduces the possible confusion that may occur within the group.

---

[50] http://www.edtech.vt.edu/edtech/id/ocs/chat.html

[51] http://www.edtech.vt.edu/edtech/id/ocs/chatp2.html, Jan 04

Voice communications is another capability that should be included in a collaborative network operations capability. Voice communication is widely used in the military but as previously mentioned, resources are limited. Fortunately, voice communications can be made possible within a collaborative environment using Voice Over IP (VoIP). VoIP is often implemented in audio conferencing functions and allows one-to-many (one person talks, others listen) or many-to-many (all can talk or listen simultaneously) conversations. VoIP implementations suffer from a couple of disadvantages though. The main disadvantage is that bandwidth is not guaranteed and to be effective, VoIP requires higher quality of service than regular packet switched standards[52]. This can cause conversations to be choppy because of latency and jitter associated with packet transfer. Various organizations are trying to develop solutions for this but currently it remains a difficult problem. Another disadvantage to audio conferencing is that there typically is no ability to record the group's conversations. This means that unlike chat, users cannot review the discussion thread later in time so the benefit is not maximized for group members.

At a technical level chat, messaging, and audio exchange provide great capabilities for a group and must be included. From a procedural standpoint these tools must be properly managed. Since these tools would be used on a DOD network, members must adhere to the appropriate use policies set forth by the chain of command. This pertains to the subject matter that is discussed or the language being used by participants. Once implemented users become responsible for their behavior and appropriate enforcement methods must be used as established by existing policy.

File sharing is the next capability that can be applied to the network operations model. File sharing can accommodate a variety of tasks in a network operations environment. The biggest benefit provided by a file sharing function is the ability of all members to have access to the same files and receive updates or automatic downloads of the latest document version. For example, this common access to documents permits fleet assets to readily view any number of policies, procedures, or instructions all related to the network operations environment. This could be a drastic

[52] http://www.tldp.org/HOWTO/VoIP-HOWTO-3.html#ss3.4, Jan 04

change in the way the Navy disseminates new information. Often times, commands must mail CD-ROMs to the appropriate commands when new or updated instructions are promulgated. Since the mail service is considerably delayed compared to electronic sharing, this imparts unnecessary delay for the intended recipients. In addition to the delay, parent commands incur the expense of distributing the CD-ROMs to the units that require the information. This becomes a cumbersome process when considering that in excess of 300 commands in the fleet would need information regarding network operations. Posting documents to an internet website is another way to disseminate information but this too has its limitations. Network operations personnel would need to actively seek the current information posted to a web site. In document sharing, group members within a virtual space are provided instant access (and possibly automatic updates) for the information as long as the collaborative environment is running. Another problem with web pages is that they require maintenance and significant effort for the command responsible for them. The time required to update a website is greater than the time required to update a document in a collaborative file sharing environment. Lastly, web sites require additional actions to prevent unauthorized personnel do not gain access. This may be a log-in, VPN, or other method. In a virtual collaborative space, the only people that can access the information are those given access by the space manager with no additional overhead required.

Application sharing is another area that should be incorporated in a network operations environment. In its strictest definition, application sharing is a function that allows "group participants to simultaneously run the same application" while "the application itself resides on only one machine."[53] Also known as desktop sharing, this allows participants the permissions to use resources on other machines. This function provides a tremendous capability for the network operations environment because it used to allow multiple clients the capability for real-time editing of documents, product/application demonstrations[54], remote presentations, or interactive training sessions[55]. As an example, the fleet could benefit tremendously with the ability to

[53] http://www.webopedia.com/TERM/A/Application_sharing.html, Jan 04

[54]http://www.lotus.com/products/lotussametime.nsf/0/f43b214ddec28b8c8525687e00583b48?OpenDocument, Jan 04

[55] http://www.wiredred.com/epop_application_sharing.html, Jan 04

conduct remote training. Every command could receive standardized network training leading to improved network performance. Regional commands responsible for network performance benefit because they know that fleet users are receiving common information and fleet assets benefit from receiving similar training across multiple platforms. Looking further, application sharing would facilitate easier transitions to new software through remote training, demonstrations, and presentations. This would reduce the overhead involved with new software installations, a relatively frequent occurrence for network operations. An additional benefit to application sharing is that it could provide another avenue for remote device management. It was mentioned earlier that SNMP incorporates remote management functionality as part of the standard but unfortunately SNMP also has security pitfalls that could allow unauthorized users tremendous control of network devices. Is it completely unacceptable for unauthorized persons to gain access, let alone control of fleet networks because of the variety of missions that the networks support. Limiting SNMP controls enhances security but also limits capabilities that the network managers could use to improve network performance. Adding application sharing in a collaborative space lets users authorize other group members to access a resource, like a network management suite for example. This would supply network managers' tremendous capabilities while alleviating some security concerns associated with remote device management.

The whiteboard function is another collaborative feature that can improve the network operations environment. Collaborative whiteboards were designed to change regular chalk or dry erase boards into interactive environments where participants could see and make changes in a common setting. Anything written or drawn onto the board is captured on a computer (or network) and each member of the group can mark up whatever is being presented. These are often used for team meetings, distance learning, and networked brainstorming sessions[56]. The typical electronic whiteboard functions can easily be integrated into network operations. The typical functions of a whiteboard are only one aspect to its use in the network operations environment. A hypothetical example points to the potential of whiteboard functions within network operations. Let's say that various network managers are viewing the same network performance information in a

[56] http://www.multimedia.co.th/e-whiteboard.htm, Jan 04

collaborative environment with whiteboard functionality. If a problem or significant event happens, an individual could mark up the screen for others to see, thereby reducing further the effort for all members of the group to identify the problem. This ability reinforces the other methods of communication within the collaborative environment.

An awareness feature should also be included in a network operations model collaborative suite. This is the ability of members to know the status of other members in a virtual space. This is important because members can instantly see who is working in that space. If a member sees another member present in a virtual space, that person can quickly know who is available to communicate with about a particular issue. It also adds a level of security because group members can verify that only authorized people are in the virtual space sharing information.

d. System Architecture

This transformed model focuses primarily on the software solution for the network operations environment based on COTS technology. Before any software is purchased or installed it is important to consider how software at node A will interact with node B. If this is incorrectly established, the system will be much less useful and in its worst case, no communication can occur because of a lack of interoperability. For this paper, the focus is on high-level network layers (OSI layer 4 and above) and more specifically whether network operations should be based on client-server or peer-to-peer architectures.

Client-server architectures involve two types of applications. The first waits passively (servers) for others to start communication. The application that starts the communication is called the client[57]. This can be explained using typical Internet browsing as an example. Assuming connectivity already exists (OSI layers 1-3), a user types the uniform resource locator (URL) into a web browser and the appropriate web page appears once transferred. When the user enters the URL or selects a hyperlink, the browser acts as the client and sends a request to the server holding the appropriate file. The server responds to the request, establishes a session with the client, transfers the web page, and it is finally displayed in the client machine. In this case, the server does nothing unless it receives a request from a client. Servers typically reside in one place and their

[57] *Computer Networks and Internets*, Douglas E. Comer, 2001, Prentice Hall

address doesn't change. If server address changes, it can be difficult for clients to find the desired information afterwards. The client-server architecture is not appropriate for the transformed network operations model because it is difficult to scale in a dynamic, widely distributed network. It is designed to operate in a centralized network environment with servers remaining available for clients to use. This does not suit the needs of the fleet because of the dynamic nature of operations.

In peer-to-peer architectures, the focus is to pool and coordinate network resources in a decentralized environment including "unstable connectivity and unpredictable IP addresses."[58] Peer-to-peer also "enhances the utilization of information, bandwidth, and computing resources"[59]. The nature of peer-to-peer suggests that it is perfectly aligned for use in the fleet. Despite the natural fit peer-to-peer has in the fleet, there are disadvantages. In large network environments, resources for individual nodes can be limited because it is difficult to find the appropriate resource location. The time required to download information is an issue that needs improvement as well[60]. Finally, the peer-to-peer model is somewhat irrational because it assumes that users will adhere to protocols without making adjustments for personal gain (even though they possess the capability)[61].

