NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IPv6 TACTICAL NETWORK MANAGEMENT

by

John F. Dobrydney

September 2009

Thesis Advisor: Alex Bordetsky
Second Reader: Michael Clement

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE September 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE IPv6 Tactical Network Management	5. FUNDING NUMBERS
6. AUTHOR(S) John Dobrydney	
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 Approve for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Current and emerging technologies and equipment, such as unmanned aerial vehicles, ground sensors, networked radios, operator-worn sensor vests, and nanotechnology applications offer warfighters unprecedented command and control and information detection capabilities, yet the use of this technology has not been fully realized. The current protocol, IPv4, is incapable of providing enough addresses due to a depletion of IPv4 address space. IPv6, however, offers unprecedented network support for tactical-level sensor and communications assets in terms of increased address space, Quality of Service (QoS), flexibility, and security.

The Department of Defense is transitioning from IPv4 to IPv6 in order to capitalize on IPv6's expanded capabilities. However, one unresolved area is proper IPv6 network management. Currently, the majority of the configuration and operational knowledge is in the mind of a very few individuals. The expertise currently available must be developed for application by the tactical network manager operating out on the edge of the network, in order to properly administer both an IPv4/IPv6 dual stacked network during the phased protocol transition and a purely native IPv6 network. Second, IPv6 features a robust Quality of Service (QoS) capability previously unavailable through IPv4, which requires research to determine the optimum configuration to support the warfighter's diverse requirements.

14. SUBJECT TERMS IP, Tactical Sensor Network, TNT, Internet Protocol Version 6, Network Management, Quality of Service, DiffServ, Information Management	15. NUMBER OF PAGES 2233
	16. PRICE CODE

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

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

IPv6 TACTICAL NETWORK MANAGEMENT

John F. Dobrydney
Major, United States Marine Corps
B.A., Iowa State University, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2009

Author: John F. Dobrydney

Approved by: Alex Bordetsky
Thesis Advisor

Michael Clement
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Current and emerging technologies and equipment, such as unmanned aerial vehicles, ground sensors, networked radios, operator-worn sensor vests, and nanotechnology applications offer warfighters unprecedented command and control and information detection capabilities, yet the use of this technology has not been fully realized. The current protocol, IPv4, is incapable of providing enough addresses due to a depletion of IPv4 address space. IPv6, however, offers unprecedented network support for tactical-level sensor and communications assets in terms of increased address space, Quality of Service (QoS), flexibility, and security.

The Department of Defense is transitioning from IPv4 to IPv6 in order to capitalize on IPv6's expanded capabilities. However, one unresolved area is proper IPv6 network management. Currently, the majority of the configuration and operational knowledge is in the mind of a very few individuals. The expertise currently available must be developed for application by the tactical network manager operating out on the edge of the network, in order to properly administer both an IPv4/IPv6 dual stacked network during the phased protocol transition and a purely native IPv6 network. Second, IPv6 features a robust Quality of Service (QoS) capability previously unavailable through IPv4, which requires research to determine the optimum configuration to support the warfighter's diverse requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

First and foremost, I want to thank God for the countless blessings He has bestowed upon me. My successes here in Monterey, or anywhere else, could not have happened otherwise.

Second, I owe a huge debt of gratitude to my wife, Kelly, who has never once questioned a matter of duty or responsibility. Without you, I would not be where I am today. You are an eternal fountain of support that never runs dry, and as we close this chapter in our lives and begin yet another one, I will not forget the patience and understanding you have shown me.

Third, to my five children, John, Joey, Christopher, Jackie, and Claire, who add a lot of color to my life. Thank you for putting smiles on my face, brightening my day, being patient with Daddy, and teaching me more than I have taught you.

Carmel, you are a loyal friend and have kept the late night watch with me while I attended to my studies. Good dog.

Special thanks to Doctor Bordetsky and to Mike Clement, who have very patiently guided me along the research path. Rather than “feeding me for a day,” they taught me how to “feed myself for a lifetime.” My best wishes for your continued success.

To all of my instructors, fellow students, and to those I am very humbled to call my friends: thank you for your time and support during my tour at the Naval Postgraduate School. To you, I pray that I may remain *Semper Fidelis*.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The size of the address space provided by the Internet Protocol version 6 (IPv6) protocol (2^{128} or 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses) is large enough to give every grain of sand in the world its own unique Internet Protocol (IP) address (Hagen, 2006). Compared to the 2^{32} addresses provided by the current Internet Protocol, version 4 (IPv4) protocol, the networking opportunities and the services that can be provided by IPv6 networks, such as globally accessible sensor networks, outpace current capabilities on an exponential scale. If each sensor on the battlefield had its own globally-unique IP address and were connected to a network, such as the Department of Defense (DoD) Global Information Grid (GIG), then information from a single sensor to clusters of tens of thousands of sensors could be directly accessed from anywhere. On the macro-level, entire mission-defined or functionally-defined clusters of thousands of sensors could provide tailored real-time information, made possible in part by the IPv6 address space and by the use of Quality of Service (QoS) mechanisms built into the IPv6 protocol. The exponential increase in on-line sensors would mean that the potential for end-to-end QoS assurances would be essential due to the increase in network traffic. In order to carry mission critical, real-time information from the edge sensor nodes through a constantly changing and adapting network to a command and control node and ultimately to decision maker(s) would mean that the network would have to “know” what information is more important at any given time. For example, a rifle company

commander could be given access, via a QoS management technique such as a Service Level Agreement (SLA) (Bordetsky & Hayes-Roth, 2007), to a set of preconfigured sensor clusters for a virtual “real-time” leader’s reconnaissance without having to leave friendly lines, spend time traveling to his vantage point, and risk breaking operational security (OPSEC). He could have battalion representatives, his company staff, and subordinate leadership physically present, (or through video teleconferencing, if at a distance), so all interested parties could build situational awareness (SA) together while viewing and discussing the information gathered from the virtual reconnaissance through the sensor network. On the move towards their attack and assault positions, the battalion staff could monitor the specific mission-tailored clusters for any deviations, as discussed during the virtual leader’s reconnaissance. During the assault, the company commander and the battalion staff could monitor the sensor nodes to detect any changes that might be exploitable or cause for alarm.

As more and more sensors of increasing capacity are deployed into the field, the current IPv4 address space will not be adequate for anything other than local use. Currently, network administrators must use creative means to ensure that each of their hosts has a “unique” IP address. Techniques such as network address translation (NAT) and port address translation (PAT) provide a way to add more hosts to a network when there are not enough IP addresses for each. The drawback is that the “outside” world cannot talk directly to the privately-addressed hosts behind the NAT/PAT network device. Global end-to-end connectivity is not a current reality. IPv4 network administrators must also

manage the process that governs the addition or removal of each network device, which requires additional personnel and equipment as the network size and level of complexity scales up. While not ordinarily difficult, problems can and do arise. In a tactical environment where sensors will add and join with a much higher frequency, the level of complexity increases. Joining two or more private space networks, such as multiple clusters of sensors, means that either one network must be renumbered or that complex translation mechanisms must be put into place. Another common issue is when planning the address space does not allow for adequate growth, or when the mission requirements outpace the space allowed. Under the IPv4 scheme, system administrators need to become directly involved when the network capacity does not match operational needs. This problem is not an issue with IPv6, although an optional implementation of DHCPv6 could be undertaken.

A. WHY IPv6?

IPv6 was developed, in part, to address the increasingly obvious shortcomings of IPv4. Developed in the early 1960s and implemented in the 1970s as a means to communicate between government-owned and academia-owned nodes separated by a physical distance, IPv4 was not designed in consideration of the enormous range of the applications it supports today. After 30 years of use, modifications, and hard lessons learned, the Internet Engineering Task Force (IETF) determined in 1993 that IPv4 would soon near the end of its service life and they began to design its successor. Address space, “auto-configuration,” security, header length, and Quality of

Service (QOS) are among the many concepts the IETF developed while designing the next generation IP protocol (as it was called); all of which are considered extremely relevant for large-scale sensor networks (Hagen, 2006).

1. Address Space

The driving factor behind the creation of IPv6 is the need for increased address space. Every networking device, whether a personal computer, server, router interface, or a sensor connected to the Internet, needs its own globally-unique address. No two devices can have the same address or delivery conflicts will arise and those devices will not be able to communicate on the network. In the Internet's infancy, IP addresses were not allocated efficiently, nor were they allocated uniformly around the world. Consequently, lesser-developed regions in the world did not receive a fair allocation of addresses. "Band-Aid" solutions have arisen as a means around the lack of address space. NAT/PAT provide a means to route from "private" address space to a globally-unique IP address, but that same node cannot be routed globally, since its address is private and, therefore, non-deliverable directly by design. End-to-end connectivity is not possible with this temporary solution. The problem becomes increasingly relevant as more and more automated systems and commercial services become dependent on IP addresses. Realizing the need for additional globally-unique IP addresses, the IETF decided to increase the next generation IP protocol address space by a factor of $2^{128}/2^{32}$ or 2^{96} to ensure that lack of addresses would not conceivably be an issue.

2. Auto-configuration

The increased address space resulting from IPv6 means that there will be a significant increase in the number of devices on the network. As each device joins the network, it will need its own IP address. Current IPv4 standards allow for a manual static address assigned by a network administrator or an automatic IP address assignment by a Dynamic Host Control Protocol (DHCP) server, which dynamically assigns addresses based on the configurations set by an administrator. While less work-intensive and more responsive to the user's needs, the DHCP server must still be managed like any other network service. When the number of possible IPv6 devices is considered, it is clear that the network administrator's workload will increase accordingly. Purely static configuration would be improbable, and currently-designed DHCP services would occupy a large portion of the administrator's time as well as network bandwidth. Recognizing this, the IETF developed a mechanism to make configuration transparent and seamless. Auto-configuration is a process whereby the joining device "requests its network prefix from an IPv6 enabled router on its link and then joins that prefix with its media access control (MAC) address or some other unique, random number to make one or more unique global address[es]" (Hagen, 2006). This feature makes the administrator's job considerably easier, makes the network less complex by eliminating the need for traditional DHCP servers, and provides a more timely solution to devices that constantly enter and leave the network, such as sensors in a tactical environment.

A separate, but related, feature is Mobile IPv6, which allows an IPv6 device to maintain its IP address regardless of what network it is connected to. This requires a device to bind its assigned IP address to a “care-of” address that is registered on its home network router. Traffic sent to the device’s static address is first sent to its home network router and then forwarded to its care-of address (Hagen, 2006). The benefit of this feature is that a device can have a permanent address that never changes as it moves to or through different networks, which provides user continuity. However, additional network resources are consumed as messages are essentially sent twice, virtually doubling the amount of traffic on the network.

3. Security

The IPv4 protocol was designed at a time when network security was not a concern. Networks were few and users were trusted to use the networks with good intentions. Security mechanisms were not built into IPv4. Over time, and as more networks and users came on-line, malicious users began to look for ways to exploit the unsecure network for personal gain, notoriety, destructive purposes, or a combination of these. Solutions to these problems included security mechanisms, such as passwords, and the eventual development of Internet Protocol Security (IPsec) (Hagen, 2006). IPsec is not widely used with IPv4 because of the difficulty of incorporating it into existing networks. Recognizing the need to co-evolve a robust security framework during the development of IPv6, the IETF stipulated that IPsec would be

incorporated in the new IP protocol. While IPsec is optional for IPv4, it is mandatory for all IPv6 implementations (Hagen, 2006).

IPsec can be implemented in two modes. The first, tunnel mode, works like a Virtual Private Network (VPN). The entire transmission is encapsulated in a new header containing the IP address of the receiving gateway (Hagen, 2006). This tunnel provides the added feature of transmission security, in that packets sniffed “off of the wire” will not reveal the source and destination IP addresses. The observer will only see the gateway IP addresses, since the real addresses are encapsulated. This method not only requires more overhead and security management, but it also introduces a performance-degrading bottleneck. The second method is transport mode, in which end-to-end users communicate without an intervening gateway. This method requires less overhead and does not create any potential bottlenecks, but the actual IP addresses are not hidden from view. Transport mode provides a real benefit for IPv6 networks. Because NAT/PAT is no longer necessary, end users can connect directly and, therefore, encrypt their transmissions without any problems with intervening networking devices.

4. Headers

The IETF designed the IPv6 header length to be both fixed in length and simpler than the IPv4 header. Figure 1 shows the IPv4 header in comparison with the IPv6 header; Figure 2 shows the number of bits in each header.

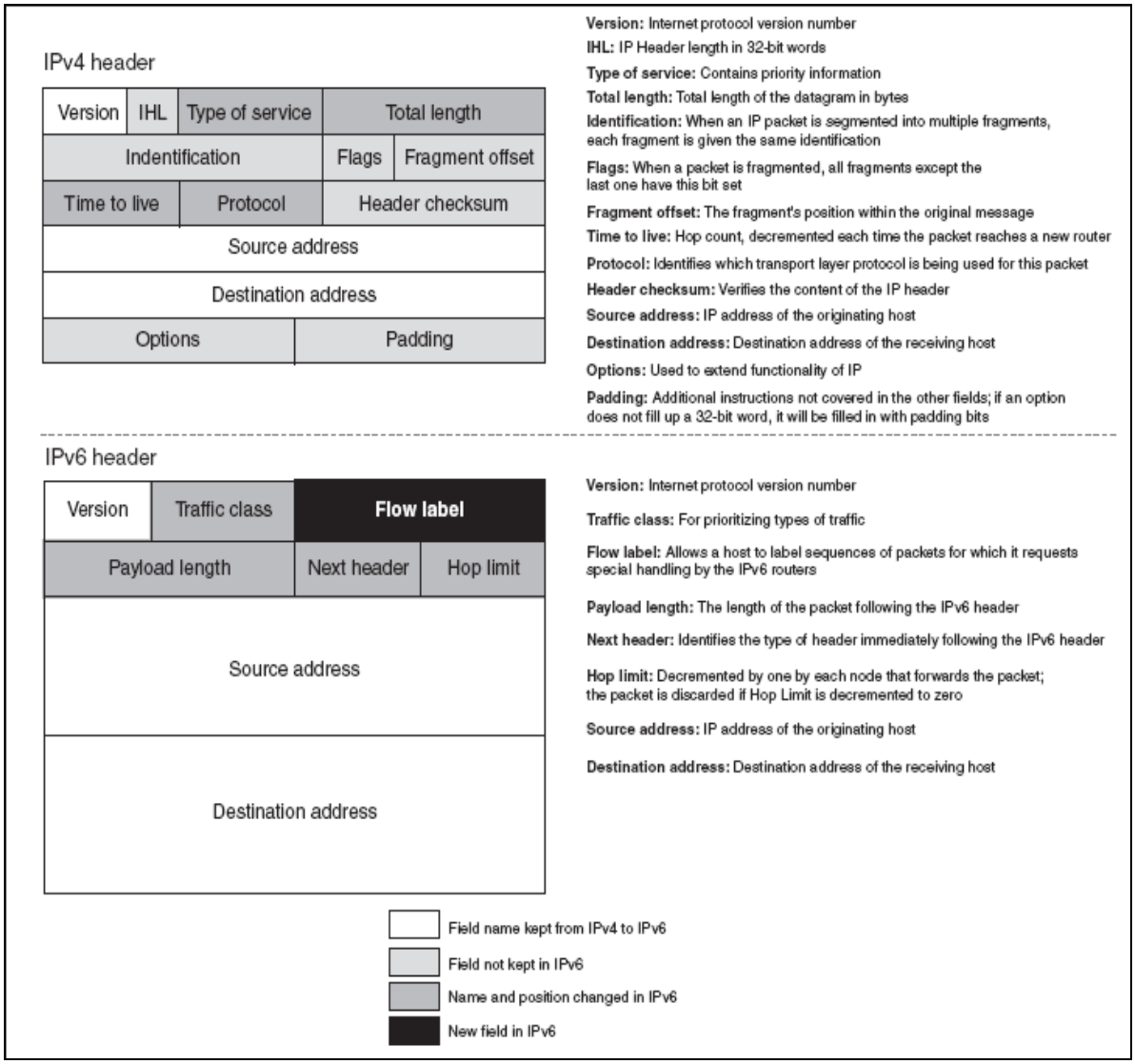


Figure 1. Comparison of the IPv4 and IPv6 protocol headers (From Adame & Kong, 2008).

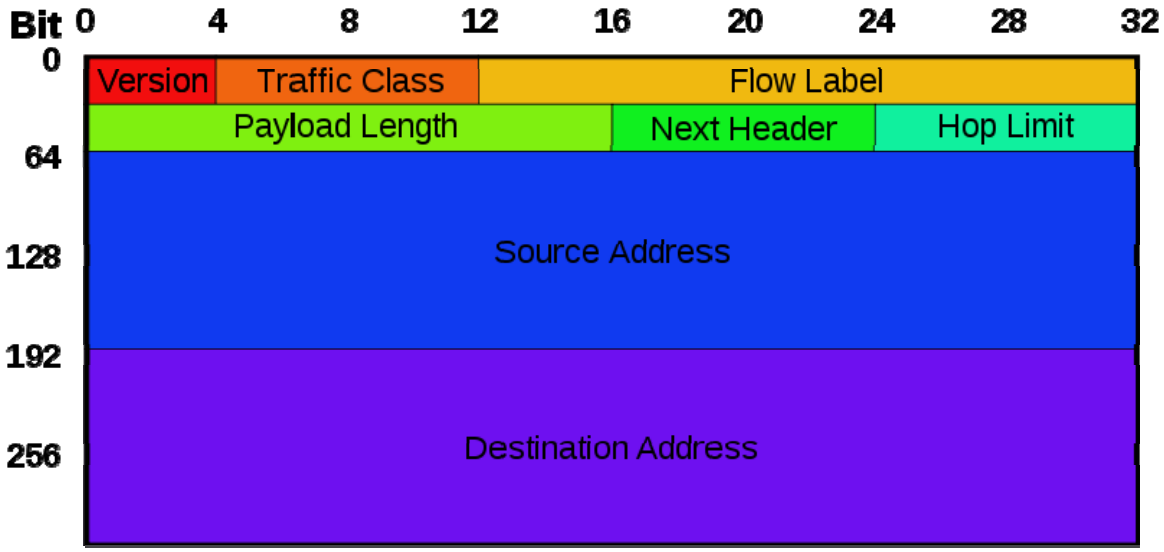


Figure 2. The IPv6 header (From Mikm, 2009).

While the IPv6 header is longer bit-wise to accommodate two 128 bit addresses, it omits information that is not necessary for routing packets through an IPv6 network; the base header also has a constant size of 40 bytes. Consequently, the following fields have been dropped (Hagen, 2006).

a. Header Length

Since the IPv6 header length is fixed at 40 bytes, this information is redundant and will only slow down the processing time.

b. Identification/Flags/Fragment Offset

The IPv6 protocol requires a minimum maximum transmission unit (MTU) size, so packet fragmentation is not normally required. If fragmentation is required, then an optional extension header will be appended to the header to denote this.

c. Header Checksum

Checksums at layer three were included in the original IPv4 specifications due to a lack of bit error detection at lower layers. Both layer two and upper layer protocols now contain error detection, which makes error detection at layer three redundant and processor intensive. . IPv6 takes advantage of these advances and saves the router’s processing power normally used for error checking.

d. Type of Service

Originally designed to denote traffic prioritization, Type of Service has been replaced with the Traffic Class field (Hagen, 2006).

e. Protocol Type/Time to Live

Protocol Type/Time to Live have been replaced and incorporated into other IPv6 fields.

The following IPv6 header fields have been added or modified (Hagen, 2006).

f. Traffic Class

This field is used to distinguish one data type from another and is used to facilitate QoS for real-time data traffic. Differentiated Services (DiffServ) makes use of this IPv6 field as specified in Request for Comments (RFC) 2474, and will be described in greater detail in subsequent chapters of this thesis.

g. Flow Label

Flow labels are combined with the source address, and are used to distinguish one data flow from another. One particular data flow may require different handling through

the network, in comparison with another, and will be transmitted with associated options. Intervening routers will interpret these options and will treat the packets accordingly. Flow labels are used in conjunction with the traffic class field form the basis for QoS in IPv6 networks (Hagen, 2006).

h. Payload Length

While similar to the IPv4 header field, total length, the IPv6 payload length field includes the length of the appended data as well as any header extensions.

i. Next Header

Similar to the IPv4 protocol field, the IPv6 next header field directs the appropriate network device to the beginning of the header it should process. Different extensions apply to different network devices; therefore, this field will change each time a device finishes processing a packet. As with IPv4, this field also contains values to denote the protocol for the appended layer four data.

5. Extension Headers

As stated previously, the IPv6 protocol standard, RFC 2460, specifies a header of fixed length, which aids in better networking performance (Hagen, 2006). Additional information in the form of options can be added to the header to provide the networking customization needed by the user. All, some, or none of these options may be used, and are placed in the order shown in Figure 3. These options are called extension headers and are positioned immediately behind the IPv6 header, and directly ahead of the layer four

header. Extension headers are added by the source node and are read only by the destination node, with a few exceptions such as router per hop behaviors.

Figure 3. IPv6 Extension Headers (From Fineberg, 2005).

The following extension headers are included in the IPv6 protocol.

a. Hop-by-Hop Options Header

This extension header carries optional information, such as the Resource Reservation Protocol intended for each node along the destination to the end node. This header must be placed immediately behind the IPv6 header. The absence of a Hop-by-Hop Options header indicates that intervening network devices can forward the packets on without any packet processing required (Hagen, 2006).

b. Routing Header

Use of this extension header specifies a number of intervening nodes that the packet must travel through on its way to its destination IP address. This option is based on loose source routing; other nodes may be visited in between, so long as each required node is visited in the specified order (Hagen, 2006). This is in contrast to strict source routing which calls for the packet to travel a specified path without visiting any other nodes.

c. Fragment Header

If a source node determines that a packet is larger than the largest supported maximum transmitted unit (MTU) on a particular link, then the source node will fragment the packet and use the fragment header to declare the fragmentation. IPv6 networks only fragment at the source node and not in network devices to increase network performance (Hagen, 2006).

d. Destination Option Header

This option carries additional information for the destination node and it is normally placed behind all other extension headers. When placed before the Routing header, it then carries information intended for each intervening node in the network (Hagen, 2006).

e. Authentication Header

Used for IPsec, the authentication header provides “integrity and authentication for all end-to-end transmissions” (Hagen, 2006).

f. Encapsulating Security Payload Header

Used for IPsec, this header provides “integrity, confidentiality, data origin, authentication, anti-replay service, and limited traffic flow confidentiality” (Hagen, 2006).