B. DECISION SUPPORT SYSTEM

The addition of a Decision Support System (DSS) is not a new concept for network operations. Most network management suites incorporate limited DSS functionality but this doesn't necessarily translate to easier network management. DSS technology currently has limitations and takes significant effort on the part of the user to provide decision making easier. Current research involving intelligent agents and the Control of Agent Based Systems (CoABS)[62] suggest that decision support systems are about to undergo a dramatic shift in capability. The new capabilities will greatly reduce

58 http://people.cs.uchicago.edu/~anda/papers/foster_grid_vs_p2p.pdf, Feb 04

59 http://dmi.ensica.fr/article.php3?id_article=229, Feb 04

60 http://dmi.ensica.fr/article.php3?id_article=229, Feb 04

61 http://www.eecs.harvard.edu/~syrah/paptoers/iptps-03/iptps-03.pdf , Feb 04

62 http://coabs.globalinfotek.com, Feb 04

the effort require by users to manipulate information systems through autonomous software agents. With this in mind, this research seeks to highlight the fundamental DSS components that should be applied to network operations.

1. Database

Databases are "integrated collections of data, organized, and stored in a manner that facilitates easy retrieval" and when incorporated into a decision support system (DSS) "provide relevant data for the particular decision context"[63]. The information presented to the user is taken from the database making it the decision support system foundation.

The database is extremely important because it may be used by multiple people and applications. In order to effectively deliver data to the services and people properly, it must be established in a logical and hierarchal manner. Databases are complex and require a carefully designed schema, or method to store and retrieve data, to be effective.

Fortunately for network operations, databases are already incorporated into network management software. Software packages including SLR and WUG contain mechanisms to easily track and retrieve information pertaining to network performance in a variety of ways including graphs and charts. This alleviates considerable effort for the network administrators and permits them to focus more on the network itself. As such, further discussion pertaining to the database is not warranted.

2. Model Base

The model base is a collection of tools that allow data to be analyzed quantitatively using a variety of methods. There are optimization, financial, and statistical models to name a few. The model base is a very distinguishing DSS characteristic for information systems[64] because these powerful tools simplify reality by looking at sample data to generate predictions in a given decision context.

Network management software incorporates some model base functionality and allows statistical analysis of network performance. Typical implementations include

---

63 *Decision Support Systems in the 21st Century*, George M. Marakas, Prentice Hall, 1999

64 *Decision Support Systems in the 21st Century*, George M. Marakas, Prentice Hall, 1999

information about node response time, packet loss, community string, throughput, utilization percentages, peak bit rates, packets per second, packet size, error, and packet discards.

Additional efforts should be applied to several model types that are pertinent to network operations. It may include optimal path models to find the appropriate information path flow. The model may seek to find the maximum flow for a network, and models seek to find the shortest path for information to travel. Transport models can be developed to optimize the distribution across multiple connection paths contributing to better network device load sharing. Additional models may be included to replicate expected performance based on the network architecture.

Network modeling tools (ex., OPNET IT Guru) that can simulate a real network should also be included as part of the model base functionality included within standard network management software. These tools allow operators to generate anticipated network performance characteristics based on the components, connections, and services in use. Using these tools, network administrators can establish virtual networks to test network architectures and performance before the actual installation occurs. Modeling tools can also be used for troubleshooting, system optimization, and configuration management functions as well. An administrator may recreate a given network architecture, services, or equipment settings to determine where problems exist or avoid them if accomplished prior to deployment. The bottom line is that network modeling improves performance and reduces the time required by operators to maintain networks.

3. Knowledge Base

The knowledge base can be considered a repository containing data about previous experiences. Technically speaking, it is "the rules, heuristics, boundaries, constraints, previous outcomes, and other knowledge programmed into the DSS or acquired through repeated use."[65] Unlike the database, the knowledge base contains information for a single problem domain. It does not usually have items that are directly related to the decision context, in this case network operations. Driven by the database, the knowledge base is used to exchange information[66] and automate routine processes[67].

[65] *Decision Support Systems in the 21st Century*, George M. Marakas, Prentice Hall, 1999

[66] http://www.theworkinggroup.ca/collaboration-benefits.html, Jan 2004

The items in the knowledge base are used for reasoning and are either facts or hypothesis. The facts the things believed to be true at a given time where the hypothesis expresses the relationships existing between facts.[68] The knowledge base for network operations is gained by obtaining individual performance parameters. As user established thresholds are met, the system recognizes a particular event. The system then updates the information presented to the user. As applied to the network operations model the knowledge base can be explained using an SNMP illustration. The agents trap the facts, the specific criteria requested by the SNMP Manager that exist for a given device. The hypothesis is established once the Manager receives the response from the Agent. The Manager evaluates the condition of network operations based on the facts presented to it. If appropriate, the Manager may recognize a significant network event and change the status information for the user. In other cases the system will observe unchanged conditions that require no additional actions.

4. User Interface

The user interface is the front end of the system that the user sees when accessing components. It is the tool that allows a human being to interact with a machine.[69] In presenting itself to the user, the interface hides the underlying structure and is the conduit between the user and the system. "The easier it is for a user to access the system the better the interface."[70] A common interface, an interface relatively familiar to many users, is successful when its operations are recognizable and fairly intuitive for the users. The importance of the interface cannot be overlooked because if poorly designed, the information presented to the user is much less useful. There is an entire research area dedicated to the study of human-system integration. This field includes computer scientists and psychologists looking towards "perceptual, cognitive, and motor theories and models of human performance"[71] to best design user interfaces. As a result, this paper barely scratches the surface.

---

67 *Groupware*, David Coleman, 1997, Prentice Hall

68 *Decision Support Systems in the 21st Century*, George M. Marakas, Prentice Hall, 1999

69 http://cfg.cit.cornell.edu/cfg/design/bkg.html, Jan 04

70 *Decision Support Systems in the 21st Century*, George M. Marakas, Prentice Hall, 1999

71 http://www.aw-bc.com/DTUI/chapters/ch1.html, Jan 04

The basic problem is that one interface must be used by multiple people and no one person is the same. What is easy for one person might be very difficult for another. The interface does not do its job if it is not easy to use for all involved. The two primary components to the interface are the communication language and presentation language.[72] The communication language is the physical means the system is accessed by the user. It may include the keyboard, mouse, scanner, joystick to name some examples. The presentation language is what the user experiences. Windows, sounds, icons, tables, and graphs are examples of the presentation language. The goal is for the DSS interface to be "user-friendly" and can't be achieved unless both the communication and presentation languages are well suited to needs of the user.[73] Since this paper is using existing products to establish the model for future operations, the input for

5. Users

The goal of the transformed network operations model is to identify the capabilities and functions that will improve the management of fleet information networks. This vision for a network operations model will not achieve the goal if the users are not considered because in the end, the major decisions are accomplished by the system users. There are a variety of important issues associated with the user including user skill set, individual motivations, knowledge, use patterns, and organizational roles.

The network operation system users will be highly motivated professional sailors that have volunteered to join the Navy in an information technology (IT) capacity. They will be familiar with information networks and receive considerable formal training in relevant areas. Once sailors complete formal school house training, they report to operational commands and begin personal qualifications and on-the-job training (OJT). Until they are fully qualified, new users work under the supervision of more experienced personnel. The way the Navy trains sailors is undergoing a dramatic change and is likely to improve the process. The new method for training will include revised school house instruction that is more streamlined and focused on relevant topics. Sailors will be encouraged to pursue civilian certifications in additional to the qualification programs resident at each command.

---

[72] *Decision Support Systems in the 21st Century*, George M. Marakas, Prentice Hall, 1999

[73] *Decision Support Systems in the 21st Century*, George M. Marakas, Prentice Hall, 1999

The organizational roles the will fill will vary depending on the operational context of the command. Currently, only tactical information networks are managed by sailors. Both classified and unclassified W/LANs are run by shore installations. Under the transformed network operations model, users may serve as an administrator for individual ships or groups of ships. The user's role will be determined by the role his/her command is assigned for a strike group similar to the methods used to assign responsibility for tactical networks. The user will only manage a group of ships if the command is assigned the responsibility.

C. AUGMENTED REALITY TECHNOLOGY

Augmented reality (AR) has the potential to radically transform network operations because of its visualization capabilities. The purpose of AR is to superimpose computer generated information (text, images, or graphics) onto the real-world sensory inputs naturally gathered by users. The biggest potential benefit provided by AR technology to the network operations environment is the potential for "unhindered cooperation of different user viewing the same visualization."[74] Once developed, this capability will drastically multiply the advantages of collaboration since users will be able to manipulate the information being presented and share that with others. Applying AR technology where all participants have the ability to visualize and alter the information presented for others takes collaboration and network operations to a higher level of performance not currently possible with other technologies. The potential for mobile network management also adds to flexibility for users. Users may be able to move around and accomplish other tasks while receiving network management information. This may alleviate the need to dedicate people to fixed NOC sites in the future.

1. Technology Definition

a. General Discussion

Augmented reality is an emerging technology where computer generated graphics or information is integrated into our natural environments[75]. There is a large amount of research being done but very little practical application of the technology. AR

74 http://www.cg.tuwien.ac.at/research/vr/studierstube/CGA98.pdf, Feb 04

75 http://www.howstuffworks.com/augmented-reality.htm, Feb 04

allows people to use their natural senses to gather real-world inputs and have augmented reality provide additional real-time information about the surroundings. This is drastically different from virtual reality where the majority of sensory inputs are generated by the computer and users are immersed in the three dimensional computer environments[76]. The three basic components of augmented reality equipment are a head-mounted display (HMD), a tracking system, and a mobile computer[77].

There are several types head mounted displays on the market but many are still bulky and cumbersome to wear. There are also HMD units that are simple lightweight glasses with a light source projector. Aside from the physical characteristics of the equipment, the two methods used to provide the user with inputs are video see-through and optical see-through[78]. The video see-through approach uses cameras to gather images and the images are projected in real-time with the augmented computer information or graphics to the wearer. Optical see-through displays present graphics or information on top of the natural visual images captured by users instead of using cameras.

The tracking systems incorporated into augmented reality systems are used to provide orientation information about the user to the computer. This is the most difficult part to augmented reality since the computer needs to monitor the geographic location of the user, the position of the head, and position of the eyes[79]. It is important to note that coordinates are not enough to establish a user's location. The important piece of information is the location relative to the user's surroundings. Examples of the type of required information include whether the user in the middle of the street, in front of a door, looking away, or moving. These issues are part of a concept called "view management"[80] which is concerned with how information is presented to the user in the augmented reality environment.

---

76 http://www.cs.iupui.edu/~tuceryan/AR/AR.html, Feb 04

77 http://computer.howstuffworks.com/augmented-reality1.htm, Feb 04

78 http://computer.howstuffworks.com/augmented-reality2.htm, Feb 04

79 http://computer.howstuffworks.com/augmented-reality3.htm, Feb 04

80 http://www1.cs.columbia.edu/graphics/publications/uist01.pdf, Feb 04

The wearable computer is the last component to augmented reality systems. Wearable computers are the weak point right now for the technology because the processing power and graphics capabilities are limited. Computing power is improving but in the foreseeable future wearable and mobile computing will lack capabilities that personal computers have. Lastly, the graphic accelerators used with more advanced AR displays only used for research[81] and have not transitioned to the wearable/mobile computing marketplace.

b. Interface Between Hardware and Software

There are a few ways that users can interface with the augmented reality equipment inputs to affect software actions. The simple implementations are based on standard computing interfaces and include small wearable keyboards and wearable pointing devices. The next level of interface technology includes personal digital assistants, graphics tablets, video cameras, and video projectors to present augmented reality information[82]. Other devices include instrumented gloves that permit users to manipulate virtual objects[83]. The most revolutionary interface technology involved with AR is voice recognition.

The physical differences are one aspect to augmented reality but the largest benefit is combining the software and hardware. The way information is perceived is enhanced when users are able to manipulate the presentation[84]. This may include manipulation of a virtual object or drilling down for additional information. Since the augmented reality system is oriented to the user's point of view, it is inherently interactive and personalized to a level not possible with other technologies[85].

---

[81] http://www1.cs.columbia.edu/graphics/projects/mars/mars.html, Feb 04

[82] http://delivery.acm.org/10.1145/350000/347714/p185-bertelsen.pdf?key1=347714&key2=7524195701&coll=GUIDE&dl=ACM&CFID=16355991&CFTOKEN=55653197, Feb 04

[83] http://www1.cs.columbia.edu/graphics/courses/mobwear/resources/p53-feiner-cacm93.pdf, Feb 04

[84] http://www1.cs.columbia.edu/graphics/courses/mobwear/resources/macIntyre-isar01.pdf, Feb 04

[85] http://www1.cs.columbia.edu/graphics/courses/mobwear/resources/macIntyre-isar01.pdf, Feb 04

There are three ways to incorporate AR technology as suggested by Mackay[86]. The technology can be used to augment the user, the object, or the environment. Augmenting the user is when the technology is attached to a person using a HMD, gloves, or goggles for example. It is also possible to augment the user with PDAs and graphic tablets[87]. Augmenting the object means that the AR device is connected to an object that can be manipulated. Augmenting the environment occurs when the area surrounding the user or object is embedded with projected information and imagery.

c. Uses of Augmented Reality

As suggested by Wendy Mackay, it is important to consider the existing real-world process to properly determine how augmented reality can be used[88]. One measure to assist with the decision of implementing AR is whether the existing process contains notable distinctiveness that is not easily repeated with standard computing interfaces (i.e. keyboard & mouse). If this is the case, then augmented reality may be a viable solution. The next consideration is how well the virtual and real information can be integrated. The two must appear seamless once implemented and if this cannot be achieved, the AR technology may not be the answer. Another issue specifically related to the interface is how create the presentation so the user can recognize the difference between augmented and real information. Lastly, AR should be used to improve the existing world and not replace it. To do this, the effect of AR should let users interact naturally with objects and the environment while providing information to add to the experience.

There is an assortment of research concerned with how to apply augmented reality technology. Certain research focuses on specific problem domains while others suggest in general terms that there is no limit to what AR can be applied towards.

---

[86]http://delivery.acm.org/10.1145/950000/948498/p13-mackay.pdf?key1=948498&key2=2277195701&coll=GUIDE&dl=ACM&CFID=16358195&CFTOKEN=7927296, Feb 04

[87]http://delivery.acm.org/10.1145/350000/347714/p185-bertelsen.pdf?key1=347714&key2=7524195701&coll=GUIDE&dl=ACM&CFID=16355991&CFTOKEN=55653197, Feb 04

[88]http://delivery.acm.org/10.1145/950000/948498/p13-mackay.pdf?key1=948498&key2=2277195701&coll=GUIDE&dl=ACM&CFID=16358195&CFTOKEN=7927296, Feb 04

Mihran Tuceryan[89] suggests that AR can be used in mechanical repair, interior design modeling, computer aided surgery, manufacturing and road repair. There are actually several groups working to apply AR to the medical field including the University of North Carolina (Chapel Hill)[90]. The Defense Advanced Research Projects Agency (DARPA) is funding a variety of groups conducting AR research but most notably is concerned with battlefield visualization. Called the Battlefield Augmented Reality System (BARS)[91] this research is being conducted at several universities including Columbia, the Massachusetts Institute of Technology, the Georgia Institute of Technology, and the Naval Research Laboratory. Other suggested uses include creating "electronic paper"[92] where the usefulness of physical documents in increased by incorporating AR technology. The Boeing Corporation has developed an AR system so mechanics can be guided "step-by-step" through a process in the hopes that errors will be less frequent and productivity and knowledge are increased[93]. What is evident is that most AR uses have not reached a practical level and most current uses exist only in the prototype stage.

2. Applying AR to an Improved Network Operations Model

a. Desired Capabilities

As already discussed, there are numerous areas where AR can be applied. In this section, the focus is identifying the desired capabilities for a transformed network operations model. This is accomplished by looking at the current uses of AR technology and applying the appropriate capabilities. In the network operations environment, information and visualization are the key and AR technology can provide several useful features.