6. Unicast, Multicast, and Anycast Addresses

The broadcast address is not used in IPv6 networks, since broadcast addresses have historically caused network problems (Hagen, 2006). A large-scale IPv6 network could risk a limited self-imposed denial of service (DOS) every

time a message is sent to a broadcast address. The IPv6 protocol makes use of three other addresses: unicast, multicast, and anycast. Note that IPv6 interfaces can have more than one address assigned to it.

a. Unicast Address

The unicast address is synonymous with the global address. It uniquely identifies the node's interface on the Internet.

b. Multicast Addresses

Multicast addresses replaced the broadcast address functionality. Interfaces can be grouped together under a single multicast address, and any message sent to a multicast address will be "processed by all members of that multicast group" (Hagen, 2006). Weather sensors can be assigned an additional multicast address identifying them as the weather group, and all will respond to messages sent to the multicast address. Weather forecasters can send a single "current temperature query" to a specific weather sensor multicast address and all weather sensors with that address will respond with the requested information.

c. Anycast Addresses

Anycast addresses are also assigned to multiple interfaces, but they differ from multicast addresses in that a message sent to an anycast address will go to the nearest node only. If a node has traffic for a video server, it can then send that traffic on the video server anycast address. From there, that traffic will go the nearest video server. This concept reduces the amount of traffic traversing the network.

7. Quality of Service

When IPv4 was developed in the 1970s, applications such as video teleconferencing (VTC) over IP, Voice Over IP (VOIP), and other time-sensitive applications, were far from the drawing board. IPv4, and the TCP/IP protocol suite that it uses at layers three and four, was designed to provide “best-effort delivery.” The definition of best-effort delivery is that a transfer can accept delay because of temporary network congestion and not degrade service. This is in contrast to a service that would be affected if network congestion affected time sensitive applications. For applications such as file transfer and email delivery delay and latency unnoticeable to the human sense of time are considered acceptable, since such applications are not considered time sensitive.

Because the need for network QoS was not anticipated when IP was first developed, when applications such as VTC over IP, streaming live video, and VOIP were incorporated into networks, the choice had to be made to either allocate a large percentage of bandwidth to those services at the heavy expense of others, or to accept a lower-quality product that could have often caused more problems than it solved. The traffic class field in the IPv4 header was originally designed to segregate different classes of traffic in order to promote certain traffic flows, thus providing real-time applications with a “clear path” through the network. A lack of fielded applications and the additional processing required on the relatively slow networking devices at the time led to a lack of QoS implementation with this header field (Hagen, 2006).

The increase in time-sensitive applications being used over limited bandwidth, and the necessity of providing QoS for time-sensitive applications are two reasons that the IETF designed the IPv6 protocol to support QoS with its “designed from the ground up” traffic class and flow label fields. The IETF also stipulated that IPv6 addresses would be assigned to interfaces rather than the nodes themselves, so that one node could have more than one address “assigned” to it. In addition to providing addresses for anycast and multicast transmissions, interfaces can be assigned multiple addresses. Each of these corresponds to an associated QoS level. An application of these concepts is discussed in more detail in Chapter II. These three areas form the basis for QoS in IPv6. Table 1 is a side-by-side comparison summary of IPv4 and IPv6.

IPv4	IPv6
Source and destination addresses are 32 bits (4 bytes) in length.	Source and destination addresses are 128 bits (16 bytes) in length.
IPSec support is optional.	IPSec support is required.
No identification of packet flow for QoS handling by routers is present within the IPv4 header.	Packet flow identification for QoS handling by routers is included in the IPv6 header using the Flow Label field.
Fragmentation is done by both routers and the sending host.	Fragmentation is not done by routers, only by the sending host.
Header includes a checksum.	Header does not include a checksum.
Header includes options.	All optional data is moved to IPv6 extension headers.
Address Resolution Protocol (ARP) uses broadcast ARP Request frames to resolve an IPv4 address to a link layer address.	ARP Request frames are replaced with multicast Neighbor Solicitation messages.
Internet Group Management Protocol (IGMP) is used to manage local subnet group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
ICMP Router Discovery is used to determine the IPv4 address of the best default gateway and is optional.	ICMP Router Discovery is replaced with ICMPv6 Router Solicitation and Router Advertisement messages and is required.
Broadcast addresses are used to send traffic to all nodes on a subnet.	There are no IPv6 broadcast addresses. Instead, a link-local scope all-nodes multicast address is used.
Must be configured either manually or through DHCP.	Does not require manual configuration or DHCP.
Uses host address (A) resource records in the Domain Name System (DNS) to map host names to IPv4 addresses.	Uses host address (AAAA) resource records in the Domain Name System (DNS) to map host names to IPv6 addresses.
Uses pointer (PTR) resource records in the IN-ADDR.ARPA DNS domain to map IPv4 addresses to host names.	Uses pointer (PTR) resource records in the IP6.ARPA DNS domain to map IPv6 addresses to host names.
Must support a 576-byte packet size (possibly fragmented).	Must support a 1280-byte packet size (without fragmentation).
Single address assigned to a single node	Multiple addresses are assigned to a single interface

Table 1. Comparison of the IPv4 and IPv6 protocols (From Adame & Kong, 2008).

B. PURPOSE OF STUDY

Given the 2003 DoD CIO memorandum citing the need to transition the GIG to IPv6, the OMB memorandum 05-22, Transition Planning for Internet Protocol Version 6 (IPv6), and the DoD IPv6 Standard Profiles for IPv6 Capable Products Version 2.0 published in 2007, debate on the merits of a IPv6 sensor network versus a IPv4 sensor network has been overcome by events. The DoD, like much of the commercial world, is transitioning to IPv6 networks. While the benefits provided by IPv6 are numerous, its challenges lie in managing a network on the scale proposed, while also operating in the relatively untried IPv6 domain. Transitioning traditional sensors, such as ground and airborne video cameras, and network devices, such as servers and workstations, is an on-going process. Likewise, testing of network management systems for IPv6 compatibility, operability, and usability in a tactical network is under way. New challenges are also presented by the need to integrate into the IPv6 segment new sensor capabilities, such as soldier battlesuit-borne IP-enabled drug injection and hormone sensing devices, as well as sensors placed in spacesuits. Accessing this information also presents challenges. Feasibility studies are conducted to show that, for these devices, the IPv6 domain is at least as capable an operating space as is the current IPv4 domain. Lessons learned from planning, installing, and operating these devices in the IPv6 domain during a series of Naval Postgraduate School (NPS) Tactical Network Topology (TNT) studies will be captured for future operational reference.

Currently, network administrators configure network management tools such as Internet Control Message Protocol

(ICMP) and Simple Network Management Protocol (SNMP) to monitor the network's health at a higher level and to make network configuration changes as needed in order to provide service over a "best-effort" network (Perkins, 1996). Bandwidth, network traffic, and route availability are in a constant state of flux. This in turn causes the network and the traffic that traverses it to constantly adapt to changing conditions. Adapting a large-scale sensor network within the IPv6 address space requires a new look at QoS techniques, so that the user can scope his view to a particular set (or sets) of sensor clusters and pull real-time information, all while contending with a multi-layered, continually-adapting network topology. A tactical network SLA taxonomy has been developed in order to show how the commander envisions having his information requirements answered by the tactical sensor network supporting his mission. This taxonomy will support the "commander's view" at a higher information level than the proposed implementation at the network level. This model is proposed to assist the operational Information Management Officers (IMOs) who will then implement it in support of their commander's information needs through a highly dynamic, capable IPv6 tactical sensor network.

C. THESIS QUESTIONS

The primary research question of this thesis is: How can the benefits and improved capabilities of the IPv6 protocol improve the integration, deployment, and operation of sensor networks, and how can those improved networks support a tactical commander's information needs?

The subsidiary questions are:

- How can the Quality of Service in sensor networks be improved by the use of IPv6 and associated Quality of Service techniques?
- How can Service Level Agreements support combat operations?
- Describe a Service Level Agreement taxonomy in support of an IPv6 sensor network.
- Describe a Campaign of Experiments for future IPv6 tactical sensor networking studies.

D. SCOPE AND LIMITATIONS

The scope of this thesis encompasses a description of the IPv6 protocol and the benefits of its application to tactical sensor networks. A feasibility study was conducted during the TNT series of experiments to qualitatively show that the IPv6 protocol is in fact valid for sensor networks. Quality of Service (QoS) and Service Level Agreements (SLA) for ensuring a certain level of QoS in IPv6 tactical networks were studied, with appropriate recommendations made. An associated campaign of IPv6 QoS experiments is proposed for future work. This study and its associated experiments made use of the TNT administered by the Center for Network Innovation and Experimentation (CENETIX) laboratory at NPS.

E. ORGANIZATION OF STUDY

This thesis is organized as follows: Chapter I introduces the IPv6 protocol, sensor networks, and why the

two domains are a natural combination. Chapter II, the literature review, addresses the optimal protocols and configurations necessary to provide (optimal) QoS for end-user decision makers in an IPv6 sensor-networked environment. Chapter III describes an IPv6 tactical sensor network feasibility study conducted during TNT 09-2 aboard Camp Roberts. Chapter IV lays the framework for IPv6 QoS techniques and related SLA support of the tactical commander's information requirements. It further develops the sensor network taxonomy, by defining tactical SLAs, defining the war-fighting functions, and then relating the information requirements of those functions to the need for service level agreements. Five example SLAs are developed using a variety of common, real-world missions; they are then compared and contrasted to develop the framework for the sensor network taxonomy. Finally, the sensor network taxonomy is described in an operational context. Chapter V describes an ambitious campaign of experimentation for future QoS studies in the IPv6 sensor network environment. Proposed variables and experimentation scenarios are discussed at length; conclusions follow the experiment description and findings. Chapter VI concludes this work with a review of the concepts introduced, and with suggestions for future work. A systems approach experimentation framework to determine the necessary design variables, relationships, and performance criteria is proposed. This framework provides a means for optimizing QoS solutions in a dynamic, large-scale sensor network. A QoS TNT experiment for the IPv6 sensor network is also proposed for future studies.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. SYSTEMS APPROACH TO SENSOR NETWORK ADAPTATION

For the purposes of this thesis, large-scale tactical sensor networks are defined as thousands of various mission-specific nodes distributed either randomly, selectively, or as a hybrid of the two; situated in a given operational area; networked together; and which form paths back to a command and control node at which point the information is aggregated and used for various operational purposes. Yu et al. (2001) simulated large scale sensor networks reaching upwards of 4800 sensor nodes scattered uniformly in a dense pattern. Eschenauer and Gilgor (2002), while studying the cryptographic key management problem in distributed sensor networks, made a distinction between “traditional embedded wireless networks” and distributed sensor networks (DSNs) by primarily numbering DSN nodes in the tens of thousands (NAI Labs, 2000). Sensor nodes can be employed to transmit streaming video from unmanned aerial vehicles (UAVs) or ground-deployed cameras; to record environmental data in an area of interest; to monitor Nuclear, Biological, and Chemical (NBC) detection; to monitor battle suit vital signs to quantitatively determine the overall health of a unit; or to perform any other mission-dictated purpose in which a sensor can provide timely information in response to the commander’s information requirements. These sensors can be deployed in many different environments and locations, some of which may render the sensors immediately useless or may cause them to degrade at rates depending on the situation and/or location. Likewise, the “physical health” of the

sensors is an additional factor in the network's ability to provide timely information (Estrin, 1999).

In systems thinking, adaptive systems alter their behavior according to changes in their environment, or in parts of the system itself (Clement, 2008). Capra (1996) refers to adaptation in his discussion of feedback loops. "The consequence of this arrangement is that the [input] is affected by the [output], which results in self-regulation of the entire system, as the initial effect is modified each time it travels around the circle." Kim and Shin (2002) define network adaptation as the link between high-quality demand applications and the underlying physical networks that exist in their own widely dynamic environment.

Current networks were originally designed to provide "best-effort service," which includes as normal and accepted latency, jitter, and packet loss, although efforts are being made to reduce these issues (Yu et al., 2002). Sensor networks are dynamic systems subject to constant change of state. Routes, bandwidth allocation, availability, jitter, complete loss of links, and nodes joining and leaving the network almost randomly are some of the constantly changing elements of a large-scale sensor network. Both the "environmental" impact and health of the network affect real-time, dynamic, uninterrupted access to information gathered through individual and clustered sensor nodes. Feedback obtained from end systems, as well as through intervening network devices, forms the impetus for network adaptation, which would mitigate the effects of and adapt to the network's environment (Bechler, 2000). IPv6, and its inherent capability to provide varying levels of QoS, is intended to take the tactical network to the qualified "QoS

level.” The QoS level is considered “qualified,” in this case, because in a combat environment, as opposed to a non-combat or commercial environment (such as a Verizon ISP in a major United States city), the likelihood of system degradation or destruction is real. Although redundancy can be built into network resources, time is limited and long-term network plans are subject to the fluid nature of war. Below a certain performance threshold, and due to the possibility of loss of equipment and/or denial of service, “best effort” service is the most one can hope for.

B. ADAPTATION APPROACHES

1. SPEED

He et al. (2003) proposed improving QoS in sensor networks by developing SPEED, a real-time sensor network communications protocol. Recognizing that data delivery is the primary purpose of sensor networks, the authors designed their protocol on the premise that “speed” across the wireless network could be used as a metric, regardless of whether the communication is between nodes, to the base station, or from the base station. By comparing the “delivery speed” to the “actual speed” of a packet from a distant node, network status can be obtained, from which delivery decisions are determined. To adapt to network conditions, SPEED takes advantage of common IPv6 communication networking services such as unicast, area-multicast, and area-anycast. Unicast is used when data must be sent to a specific device. Area-multicast is preferred when communicating to a specific set, or a cluster, of sensor nodes such as allNBC for all nodes with the ability

to detect NBC contaminants, or allWindSpeed sensors for sensors that can detect wind speed on certain mountain passes and peaks. Area-anycast is used when the same information can be obtained from any one, random, sensor in a cluster (He et al., 2003). Proactively, SPEED uses several adaptive mechanisms to determine an optimal route path based on real-time network behavior. The data-link layer determines routes and relay speeds to downstream nodes while the network layer employs a concept known as back-pressure, to reroute traffic when the data-link layer has determined that a particular downstream route is not optimal. In addition to finding route congestion, SPEED also finds the non-congested paths in the network and redirects traffic to take advantage of unused bandwidth subject to overall performance. When used together, the protocol is shown to improve QoS from end-to-end, and then to provide a linkage between the need for real-time information and navigating a dynamic network (He et al., 2003).

2. FICCRD

Yu et al. (2001) have taken a similar tack in developing the Fair Intelligent Congestion Control Resource Discovery (FICCRD) protocol in which, simply stated, the QoS issue is addressed by core routers determining optimal routes and available bandwidth and then forwarding that information to the edge routers for routing determination decisions. FICCRD intends to achieve a fairness of network resource allocation and therefore to improve end-to-end connectivity. Since layers three and four of the TCP/IP model are essential to providing optimal QoS they are continually sampled for environmental impacts. As an

example, feedback loops from layer three support TCP with their connections and buffer window sizes. The current state of the physical resources available is also determined and combined with the upper TCP/IP stack information to determine the network's state. This feedback, in turn, provides the core routers with the information on the current state of the network. The information is then pushed back out to the edge routers, thus providing an adaptive QoS link between the sensor nodes and the user needing real-time information (Yu et al., 2002).

3. User-defined Priorities

Bechler, Ritter, & Schiller (2000) researched QoS in end-user wireless "node" environments where a user is able to make QoS decisions and determine which service(s) will be given priority. For example, a user may want to make a phone call and need to download email prior to boarding a flight in an environment with limited bandwidth. By determining that the phone call is the application most in need of the limited resources, the user enables a QoS application that makes the phone call the priority. At the expense of other running applications the phone call will get at least the minimum amount of network resources. This example describes an architecture proposed by the authors that provides QoS to three types of applications: common, adaptive, and proactive. Common applications are considered "best-effort" and are not capable of obtaining resources to guarantee services. Adaptive applications make use of available network resources and use techniques such as compression to provide QoS in a constricted environment. The authors label adaptive applications as "passive" and note that the

adaptive application will provide QoS in proportion to the available network resources (Bechler et al., 2000). Proactive applications, such as the one described above, will fence off resources such as bandwidth and processing time, should the initial adaptation step not provide minimal QoS. These applications give the end-user the ability to choose the best service depending on his situation (Bechler et al., 2000). The next step in this architecture proposal could be one in which the system determines QoS level remotely to determine which sensor cluster(s) receives the appropriate QoS.

4. Differentiated Services (DiffServ)

Bouras et al. (2004) noted that many of the QoS services available have been designed to operate in the IPv4 address space and, thus, to operate under IPv4 conditions. Understanding that IPv6 network behavior is considerably different than that of IPv4, they hypothesized that the QoS services would need to be reexamined. In an effort to determine supported QoS mechanisms, they tested DiffServ in the IPv6 domain, which puts “strict priorities of packets coming from real-time applications” and sends the rest through best-effort mechanisms. Different network conditions were simulated and the authors’ final qualified conclusion is that QoS services can operate in an IPv6 domain; at the time of publication they also stated that considerable research still needs to be done.

RFC 2474 defines the traffic class field in the IPv6 header to be the differentiated services field. This field provides the intervening DiffServ-enabled routers with the information needed to process the packets in accordance with

standardized forwarding rules. Operating within a DiffServ domain, the field implements the policies prescribed for all networking devices within the DiffServ domain; by extension, every network device must have consistent, up-to-date instructions on how to handle each packet received in each domain. Traffic entering the domain is classified at the boundary and labeled in accordance with domain policies. Intra-domain traffic is classified at the source device. As shown in Figure 4, the first six bits of the field provide a combination of 64 codepoint values that provide DiffServ routers with handling instructions as each packet header is processed while the remaining two bits, congestion notification, are not currently used according to RFC 2474.

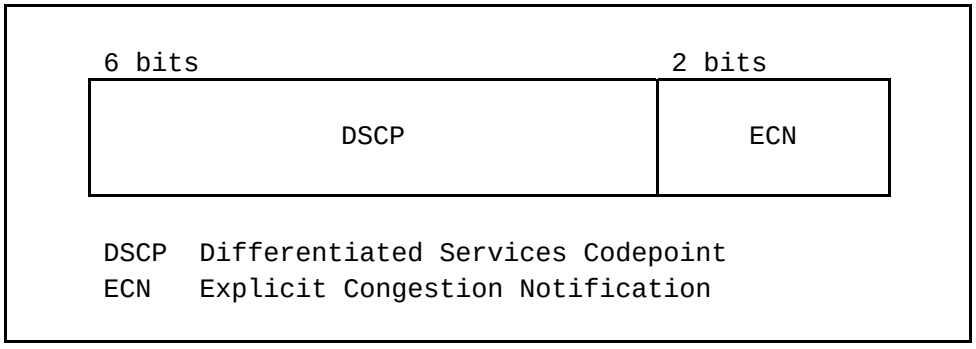


Figure 4. Format of the DS field (From Hagen, 2006).

Table 2 contains the standard codepoints that are defined as “pool one.” Thirty-two codepoints are contained in this pool, while the remaining 32 are divided among pools two and three for experimental or local use.

Name	Registry: Space	Reference
CS0	000000	[RFC2474]
CS1	001000	[RFC2474]
CS2	010000	[RFC2474]
CS3	011000	[RFC2474]
CS4	100000	[RFC2474]
CS5	101000	[RFC2474]
CS6	110000	[RFC2474]
CS7	111000	[RFC2474]
AF11	001010	[RFC2597]
AF12	001100	[RFC2597]
AF13	001110	[RFC2597]
AF21	010010	[RFC2597]
AF22	010100	[RFC2597]
AF23	010110	[RFC2597]
AF31	011010	[RFC2597]
AF32	011100	[RFC2597]
AF33	011110	[RFC2597]
AF41	100010	[RFC2597]
AF42	100100	[RFC2597]
AF43	100110	[RFC2597]
EF PHB	101110	[RFC3246]

Table 2. DSCP Pool 1 Codepoints Reference (From RFC 2474).

CS in the first column refers to class selector codepoint, AF refers to assured forwarding, meaning better-than-best effort, and EF refers to expedited forwarding, which is the best service the network can provide. These designations provide for differing levels of backwards compatibility and precedence setting. The codepoint values are mapped to Per-Hop Behaviors (PHBs), which specify how packets are to be forwarded. PHBs can be individually defined within each DiffServ domain with the exception of the default value of 000000, which stands for best effort delivery/no priority. Where a maximum of 64 codepoint values

exists any number of PHBs can exist (Hagen, 2006). Each domain can, therefore, specify its own prioritization policies.

The 20-bit flow label in the IPv6 base header is used by the source node to specifically and uniquely identify a flow of information between the source and destination nodes. RFC 3697 defines a flow as a "sequence of packets from a [source] to a specific unicast, anycast, or multicast address labeled as a flow by the [source]" (Hagen, 2006). Flow labels are chosen in a random fashion to "provide a hash key for routers in order to look up the state associated with the flow" (Hagen, 2006). Source nodes can handle multiple information flows, since each is uniquely identified by a combination of the source address, destination address, and flow label. When flow labels are combined with the traffic class, field dynamic QoS can be attained within a DiffServ domain that is configured with the appropriate polices (Hagen, 2006).

It must be noted that both the DoD IPv6 Standard Profile for IPv6 Capable Products and NISTs Profile for IPv6 in the US Government stipulate that IPv6 hosts and routers must support DiffServ (Office of ASD/DoD CIO, 2007; NIST, 2008).

C. SENSOR NETWORKS AND TACTICAL NETWORK TOPOLOGY (TNT)

Initiated in 2001 as a platform to develop unmanned systems and wireless networking capabilities, the TNT experiment series, detailed in Figure 5, has developed into a large test-bed with which DoD, USSOCOM, and other partners can research new technologies for operational use.