---

89 http://www.cs.iupui.edu/~tuceryan/AR/applications.html, Feb 04

90 http://www.cs.unc.edu/~us, Feb 04

91 http://www.ait.nrl.navy.mil/vrlab/projects/BARS/BARS.html, Feb 04

92http://delivery.acm.org/10.1145/950000/948498/p13-mackay.pdf?key1=948498&key2=2277195701&coll=GUIDE&dl=ACM&CFID=16358195&CFTOKEN=7927296, Feb 04

93 http://www.boeing.com/defense-space/aerospace/training/instruct/augmented.htm, Feb 04

The AR technology must allow network managers in the NOC an ability to visualize network performance in a multi-dimensional manner. As previously discussed, network management software allows administrators to visualize network performance but provides a limited capability to drill down to various levels on the network. Solarwinds provide a summary view of network connections in a tabular form including status and basic information. In What's Up Gold, the network representation is graphical but also only allows users to pull up cursory information. In both cases, users must manually sort through various pull-down windows, tabs, or modules to gather additional information. AR equipment could allow users the ability to focus on a particular network device and select information with a click of the mouse or point of the finger getting more granular information with each attempt. For example, assume that a network management package recognizes that a network device interface and is not working because traffic flow is flowing through it. With that prompt, AR equipment could instantly present the device and the interface visually so the user easily recognizes the problem. AR would not only show the problem but also instantly shows the impact of that fault since the affected nodes connected to that interface are shown as well. It is possible to determine this information with existing software, but it is much more difficult and requires more actions and interpretation by the user.

AR should have the ability to visualize packet collisions. This occurs on networks are collisions when packets of information interfere with one another and do not reach the destination. Depending on the protocol in use, the data either needs to be retransmitted or gets lost. When high packet loss or retransmission occurs, network performance becomes seriously degraded and certain network services cannot be used (ex VoIP). Current network operations techniques do not allow users to identify specifically where collisions are occurring and is a very difficult problem to overcome. Using AR technology, NOC personnel could be shown the place where collisions are occurring, and then determine the extent of the problem so the appropriate action could be taken.

AR technology should also provide the ability to visualize bottlenecks in network traffic flow. Imagine a network manager located on a ship is experiencing greater than expected network latency and data throughput is lower that it should be. Having AR provide a visual interpretation of the ICMP TraceRoute where the person

could use the presentation to easily determine where problems exist. Once the route is visualized and the problem location is identified, the user can then drill down into that device to determine what the problem might be. Using current methods, traffic bottlenecks can be very difficult and time consuming to find. Applying AR to the problem would improve the process considerably.

b. Augmented Reality Benefits

Augmented reality will provide significant benefits to the network operations environment. The information presented is fused from real-world sensory inputs and computer information. Instead of redefining a person's natural surroundings, it enhances them. AR technology provides information that computers cannot easily duplicate[94].

The most noteworthy benefit of AR is the capability to present a problem visually in addition to the standard information network management suites provide. Networks are complicated systems and the ability to see things greatly increases user understanding resulting in significantly greater situational awareness for the operators. With improved understanding and awareness, the decisions made by the users will be much and this is critical since the importance of networks in tactical environments is continually growing.

Lastly, augmented reality technology is being researched in several areas with different methods of implementation. This evidence suggests there is a tremendous amount of flexibility that AR. This flexibility allows the technology to be properly aligned with objectives and is more likely to be successful accomplishing tasks.

c. Augmented Reality Disadvantages

While augmented reality holds great promise for the transformed network operations model, there are disadvantages to the technology that must be addressed.

The first of those is the cost of the augmented reality equipment. Wearable computers are drastically more expensive than desktops and laptops. As an example, a personal computers (desktop) with a Pentium 4 processor operating at 3.4 GHz and 4 GB of RAM costs approximately $3900. A wearable computer company's primary device is

[94] http://www.se.rit.edu/~jrv/research/ar/introduction.html, Feb 04

powered by a Celeron 500 MHz processor with maximum 256 MB of memory (RAM) that cannot be upgraded. Even though it is significantly less capable, the wearable computer costs approximately $5,500 (without accessories) because it is smaller and is forced to handle several problems that the desktop is can easily overcome (like power supply and heat dissipation). This does not include the cost of displays, or the tracking equipment used for orientation. An individual AR unit can cost in excess of $10,000 when fully outfitted. Although network operations are an essential part of the Navy's mission, the current costs of AR equipment are prohibitive when compared with other fleet requirements.

The next problem is the level of technological maturity. AR is still in the very early stages of development and only prototype versions were discovered while conducting research for this paper. While evidence of its potential does exist, it is not ready for near-term deployment into the fleet. Further research is required to quantitatively determine if AR is suitable for network operations. This technological immaturity also means that a solution is not currently available from industry. AR software would require development and this would further add to the costs of acquisition.

Lastly, most fully capable AR equipment sets are still cumbersome and uncomfortable. The worst example indicated that a set of AR equipment weighed 28 pounds. This presents difficulties for the user and detracts from their ability to properly conduct network management. In addition to user discomfort, cumbersome wearable equipment is not suited for shipboard employment. Passageways are narrow, ladders are steep, and objects protrude from all directions.

THIS PAGE INTENTIONALLY LEFT BLANK

V. TEST AND EVALUATION

Testing and evaluation is an integral part to the research conducted for an improved network operations model. The methods identified for future network operations were derived from a combination of methods including a review of existing research, testing and evaluation in a controlled lab environment, and test and evaluation during a dynamic field experiment. The goal of the testing and evaluation was to validate the network operations core capabilities identified during research. Evaluation was the primary method used to confirm the research.

Network management is not a new area so this was the most straightforward testing conducted. Existing network management software packages (Solarwinds, What's Up Gold) were used to evaluate the core network management functions once an understanding of current network operations was obtained. Both software packages included a plethora of features intended to aide network managers but only the features applicable to the core network operations capabilities was tested.

Testing for Decision Support Systems was also conducted using existing tools but on a limited scale. The Groove software suite was used to test and evaluate various peer-to-peer collaborative functions while other software packages including Solarwinds, Ipswitch's What's Up Gold, OPNET Modeler, and OPNET ACE (Application Capture Agent) were used to evaluate individual DSS components at the IP and application layers respectively.

The final area of testing involved augmented reality. Research demonstrated that AR is still a very immature technology with tremendous potential but with few actual implementations. At this point in time, it is not possible to call a single vendor to order an augmented reality suite that includes all the necessary hardware components and software applications. The AR testing and evaluation conducted was based on a considerable amount of simulation. The computer, display, and peripheral components are all items that might be used in a fully operational AR package but that's not the entire story. Tracking equipment that would monitor body movements were not used and that is a big

piece to AR'S functionality. The evaluations highlighted the potential and limitations of AR technology and are still valid to discuss.

A. LOCAL TEST AND EVALUATION

The steps taken during local testing will be described in this section. The majority of testing occurred in a laboratory environment and occurred in several phases. In this, the environment was very controlled and variables were minimized. Network connectivity was not an issue since both Ethernet and Wireless (802.11b) networks were stable and reliable.

1. Equipment Used for Testing and Evaluation

Commercially available computer equipment was used to simulate what is being used in the fleet. Two laptop computers and one wearable computer were used as network nodes. Each laptop was loaded with VMware Workstation 4 since it allows additional "virtual" network nodes to be easily added while mitigating the cost of additional hardware. Virtual machines run simultaneously on top of the parent machine so the total number of nodes equals the number of virtual machines plus one. Virtual Machines are appropriate to simulate a network node because each one appears as a distinct computer to other network devices. The number of VMware virtual machines running on a physical machine is limited by the random access memory (RAM) of the parent computer since each virtual machine receives a portion of physical computing resources. One laptop was configured with two virtual machines with the second loaded with 1 virtual machine. The wearable computer was not loaded with VMware because of processor and RAM limitations. There were a total of six nodes used to simulate a fleet strike group. In addition to the end nodes, an 802.11b wireless access point was used to simulate a satellite for each node. The access point was a reasonable simulation for a satellite since each device is required to communicate through it as dictated by the 802.11b standard under "infrastructure mode" (not ad hoc between devices).

2. Familiarization

This was started only after visits to network operation centers were visited and a literature review was conducted. The first step in the testing and evaluation phase was to get familiar with network operations. Specifically, the Solarwinds and What's Up Gold software packages were used to gain an appreciation for their features and capabilities.

Both software packages offer robust network operations capabilities but are very different when in comes to implementation. As discussed in more detail in earlier chapters, the What's Up Gold software presents network information with graphics as the primary view for devices and connections. To use additional functions, users must navigate through pull down menus at the top of the display. Solarwinds presents information in a tabular fashion with text-based information. Most of the functions for a particular tool are listed in the primary window as a button. An important consideration is that these software packages are intended to be used continuously so network performance statistics can be collected over time and trends can be established. This is explicitly presented to users when an attempt is made to shut down the software (for Solarwinds, this depends on the tool in use). A pop-up window is generated so the user must confirm the shutdown of the network monitoring software in both cases. In this research, the software was run for various amounts of time to allow the capability to be demonstrated by each software package. An actual performance history was not required since the goal was to determine the necessary core capabilities for fleet network operations. Additionally, the devices used to create the test network were used for other non-related tasks so connectivity was not maintained continuously between devices.