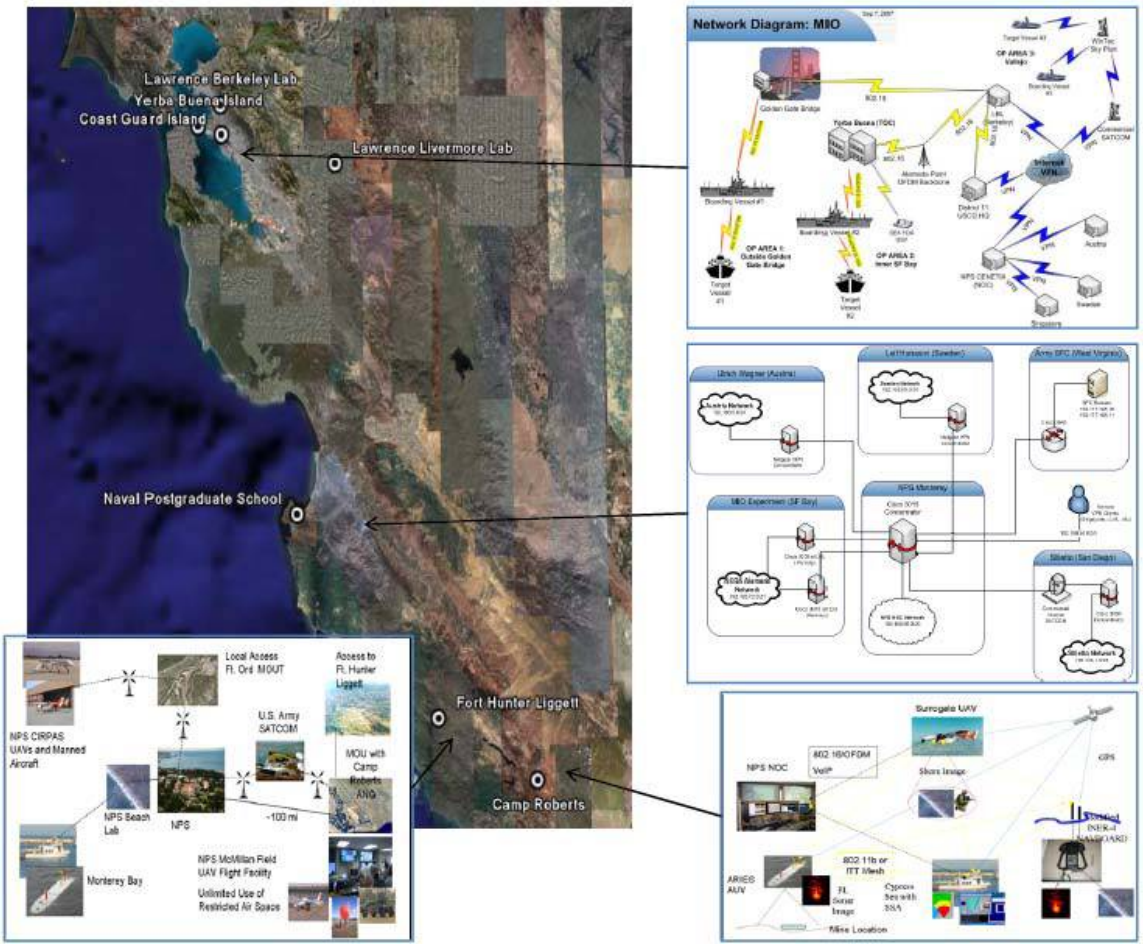


Figure 5. Diagram showing the Tactical Network Topology (TNT) (From Adame & Kong, 2008).

Incorporated with the CENETIX the lab's mission is to:

> support advanced studies of wireless networking with unmanned aerial, underwater, and ground vehicles in order to provide flexible deployable network integration with an operating infrastructure for interdisciplinary studies of multiplatform tactical networks, Global Information Grid connectivity, collaborative technologies, situational awareness systems, multi-agent architectures, and management of sensor-unmanned vehicle-decision maker self-organizing environment. (Ferrell, 2006)

The TNT testbed provides the opportunity and means to test sensor network capabilities and proofs-of-concept on a quarterly basis in a plug-and-play network. It is a unique environment, in that it enables military and civilian users alike to use the TNT testbed on a multitude of layers and applications. Examples include:

- The TNT [users] can integrate their sensors and mesh networking elements in the unclassified but closed IP space of the TNT testbed by getting fixed IPv4 and lately IPv6 addresses. […] This illustrates the online portal enabling rapid integration of experimental assets in TNT testbed IP space,

- Users can connect their remote local area network, including command and operation centers, via the virtual private network (VPN) client on top satellite or commercial IP cloud services,

- Sensors and unmanned vehicles can be integrated with the TNT Situational Awareness Environment via the applications layer interoperability interface. The current option includes Cursor-on-Target (CoT) integration channel, initially developed at MITRE (Miller, 2004), comprised of the CoT message router and CoT XML adapters for each node need[ing] to be integrated[…]. In the very near future we will consider adding the Common Alert Protocol (CAP), which is becoming widely used by the DHS community,

- Human operators (both remote and local) can access the testbed collaborative environment via the collaborative portal or [via] peer-to-peer collaborative clients, situational awareness agents, video conferencing room […], and video client. This is human layer interface to the testbed.

- At the physical level the testbed reaches to even lower levels (like multiple mesh network enabled unmanned systems), which permits

> researchers to experiment with such things as airborne sensors and cooperative control […] without having to be concerned about network connectivity. (Bordetsky & Netzer, 2009)

In the TNT environment, Bordetsky et al. (2004) performed experiments aboard the Naval Postgraduate School to explore network performance awareness in a peer-to-peer (P2P) collaborative environment. While a P2P environment is somewhat different from a sensor environment, their position is similar to that of Bechler, Ritter, and Schiller (2000) in that the users need to actively participate in determining which applications will have QoS in a resource constrained environment. Bordetsky et al., (2004) proposed that both application end-users and NOC operators have the ability to determine network performance in order to decide how to improve QoS, whether it involves moving to a better transmission location and/or terminating excessive background applications that are hoarding network resources. However, sensor networks containing thousands of nodes cannot be moved arbitrarily, so some automation is required to self-determine the optimal routes for data delivery. In "Adaptive management of QoS requirements for wireless multimedia communications," Bordetsky et al. (2003) support this idea in their focus on real-time networking applications traversing DoD's GIG, which requires minimal amount of bandwidth in order to function properly. Their model, based on the Telecommunications Management Network (TMN) model, relies on capturing the information from, and adapting to, several layers of feedback controls to provide the appropriate levels of QoS for future use. For example, at the application layer, Call Preparation Control records information on end-to-end application connections and

determines minimal requirements for future uses. Connection Control monitors the current connection and arbitrates for necessary network resources to maintain minimal requirements. The transport layer makes use of the Real Time Protocol (RTP), which determines network performance through sub-protocols sending and receiving reports from which adaptive decisions can be based on (Bordetsky et al., 2003). This layered approach is similar to the approach taken in Yu et al.'s (2002) FICCRD approach and He et al.'s (2003) SPEED approach. Bordetsky & Hayes-Roth (2007) propose adding an eighth layer to the OSI stack to provide a "human-like operator inside the network" between the deployed sensor nodes and the consumers of the information provided in order to increase the QoS capability. A human operator in the NOC or technical control facility can monitor the network status at near real-time and can then reconfigure the network to provide various levels of service. There is, however, an inherent delay in this process that may exceed the value gained by directing the real-time information to the right person at the right time. This eighth layer serves to solve the delay introduced by human operators by providing each node the capability of a NOC, which automatically provides the level of service required or desired, as stated in a Service Level Agreement in a network that is undergoing constant change (Bordetsky & Hayes-Roth, 2007). During TNT 09-1, nanotechnology sensors were included as part of a developing series of experiments to determine appropriate communication and network management methods. Follow-on experiments included testing the sensor network within an IPv6 network extension within the TNT testbed to test QoS issues and other IPv6 network management research.

Table 3 presents a comparison among the QoS mechanisms used in each protocol discussed in this chapter.

	QoS Solutions for Sensor Networks				
OSI Model	**IPv4 Solutions**			**IPv6 Solutions**	
Layer 2	SPEED	FICCRD			
Layer 3			DiffServ	Flow Labels in header	DiffServ/IntServ
Layer 4					
Layer "8"	Hyper-Nodes			Hyper-Nodes	
Advantages				-2^{128} global address space enables end-to-end connectivity from anywhere -"RFC-backed" Flow labels -IPv6 designed for QoS	
Disadvantages	-2^{32} address space cannot support end-to-end connectivity -IPv4 QoS never matured				

Table 3. A comparison of IPv4 and IPv6 QoS mechanisms.

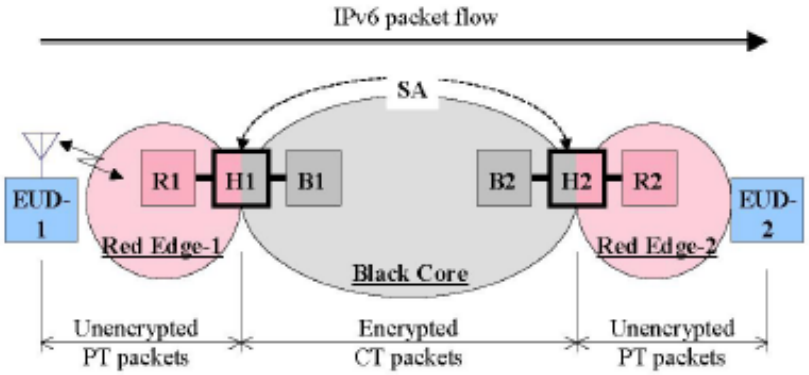
D. IPV6 QUALITY OF SERVICE IN THE GLOBAL INFORMATION GRID

The Department of Defense (DoD) Internet Protocol version 6 (IPv6) Transition Plan, Version 2 is the policy that directed the GIG to run IPv6 either is a dual-stacked mode or in a native environment by FY2008. During the planning and preparation phase, many networking issues were examined; one of these was providing QoS through the IPv6's inherent capabilities. Fineberg, in "IPv6 Features for Enhancing QoS in the GIG," (2005) proposes several

innovative uses of the IPv6 protocol to provide QoS in a unique environment such as the GIG. Fineberg (2005) also identifies “two QoS distinctions that exist between the GIG and commercial-world networks.” One is that the categories of the traffic class field in the IPv6 header are much broader and more diverse in the GIG. Commercial networks tend to have a known customer base and a known set of applications running on the network. The GIG must support a wide range of DoD organizations, the intelligence community, and any other organization using the GIG for national security interests. The range of users and applications is significantly higher than in the commercial world and, therefore, requires a greater traffic class classification system. Classifications such as Precedence and Preemption (P&P), Communities of Interest (CoI), and Quality of Protection (QoP) are included as QoS sub-classifications in the GIG and are labeled at the end user nodes. Additionally, Fineberg (2005) underscores the fact that IPv6 assigns addresses to interface vice nodes meaning that, from the application’s point of view, more than one address can be used as a source address. By assigning an address to a particular QoS sub-classification level, the application can “assign” the appropriate QoS level and inform the network of this assignment as the packet is routed to its destination. In the same manner, the destination address can indicate a different classification by the destination address it forwards the packet to as well (Fineberg, 2005).

The second issue is that traffic will likely have to cross encryption boundaries necessitating a unique solution to maintaining the intended level of QoS set in the originating node. As shown in Figure 6, traffic originating

from classified “red” networks that must travel through unclassified “black” networks must be encrypted. Since potentially damaging information could be obtained by analyzing the unencrypted protocol headers information, assurance procedures dictate that an assortment of QoS markings be stripped as the packets cross classification boundaries (Fineberg, 2005). As shown in Figure 6, the proposed solution creatively uses the IPv6 router extension header in addition to the proposed multiple interface.



EUD: end user device

R: router in the classified network

B: router in the unclassified network

PT: Plain Text packets

CT: Cypher Text packets

H: High Assurance Information Assurance Encryption (HAIPE) device

SA: Security Associations between HAIPE devices

Figure 6. Packet transition in the GIG (From Fineberg, 2005).

Using the interface corresponding to the proper QoS level, the end user will input the EUD2 destination address in an extension header, and will then input the R1 address corresponding to the same QoS level as the IPv6 header’s

source address. When the packet arrives at R1, the HAIPE device will read the destination address in the router extension header and will then insert this address in the header to become the new destination address. The HAIPE device will then encrypt the packet, forward it to B1 for transmission to the destination interface corresponding to the QoS level associated with it (Fineberg, 2005). The author’s proposal represents a creative application of IPv6’s capabilities to overcome a unique problem, ensure that information security is not violated, and provide an expanded level of QoS found in the GIG environment.

THIS PAGE INTENTIONALLY LEFT BLANK

III. TNT 09-2 IPV6 SENSOR NETWORKING STUDIES

A. TNT IPV6 SENSOR NETWORK FEASIBILITY EXPERIMENT

The Battlefield Medical IPv6 Sensor Network field experiment is a feasibility study that leverages both the architecture and successful discovery and constraints analysis step conducted during TNT 09-1 aboard Camp Roberts, California. This previous experiment combined new sensor and UAV networking solutions capable of supporting the battlefield medic in finding, identifying, and assisting casualties in the hostile area. The set of solutions included reading casualty e-tags (an electronic means of identifying an object, as well as the object's static and dynamic characteristics) from a very low-altitude UAV, communicating e-tag data to the remote medical data base, facilitating medication drop-off from a UAV, and improving the battlefield medic's situational awareness. The 09-1 experiment had two main objectives. The first was to explore the feasibility of integrating a biomedical microdevice, developed at the MIT Institute for Soldier Nanotechnology, into the TNT testbed; the second was to determine the feasibility of activating the device via a remotely located medic via the tactical GPRS network or via the UAV loitering above the casualty location. These two objectives were successfully accomplished by the NPS CENETIX-MIT ISN team.

The TNT 09-1 battlefield medical experiment was conducted in the IPv4 address space. The next logical step in the battlefield network sensor series is to show that the network will operate in the IPv6 address space. The main objective for the TNT 09-2 experiment was to place the

Battlefield Medical Network in a native IPv6 environment and show the feasibility of a tactical IPv6 sensor network. It is assumed that there will be no loss of previously-discovered IPv4 network capability in this new IPv6 configuration. Figure 7 depicts a TNT experiment in operation.

Figure 7. A view of the TOC at Camp Roberts (From Clement, 2008).

A scenario has been developed to encompass many different aspects of the battlefield medical experiment series in the anticipation of continued feasibility studies in future TNTs. A recommended TNT QoS experiment is discussed in Chapter VI.

B. RESEARCH QUESTION AND DISCUSSION

1. Question

It is feasible to operate a ground video sensor and a UAV video sensor over an IPv6 network in support of the battlefield medical scenario?

2. Discussion

This experiment was designed to demonstrate the following:

- The IPv6 protocol is mature enough to operate with a sensor network. The video feeds from both the ground and airborne camera were sent to the TOC via the IPv6 protocol.

- The dopplerVue network management system can support the network management requirements for IPv6. Performance values from the IPv6 laptop in the casualty site and from the server located in the UAV were gathered to determine the performance of the overall IPv6 sensor network. Wireshark, a network protocol analyzer, supported the demonstration by capturing packets for later analysis.

C. BATTLEFIELD SENSOR NETWORK EXPERIMENT SERIES SCENARIO

A six-man reconnaissance team has been inserted into a denied area for the purposes of surveillance and gathering intelligence on a target that is suspected to be in the area. A set of targets is suspected of planting IEDs in and among protected areas such as mosques, hospitals, and other

areas deemed neutral zones. The team needs to record the target’s actions both in wide-view for general situational awareness and close-up view for identification purposes, and then to transmit that imagery for real-time viewing. In addition to the real-time intelligence evaluation carried out by intelligence analysts in a separate location, a legal team in yet another location needs to validate the target’s actions as illegal before action can be taken against the target. The imagery from the two camera views, as well as still images from the digital camera, needs to be within certain parameters in order to constitute irrefutable proof of the target’s activities, and thus provide the basis for follow-on action. Likewise, the follow-on action needs to be documented in order to show that the appropriate actions were taken. Hence, video quality needs to be protected, as it streams through the network by use of QoS mechanisms in the IPv6 protocol.

The team has set up their video imaging systems and has ensured that the imagery is being received in the manner required. They have also received assurance that their battlesuits are communicating normally with each other and with the gateway to their higher headquarters. The team has received several reports indicating that the medical and environmental messages received show that everything is within normal parameters.

After a period of time, the target has appeared in the recon team’s area of observation. The video and still image cameras pick up the imagery and are transmitting as required; radio chatter with the intelligence and legal teams begins to increase as the activity level increases. The VHF nets are relaying through the gateway as well, using

the Radio-over-IP network (RIPRNET), which requires a QoS level to maintain an intelligible conversation. The battlesuits begin to relay signs of increasing stress as heart rates begin to quicken. Some of the heartrates exceed what is considered normal, which elevates the QoS level of the packets associated with those messages. Confirmation comes from the legal team that the activity carried out by the target does warrant appropriate action. The recon team leader then calls in air support to attack the target as it leaves the protected area. The attack must be video recorded, as well as narrated by the recon team, to provide proof that the protected area was not harmed. It is most critical at this point that the video and voice stream level of QoS do not suffer. At this point, a section of attack helicopters attack the fleeing targets, causing the video imagery to increase its needed bandwidth to capture rapid movement and changes. The narration is quicker, which again stresses the data and voice streams that are transmitting to the higher headquarters viewing the video and hearing the narration. At that moment, two battlesuits begin sending medical alarms. Two members of the recon team have been wounded in an ensuing small arms fight that has erupted in the vicinity of their position.

The recon team then returns fire on a previously hidden security team that was providing cover for the target’s IED activity. The battlefield medical collaboration team (BMCT) begins evaluating the alarms from the battlesuits, projecting possible outcomes based on the situation, and discussing possible medical courses of action that could be taken should they need to intervene. One item that the BMCT can work on is alerting the hospital staff to injuries that

they will have to treat when the team returns. This then allows the ER team to prepare, and to begin working faster. As this happens, the wounded team members radio back that they are “OK” for the time being and will extract with the team.

The recon team leader has successfully serviced the fleeing target with the section of attack helicopters and now asks for the helicopters to return and attack the enemy security team. The gunships do so, which allows the recon team to maneuver and assault the enemy position. At that point, the planted IED explodes and subsequently sets off other IED-making material that the enemy security team has with them. The IED explodes in the vicinity of a marketplace, causing a mass casualty situation; secondary explosions severely wound two more recon team members. The BMCT now has to go to work.

Following this event, voice messaging increases and video recording must continue; wounded team members also need medical attention that can be provided through their suits from the battlefield medical team. A UAV has just checked in on-station that needs to relay its video feed of the ensuing gunfight through the same gateway. In addition to these concerns, mission-critical video, audio, and messages with high precedence from the battlesuits must be delivered in the manner expected. Figure 8 depicts the operational topology.

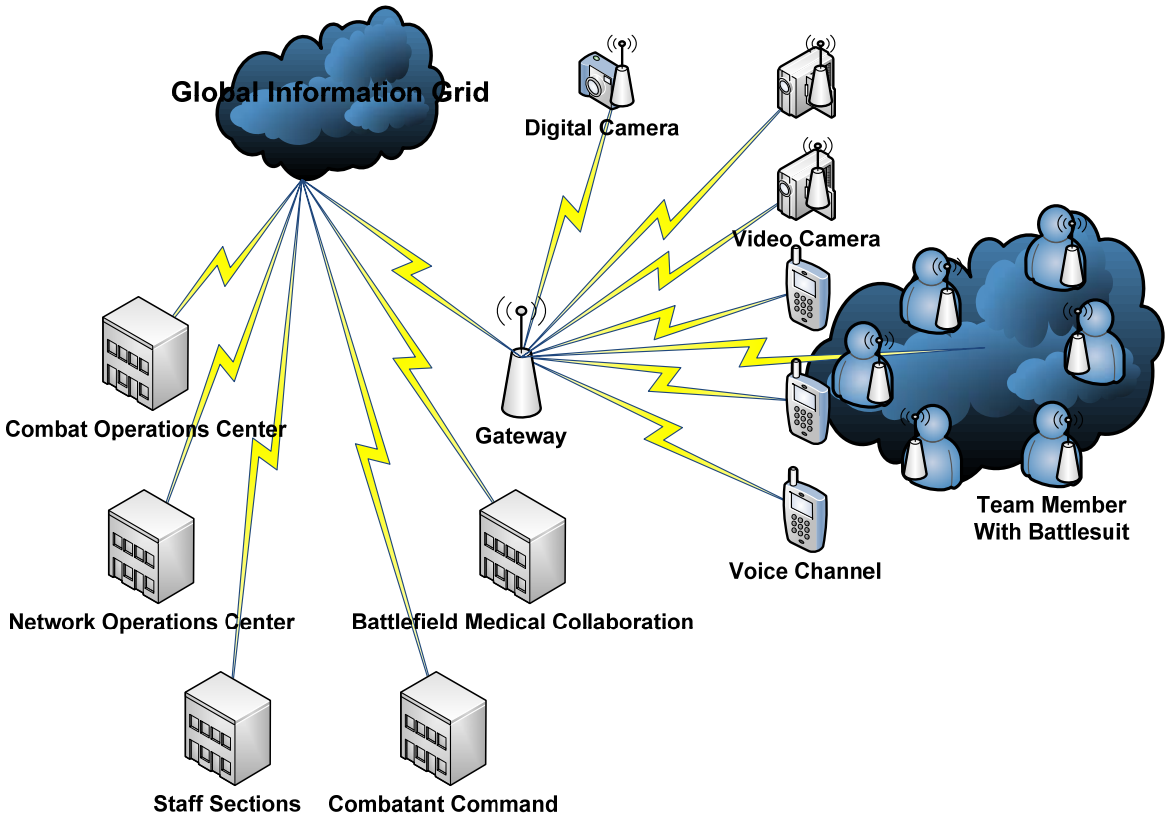


Figure 8. Operational Topology.

D. EXPERIMENT PREPARATION

Following several weeks of experimental design work and experimental topology development, actual preparation with the physical devices began ten days prior to the start of TNT 09-2. A building block approach was used to ensure that all experiment components would work together and that all those involved with the experiment understood each application and network device. Building the level of component understanding was important to ensuring that the experiment was conducted properly, that problems could be quickly resolved, and that the experiment results were

valid. The experimental topology shown in Figure 9 was broken into its basic parts for configuration testing and concept validation.