3. Core Network Operations Capability Identification

Once an appropriate level of familiarity with the network operations software was obtained, the next step was to identify those necessary capabilities desired for network operations centers. The purpose here was to establish the baseline network operations capabilities that would be used to monitor fleet information networks. These functions are the core to the future fleet network operations centers.

This was established using a combination of methods. The existing methods used by NOCs were evaluated to determine current methods. The Pacific Region NOC in Hawaii was visited in addition to the Naval Postgraduate School (NPS) NOC. A discussion with the subject matter experts yielded tremendous information but that was only the first step. Next the individual nodes were connected using both Ethernet and WLAN architectures. Only information from the test laptop and wearable computers was collected when Ethernet connectivity was established on the NPS network.

Once the devices were connected, the real capability discovery began. Initially, very limited information was collected because of user training issues. It was not realized that the SNMP functionality must be installed as an add-in Windows component. This hampered the effort to determine the functionality of network management software because many of the tools required SNMP to be enabled. Once this limitation was overcome, testing of the specific capabilities progressed rapidly. The application to the fleet environment was considered as each software tool was evaluated. It was important that the focus be maintained because of the unique nature of the fleet operating environment.

4. Collaborative Capability Identification

From the start of this research, it was recognized that collaboration was an important aspect to future fleet network operations. As stated previously, the focus was in how to apply these tools to the fleet. There are various collaborative tools suites on the commercial market but the goal here was to identify the core collaborative functions that would add benefit to the network operations environment. The suite chosen was the Groove collaboration suite because of an existing relationship with NPS and because it possesses a wide variety of collaborative tools including multiple awareness features. The awareness features present users the status of other participants which is a enormous capability in peer-to-peer architecture where members may dynamically enter or exit a space at different times. This evaluation conducted was not intended to validate Groove, rather it was intended to identify the functions pertinent to the fleet network operations environment.

Groove was installed on the same computers mentioned earlier. Once loaded onto each computer, a collaborative space was created with all available modules included. From here, the individual modules were evaluated for their potential value to network operations. Many of the functions covered included in Groove were relevant to network operations. Most of the research looked to see where communications could be improved between fleet units. Other capabilities (ex file sharing) were examined for the ability to disseminate information to the necessary users.

A significant consideration in the identification of the collaborative tools was that local testing did not validate the required capabilities. Each was viewed with the network

operations environment in mind, but only a theoretical application was determined. The validation for the chosen functions occurred over the course of the STAN experiment.

5. Simultaneous Network Management and Collaborative Suite Operation

The vision for the transformed network operations model includes the fusion of collaboration and network management packages so there is one single application presented to users. The testing for this in the laboratory was very limited as no human-system integration testing was accomplished. The testing for this focused on concept demonstration instead of a final implementation perspective. The test objective was to demonstrate that adding collaborative tools would benefit network management efforts.

This testing was not accomplished until after a familiarization with both collaborative tools and network management was obtained. The early efforts with this research were directed towards the network management software because the researcher had used Groove extensively in other areas. The testing commenced once familiar with the network management packages. Preliminary evaluation was conducted in the lab but the true testing occurred outside the lab environment during the STAN experiment (see next section).

To accomplish this evaluation, both the collaboration and network management software were opened at the same time on two different computers. The primary computer used allowed both to be viewed (100% display size) because of a very high-resolution screen. The secondary computer required manual actions to switch between software packages in order to see full views. This limitation was minor and did not affect the overall test objective.

The tests showed that combining the two capabilities did provide benefit to network operations. Users on both sides were able to effectively communicate about the status of the network. As problems or questions arose, it was very easy to share with other members of the group using a variety of tools including chat, voice, and message posting. While the communication capabilities increased, a major benefit observed was the ability of users in different locations to see the exact same information (including content and presentation) about the network. Situational awareness software was enabled to further enhance information sharing but it was not initially clear if the wearable

computer interface possessed the appropriate capabilities to provide benefits to users. Overall the benefits were was possible because the same network management packages were used during the testing on both computers. The communications capabilities of the collaboration software allowed users to be see the same information displays. In this, the time to explain a situation is greatly reduced and users can focus on fixing a problem or adjusting settings much quicker.

6. Decision Support System Capabilities Evaluation

Although listed separately, DSS testing occurred simultaneously with the evaluation of the network management software. After conducting a literature review, it became apparent that certain DSS functions already resided within network operations suites. In this case testing was not the goal. The goal of this research portion was to evaluate the DSS functions already existing in network management software packages. The result of the evaluation was the exposure of DSS functionality within network management software packages.

7. User Interface

No testing or evaluation was conducted in regards to the desired user interface for the transformed network operations model.

8. Augmented Reality Testing

The potential of augmented reality was evaluated but not the actual capabilities. Additional tracking equipment and specially developed software are required for full AR testing to occur. This research sought to examine the concept rather than evaluate a specific implementation.

A wearable computer with a head-mounted display was used. The display allowed the user to receive real-world sensory inputs (sight, hearing, etc) while computer generated information was projected to the head- mounted display. To simulate the actual AR software that would display augmented network information, an existing network management software package was used (Solarwinds).

It was evident that that AR has definite promise for network operations. First, it was possible to monitor network performance while working on other things. This benefit was not realized previously but is an important consideration. This means that man hours can be maximized during times of acceptable network performance. For example,

personnel can work on training or qualifications while simultaneously maintaining situational awareness about network performance. This is a huge capability because it adds flexibility to fleet units that will experience reduced manning in the future. Looking more directly at the end AR implementation, it would be very beneficial to receive information about a particular device simply by looking at it. This capability exists in prototype form (in other contexts) with the tracking gear and software mentioned earlier. This allows the NOC to be mobile onboard a ship instead of forcing an operator to remain in location for a given amount of time. These capabilities are impressive but needs to be reemphasized that actual testing did not occur. The potential benefits of AR technology were looked at but future research is required.

B. SURVEILLANCE AND TARGET ACQUISITION NETWORK EXPERIMENT

The Surveillance and Target Acquisition Network (STAN) experiment is a series of field experiments that seeks to enhance Special Operations Forces (SOF). The experiment recently completed its fifth cycle of experimentation with several organizations contributing various things including vendors, contractors, and DOD entities. The experiment seeks to accomplish the following items.

Table 8. STAN Objectives

1. Enhance SOF ability to find, fix, and identify enemy personnel and equipment
2. Reduce blue-on-blue incidents
3. Design, develop and provide recommendations for integration of a tetherless transmit/receive link between soldier, tactical vehicles, ground sensors, manned and unmanned aircraft, and autonomous underwater vehicles; push-pull of secure voice, data, and video
4. Incorporate Biometric Software for identification of enemy personnel and equipment
5. Obtain quantitative Measures of Performance for the STAN
6. Obtain quantitative Measures of Performance for SOF effectiveness using STAN

In addition to the primary objectives listed in Table 8, the experiment provided the opportunity to test concepts for the transformed network operations model. A large part of the experiment was integrating various network devices and sensors across a

variety of communication paths. The paths included local Ethernet connections for multiple sub-networks, long-haul terrestrial data links, and airborne communication links using unmanned aerial vehicles. A NOC was established in order to monitor the traffic throughout the experiment and served as the perfect environment to test the NOC model for the fleet. The reason this was able to replicate the fleet network is because it was a dynamic network that would frequently change as individual experiments required. It required personnel across the network (end nodes and NOC personnel) to establish connectivity, monitor network performance, and troubleshoot problems to support experiments. Additionally, the personnel involved were distributed across several remote sites throughout the experiment which allowed the methods of communication and coordination to be evaluated.