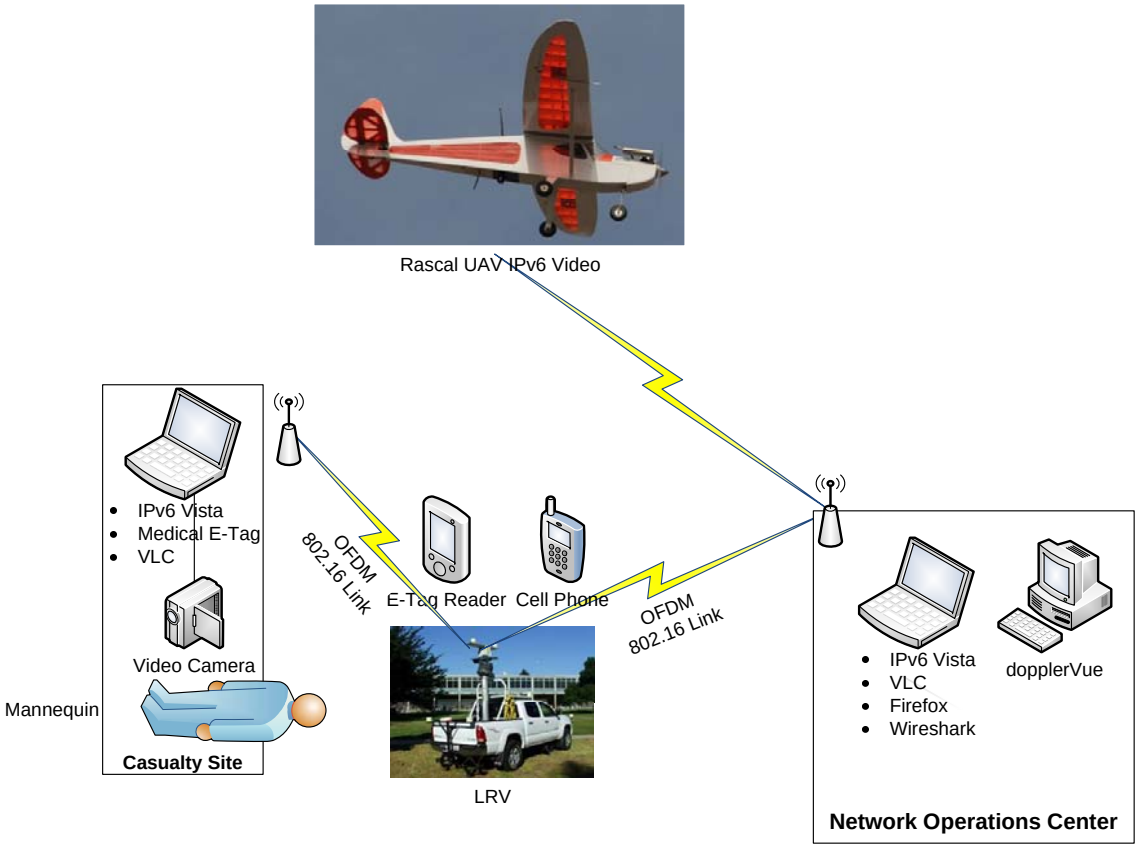


Figure 9. Experimental Topology.

1. Operating System, Video Camera, and Media Player Selection

Microsoft's Vista and XP operating systems (OS) were tested for use with the IPv6 protocol. XP with Service Pack 3 is reportedly IPv6 compatible, but IPv6 configuration tests with the OS were not intuitive. Vista is IPv6 compatible "right out of the box" and is very easy to configure for native IPv4 use, native IPv6 use, or a combination of the two. Pinnacle System's Dazzle was

originally selected for video camera use but it was discovered that the appropriate drivers did not exist for Vista. A Logitech camera was selected in Dazzle's place and was installed on one Vista laptop. A media player is needed to view streaming video across the network; VLC media player was recommended and installed on both laptops. A freeware application, VLC is capable of sending and receiving both unicast and multicast video over IPv4 and IPv6.

2. Proof of Video Streaming Concept

In order to ensure that the Logitech camera and VLC would work during the experiment, a small network was constructed. Both laptops were set to IPv4 as a baseline. The VLC application was opened on the laptop with the camera connected to it, and the video image was streamed to the second laptop. VLC was then opened on the second laptop, the stream was captured, and the video appeared on the second laptop's screen. Concept proofing continued with refining the streaming protocol, as well as the maximum packet size to be streamed. UDP was selected for video streaming since UDP is a "connectionless protocol" and would not consume bandwidth with additional overhead. It has been noted that video is very tolerant of a few dropped packets, whereas voice is not (Brosh, 2009). In fact, there was a noticeable lag between the video and audio during this phase of the benchtest. After a series of codec (coder decoder) tests, MPEG-2 was selected since it provided the best quality video and voice stream. Wireshark was used to capture packets and assist in refining the stream. Figure 10 depicts this process.

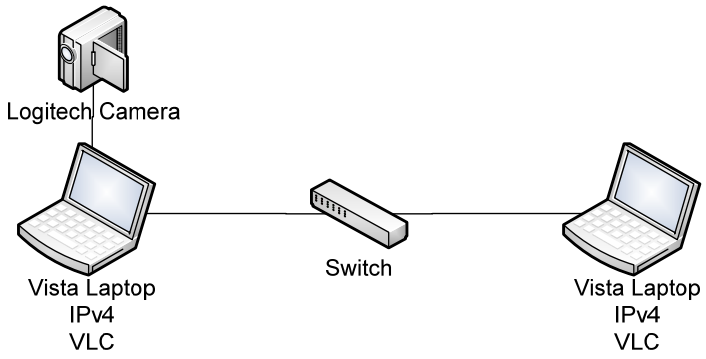


Figure 10. Video streaming proofing in IPv4.

3. IPv6 Networking

After the video proofing using IPv4, the two laptops were switched to a native IPv6 network by enabling IPv6 and disabling IPv4. Again, the video stream was transmitted from the first laptop, with the video camera, to the second laptop in the network. The IPv6 link-local address of the second laptop was used for streaming as before. Configuring took some time because it was necessary to input IPv6 address-specific syntaxes and then to ensure that the syntaxes were correct. Once configured, video streamed across the network in the same manner it did on the IPv4 network. Wireshark was again used to throttle the packet size and to watch the IPv6 stream.

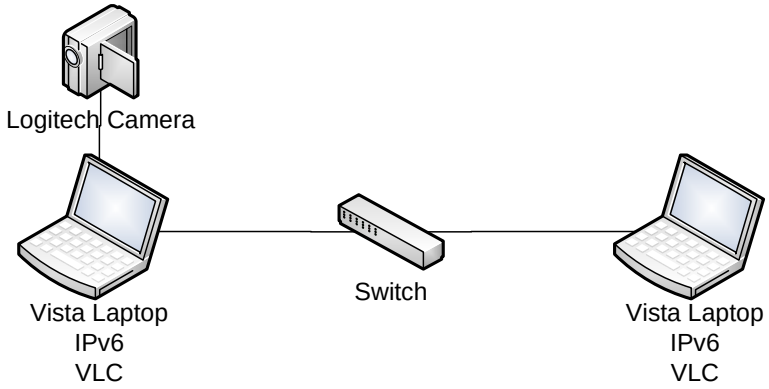


Figure 11. Video streaming proofing in IPv6.

4. Video Streaming Proofing over Wave Relay Radios

As shown in Figure 12, the next step was to ensure that the laptops and the video stream would work properly over the actual transmission system to be used during TNT. The first step was to connect the laptops to the radios and ping back and forth in order to ensure that there was a connection between the two. For this step, the network needed to be switched back to IPv4, since the radios had an IPv4 address. The radios could be reconfigured using a Web browser and the radio's IP address. During initial testing, it was determined that the radios were set to different data rates. Once adjusted, the laptops were able to ping back and forth. Video streaming was then tested in IPv4 and once it was working correctly, the network was switched back to IPv6 for another streaming test; IPv6 video streaming also worked. The results of this important test were an understanding of how the transmission link would work, how it could be troubleshot, and that IPv6 video streaming would work over the link as well.

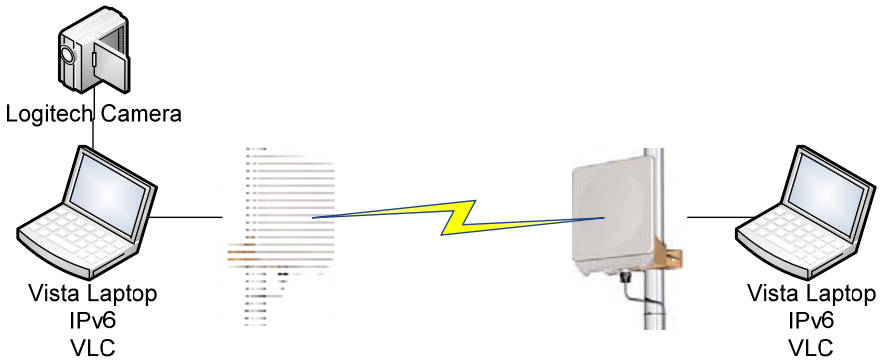


Figure 12. Video streaming proofing with Redline wave relay radios.

5. UAV Connectivity

The UAV segment represents the second segment of the experimental topology requiring validation. A Vista IPv6 laptop was connected into the Rascal control station van, which also had connectivity with the Rascal. During testing, Rascal was on the ground and cabled into the van. Connectivity between the laptop and Rascal was tested with the ICMP ping utility. Once connectivity was ensured, Rascal's IPv6 address, 2001:480:211:1100::164 was entered into the Firefox Web browser. This address is the location of Rascal's onboard Web server, where its aerial photographs are stored for viewing over the network. Connecting to Rascal and viewing the Web site indicated a successful test of the UAV segment.

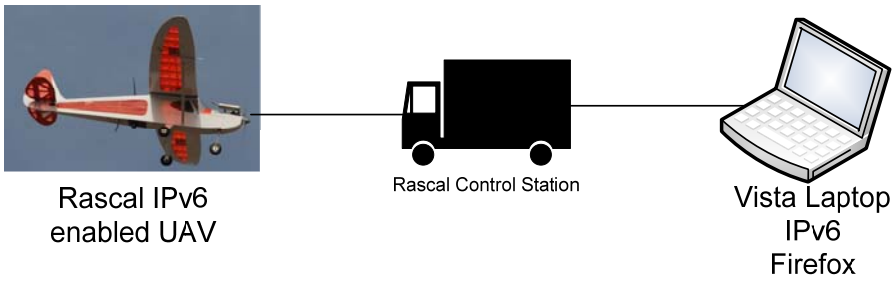


Figure 13. IPv6 connection testing with Rascal.

6. Network Management System (NMS) Test and Configuration

An NMS was put on-line as part of the IPv6 sensor network feasibility test since network management in the IPv6 address space is underdeveloped and challenged. While auto-configuration, a large address space, and the ability to autonomously move nodes cross-domain are benefits of the IPv6, they also challenge network managers. Having nodes that can join and leave networks with little to no human intervention is a new concept for most managers. However, having an NMS that is fully compatible with IPv6, as well as having a deep understanding how IPv6 works, is crucial for NMS tuning specifically, and for IPv6 network management generally. For instance, knowing that routers interact with IPv6 nodes as they join and leave the network is a key to knowing how to track the number and types of nodes on a network. NMSs that use the Simple Network Management Protocol (SNMP) can periodically send “get” requests from the NMS server to the SNMP agents in the routers for updates. Alternatively, the agents themselves can notify the server with network configuration changes. These are known as “traps.”

The most challenging aspect of this experiment was configuring and implementing the network management system. “dopplerVUE” was selected for this experiment’s NMS because it has a long history of success and, more importantly, because it is IPv6 compatible (Adame & Kong, 2008). As shown in Figure 14 the IPv6 laptops were reconnected to the switch along with a desktop running the Vista OS.

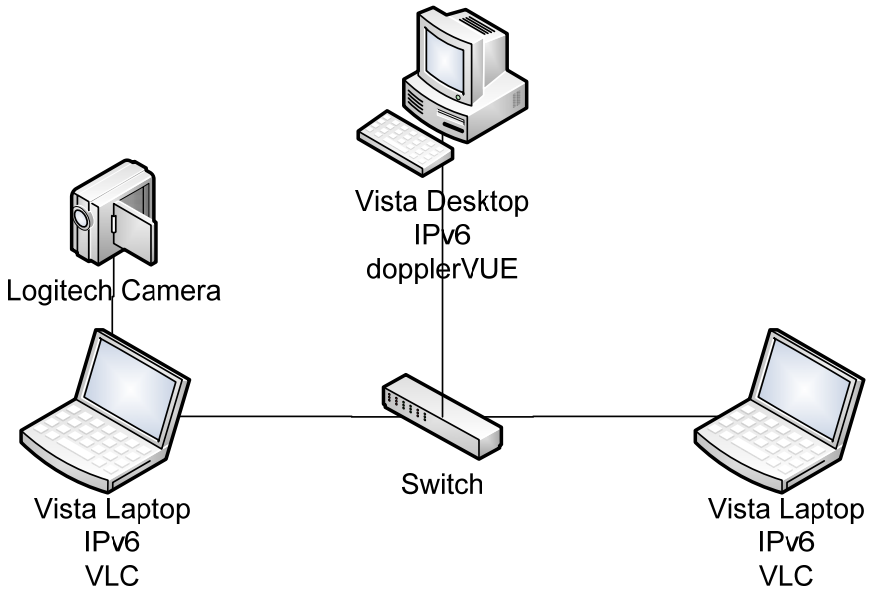


Figure 14. Network performance testing with dopplerVUE.

The original plan called for installing dopplerVUE on the NOC laptop, but after a trial of several days (and following several phone conversations with the service representative), it was determined that the laptop was not capable of running the NMS. Once installed on the desktop, however, dopplerVUE worked as advertised with a few exceptions. This experiment was not representative of a “true” network with an assortment of servers, routers, and many other nodes, and since the Vista OS was used, some

workarounds had to be introduced. This network does not have any routers for IPv6 address querying; consequently, the node's network addresses had to be manually entered into dopplerVUE's discovery process. Second, unrelated to dopplerVUE, the SNMP services on each of the Vista computers had to be restarted each time the node was restarted, and then reintroduced to dopplerVUE. Third, each time the NMS desktop was restarted, the network management and license services had to be restarted as well. Discovering the problems and solutions among dopplerVUE, IPv6, the Vista OS, and the small-scale network designed for the experiment were time-consuming, yet simple to resolve during network operation. While this experiment was not designed to test dopplerVUE in a large-scale network, it would be a very relevant feasibility study to conduct.

The purpose of incorporating dopplerVUE into the network was to measure the IPv6 sensor network's performance over the TNT network. dopplerVUE makes network management fairly transparent by using common performance MIBs as a default setting. It also offers the ability to customize the performance metrics for each node by providing a list of the available MIBs. The following SNMP Management Information Base variables (MIBs) were selected from RFC 4293, *Management Information Base for the Internet Protocol* (IP). (RFC 4293 is the current RFC addressing MIBs for networking use.) dopplerVUE contained these MIBs as well (Routhier, n.d.).

a. ipv6IfEffectiveMtu

DESCRIPTION: "The size of the largest IPv6 packet, which can be sent/received on the interface, specified in octets."

b. ipIfStatsInOctets

DESCRIPTION: "The total number of octets received in input IP datagrams, including those received in error. Octets from datagrams counted in ipIfStatsInReceives MUST be counted here. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ipIfStatsDiscontinuityTime."

c. ipv6InterfaceReasmMaxSize

DESCRIPTION: "The size of the largest IPv6 datagram that this entity can re-assemble from incoming IPv6 fragmented datagrams received on this interface."

d. ifOperStatus

DESCRIPTION: “The current operational state of the interface.”

e. ifOutOctets

DESCRIPTION: "The total number of octets transmitted out of the interface, including framing characters. Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of ifCounterDiscontinuityTime” (Routhier, n.d.).

The following Tables (4-6) are a summary of all the devices used, their associated characteristics, and their IP addresses. The IPv4 addresses are included, since they were used for the initial benchtests and connectivity tests over the TNT network.

Device	Location	OS	Applications	Camera	RAM	Speed
Sony Laptop	NOC	Vista Home Premium	1, 2, 3	Attached, not used	2 GB	2 GHz
Toshiba Laptop	Casualty Site	Vista Home Premium	3	Attached	1 GB	1.8 GHz
Dell Desktop	NOC	Vista Business	4	N/A		
Rascal UAV	Airborne over Casualty Site		5	Attached		
Switch	NOC	N/A	N/A	N/A	N/A	N/A

Notes:
1. Firefox
2. Wireshark
3. VLC
4. dopplerVUE
5. Web server

Table 4. Experiment Devices and their characteristics.

Device	IPv4 Address	IPv6 Address
Sony Laptop	192.168.78.48	2001:480:211:1100::1234
Toshiba Laptop	192.168.78.49	2001:480:211:1100::1235
Dell Desktop	192.168.78.50	2001:480:211:1100::1235
Rascal UAV	N/A	2001:480:211:1100::164

Table 5. Device IP addresses.

Application	Type	Version
dopplerVUE	Network Management System	N/A
Firefox	Web browser	3.0.6
VLC	Media Player	0.9.8a Grishenko
Wireshark	Network Protocol Analyzer	1.0.6

Table 6. Application Versions Used.

E. EXPERIMENT STEPS

Figure 15 shows an aerial view of the physical setup of the three nodes for the battlefield medical experiment. The LRV, mannequin, video camera, and one IPv6-enabled laptop were located at the casualty site. The second node, at the TOC, contained one IPv6 enabled laptop and one desktop on which the network management system application operated from. The third node was the Rascal UAV, which was airborne over the casualty site.

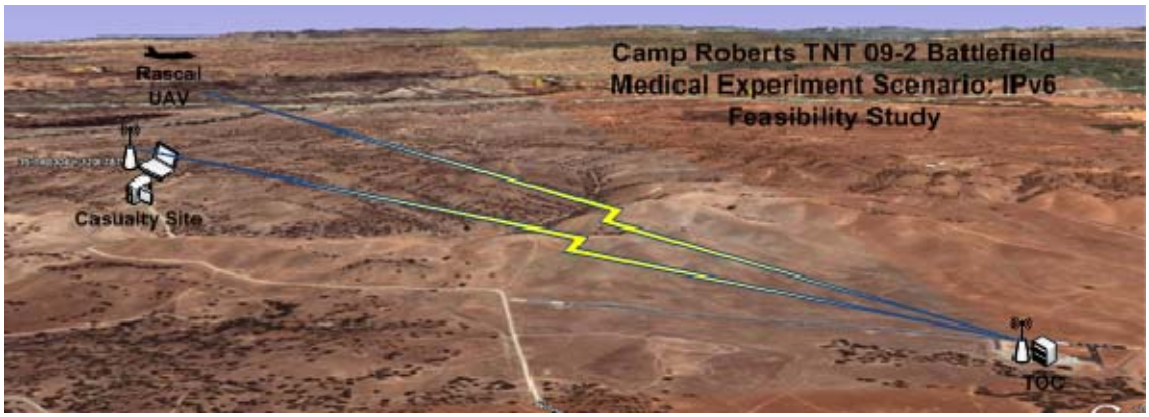


Figure 15. Aerial depiction of the TNT 09-2 Battlefield Medical Experiment.

The following steps were followed during the experiment:

1. Step 1: Movement

The LRV, along with other personnel and vehicles supporting this experiment, drove to the casualty site (35.740N, 120.787E) located in the vicinity of MacMillan Airfield aboard Camp Roberts, California and within direct line of sight of the airfield radio tower. Once the LRV was in place, its radio was connected to the TNT backbone at the TOC via the OFDM 802.16 link. The casualty site laptop was then cabled in to the LRV's switch, and subsequently connected to the TNT network using IPv6. Once connected, VLC was started and video was streamed using UDP over IPv6 to the TOC laptop. The TOC captured the stream via VLC and viewed the unidirectional voice and video projection from the casualty site.

2. Step 2: Site Setup

The casualty role-playing mannequin was positioned at the remote area and within view of the laptop mounted video camera. The e-tag reader was then positioned with the mannequin and was queried by the GPS device to determine its position. The e-tag health data was propagated further via the GPRS link to the medical database in the TOC. Successful e-tag reading was visually confirmed at the TOC on the NPS SA screen and by audible alert.

3. Step 3: System Activation

The B-TAC system (a system designed to assess and send alerts if certain health parameters are met) was activated. An alert was issued in response to the B-TAC assessment of the casualty health status. The video camera at the casualty

site continued to stream UDP over IPv6 video and audio recordings of the casualty's condition and surroundings.

4. Step 4: Rascal Overflight

The IPv6 enabled Rascal UAV flew to the casualty site to take aerial photos of the casualty and the surrounding area.

5. Step 5: UAV Imagery

The onboard high-resolution camera took digital photographs of casualty and delivered it to the TOC for viewing by the IPv6 laptop, using Firefox to access the file server.

6. Step 6: Drug Delivery Device Activation

The drug delivery device was activated from the TOC via Voice Portal interface over the medical commander's telephone located at the TOC. The drug delivery activation process was observed and recorded by the casualty site video camera, and then streamed back to the TOC.

Concurrent with the IPv6 sensor network experiment, dopplerVUE captured the IPv6 network performance metrics, while Wireshark captured the packets traversing the link to determine the type of traffic traversing the links.

F. CONDUCT OF THE EXPERIMENT

1. Casualty Site

The LRV was set into place at the casualty site in the vicinity of MacMillan Airfield and a radio link was established with the TOC. The casualty site IPv6 Vista laptop, with an attached video camera, was cabled into the

LRV and a connection was established with the IPv6 Vista laptop at the TOC. The connection was checked via an ICMP “ping” from the casualty site laptop to the TOC laptop, and again from the TOC laptop to the casualty site laptop. Upon confirmation of a good connection, VLC was opened on the casualty site laptop and video and audio were streamed to the TOC laptop’s IP address.

Concurrent with the laptop installation, the mannequin, shown in Figure 16 was placed on the deck at the casualty site and the associated GPRS equipment was switched on. The e-tag reader was then queried by the GPS device to determine its position; it transmitted that information back to the SA agent in the TOC. Following confirmation of the TOC receiving the mannequin’s position via the SA agent, an alert concerning the “patient’s” status was sent through the GPRS system to the TOC. The video camera was then positioned to observe the mannequin and its immediate surroundings.

Figure 16. Mannequin at the Casualty Site.

2. UAV–Rascal

The alert from the medical e-tag triggered an additional event. Using the position information relayed from the GPRS system, the Rascal UAV launched from the airfield and was directed to overfly the casualty site and take multiple pictures of the casualty, the casualty site, and the surrounding area. These pictures were stored in Rascal's onboard video server, which could then be accessed over the data link through a Web browser.

Figure 17. Rascal in flight (From Clement, 2008).

Figures 18 and 19 are images of the video captured by Rascal while overflying the casualty site. While the pictures are not as revealing as the streaming video, they provided an additional, non-repetitive view of the casualty site. They also provided different types of information to those who would need to see it such as the unit commander, medical personnel, or the intelligence section. It bears mentioning that the real world application of this IPv6

enabled video sensor is that the video can be accessed by anyone authorized to see it from anywhere in the world. The second point is that the IPv6 address can be set once and then published to all who need it. By not changing the address as it moves from network to network, sensor address management is made easier for the operators who rely on the feeds.

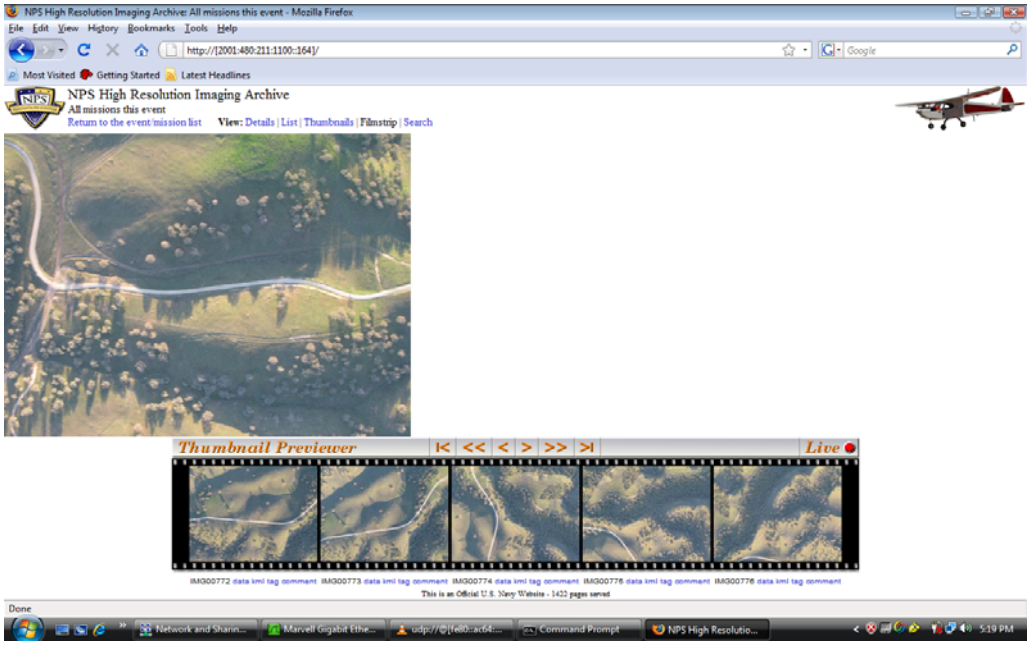


Figure 18. Screenshot of still images from the Rascal UAV during TNT 09-2.

Figure 19. Examples of 2-D and 3-D views of the images captured by Rascal (From Clement, 2008).

3. TOC

Figures 20 and 21 show the two nodes that were located in the TOC. The desktop ran the network management system, dopplerVUE, while the laptop displayed the streaming video feed from the casualty site, the video images from the Rascal UAV, and Wireshark, a packet capturing application. The two nodes were cabled into a switch, which was then cabled into the TNT network. Prior to the experiment, each node was put on-line and a series of ICMP pings was then sent to ensure connectivity with each other and through the network. Configurations, such as firewalls and the experiment's applications, were tested to ensure that each would work on the Camp Roberts TNT segment.

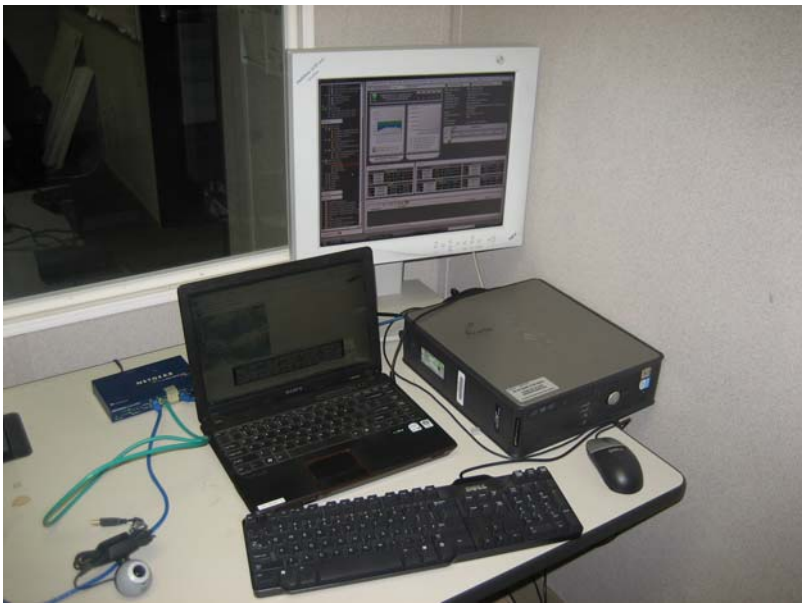


Figure 20. The TOC laptop and desktop.

Figure 21. Screenshot of dopplerVUE.

During the experiment, VLC was opened on the TOC laptop and the stream from the casualty site was captured for viewing. Similar to Rascal's "permanent" IPv6 address, each node's globally-assigned IPv6 addresses did not have to

change, regardless of which network they were on. Assuming that the addresses did not change for arbitrary reasons, the sender could be confident that the address he entered was the correct address for the duration. The Firefox Web browser was opened and Rascal's video server address, http://[2001:480:211:1100::164], was entered in anticipation of Rascal overflying the casualty site. Wireshark, as shown in Figure 22, was also opened and started in order to capture and view the packet stream.

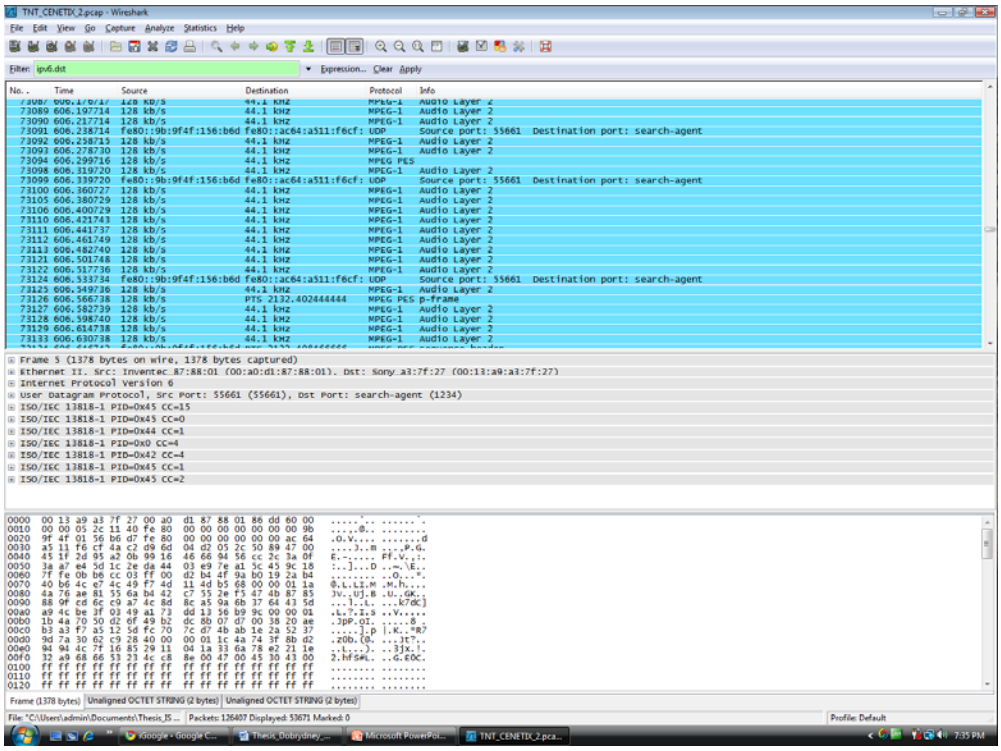


Figure 22. Screenshot of Wireshark.

Visual evidence showed that IPv6 packets were in fact streaming through the network to the TOC laptop. Wireshark also provided the MTU size and the application protocol that VLC was using. This information helped with QoS fine-tuning

at a later date. Unfortunately, Wireshark crashed at the end of the experiment and all of the captured packets were lost.

During this time, dopplerVUE was opened on the TOC desktop. As before, the network management and license services had to be restarted in order for dopplerVUE's license to operate properly. The discovery process was then enabled and the NMS began to search for all four of the IPv6 addresses, as shown in Table 6. Initially, the only two that were discovered were the two PCs in the NOC. The UAV and casualty site laptop were not yet on-line. The two discovered nodes were queried for the default networking and individual node information, which was soon displayed on several of dopplerVUE's many views. From a networking perspective the two nodes were reclassified as workstations and were displayed as such. "Drilling down" to each of the two workstations revealed CPU performance, interface information, and other metrics pertaining to overall performance. Each individual node's page was then reconfigured to show bits-per-second input and output on the active interfaces. This visual information demonstrated how the traffic was flowing across the network.

4. Casualty Site

While this activity was occurring in the TOC, the casualty site personnel travelled to the site and set up the LRV and other equipment for operation. Shortly after, the casualty site laptop came on line. This was indicated by dopperVUE canceling its alarm indicating a failure to connect by the ping poller, and showing connectivity to the distant laptop. This event was alternately confirmed by a cell phone call to the TOC. The NMS also began to show the

same network performance statistics as the other two workstations. When connectivity was confirmed by several ICMP pings back and forth, the VLC stream was captured from the sending casualty site laptop. dopplerVUE and Wireshark began to show signs of the video and audio packets streaming across the network. Wireshark showed a constant running stream but observers were not able to detect the subtle starts and stops as the traffic was received. dopplerVUE, on the other hand, showed the interfaces sending and receiving the packets in bursts, as traffic congestion across the network increased and as audio and video activity from the casualty site increased; these bursts appeared as spikes on the interface views. In other cases, when the network was less congested and when there was no change to the video picture the stream evened out and was flatter.

5. Rascal UAV

As part of the battlefield medical scenario, the Rascal UAV was launched in response to the medical tag alert. The link to Rascal was established shortly after becoming airborne. dopplerVUE established connectivity to the new node it discovered as part of its default discovery process, but the NMS was unable to pull SNMP data from the UAV. After confirmation of connectivity to the Rascal, the Firefox Web browser was opened and video images were received in the TOC. The images were aerial pictures taken of the casualty site, as shown in Figure 17. In a manner similar to that of the streaming video from the casualty site, the video images were transmitted through the network in bursts. This was to be expected since the UAV was sending still video images and not streaming video.

G. EXPERIMENT CONCLUSIONS

The primary question for this experiment was whether or not operating a ground video sensor and a UAV video sensor over an IPv6 network in support of the battlefield medical scenario was feasible.

1. Performance Non-degradation

There was no noticeable performance degradation between the IPv4 and IPv6. An important reason for using IPv6 in sensor networks is to ensure that there is no loss of performance in comparison to the performance provided with the older IPv4 protocol. Even a 5% loss of performance could be considered unacceptable, if that 5% means the difference between mission success and mission failure.

During the testing and experimental phases, IPv4 was used at the beginning of each step in order to isolate any problems to the application or the device undergoing usability and configuration testing. Segregating the two layer three protocols from the applications meant that only one change variable was being tested at a time. When the application was configured properly and shown to work, the layer three protocol was then shifted to IPv6 to determine if the application under consideration would work under the new network conditions. In all cases, each application showed no noticeable signs of performance degradation or any indications that IPv6 would lead to an application error. This is as it should be, since the TCP and UDP/IP stack is modularly designed so that changes to one or more layers should not affect any other layer.

2. IPv6 Address Space

The IPv6 address space is ideal for tactical sensor networks. The vast IPv6 address space means that the number of globally assigned addresses is almost limitless. The benefit of the address space size means that device interfaces can be assigned one or more unique global IPv6 addresses and those addresses will stay with that device, regardless of the network it joins or where in the world it is. For the purposes of this TNT experiment, the requested IPv6 addresses were consistent throughout the testing and experimental phases. The IPv6 addresses were assigned to the interfaces, configured, and tested in the CENETIX lab at NPS in Monterey. The address's first 64 bytes, 2001:480:211:1100, is used by TNT. The second 64 bytes were limited to shorter, more manageable numbers such as ::1234 and ::164, since globally-routable addresses were not needed and the closed network provided the opportunity for simplification. In practice, the MAC address would have been used. Assigning the IP address just one time means that the devices' address(es) can be published in a database for easy access and the devices will not have to be continually readdressed as is often the case with IPv4 networks. However, for this assignment to function properly, "Mobile IPv6" must be employed. Mobile IPv6 allows a device to cross networks and maintain both a seamless connection and its IP address, similar to the way cellular phones work (Hagen, 2006). These same devices were then put on line at Camp Roberts during the experiment phase and successfully joined the network using the previously-configured IPv6 addresses. The same concept applies to IPv4 but in fact, the IPv4 addresses had to be changed mid-way through the testing and

experimental phases since X.X.99.X is used at NPS and X.X.98.X at Camp Roberts, which necessitated a configuration change prior to joining the TNT network at Camp Roberts.

3. Autoconfiguration

Autoconfiguration is ideal for sensor networks with a large number of IP addressed nodes that autonomously enter and exit the sensor network. When an IPv4 device joins a network, it will either need to be assigned a new static IPv4 address from a pool of limited addresses by a network administrator, or a Dynamic Host Configuration Protocol (DHCP) server will lease the device a dynamic address for a specified period of time. When that time has expired, the node will need to request a new address. If the node goes off line, then the address is released for reassignment. Dynamic addressing is beneficial because the only human intervention required is to administer the DHCP server. IP addresses can also be used more efficiently. Not all network devices are on-line all of the time, so dynamic addressing reuses a limited number of IP addresses to serve a larger number of nodes. In both the static and dynamic address assignment cases, the device will have at least one, and possibly many, different network addresses *for every new network it joins.* Assuming the new devices are accessible from outside the network, the new static addresses must be made known to all who might need access to them. This process can be cumbersome and consume resources that could be dedicated to higher priority tasks. In practice, devices requiring access are not assigned static IP addresses, so attempts to publish updated dynamic IP addresses are improbable. IPv6 autoconfiguration eliminates the cumbersome

task of statically assigning IP addresses, as well as eliminating the need for a DHCP server (although DHCPv6 exists to provide network administrators with tighter control of their network). Once a device has joined the IPv6 network, routers can be queried at regular intervals to alert users to the presence or absence of a new device, or routers can be assigned a “trap” to alert users each time a device enters or leaves the network, at the moment it happens.

As explained previously, IPv6 addresses can be permanently assigned to a device and can, in theory, remain assigned to the device for the duration of its service life. Since each IPv6 device interface can be initially configured with its address, it will not require a new address as it moves from network to network. Human intervention, after the initial address assignment, is no longer required. Stateful DHCP servers will no longer be required to dynamically assign addresses, and network administrators can spend their time on other tasks. The disadvantage to assigning a unique, static IPv6 address to a device is that Mobile IPv6 will need to be employed to allow that device to communicate using its IP address on a different network. This adds a layer of complexity to the tactical network and so it may not always be advantageous to use this functionality. A balance must be struck between the level of network complexity desired and the advantages of maintaining a single IP address assigned to a device. For example, an aircraft designed for Strategic Intelligence, Surveillance, and Reconnaissance (ISR) missions would benefit from statically-assigned IP addresses, since it would have its own access to the GIG and would not rely on other networks

for Mobile IPv6 functionality based on its mission profile. Conversely, a UAV would be a more appropriate use of dynamic IP addresses, since it would rely on tactical networks that are better suited to local, autonomous network administration via autoconfiguration, rather than reliance on Mobile IPv6.

During the TNT 09-2 experiment, autoconfiguration was not demonstrated but an experience during the experiment highlighted its usefulness. While at Camp Roberts, the static IPv4 addresses that were assigned to this experiment for connection testing were double-assigned and IP conflicts occurred as a result. Since no address can be assigned to more than one device, the TNT network administrator needed to assign another set of static IPv4 addresses to this experiment's laptops. This took time, since he was busy with other, more pressing tasks and it must be noted that in a real-world situation the network administrator and the sensor network operator would not be located in the same room for IP address deconfliction. If autoconfiguration were available each device, would be able to transparently join and exit the network with its own globally-unique IP address without the need for humans to enter the configuration loop. The network administrator would not need to assign addresses, nor would he have to track down IP address "grabbers," or people who arbitrarily "grab" IP addresses without prior coordination or permission. To prevent IP conflicts, the near-term solution for TNT experiments will involve a DHCP server for dynamically assigning IPv4 addresses. A recommended longer-term solution would involve shifting the entire network to native IPv6.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SERVICE LEVEL AGREEMENT TAXONOMY AND OPERATIONS IN SUPPORT OF THE IPV6 SENSOR NETWORK

A. IPV6 APPLICATION TO TACTICAL NETWORKS

1. Identified Need for IPv6 QoS Mechanisms in the Department of Defense Global Information Grid (GIG)

The GIG, depicted in Figure 23

> shall support all DoD missions with information technology, …[such as] national security systems, joint operations, joint task force (JTF), and/or combined-task force commands, that offers the most effective, efficient, and assured information handling capabilities available, consistent with national military strategy, operational requirements, and best-value enterprise-level business practices. (DoD, 2002)

The Joint Task Force Global Network Operations (JTF-GNO), a subordinate command of the United States Strategic Command (USSTRATCOM), operates and maintains the GIG for worldwide support of DoD, intelligence, and national security operations.

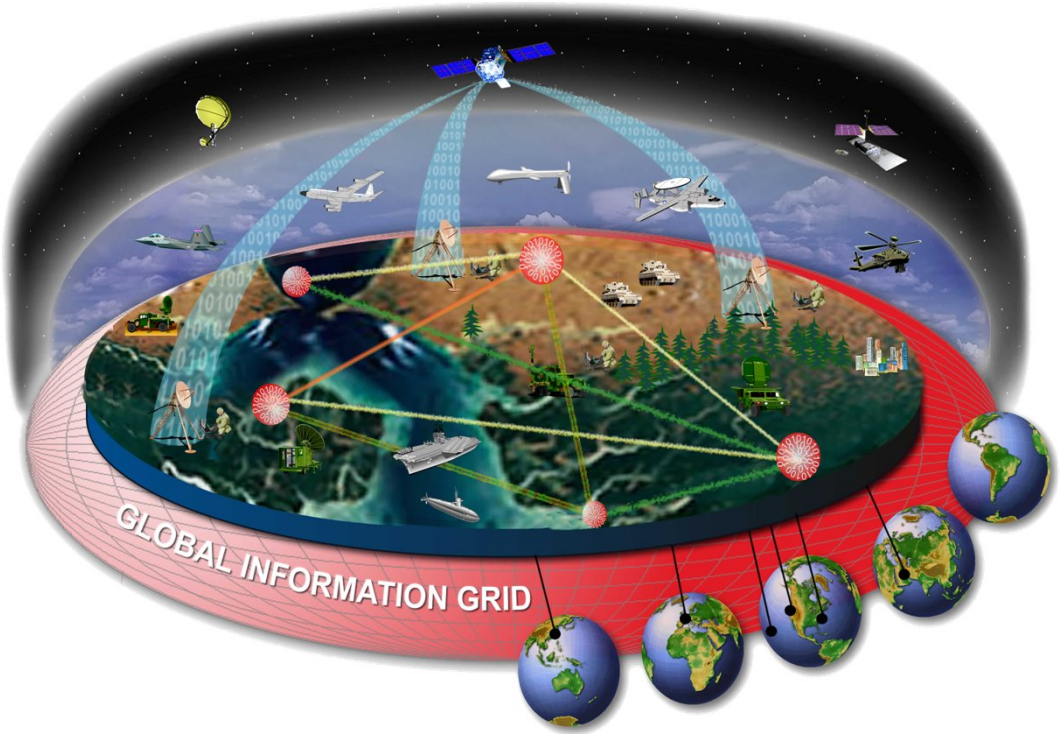


Figure 23. The GIG (From JTF-GNO, 2009).

In a memorandum published in 2003, the DOD Chief Information Officer, John P. Stenbit, cited the following reasons for directing that the GIG be transitioned from native IPv4 to native IPv6:

> IPv6 is the next generation network layer protocol of the Internet as well as the GIG, including current networks such as NIPRNET, SIPRNET, JWICS, as well as emerging DoD space and tactical communications. Implementation of IPv6 is necessary due to fundamental limitations in the current IPv4 protocol that renders IPv4 incapable of meeting long-term requirements of the commercial community and DoD. IPv6 is designed to overcome those limitations by expanding available IP address space to accommodate the worldwide explosion in Internet usage, improving end-to-end security, facilitating mobile communications, providing new enhancements to quality of service, and easing system management burdens. Furthermore, IPv6 is

> designed to run well on the most current high performance networks (e.g. Gigabit Ethernet, OC-12, ATM, etc.) and without experiencing a significant decrease in capacity on low bandwidth systems. (Office of the ASD/DoD CIO, 2007)

While the CIO acknowledges the complexities of completely transitioning a network the size of the GIG from one layer three protocol to another, he reiterates the DoD's position that the transition is necessary in order to provide a network capable of supporting network-centric operations and warfare. In other words, IPv4 is obsolete and IPv6 is the way ahead.

2. Battlespace Awareness and Knowledge

According to Akyildiz et al. (2002) in "A Survey of Sensor Networks," a sensor network is

> composed of a large number of sensor nodes that are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or predetermined. This allows random deployment in inaccessible terrain or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities.

The author continues by clarifying that tactical sensor networks exist as both deliberate networks and ad-hoc networks:

- The number of sensor nodes in a sensor network can be several magnitudes of order higher than the nodes in an ad-hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failure.