1. Simulation of Current Fleet Network Operations

Although unintentional, the early attempts to establish the STAN replicated the current methods used to manage fleet networks. A network architecture was established, devices were configured with the appropriate settings (ex., assigned IP Addresses), and then the devices were deployed to the appropriate locations. Once on location, the devices were powered up to see if connectivity could be established. If all goes well, the devices connect to the network and become visible to nodes on either side. Visibility is determined through PING functions or through network management software. Once the network is established, the real experiment can begin. This is similar to the way ships join the fleet wide network once they are underway. Ships will first disconnect from the shore network and connect to the appropriate satellite. Once connected to the satellite, they can then attempt to connect to the NOC.

Coordinating network problems was very challenging because communications were lacking and the remote sites could see the overall network picture with a network management software package. Handheld two-way radios provided the primary communications between the TOC and remote site, again mirroring the fleet methods. This became problematic over long distances and users were forced to use cellular phones instead. It required people at the NOC to describe individual steps for users to take when attempting to correct network problems. Establishing network connectivity was troublesome and it was very difficult to coordinate between sites during this time

period. It took tremendous effort to provide a physical network that was effective enough to conduct experimentation. Once connected, the remote sites and NOC didn't regularly communicate unless a problem arose.

2. Evaluation of Improved Network Operations Model

Once the physical network could be established with regularity, the next step was to use collaboration tools while conducting network operations. During the experiment, Microsoft NetMeeting was used between the NOC and remote users. The remote users also had software management packages installed so it was possible to view the exact information without the NOC having to describe the situation.

It is important to note that the network connection must be established before collaboration could happen. This would apply to the fleet as well. Once connected, the different users connected to the network could work together the status of the network as a whole, or for specific devices that may be experiencing difficulty.

The following figures are typical views of what was observed during experimentation. Figure 1 is a network performance summary generated by Solarwinds. Figures 2 and 3 are screen captures of the Situational Awareness application that incorporated various collaborative tools and capabilities.

Figure 1. STAN Experiment Network Performance Summary

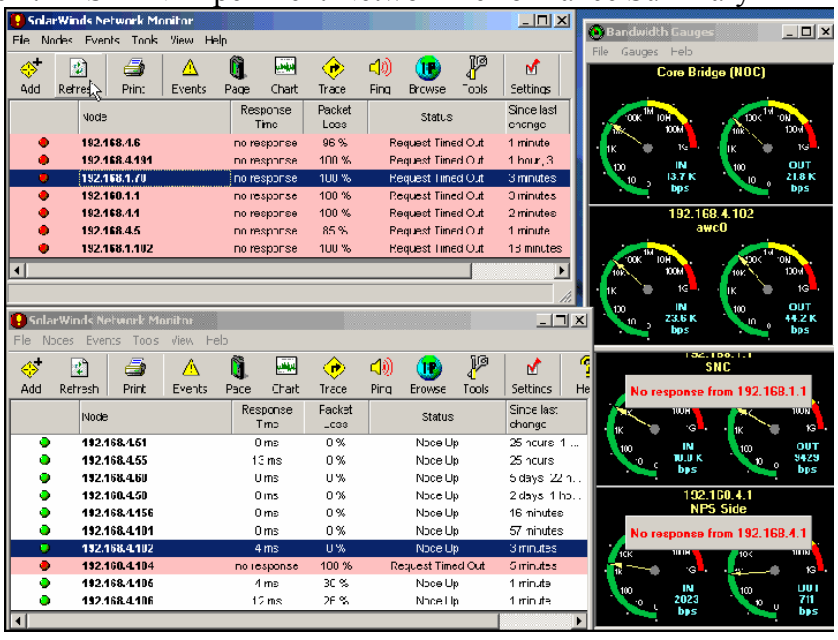


Figure 2. Situational Awareness (SA) Picture with Network Information

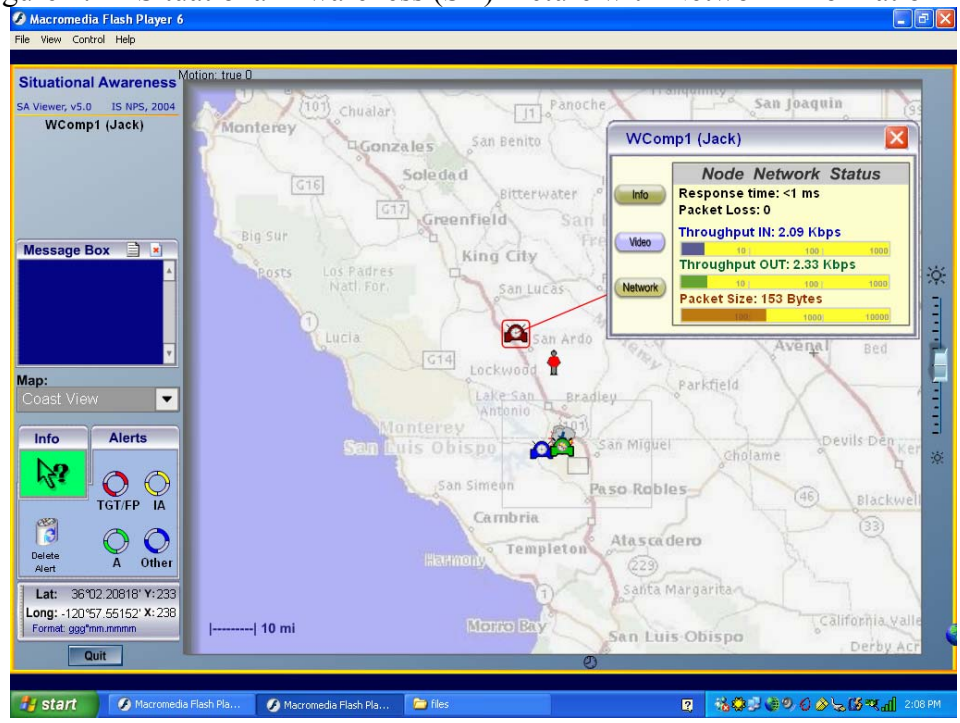
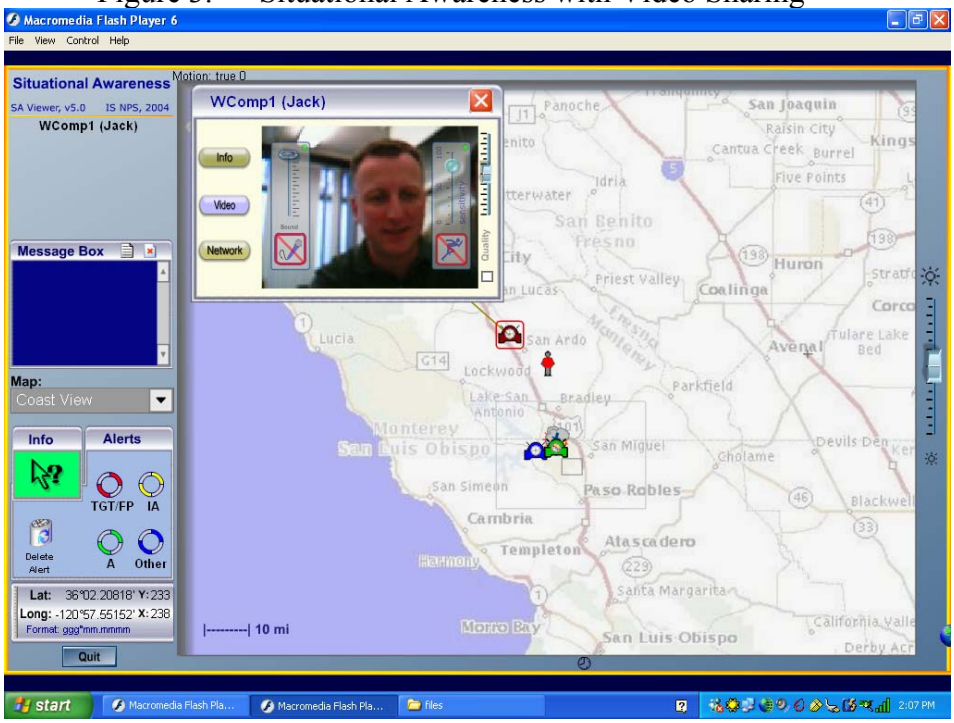


Figure 3. Situational Awareness with Video Sharing



For the STAN experiment, video and audio were used between remote sites and the NOC to determine network status. Users were easily able to exchange information regarding network performance and it took much less time to gain situational awareness

for the network operations environment. The AR concept was also tested during the experiment because the remote site conducting collaboration and network monitoring was a wearable computer with the head-mounted display. Users were able to conduct network monitoring, collaborate, in addition to secondary tasks during this phase of the experiment. This single series of experiments served to validate the research conducted for this paper.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

FORCEnet is intended to enable Seapower 21, the strategic vision set forth by the Chief of Naval Operations, by integrating the individual components Sea Strike, Sea Basing, and Sea Shield with a combination of sensors, networks, weapons systems, and platforms. With this in mind, the importance of fleet information networks grows tremendously. This concept will require significant technological advances to become reality but more importantly, a new method of managing information networks is required. This research identifies a transformed network operations model for the fleet in support of FORCEnet.