- The topology of a sensor network changes very frequently.
- Sensor nodes mainly use a broadcast communication paradigm, whereas most ad-hoc networks are based on point-to-point communications.
- Sensor nodes are limited in power, computational capabilities, and memory. (Akyildiz et al., 2002)

Sensor networks, as shown in Figure 24, give the commander and his staff increased battlespace awareness in order to provide a basis for battlespace knowledge and to ultimately increase the overall operational tempo (Alberts, Gartska, & Stein 1999).

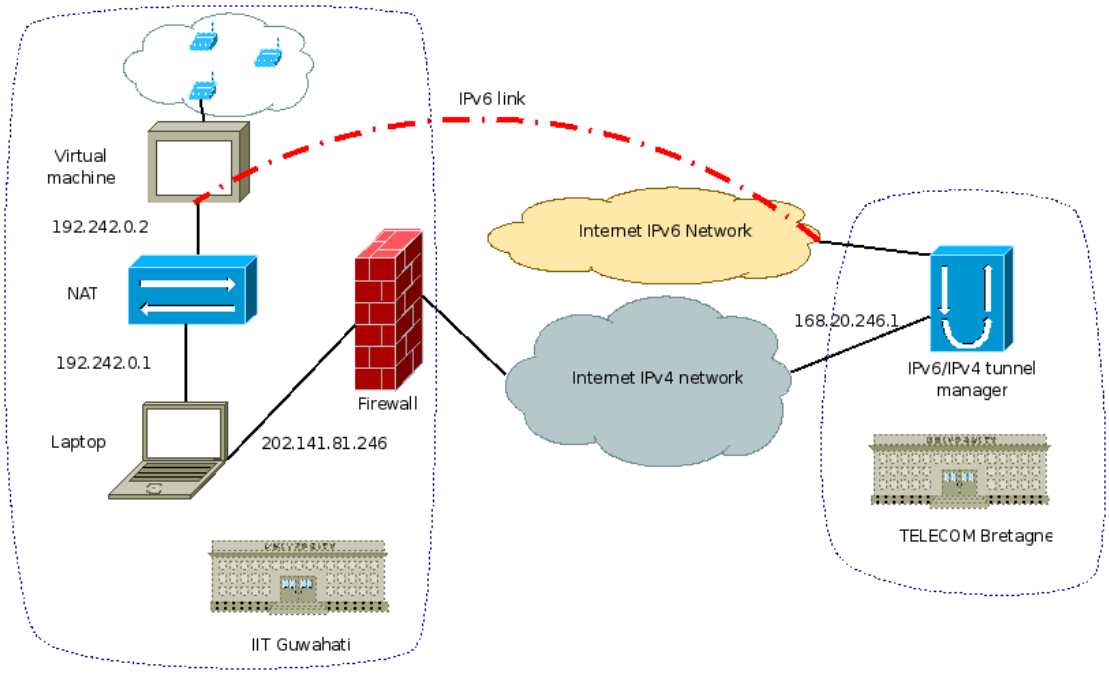


Figure 24. IPv6 Sensor Network (From VieSurIP, n.d.).

Digressing from the large-scale system point of view, the sensor networks are composed of several subsystems. As shown in Figure 25, the sensor nodes themselves, regardless of their intended purpose, have some basic physical

components common to all: a sensing unit, a transceiver radio, an energy source, a processor, software to include networking protocols, and some small memory capacity (Dohler, 2007). The sensor node's mission purpose dictates the type of sensing unit employed, which then determines the makeup of the other sensor components. Each sensor node can, therefore, be viewed in terms of "processing capability, memory, number of network interfaces, and each network interface's performance characteristics" (Clement, 2006).

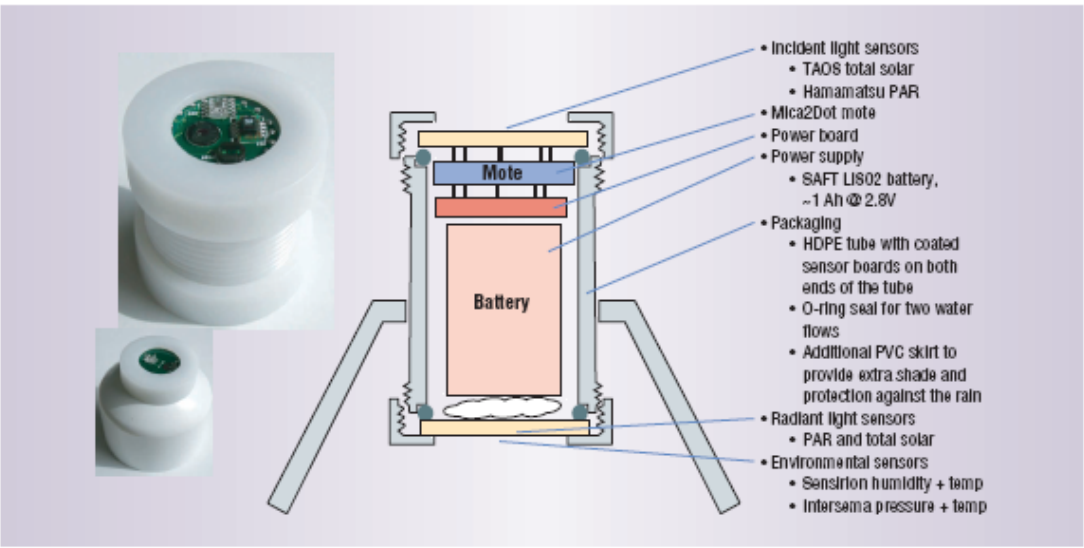


Figure 25. Example of an environmental sensor (From Culler, Estrin, & Srivistava, 2009).

Each of these sensor nodes is networked with surrounding sensor nodes to form paths back to a gateway, through which each sensor's information is transmitted back to the destination command and control node. Paths on the physical network where each node is considered both a sensor and a router are determined using routing protocols, which then determine logical routes. The routing tables are then updated based on the protocol's standards (Wilson et al.,

2005). As stated in “Sensor Network QoS in an IPv6 Environment”, sensor networks are dynamic systems subject to constant change of state (Dobrydney, 2008). Routes, variable bandwidth allocation, availability, jitter, complete loss of links, power loss, higher bit error rates (BER), and nodes joining and leaving the network in an almost random fashion, are some of the constantly-changing elements in a large-scale network. Each of the aforementioned attributes can be used to provide network performance measurement parameters and, therefore, can provide feedback for network adaptation.

3. Understanding the Battlespace

Data collected from each sensor in the network are considered to be explicit facts, which are then fused together to provide battlespace awareness. As shown in Figure 26, battlespace awareness is a compilation of three elements: the friendly situation, the enemy situation, and the environment. The friendly situation is determined by sensors, which are carried by friendly forces, and which in turn inform the network and provide updated data for the COP and human operators who need it.

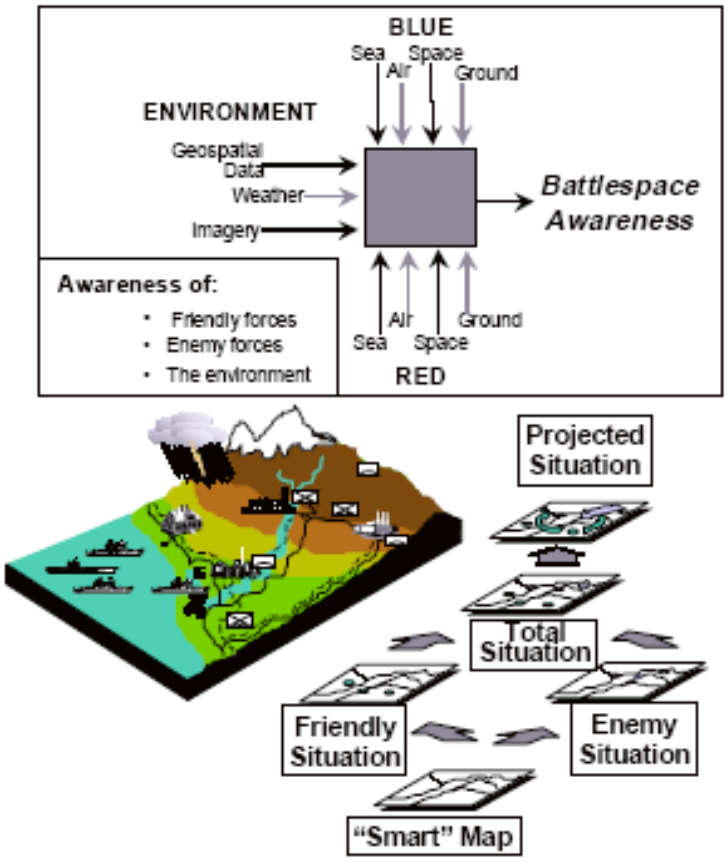


Figure 26. Elements of Battlespace Awareness (From Alberts et al., 1999).

Likewise, the environmental situation is updated by means of mission specific sensors, which aid in understanding the current and predicted weather situation. Finally, the enemy situation is updated by sensors placed in the battlespace in a manner that allows them to collect specific information. The information fused from the battlefield sensors forms the COP as shown in Figure 27 and provides all who view this information with the battlespace awareness needed to plan and execute missions. From the COP, several elements of information can be derived to describe the current and projected situation:

- Location (current positions, rate of movement, and predicted future locations)
- Status (readiness postures including combat capability, enemy contact, logistics posture)
- Available courses of action (COA) and predicted enemy COA's (offensive and defensive weapons and sensor capabilities and damage assessment)
- Environment (includes current and predicted weather conditions, the predicted effect of weather on planned operations and enemy options, and terrain features such as trafficability, canopy, lines of sight, and sea conditions). (Alberts et al., 1999)

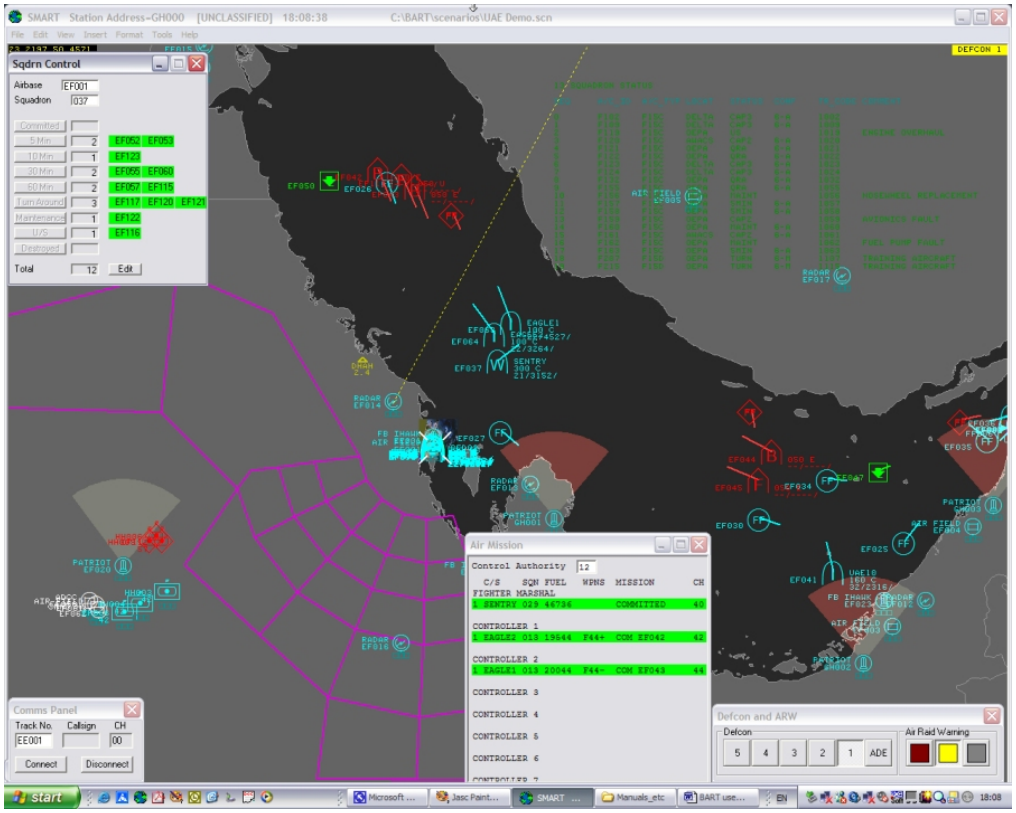


Figure 27. Example Common Operating Picture (From Intaero, 2009).

More importantly, however, the COP provides input for battlespace knowledge. Whereas battlespace awareness is

derived from explicit facts, battlespace knowledge is derived from tacit information gleaned from the COP and from the experience of those who view this information. In contrast to battlespace awareness, which answers the question “what happened?”, battlespace knowledge gives the commander and his staff an understanding of “why did/is this happening?” (Alberts et al., 1999). When this understanding is more solid, faster decisions can be made.

4. IPv6 Enabled Sensor Networks—Supporting the Commander’s Information Needs

Previous sections and the summary contained in Table 1 have described the benefits of using the IPv6 network protocol in comparison with the IPv4. The fact that IPv6 sensor networks provide global addresses for virtually every networking device, inherent QoS and security, as well as the ability to join and delete nodes transparently without the need for human involvement or excessive networking equipment, gives these sensor networks significant advantages when compared to the limits IPv4 imposes on sensor networks. An IPv6 sensor network gives the rifle company commander, introduced at the beginning of the chapter, the tools to derive an information-and time-competitive advantage over his adversary. QoS provides the commander and his staff an information-providing guarantee to obtain the requested real-time information from the sensor network to make time critical decisions. Sensor placement will no longer be limited by the allotted number of unique IP addresses; constrained only by the quantity on hand and delivery methods, sensors can be placed anywhere they are needed and can each be accessed by anyone

supporting the mission. A CONUS-based UAV squadron operating in support of the company commander's mission overseas can quickly access emplaced sensors to determine local weather as it affects UAV flight and mission supportability. Personnel can monitor their health and their unit's health levels and can even remotely administer drugs through IP enabled sensor battlesuits. Sensors placed on roads can help determine traffic patterns in an area of operations, as it affects logistical support, indigenous population movement, and enemy movement. Information provided by these roadside sensors can be of great interest to different organizations for different reasons. An IPv6-enabled sensor network allows each organization in the intended audiences to pull this information for its own purposes autonomously, without concern for continually-changing network configuration. Autoconfiguration streamlines the sensor network joining process so that sensors can join without needing human intervention. Inherent security features, such as IPSec, ensure that not only are end-to-end transmissions not being read by unauthorized personnel, but that network encryption concerns are simplified from the communications personnel's point of view. IPSec key management is administered through the public key distribution, whereas intervening networking devices currently require encryption devices that require manual rekeying.

The COP and the information derived from it are only as good as the information provided to it, which highlights the second key element of the opening scenario. Service Level Agreements and the associated need for QoS in a sensor network are requirements for ensuring that the commander gets the information he needs in the manner he needs it. One

potential drawback of a large address space, given a finite amount of bandwidth, is the fact that a large number of network devices have the potential to consume network resources to the point that critical information will not reach the intended audience in the time and the manner needed. Put another way, if everyone is trying to answer their critical information requirements to the best extent possible, no one will be able to fully answer their critical information requirements. Commanders and their staffs need key pieces of information at key times in order to capitalize on fleeting opportunities. During the planning process, critical information requirements are determined and a plan is then developed to place collections resources against those information needs; this enhances the decision-making process and allows commanders to achieve superior and timely action relative to the adversary. SLAs are used to put in place temporary control mechanisms, which provide a level of guarantee that the information collected from a set of sensors will reach its destination in the time and manner requested. IPv6 QoS mechanisms and the DiffServ technique of providing QoS in a DiffServ network provide the means to implement tactical sensor network SLAs.

B. TACTICAL SERVICE LEVEL AGREEMENTS

1. Significance to the Warfighter

The brief scenario presented at this beginning of this thesis describes a company commander conducting deliberate planning in order to accomplish his assigned mission. As part of his planning efforts, he determined that he had many information requirements about his particular mission that

he could not readily answer. These “gaps” in his knowledge of his area of operations (AO) include enemy strengh and disposition, the impact of weather on his mobility, battlefield visibility, the enemy’s ability to reinforce, the current composition and disposition of fire support positions, and locations of known non-combatants. While the battalion’s intelligence section can provide many of these answers, it is the company commander’s prerogative to have as clear and up-to-date a picture as he needs, in order to successfully complete his mission within the Battalion Commander’s intent. As part of the Marine Corps Planning Process (MCPP), the commander and his staff determine the information requirements that need answering in order to tip the scales toward mission success. Those information requirements deemed critical to the unit’s success are called the commander’s critical information requirements (CCIRs). They are also known as the commander’s “wake-up criteria.” If information is obtained that answers or partially answers a CCIR, then the commander must be notified—even if he is sound asleep.

As an illustration of a tactical-level SLA development proposal and a new and expanded role for the Information Management Officer (IMO), consider this scenario. The company commander submits information requirements and CCIRs as a request to the Intelligence Officer (S2) and the Battalion IMO. As part of his request, he asks for real-time or near real-time information pull within his company’s AO during both the company’s planning and execution phase. Consolidating all of the battalion’s information requirements, the IMO determines what sensor capabilities exist in the battalion’s AO and how those capabilities could

answer the battalion’s information requirements. The IMO will then build and submit an SLA request based on this analysis. Assuming that the SLA, or some modification thereof, is approved, the company commander and the other staff personnel can then be assured (within the realities of the friction of war) that the network will provide him with the means to satisfy, or help satisfy, his information requirements. It must be carefully noted that network SLAs by themselves will not provide the answers to his questions or provide him with the situational awareness he needs. The SLAs will only ensure that the network will provide the resources necessary to deliver the information he requested. It is up to the judgment and expertise of both commanders and staff alike to properly map the information requirements to the proper information-providing capability and to ensure that the proper assets are in the proper place. This process is shown in Figure 28.

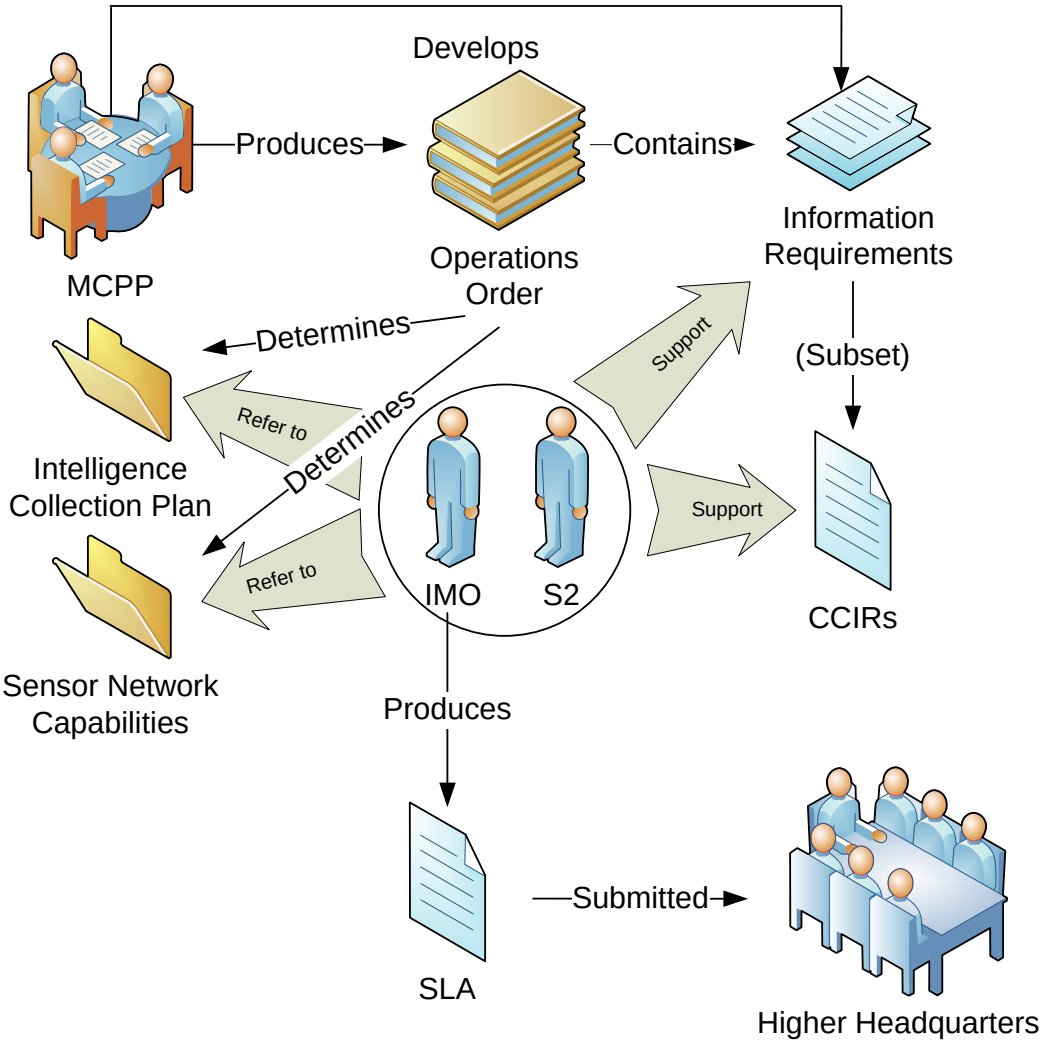


Figure 28. SLA Development Process Model.

2. SLA Defined

In the commercial world, service level agreements are commonly defined as:

> a contract between a network service provider and a customer that describes specific, measurable services to be performed, the quality level of those services, and the time duration those services will be made available to the customer. (Marilly et al., 2009)

The contract will also routinely specify penalties for non-compliance in the hope that damage can be mitigated by collecting on those penalties. The ability to consistently fulfill the terms of an SLA contract and to provide the desired QoS level(s) is what separates one network service provider from another. The following requirements have been identified as the three which are most important to consumers of SLAs:

- Reliable measurement of the QoS
- Provisions of the expected QoS
- Optimization of the resource usage (Marilly, 2009)

A well-defined SLA must contain easily measurable metrics in order to allow both the customer and service provider to monitor the effectiveness of the SLA and to permit the network to properly manage itself in order to maintain the expected QoS levels as defined in the SLA. “Metrics” will have different meanings to different people. Information users will use metrics to define what they want to see, while network operators will translate the user’s metrics into measurable networking terms. The user will not need to understand how the network measures its effectiveness, he will simply know if the SLA is effective by determining if his metrics have been met.