A. FINDINGS RELATED TO RESEARCH QUESTIONS

1. Establish a Collaborative DSS Model That Improves Network Operations for Distributed Sea Based Forces Using Existing Hardware and Software

This question was the primary focus for the transformed network operations because it addresses the core processes and functions involved with fleet network operations. To answer this question the research sought to discover the correct application of existing concepts and proven technologies. The fleet environment was the focus throughout the establishment of the transformed fleet network operations model. In addition to the fleet perspective, testing and evaluation were performed to validate the concepts identified.

a. Findings

The current methods and tools used by the fleet for network management were considered when developing an improved network operations model. These observations were addressed according to the OSI FCAPS Model to properly break down the key areas of network management. Current network operations are too centralized for such a dynamic operational environment. Three fleet NOCs manage the networks for many ships and the communication between ships and NOC is limited. The end users are not involved in the process and the communication between the NOC and fleet assets is occurs.

The collaborative DSS model for network operations combines network management tools, collaboration tool package, and augmented reality technology to deliver greatly improved capabilities for fleet network operations centers. Introduced in Chapter IV, the transformed network operations model is the fundamental system architecture that will support a dynamic and distributed sea based force by providing ships the ability to conduct network operations. It reduces the complete reliance of the fleet from the three existing NOCs for network performance monitoring and allows increased situational awareness for the fleet. The fusion of these technologies into a single system focused on revolutionizes the war fighter's ability to manage information networks. The model addresses the dynamic and distributed nature of the fleet, provides a reach back capability to vital network links, and is based on commercial-off-the-shelf technology to reduce costs and expedite acquisition.

The transformed network operations model allows ships at sea to manage vital information networks as dictated by the operational environment. It would allow strike groups to monitor and manage allocated network resources independently of external activities. The information exchanged between network managers at individual nodes increases user knowledge, thereby increasing the collective effectiveness of NOC personnel.

2. Incorporate AR Technology for Real-Time Collaboration and Improved Visualization of Network Performance

This question addressed a more radical concept. Augmented Reality is a completely new technology for network operations since it has never been applied previously. While there is not an existing AR product for network operations, it was possible to simulate the concept using existing hardware and software: wearable computer loaded with collaborative and network management software.

a. Findings

There are a couple of reasons to incorporate AR technology into the network operations domain. The biggest is the ability of a computer to automatically present tailored visual information appropriate to the users operating environment. The technology also demonstrated the ability for users to perform additional tasks while maintaining network situational awareness. In this research, the application of AR

technology to network operations was simulated by combining a wearable computers, head-mounted display, and network management software.

The ability of users to visualize network performance was the key benefit observed during research. Even though the displays were not complete AR suites the information gathered demonstrates the promise of the technology. A second benefit that was noted during the research is the flexibility of AR technology. Users were able to manipulate the displays so they were customized for a particular operating environment. The flexibility was shown when users were switching between network management and situational awareness applications. Users could easily switch the display so it was tailored to the specific situation.

The networking feasibility of AR equipment is the next area for discussion. The mobile computers used during this research are intended to be mobile so standard Ethernet interfaces are not included. Network connectivity was established using standard wireless local area network technology (802.11b). While operating in the lab environment and benign TOC environment, a compact flash WLAN interface card was used. During the STAN experiment difficulties were experienced when operating in an environment where 802.11 signals were amplified. It was suspected that the compact flash WLAN card could not overcome the additional noise associated with the amplified signals. A standard WLAN card was used vice the compact flash version and network connectivity was achieved. This is an important consideration for the fleet environment because currently while it is physically possible to network the devices, Navy policy prohibits the use of WLANs in operational commands.

While the benefits of the technology were apparent there were also some problems identified. The largest problem is the equipment used during this research was cumbersome. Any AR solution applied to the fleet would require equipment that did not have as many wires or peripheral devices protruding from the user. It was too easy to get caught on furniture and other obstacles while wearing the wearable computing equipment. Considering that the tracking equipment was not used, this is a significant hindrance for AR. The final fleet implementation must be designed with better device integration in mind to alleviate this problem.

The interface also needs to be improved over the methods used during this research. The hand-held mouse used was difficult to use because of its size and required some adjustments on the part of the user. The method of data entry was less than ideal because the wrist worn keyboard used had only 59 keys. This is significantly less than traditional keyboards and while the buttons were multi-functional, it was a very slow and awkward process to enter data into the computer. The interface problems are likely related to the level of technological maturity. AR is still a young technology and continued development would probably overcome these shortfalls.

B. FURTHER RESEARCH

Although it is clear that the transformed network operations model will improve the effectiveness of fleet network operations, several topics discovered would reap significant benefits with additional research.

1. Technical Aspects

a. Self-Forming/Self-Healing Networks

Research in ongoing by other groups about self-forming and self-healing networks and this concept would benefit the fleet tremendously. This concept would permit fleet network nodes to automatically join and recognize available networks. The benefit of this type of network is significant because it would alleviate some of the requirements to have a "man in the loop" for network monitoring and management.

Furthermore, this would also allow network to automatically identify and correct problems including communication path or device failures. Other network devices or sensors could recognize a problem and adjust to the situation providing human decision makers with consistent information.

b. Augmented Reality Development

As stated during previously in this paper, Augmented Reality technology has great promise for the network operations environment. This potential can be turned into a working product with additional equipment and some software development.

The additional material required is commercially available tracking equipment to monitor the movements of the user. This would permit the computer to recognize what the user was looking at and present the appropriate information about a

network device or connection. The software requirement would provide the capability for a user to visualize network devices or connections with the respective performance. The user must be able to "drill down" to increased levels of granularity. To illustrate, as a user is walking through a space where a network switch is located, the person receives a performance update simply by looking at the device. If the switch is shown to have a fault, the user should be able to instantly adjust the computer-generated visualization to get the details about the problem.

c. Identify Specific Network Management Software

This research looked at two network management software packages and specifically avoided recommending one product. The core capabilities identified by this research for the network management function are a combination of features resident within Solarwinds and What's Up Gold. This is not the final answer to the transformed fleet network operations model.

Follow-on research should identify the specific software tool (or tools) that should be incorporated into the fleet. This is important when configuration management is considered because it is vital that each fleet unit have access to the same information (content and presentation) to reap the full benefits of collaboration.

d. Develop Decision Support System Technology for Network Operations

Since self-forming/self-healing networks are in the very early stages of research, the short-term solution that will alleviate burdens for NOC personnel are increased Decision Support System functionality. More specifically, agents should be developed that can automatically monitor network performance as desired by the decision maker. This technology is available through SNMP or commercially developed solution like OPNET Application Characterization Environment (ACE) but would need to be further refined the fleet. This would permit users to have autonomous network monitoring so the manual efforts required by users would be reduced.

Additional research within the DSS domain involves the user interface. Human-systems integration subject matter was not addressed during this research because of the many variables involved. This research evaluated the concept to joining collaboration and network management by having two separate applications running

simultaneously to simulate an end system. Additional research should be accomplished to integrate the concepts into a single manageable solution for NOC personnel.

e. Quantitative Testing

This research identified concepts and attempted to validate them through demonstration and testing. A limitation of this approach was that quantitative modeling was not accomplished. Additional research should look to quantify the benefits generated from incorporating the technologies identified by this research.

2. Network Operations Processes

a. Accomplishing Network Operations the Vision

This research suggests changing the way the fleet conducts network operations but does not address how to accomplish it. Considering there are varied stakeholders involved in this process and the importance of fleet information networks, the additional research should identify the best way to make the changes for the fleet to maximize the chances for success.