An SLA, for the purposes of a tactical sensor network, is defined as a single non-legally binding “contract” between the Commander of the network service provider (Communications Section, G/S-6) and the headquarters of the service requester. It promises to provide a specified level of guaranteed service through measurable performance

criteria, or services, through the network from the sensor source, to the requesting unit’s specified end-user, and back again, if required. The term “non-legally binding” is used in contrast to the previously-described commercial SLA definition, in which a legally binding contract is agreed upon between a user and a provider in exchange for money or some other form of compensation. A breach of contract can result in a lawsuit or some other type of settlement which compensates for losses. In the military sense, a “contract” is replaced by a formal order and is thus an extension of a commander’s legal authority. It can also take on the form of a trust relationship between non-related units or entities in unconventional situations. Forms of compensation are irrelevant in the former case and may be completely necessary in the latter depending on the relationship and the anticipated outcomes of the services provided by the SLA. A “breach of contract” takes on a different connotation in a tactical network as well. Networks in austere combat locations such as the desert or the mountains are extremely difficult to operate, manage, and maintain, due to the additional challenges imposed by the environment and the opposing side’s will. Providing network connectivity between distributed command-and-control nodes, ensuring consistent power availability, and providing basic life necessities for human network operators at nodes which require human intervention must still occur, regardless of the difficulty, lack of logistical resources, or amount of time required. Command-and-control nodes are considered high-value targets and thus may be under constant attack, whether by kinetic or non-kinetic means, with the intention of undermining network effectiveness.

Perhaps the most important aspect of tactical SLAs is that they are explicitly defined in measurable terms which can be compared to stated performance criteria. While the same argument can be made for SLA applications in the commercial world, SLAs for tactical use are designed to support specific operations and are either event-driven or time-driven, based on some actionable information or on a commander's judgment. Opportunities in combat are fleeting and rarely present themselves more than once. Commanders in need of specific real-time information for planning and/or executing operations count on the availability of that information as part of their risk-management process when they decide where and when to wage battle. An SLA must be designed to capture the mind's eye view of the commander and what he expects to see when viewing that information feed; at the same time, it is important to realize that there are limitations on the network. Quite often, those mind's eye views are qualitative in nature, since most people know what they want to see when they see it, but may not be able to quantify those same expectations. Thus, expectations management is critical at this point. During this process, exact metrics and a range of those metrics must be determined in order to meet the commander's expectations, while balancing those same expectations within the bounds of the network's performance. Understanding the different perspectives that different role players have on SLAs is important. The commander has a preconceived notion of what he is looking for, which forms the basis of his expectations and perspective for what he should see. The IMO has a perspective and a notion of what he should see, based on the information requirements inputs he has received and the SLA

request he builds, forwards, and tracks. The network-operating center has another SLA perspective, based on whether or not the quantitative network performance requirements are being met. Regardless of whether or not the network supported the SLA performance criteria, if the commander does not believe that his qualitative expectations were met, in his view the SLA failed to support his operation. For this reason, a SLA tactical network sensor taxonomy will be proposed in the latter part of this chapter to provide structure for mapping the network support of the operational commander's information requirements; this will in turn provide his operational missions with measureable network SLA performance criteria. To develop that taxonomy, several SLAs will be developed based on operational missions derived from the six warfighting functions that are critical to planning for and successfully executing operations at all levels.

3. SLAs in Support of the Six Warfighting Functions

Marine Corps Doctrinal Publication (MCDP) 1-0 defines the six warfighting functions as:

> Conceptual planning and execution tools used by planners and subject matter experts in each of the functional areas to produce comprehensive plans. [They] help the commander achieve unity of effort and build and sustain combat power. Their effective application, in concert with one another, will facilitate the planning and conduct of expeditionary operations. (Marine Corps Operations, 2001)

The six functions are listed, defined, and put into context with SLAs as follows:

a. Command and Control

Command and Control is defined as:

> The exercise of authority and direction over assigned and attached forces in the accomplishment of a mission. Command and control involves arranging personnel, equipment, and facilities to allow the commander to extend his influence over the force during the planning and conducting of military operations. Command and control is the overarching warfighting function that enables all of the other warfighting functions. (Marine Corps Operations, 2001)

It must be noted that the mission of Marine Corps Communication operations is to support this warfighting function by providing communication networks and network operators that facilitate command and control provide the commander the ability to command and control the forces under his control. SLAs support command and control by providing the commander with the ability to have a defined level of network service that allows him to “virtually” insert himself wherever he needs to be, within the constraints of the network.

b. Maneuver

“Maneuver is the movement of forces for the purpose of gaining an advantage over the enemy in order to accomplish an objective” (Marine Corps Operations, 2001). One key question commanders often ask is “When and where do I need to array my forces in order to achieve a favorable decision?” A general rule is that larger units require more lead-time to maneuver over greater changes of direction or position. A rifle platoon comprised of 40 Marines can

maneuver within its battlespace quickly, whereas a Marine Division requires considerably more time to maneuver within its battlespace. The key to the decision of when and where to maneuver is the ability to make that decision as early as possible and with as much relevant information as can be obtained about the enemy's forces; it is crucial to then monitor the situation to determine the correctness of that decision.

A well-placed sensor network, composed of a combination of ground mobile, ground static, and air sensors capable of collecting a variety of information types, with the proper SLAs supporting the commander's information requirements, can provide real-time indications of when and where to move forces into a positional advantage, as well as providing a means to monitor both enemy and friendly movement during this phase.

c. Fires

> Fires are the employment of firepower against air, ground, and sea targets. Fires delay, disrupt, degrade, or destroy enemy capabilities, forces, or facilities, as well as affect the enemy's will to fight. Fires include the collective and coordinated use of target acquisition systems, direct and indirect fire weapons, armed aircraft of all types, and other lethal and nonlethal means, such as electronic warfare and physical destruction. Fires are normally used in concert with maneuver and help to shape the battlespace, thus setting conditions for decisive action. (Marine Corps Operations, 2001)

SLAs can support fires by providing real-time information guarantees to support the targeting process

during fire-support planning, as well as during operational execution. If the operation requires destroying a mobile, high-value target, guaranteed real-time information is extremely important. Likewise, a commander who is accepting risk by maneuvering his forces through restrictive terrain would want an SLA in place to ensure that he has real-time sensor information alerting him to any dangers and potential targets that threaten his exposed forces.

d. Intelligence

> Intelligence provides the commander with an understanding of the enemy and the battlespace, as well as identifying the enemy's center of gravity and critical vulnerabilities. Intelligence drives operations and is focused on the enemy. (Marine Corps Operations, 2001)

SLA support of intelligence collection is perhaps the most common thought of application for tactical sensor networks and SLA guarantees of real-time information. The enemy is always operating in some fashion and the enemy situation needs constant updating. The commander has information requirements that must be answered, and it is the intelligence section's responsibility to provide the answers the commander needs to maneuver his forces, determine his targets for fires, where to place his sensor networks, and determine the threat to his ability to command and control his forces. Since intelligence drives operations, it is critical for the intelligence to be as accurate as possible, so the commander can commit to a course of action and a favorable outcome.

e. Logistics

"Logistics encompasses all activities required to move and sustain military forces" (Marine Corps Operations, 2001). Communications equipment requires maintenance, power, spare parts, people, food, shelter, and transportation in order to function properly and to support sustained combat operations 24 hours a day. Common supply routes need to be protected, so that supply and logistical support items can travel along those routes unhindered. Sensor networks can support this effort and SLAs can provide real-time information in support of the logistics effort when the commander determines its necessity.

f. Force Protection

"Force protection consists of those measures taken to protect the force's fighting potential so that it can be applied at the appropriate time and place" (Marine Corps Operations, 2001). Force protection is a constant and continuous mission, but there are several occasions when military forces are most vulnerable and require a heightened protective posture. Large troop movements into and out of theaters, amphibious landings, helicopter insertions and extractions, and moving into assembly areas prior crossing the line of departure (enemy spoiling attack prevention) are some events where the ability to generate overwhelming combat power is limited by the evolution that a force is undergoing. These stages require a heightened awareness of the physical threats the force faces and represent an occasion where real-time information guaranteed by an SLA will support the commander's force-protection mission and preserve potential combat power.

4. SLA Cross-functional Supportability

In addition to supporting individual warfighting functions, the SLA support provided to one function enables that warfighting function to in turn provide support to another function. For example, SLA support to force protection will enable the force to maneuver, provide logistical support, and properly apply decisive fires. SLA support to logistics will help support command and control and maneuver, by ensuring that the correct people and gear arrive at the correct location, at the proper time. SLA support to intelligence will support maneuver, fires, command and control, logistics, and force protection. Finally, SLA support to command and control will support the entire operation, since command and control is the function that binds all of the other functions together into a cohesive system more capable than its individual parts. SLAs, when properly used, are an additional combat multiplier for the operational commander.

C. EXAMPLE TACTICAL LEVEL SLAS IN SUPPORT OF WARFIGHTING FUNCTIONS

1. Introduction

In order to develop an SLA taxonomy that supports tactical SLA development, five examples of SLAs have been developed that support each a unique mission. Each SLA incorporates different roles, units, and missions of a Marine Air Ground Task Force (MAGTF) at the MEF level and below. From these five examples, commonalties have been extracted, which then aids in developing a corresponding SLA taxonomy. Each mission has both unique characteristics and

requirements that distinguish it from other missions. For example, a reconnaissance mission is different than an offensive attack in that enemy contact is not desired in the former, but it is most definitely desired in the latter. At the same time, commonalities among all of these exist in the form of the warfighting functions, although each mission will emphasize each function differently.

2. Infantry Battalion on the Offense

An Infantry Battalion Commander conducting offensive operations is primarily concerned with supporting maneuver with his remaining warfighting functions. Collecting, developing, and using timely intelligence to support the commander's maneuver plan is of primary concern. When the maneuver plan requires movement through restrictive terrain, or involves moving a small assault force rapidly through an unsecure area, precise information about the tactical situation can be the difference between mission success and mission failure. Knowing how to support that maneuver force just prior to enemy contact on the objective, and while the assault is taking place, assists the commander with the proper application of fires, as well as assisting with a more accurate after-action report to help refine the intelligence picture. The following SLA request is from an Infantry Battalion assigned the mission of assaulting an objective and doing so on a compressed timeline in order to take advantage of a fleeting opportunity provided by intelligence. Planning must be kept short and operational security (OPSEC) is strictly enforced so that the enemy is prevented from either making preparations to repel the assault or from withdrawing. The "main effort" company will

travel along a threatened route, while “supporting effort” rifle companies will travel along alternate routes. The SLA request is intended to support the main effort company’s mission to attack rapidly along Axis BLUE, to assault the objective, and to prepare to defend that objective from counterattack until the rest of the battalion can consolidate on that position and transition to a battalion defense.

> From 0445Z until 2200Z on 25 Oct 08, 2d Battalion, 3d Marines requests real-time feeds from:
>
> 1. UAV’s orbiting grids AZ123456, AZ234567, and AZ345678 – video resolution of 1 meter.
>
> 2. Ground sensor clusters located in boxes X1Z, X2Y, and X3Y- video resolution of 1 meter.
>
> 3. TACON of one platoon from the ground mobile sensor company to be initially positioned at grid AY987654 and prepared to move in a northerly direction to provide streaming video of all action to the west of their direction of travel.
>
> 4. One reinforced rifle company operating along Axis BLUE will need access to feeds in priority of UAV’s; the ground sensor clusters X3Y, X2Y, and X1Z; and finally the ground mobile sensor platoon.
>
> 5. This HQ requires access to all feeds during the time allotted and will have GW’s located at

grids AZ124578, AZ123987, and AZ987123. The main COC will be located at grid AY 987650 and it is anticipated that the forward COC will be located in grid square 0102.

3. Air/Ground Reconnaissance Mission

Reconnaissance gives the commander better situational awareness of his assigned battlespace and of the areas surrounding it. Reconnaissance can be conducted to develop an unknown situation in a new area of operations, determine an adversary’s habits or patterns of operations, determine bomb damage assessment (BDA) after a strike, and to support a maneuver force in the conduct of offensive operations. This mission directly supports the intelligence warfighting function, although it can also directly support maneuver, if the situation specifically calls for it. Reconnaissance support to the overall intelligence picture will support the entire force.

Reconnaissance can be carried out by either ground or airborne vehicles. Ground reconnaissance can be conducted by Special Operations Forces (SOF) using radios to transmit real-time information back to their headquarters, by static sensors emplaced that will transmit their mission-designed information through a sensor network, or by mobile sensors mounted on vehicles or personnel which transmit their information in a manner similar to that used by static sensors. Air reconnaissance can be conducted by UAVs, by manned aircraft, or by spacecraft, such as satellites designed for specific information gathering tasks, as shown in the figure below.

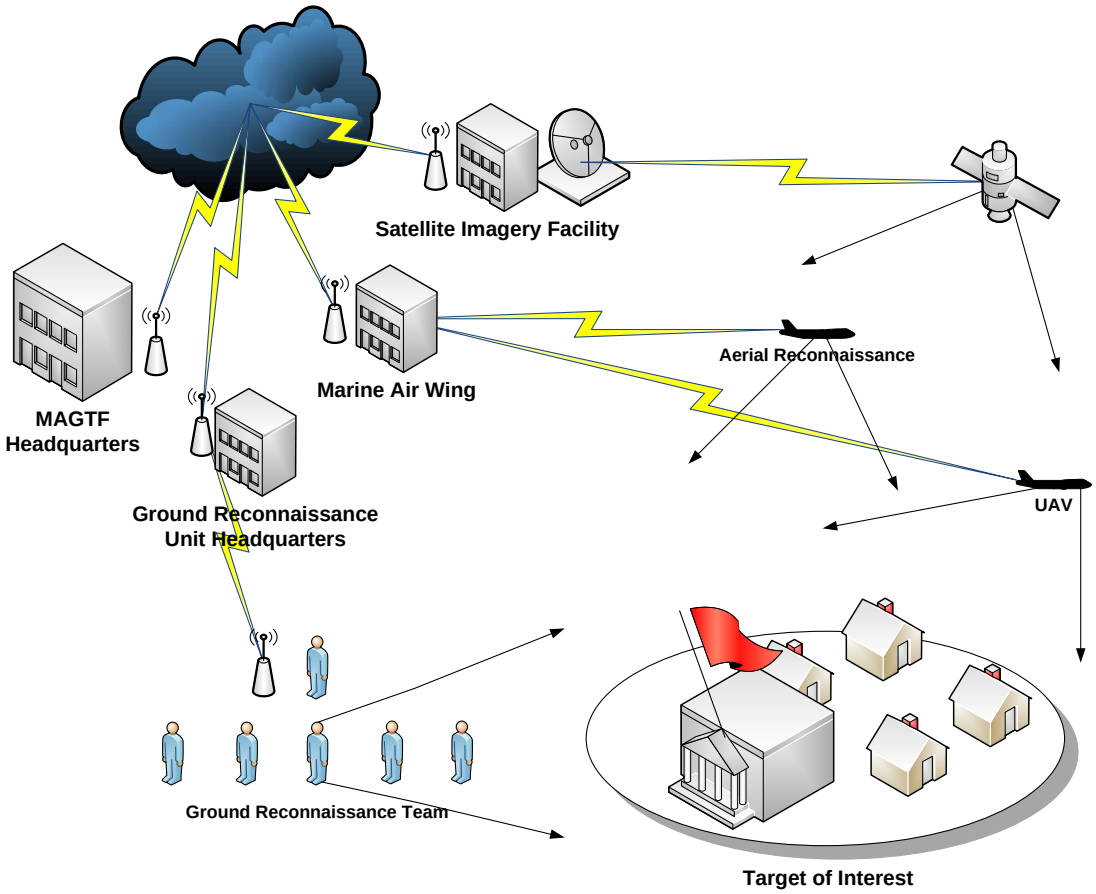


Figure 29. Air/Ground Reconnaissance.

A MAGTF commander needs to gather information about his AO and specific enemy operating patterns in as near real-time as possible. He has several intelligence-collecting assets at his disposal, and it would be prudent to develop a diverse collection plan in an effort to provide alternate means to verify the gathered information and properly analyze and fuse it for possible follow-up action. The following SLA request is submitted for the express purpose of developing knowledge of an elusive adversary's operational habits. Real-time information collection is important since different sources are feeding information

and the time-stamp on the data must be correct in order for a more accurate analysis to take place.

From 0200Z on 1 Nov 08 until 1800Z on 2 Nov 08, 3d Marine Division requests real-time video feeds from:

1. Three UAV's orbiting grids AZ123456, AZ234567, and AZ345678 – video resolution of 1 meter. The UAV's need to focus on building rooftops, street level between buildings, projections from windows, movement to and from buildings, and other taskings from the division that can be executed within one minute of request in order to provide indications and warnings of pending insurgent activity.

2. The ground sensor clusters located along:

a. ROUTE SIXPACK from grid 123456 to 234561

b. ROUTE SHIRLEY TEMPLE from grid 345612 to 456123

c. ROUTE TOM COLLINS from grid 654321 to 543216

3. SOF team 1: from a concealed position located vicinity 123456, position a video sensor to take real-time video of insurgent identified vehicles operating alone ROUTE SIXPACK in order to fully develop the enemy's daily and weekly battle rhythm.

4. This HQ requires access to all feeds during the time allotted and will have GW's located at grids AZ124578, AZ123987, and AZ987123. One UAV will remain overhead to provide additional GW access. The main COC will be located at grid AY 987650 and it is anticipated that the forward COC will be located in grid square 0102.

4. Conduct of an Amphibious Landing

The landing phase of an overall amphibious landing operation is perhaps the most dangerous time for an amphibious force. Moving ashore from sea leaves the landing force exposed both visually and from the effects of enemy fire. Once committed, there is no turning back without admitting defeat and suffering sizable losses. While D-Day (the landing date), H-Hour (the time the landing force crosses the beach), L-Hour (the time the helicopter-borne force lands), and the landing beach locations can be kept secret until the last minute, once the secret is out the date, time, and destination will be known. Obtaining this vital information will give the enemy an additional advantage over the classic defender's advantage. In addition, the defender can absorb the landing force's combat power by trading space for time while the landing force risks getting thrown back into the sea. Forward, increasing, and sustainable momentum for the amphibious force must be maintained.

The landing force commander needs to know a great deal of information about his landing beaches, the terrain beyond, and, most importantly, the enemy situation and how

the enemy can use his capabilities to oppose the landing force. As shown in Figure 30, information concerning the beaches can be obtained from many sources such as overhead imagery, open-source human intelligence derived from locals familiar with the operating area, or hydrographic reconnaissance performed by Sea, Air, and Land (SEAL) Teams or other reconnaissance units. However, well-placed sensors can provide the commander with real-time information on enemy locations, capabilities, and intentions. Sensor emplacement would be conducted in phases, as the situation and the commander's essential elements of information are further developed.

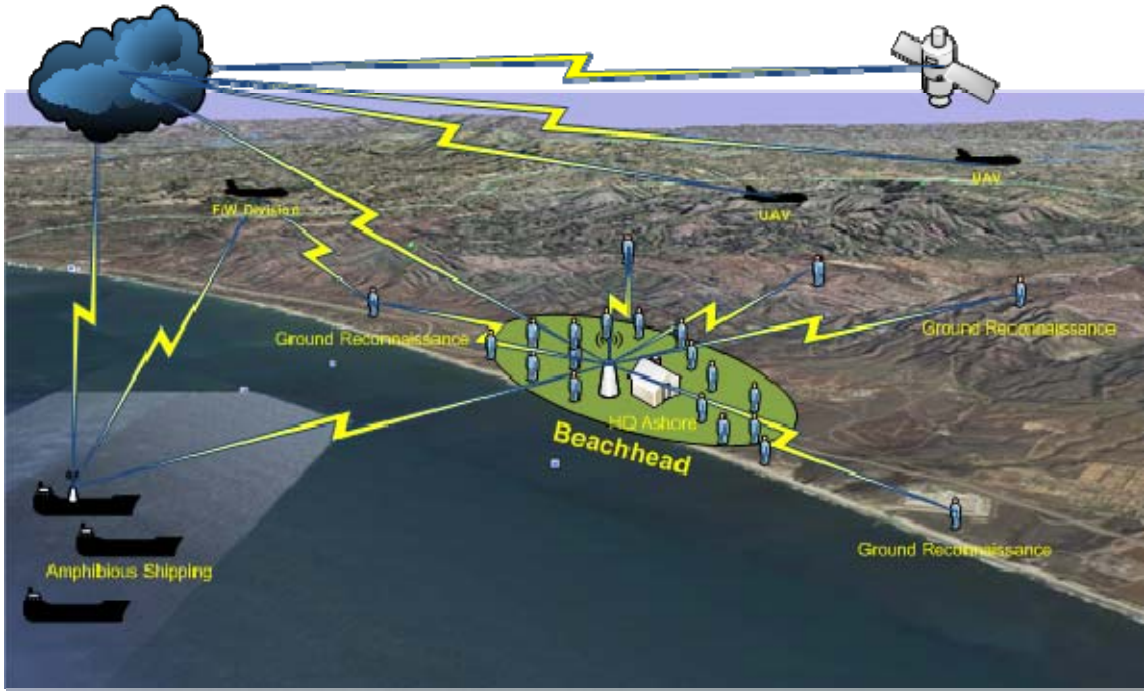


Figure 30. Amphibious Landing.

It must be noted that any type of unusual activity observed, combined with other information, can provide an indication that action may occur, which is why a firm

balance among the six warfighting functions is essential. The quest for better intelligence must be tempered with the need to maintain a high level of force protection. An obvious example is flying UAVs or manned aircraft over the landing area days and weeks prior to the operation. If the aircraft were detected, the enemy could reasonably assume that the area in view of the airborne sensor is of interest to someone with both the capability of flying UAVs and potentially landing a force. This works both ways as well. The clever commander would consider using this perceived risk to his advantage by feeding false information to the enemy while obscuring his real intentions. Therefore, sensor and gateway emplacement must be well thought-out, coordinated with other ongoing operations, and complimentary to the intelligence plan. Initially, ground sensors would consist of static sensors emplaced by SOF teams as well as SOF teams themselves recording and transmitting real-time information back to their higher headquarters for analysis and incorporation into the planning process. Timing for amphibious landings is critical. As D-Day, and then H- and L-hour, count down, different fire support, information operation, and troop movement plans are executed. An opportunity to emplace and take advantage of information gained from additional sensors should not be missed during the conduct of the above supporting missions. Just before the execution of the fire support plan for the landing force has begun, the sensor network must have rapidly expanded to its fullest, pre-D-Day capability. At this point, known enemy locations must be confirmed, net enemy locations must be detected for possible targeting, and enemy intentions and capabilities must be detected and assessed to determine the

threat posed to the landing force. UAVs, manned aircraft, SOF teams, and the other ground sensors will form the basis of the active landing sensor network. As forces flow ashore via seaborne and airborne vehicles, more sensors will be added to the network. Battle suits, ground mobile units, additional gateways, and other information-gathering devices will continue to automatically join the network via the IPv6 auto-configuration capability.