Another aspect to this research is identifying the coordination mechanisms that would be used to perform network operations. This would involve developing the procedures that ship and shore NOCs would use to establish decision-making rights and assign responsibility amongst members of the group.

b. Implementation Cost Model

The last area identified during this research involves the business case for transforming fleet network operations. While this may not be a major acquisition program, it involves spending Navy resources on new systems. Before the Navy commits to this, further research should identify the value added along with the cost model so a possible return on investment can be determined. This is an important consideration as the DOD moves to execute its mission and justify its expenditures.

LIST OF REFERENCES

1. *Computer Network and Internets*, Douglas E. Comer. Prentice Hall Publishing
2. http://www.usni.org/Proceedings/Articles03/PROmayo02.htm#defining, Feb 04
3. http://www.usni.org/Proceedings/Articles03/PROmayo02.htm#defining, Feb 04
4. *Decision Support Systems in the 21st Century*, George M. Marakas, Prentice Hall, 1999
5. ITU-T Recommendation M.3400 (02/2000), TMN Management Functions
6. http://www.iec.org/online/tutorials/ems/topic3.html, Feb 04
7. http://www.nwfusion.com/news/2003/1201apm.html, Feb 04
8. Inside Network Perimeter Security, Northcutt et al, New Riders Publishing, 2003
9. http://www.ndu.edu/library/goldnich/goldnich.htm, Oct 03
10. http://www.jitcwashops.disa.mil/projects/jtcb_dcts.htm, Oct 03
11. Secretary of Defense Message, DTG 291130 Jan 01
12. http://www.jitcwashops.disa.mil/download/Who%20Must%20Be%20Tested%20for%20Collaboration%20Interoperability.doc, Oct 03
13. http://www.fvc.com/eng/usgov/dcts.htm, Oct 03
14. *Delivering on the promise of 'plug and play'*, Daniel Verton, Dec 6, 1999, Federal Computer Week
15. FORCEnet Initial Operaional Capability Brief, CNO N7 (Warfare Requirements and Programs), 22 March 2002
16. http://www.chinfo.navy.mil/navpalib/cno/proceedings.html, Jan 04
17. http://www.chinfo.navy.mil/navpalib/cno/clark-guidance2004.html, Jan 04
18. http://www.e-government.govt.nz/docs/govis2002-procurement/chapter10.html, Jan 2004
19. http://www.kjmassoc.com/e_onlinecollaboration.asp , Jan 04
20. http://www.hyperdictionary.com/dictionary/collaboration, Dec 2003
21. http://www.ltscotland.org.uk/connectingcommunities/benefits_collaboration_on_the_Net.asp, Jan 2004
22. http://www.buffalolib.org/ComputerTraining/training.email.pros.html, Jan 04
23. http://www.homebusinessmanual.com.au/technology/email.html, Jan 04
24. http://klingon.cs.iupui.edu/~aharris/mmcc/mod8/abip23.html#@l123, Jan 04
25. http://www.sei.cmu.edu/cbs/overview.html, Feb 04
26. http://www.sei.cmu.edu/cbs/lessons/program-management/rec3.htm, Feb 04
27. *Network Management Tools and Trends*, Mike Jude, Business Communications Review, May 2002
28. Electronic Communication Systems Fundamental through Advanced 4th Ed, Wayne Tomasi, 2001, Prentice Hall
29. IS4920 Intro to C4I Systems, Prof Rex Buddenberg

30. What's Up Gold User's Guide, software version 8
31. http://www2.rad.com/networks/1995/snmp/snmp.htm, Feb 04
32. *Internetworking Technologies Handbook*, Cisco, Author and Date unknown
33. *Understanding SNMP MIBs*, David Perkins and Evan McGinnis, 1997, Prentice Hall
34. http://www.nwfusion.com/reviews/2003/0728bg.html, Jan 2004
35. http://www.usabilityirst.com/groupware/intro.txl, Jan 04
36. *Collaborative Technology Takes on More Critical Role*, Dennis Callaghan and John S. Mccright, EWeek, Feb 24, 2003
37. *An Empirical Investigation of the Impact of Electronic Collaboration Tools on the Performance of a Supply Chain*, Elisabeth LeFebvre et al, 2002, IEEE Computer Society
38. http://www.edtech.vt.edu/edtech/id/ocs/chat.html, Jan 04
39. http://www.edtech.vt.edu/edtech/id/ocs/chatp2.html, Jan 04
40. http://www.tldp.org/HOWTO/VoIP-HOWTO-3.html#ss3.4, Jan 04
41. http://www.webopedia.com/TERM/A/Application_sharing.html, Jan 04
42. http://www.lotus.com/products/lotussametime.nsf/0/f43b214ddec28b8c8525687e00583b48?OpenDocument, Jan 04
43. http://www.wiredred.com/epop_application_sharing.html, Jan 04
44. http://www.multimedia.co.th/e-whiteboard.htm, Jan 04
45. http://people.cs.uchicago.edu/~anda/papers/foster_grid_vs_p2p.pdf, Feb 04
46. http://dmi.ensica.fr/article.php3?id_article=229, Feb 04
47. http://www.eecs.harvard.edu/~syrah/paptoers/iptps-03/iptps-03.pdf , Feb 04
48. http://coabs.globalinfotek.com, Feb 04
49. http://www.theworkinggroup.ca/collaboration-benefits.html, Jan 2004
50. *Groupware*, David Coleman, 1997, Prentice Hall
51. http://cfg.cit.cornell.edu/cfg/design/bkg.html, Jan 04
52. http://www.aw-bc.com/DTUI/chapters/ch1.html, Jan 04
53. http://www.cg.tuwien.ac.at/research/vr/studierstube/CGA98.pdf, Feb 04
54. http://www.howstuffworks.com/augmented-reality.htm, Feb 04
55. http://www.cs.iupui.edu/~tuceryan/AR/AR.html, Feb 04
56. http://computer.howstuffworks.com/augmented-reality1.htm, Feb 04
57. http://computer.howstuffworks.com/augmented-reality2.htm, Feb 04
58. http://computer.howstuffworks.com/augmented-reality3.htm, Feb 04
59. http://www1.cs.columbia.edu/graphics/publications/uist01.pdf, Feb 04
60. http://www1.cs.columbia.edu/graphics/projects/mars/mars.html, Feb 04
61. http://delivery.acm.org/10.1145/350000/347714/p185-bertelsen.pdf?key1=347714&key2=7524195701&coll=GUIDE&dl=ACM&CFID=16355991&CFTOKEN=55653197, Feb 04
62. http://www1.cs.columbia.edu/graphics/courses/mobwear/resources/p53-feiner-cacm93.pdf, Feb 04

63. http://www1.cs.columbia.edu/graphics/courses/mobwear/resources/macIntyre-isar01.pdf, Feb 04
64. http://delivery.acm.org/10.1145/950000/948498/p13-mackay.pdf?key1=948498&key2=2277195701&coll=GUIDE&dl=ACM&CFID=16358195&CFTOKEN=7927296, Feb 04
65. http://delivery.acm.org/10.1145/950000/948498/p13-mackay.pdf?key1=948498&key2=2277195701&coll=GUIDE&dl=ACM&CFID=16358195&CFTOKEN=7927296, Feb 04
66. http://www.cs.iupui.edu/~tuceryan/AR/applications.html, Feb 04
67. http://www.cs.unc.edu/~us, Feb 04
68. http://www.ait.nrl.navy.mil/vrlab/projects/BARS/BARS.html, Feb 04
69. http://delivery.acm.org/10.1145/950000/948498/p13-mackay.pdf?key1=948498&key2=2277195701&coll=GUIDE&dl=ACM&CFID=16358195&CFTOKEN=7927296, Feb 04
70. http://www.boeing.com/defense-space/aerospace/training/instruct/augmented.htm, Feb 04
71. http://www.se.rit.edu/~jrv/research/ar/introduction.html, Feb 04

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Dr. Dan C. Boger
   Naval Postgraduate School
   Monterey, CA

4. Dr. Alex Bordetsky
   Naval Postgraduate School
   Monterey, CA

5. Dr. LorRaine Duffy
   SPAWAR SYSCEN San Diego
   San Diego, CA

6. Dr. Jerry Kaiwi
   SPAWAR SYSCEN San Diego
   San Diego, CA

7. Dr. Cheryl Putnam
   SPAWAR SYSCEN San Diego
   San Diego, CA

8. Dr. Gurminder Singh
   Naval Postgraduate School
   Monterey, CA