It is critical to plan SLAs in support of the amphibious landing in concert with the flow of forces ashore and the scheme of maneuver of forces once ashore. During the planning phase, bandwidth is limited by the number of gateways emplaced and the connectivity of the gateways to the GIG. Connectivity to the sensor network and responsibility for maintaining the COP will be provided by the amphibious ships that the landing force is embarked on, until the landing force can establish itself sufficiently ashore. During the landing phase, the bulk of the landing force's communication equipment is moving ashore and is, therefore, offline and incapable of providing bigger pipes to handle the growing network ashore. However, the sensor network ashore is still operating and will be capable of providing information, even as more and more sensors come ashore and join the network. Once established ashore, the landing force will be responsible for providing its own connectivity to the GIG and for maintaining the COP for the amphibious force. One critical event for SLAs will be the transfer of control for the landing operation from the amphibious task force to the landing force.

Table 7 shows several phases of an amphibious landing and the network characteristics that an SLA request would need to support per given phase, in order to support the amphibious landing operation. Once the landing force is established ashore, the force will then transition to sustained combat operations and SLAs will no longer support the amphibious landing phase.

Phase	**Network Size**	**Connectivity**	**Information needed**	**SLA Issues**
Planning	Small, SOF teams, static ground sensors	Limited by OPSEC and bandwidth. A limited number of gateways linked to a geostationary satellite.	Data on enemy composition, disposition, and strength	Low bandwidth, low number of sensors, low mobility, long reachback to NOC
Pre-landing	Growing in size to max pre-landing capacity, SOF teams, static ground sensors, UAV's, manned aircraft	Number of gateways grows as the number of capable platforms increase. Amphibious shipping.	Real-time information needed for targeting, enemy locations, and BDA.	Increase in real-time information demand, operational and network chaos. Additional sensor assets coming on station to deliver real time information feeds to the requesting units
Landing	Growing on an increasing scale as forces flow ashore and join the	Introduce additional gateways, new ground static/mobile, airborne sensor nodes	Real-time information needed for targeting, enemy locations, BDA, threats to the	Peak level of operational and network chaos. Increase in number and type of

	network		landing force, and enemy movements	sensor units and clusters joining and leaving the network.
Landing Force Established Ashore	Growing at a decreasing rate	Networking equipment on-line and providing increased connectivity		Transition

Table 7. Amphibious Landing SLAs.

5. Military Operations on Urbanized Terrain (MOUT)

One of the most complex and dangerous combat environments is urbanized or built-up areas. Locating the enemy, reducing collateral damage and civilian casualties, preventing fratricide, and maneuvering faster than the adversary are all much harder than in other combat scenarios. This type of terrain is a great equalizer and can nullify some of the advantages of a militarily superior adversary. Movement through these areas is very slow and confused; an area thought to be cleared one day can be tomorrow’s trouble spot. MOUT can be very costly in terms of human lives, infrastructure, and even in the political arena. The action that occurred in October 1993, in Mogadishu, Somalia, is one of the more recent examples of MOUT in which a militarily superior force found itself decisively engaged with thousands of indigenous attackers. Through sheer willpower, the Americans completed their original mission of capturing two of Somali warlord Mohamed Farrah Aihid’s lieutenants, while extracting its stranded assault force. The human toll was politically damaging, with 18 American dead, 70 casualties and thousands of Somalis

killed; broadcast news showed scenes of jubilant Somalis dragging dead Americans through the streets. While the mission was a “success” in the eyes of the world, it was viewed as an American failure in a small, third world country (Bowden, 1999). The more recent examples of fighting in the cities of Fallujah, Baghdad, and Nasariyah, Iraq, further illustrate the ferocity of fighting in an urban environment.

Villages, towns, and cities have some of the most challenging terrain to operate in, and are described as three-dimensional battlefields. For the defender, multi-story buildings offer good, all-around visibility, multiple firing points, cover from return fire, and a good command-and-control vantage point. From the inside, each floor offers additional protection, since the attacker must contend with a defender who is defending from above. A city block typically contains several buildings from which mutually-supporting and interlocking fire can be employed; one building can observe targets and direct the fire from another building or a row of buildings. Additionally, the streets between city blocks are narrow corridors, which naturally channel traffic. Very little cover, protection, and concealment are offered, which makes unobserved mobility extremely difficult. In some areas, sewer systems and subways are below ground. For both the defender and attacker, these underground routes provide mobility that is unobserved from street- and building-level, and must be guarded accordingly.

Referring to the warfighting functions detailed above, intelligence drives operations. Intelligence support to

operations and an intelligence collection plan focused on the enemy in a MOUT environment are essential to success. Knowing where the enemy is and understanding the enemy's battle rhythm, capabilities, and external operational support beyond the urban environment are all essential to a successful operation in urbanized terrain. A well-placed sensor network can assist in intelligence collection by providing real-time information from multiple sources in varied locations. The IMO, Operations, Intelligence, and Communications section must keep track of and balance both operational requirements and command-and-control capabilities. The best case is when the sensor network can support any operational contingency with the appropriate mix of sensors in place in time to support the SLA and, therefore, the operation. This could be achieved over the long-term, with tactical situation and terrain sensor network optimization, where an analysis is conducted to study the enemy's patterns, the terrain, the operational habits of allied forces, and the capabilities of the sensors and gateways to be placed. However, urban terrain can keep both friendly and enemy forces off balance. Initially, SOF teams operating in the environment can place sensors in buildings, underground structures, on top of buildings, and on the approaches in and out of the environment. UAVs and manned aircraft orbiting over the city can take general observations or can be tasked to target specific locations for a specific length of time. When sensor support for an operation or a specific intelligence collection task is required, an SLA can be put into effect so as to ensure that the network will support the stated mission. Below is an example of a SLA request submitted to support an infantry

battalion whose mission is to cordon and search several buildings within a hostile city block. These buildings have been previously identified as terrorist weapons caches, and one contains facilities and equipment for an operational planning cell. All equipment is to be confiscated, and all persons seen within the vicinity of this equipment are to be detained for identification and questioning. The battalion's main effort company will begin its mission when terrorist activity is at its lowest point, as indicated by intelligence analysis derived from information collected in part by the sensor network. It will be assumed that once the battalion's mission begins, the enemy will begin to discern the battalion's intent and will try to counterattack, so the battalion needs to know of all activity within the target's vicinity 24 hours prior to the start of the operation to determine enemy and civilian positions. Approaches to and from the area need to be observed, as do any surrounding buildings from which enemy observation and fire can come. UAVs orbiting the area will be tasked with providing observation of key locations. By having key routes and buildings identified as high-risk under observation, the unit will have the early warning it needs to either launch a spoiling attack or to bring the target under fire. Drawing on history and previous experience, both the primary and alternate egress routes will be under real-time sensor surveillance in order to provide the commander with an accurate picture of the enemy situation as the battalion egresses. The regimental rapid reaction force's insert and egress routes will be covered by real-time sensors as required in order to safely and quickly reach the infantry battalion assault force, should they need the assistance.

From 0200Z/1 Nov 08 until 1800Z on 2 Nov 08, 2d Battalion, 3d Marines requests real-time video feeds from:

1. Three UAV's orbiting grids AZ123456, AZ234567, and AZ345678 – video resolution of 1 meter. The UAV's need to focus on building rooftops, street level between buildings, projections from windows, movement to and from buildings, and other taskings from the supported battalion that can be executed within one minute of request.

2. The ground sensor clusters located in the following buildings:

a. 12145-X1Z: face north towards the city block containing target buildings located in grid square 123456–video resolution of 1 meter, focus on building windows, avenues of approach, and movement to and from the target buildings along the adjacent streets and avenues of approach.

b. 12145-X2Y: face north towards the avenues of approach leading towards the building for possible enemy reinforcement.

c. 12145-X3Y: face south and west- video resolution of 1 meter, focus on building windows, avenues of approach, and movement to and from the target buildings along the adjacent streets and avenues of approach.

d. SOF team 1: from a concealed position located vicinity 123456, position a video sensor to take real-time video of insurgents entering or leaving building 12145-ZZ1, a suspected operational planning cell in order to refine the terrorist cell network that exists in this vicinity. In addition, be prepared to video in real-time any movement to and from the target buildings in order to fully develop the enemy situation prior to the assault.

e. SOF team 2: Emplace seismic sensors along the drainage system in order to detect motion and provide early warning of possible incursion.

3. One team from Combat Camera to record and transmit real-time video from the assault to counteract any negative propaganda, which may result from the assault on this city block. After the assault, record video of all captured equipment and any personnel detained for further intelligence analysis.

4. Two supporting reinforced rifle companies performing the cordon within a 0.5 radius of the target buildings will need access to the UAV feeds and the sensors located along routes GUINESS, ST PAULI GIRL and BUD LIGHT in order to locate and identify insurgents, allied personnel, or civilians attempting to approach, leave, or breach

the cordon. The two company HQ’s will be located at grids 12345678 and 23456781. These two companies are third in priority.

5. The main effort company performing the search mission will have priority access to all of the feeds requested in this SLA. The company HQ will be co located with the battalion forward CP.

6. The Regimental Reaction Force (RRF) will require access to UAVs and sensors located along routes PALE ALE, COORS, ANCHOR STEAM, and SAM ADAMS. Priority will shift to the RRF when the RRF has been activated.

7. This HQ requires access to all feeds during the time allotted and will have GW’s located at grids AZ124578, AZ123987, and AZ987123. One UAV will remain overhead to provide additional GW access. The main COC will be located at grid AY 987650 and it is anticipated that the forward COC will be located in grid square 0102.

6. MEF-level Sustained, High-tempo Combat Operations

This level encapsulates the operations of the five preceding examples before it. An MEF that has been deployed overseas for the purposes of engaging and defeating an enemy may have to perform an amphibious landing, or may have to conduct sequenced offensive operations as part of a larger campaign in support of strategic objectives. It may also be ordered to perform deep reconnaissance missions to determine

when and where to engage the enemy as part of the sequenced offensive operations, and may have to engage the enemy in an urbanized environment. Some of these operations may occur simultaneously, some may occur sequentially, and all may occur at the same time. Ultimately, the communications network and the information that is transferred over that network must support the unit's operational needs. As in the case of air support, fire support, and other forms of low-density, critical resources, not every unit can have a priority on network resources. SLA requests, and the management system that the IMOs within the information management hierarchy use to determine which SLA requests will be approved or denied, should support the operational plan. Main effort units should have priority on SLA requests, while supporting effort units' requests should be prioritized; likewise, the management system will have to determine if there are enough resources to equitably support the supporting units' needs. In addition, if the main effort unit designation will shift based on time or events then the SLA's management system should accommodate, and even anticipate, the network resource shift to the new unit.

7. Compare/Contrast of Sample SLAs

Five examples of SLAs are compared and contrasted in Table 8:

		Example Tactical Service Level Agreements				
		Infantry Battalion on the Offense	**Air/ Ground Recon Mission**	**Conduct of an Amphibious Landing**	**Military Operations on Urbanized Terrain (MOUT)**	**MEF-level sustained high-tempo operations**
Physical Layer	**Sensor Types/ Number Employed with Unique IPv6 Address**	UAV, sound, seismic, environmental, video camera, battle suit ~500 sensors	UAV, sound, seismic, environmental, video camera, aircraft, satellite, battle suit ~20 airborne sensors ~200 ground sensors	UAV, sound, seismic, environmental, video camera, aircraft, satellite, battle suit, hydrographic ~5,000 to 10,000 sensors	UAV, sound, seismic, environmental, video camera, aircraft, satellite, battle suit ~10,000 to 100,000 sensors	UAV, sound, seismic, environmental, video camera, aircraft, satellite, battle suit, hydrographic >100,000 sensors
	Geographic Size	Battalion AO	Small area to MEF-level AO	MAGTF AO size	Unit level AO	MEF-level AO
	Terrain	Ground/any type terrain	Air and Ground/any type terrain	Beach, hinterland, inshore	Urban environment, buildings	All
	Network Size/Type	Small/Static	Large/Static or Dynamic	Size dependent /dynamic	Large/Dynamic	Large/Dynamic
	Number of nodes	Relatively low	Relatively high	Initially low with large increase during conduct of operation	Increases with the length of the operation	High
	Transmit Media	Wireless, satellite, terrestrial	Wireless, satellite, terrestrial	Wireless, satellite, terrestrial	Wireless, satellite, terrestrial	Wireless, satellite, terrestrial
	NOC/COC location	Within AO, close	Within AO, remote	Afloat, phasing ashore, close	Co-located within the urban environment	Within the AO, remote from the edges
	Sensor Node Locations	Any	Any	Any	Any	Any

Data Flow Layer	**Average Sensor to AO Density**	Low	Low to High	Increases as the mission progresses	High	Medium
	Ratio of nodes to gateways	High	Low	High until more gateways are on-line	Low	Low
	Network Congestion Level	Relatively high due to low data rates	Relatively low due to higher data rates and mix of sensor nodes	Variable depending on level of nodes and gateways on-line	Variable depending on transmission paths	Dependent on missions, and locations
	Data Rates	"Tactical level" therefore low	High	Initially low with large increase during conduct of operation	High	Increasing as the network develops
SLA Layer	**Level of network control**	Low	High	Low	High	High
	Ability to maneuver mobile sensor nodes	Dependent on who controls the nodes	Yes	Increases with execution	Dependent on who controls the nodes	High
	Ability to emplace static sensor nodes	Low	Yes	Pre-landing low, Landing high	Yes	Yes
	Data Types	Video, voice, application data (NBC, seismic, weather, blue force tracker), real-time data	Video, voice, application data (NBC, seismic, weather, blue force tracker), real-time data	Video, voice, application data (NBC, seismic, weather, blue force tracker), real-time data	Video, voice, application data (NBC, seismic, weather, blue force tracker), real-time data	Video, voice, application data (NBC, seismic, weather, blue force tracker), real-time data
	Classes of Traffic	Low	Medium	Increasing	High	High

Information Layer	**Number of SLAs to support OPRD/CCIR**	Low	Low	High	Med	High
	Operational phase shift	No	Yes	Yes	No	N/A, supporting many different operations
	Level of Quality needed for decision making	Relatively low	Relatively high	High	High	Mission dependent
	Expected Mission Duration	Short	Any	Short	Any	Long/Mission dependent
	COP/UDOP	One battalion COP	Intelligence Section UDOP	COP/staff section UDOPs	COP	MEF COP/staff section UDOPs

Table 8. SLA Comparison.

a. Physical Layer

Table 8 depicts a side-by-side comparison of five example tactical level SLAs written in support of the warfighting functions. The first section, the physical layer, shows a commonality among the sensor types, geographic size, and terrain. Sensors such as UAV video cameras, weather, and seismic detectors are not mission-specific, so they can be used for a wide variety of tasks and to support a wide range of missions. Geographic size indicates the size of the unit's AO, while the terrain is a key indicator of the difficulty in establishing links among the nodes. Since combat units must be able to operate in all types of terrain, terrain cannot be a limiting factor in providing QoS. The physical layer must take distances and

terrain into account when the network nodes are emplaced and the links between them are established.

Table 8 differentiates among network size and type, including an infantry battalion’s network that is comparatively smaller then the MEF’s network, the size of a network in an urban environment, or a dynamically-changing network supporting an amphibious landing. The infantry battalion will have fewer nodes and gateways to place and, with the exception of human sensors, will not have the means to continually relocate them around the battlespace. An infantry battalion’s generic mission statement is to locate, close with, and destroy the enemy; thus, the battalion commander will want to place his limited assets in a way that achieves his goal by shortening his decision-making cycle.

The assets that the battalion receives for a specific mission will be tasked by higher headquarters, and will be appropriate to its role in the mission. While the battalion commander can request more assets, it is the higher unit’s prerogative to deny the request. The battalion commander can also submit requests for information (RFI) and take advantage of the information gained from higher headquarters’ sensor assets. Reconnaissance missions are focused on answering information requirements; for this reason they can be very focused on specific locations; alternately; alternately, they can be broad in scope and cover virtually the entire AO. Operational success relies on timely answers to the commander’s information requirements (assuming the information requirements are both correct and relevant), so the proper mix of ground, air, static, mobile,

and SOF sensor assets will be deployed to properly capture the data to answer the information requirement(s). An amphibious landing network environment will be initially small, but will increase as more assets move ashore and begin to join the network. The network will then expand and grow denser as the landing force expands the AO by pushing inland and joining even more assets to the sensor network. In contrast, the MOUT environment is more compact and needs a larger, denser network, since the "sensing distance" of most sensors is far more constrained by the urban environment than it is by a more open environment. The MEF has many more assets and operations to manage, so network size is not a matter of a linear scale. Transmission media is predominantly the same, regardless of the type of supported mission.

The network operations center (NOC) and combat operations center (COC) location are listed in this layer, since the information received from the sensor nodes must be relayed to these two locations in a timely manner for it to be of value; it should also be noted that the NOC/COC are considered nodes themselves. Doctrinally, these locations must support the commander's ability to command and control his forces. Therefore, the COC/NOC must be in a protected location, but still in a position to communicate. More often than not, these two requirements are opposed to each other and the need for protection is deemed the more important of the two.

b. Data Flow Layer

The next section, the data flow layer, depicts the variations in the flow of data among the different mission

SLAs. The infantry battalion SLA shows a low ratio between the average number of sensor nodes and the size of the AO, whereas the reconnaissance mission, amphibious landing, and MOUT operation have notably higher ratios. The infantry battalion's sensor assets are relatively limited because units at that level can have a reasonable expectation that higher headquarters' assets will provide the information they need. Any information gaps identified by the battalion staff can then be covered with the battalion's assets.

Reconnaissance, amphibious landing, and MOUT operations will have a higher ratio since operations such as these require a higher degree of battlespace knowledge in order to generate the higher operational tempo required for mission success. Reconnaissance missions are specific in nature and are executed to answer the commander's information requirements. As noted previously, amphibious landings and MOUT operations are comparatively more complex and dangerous then a typical infantry battalion offensive operation in more permissive terrain. Network congestion is mission-dependent but will most likely be related to the sensor node/AO ratio. More congestion is likely for units and missions with a smaller ratio of sensors to AO size.

c. SLA Layer

The next set of categories is grouped under the SLA layer heading. This layer includes the areas in the SLA specifically related to providing QoS within the network. As this SLA compare/contrast analysis progresses up the layers an expected pattern begins to emerge with respect to the SLAs and the unit level and mission types. As one might expect, the infantry battalion's more generalized offensive

operations receive fewer resources to support QoS than do more specialized operations and higher echelon units. The infantry battalion will have fewer resources to use and will have less capability to control the network once operations are underway, since every additional person and resource above the minimum required to run the network will be one less person and resource devoted to mission accomplishment. Mission failure with perfect information is still mission failure.

The next two categories, mobile and static sensor emplacement, again highlight the differences in units and missions. The value of increased battlespace knowledge includes a higher operational tempo and more effective action in accomplishing the unit’s mission. While infantry battalions theoretically have the ability to implant and replant sensor nodes, the time and resources required to do so take away from its ability to take advantage of increased battlespace awareness and thus to accomplish its mission more effectively. The ability to maneuver mobile units is dependent on whether or not those same units are under the battalion’s span of control. This is a command-and-control issue that would be resolved during the planning process or during execution with requests and fragmentary (frag) orders to the involved units.

With respect to the remaining missions and higher echelon units, the level of control and the ability to move static sensors and mobile sensors increases with mission complexity and the size of the unit involved. More specialized missions will have the appropriate resources

devoted to them in order to ensure mission accomplishment since other, more far-reaching missions rely on the success of those specialized missions.

The data types category lists the data types common among the different SLAs. With the exception of the hydrographic data needed for an amphibious landing, the data types are the same throughout. This makes sense, since the information provided by the different data types is very similar within the warfighting model so as to provide the commander with the intelligence he needs. The statement from MCDP-1, “[i]ntelligence provides the commander with an understanding of the enemy and the battlespace, as well as identifying the enemy’s center of gravity and critical vulnerabilities,” is true across the spectrum of operations and from a tactical perspective collection methods are basically the same.

The traffic class category uses the traffic class field in the IPv6 header to denote different levels of QoS for each flow label. Within the MEF sensor network each of the 64 codepoint values will map to MEF-defined PHB’s for each DS domain. These domains can be built around the traditional MEF command structure.

The Command Element, Air Combat Element, Ground Combat Element, Combat Service Support Element, and the new “fifth element of the MAGTF” will each have their own DS domains and sub-domains with PHBs defined for each.

The codepoint, PHB values, and the IP addresses on the node interfaces will be structured so that traffic flows passing through higher, adjacent, and/or subordinate units will receive the same level of QoS treatment until they

reach their intended DS domain. From this point the individual units can then define the PHBs as required. The primary means to communicate this QoS information to all interested units is through the SLA request.

d. Information Layer

The final categories are grouped under the Information layer heading. This layer captures specific operational characteristics that directly affect the level of QoS provided for the conduct of the operation. As with the lower layers, the sample SLAs emphasize the differences between unit size and mission types.

The infantry battalion will be allotted relatively few SLAs to implement in the network. The reasoning for this is simple: the infantry battalion is the smallest self-reliant tactical unit capable of managing network functions and, therefore, the smallest tactical unit capable of coordinating and submitting SLA requests. In a manner similar to the fire support restrictions governed by the supporting artillery battalion and its ability to support a finite number of targets at any one given time, an infantry battalion staff must determine which information requirements cannot be answered by higher headquarters (the information requirement gaps) by means of RFIs and referring to the MEF SLA request database. If these gaps still exist, the staff must determine which information requirement gaps will be most effectively served by submitting the battalion’s sensor network SLA request. This SLA request will be incorporated into other SLA requests submitted throughout the MEF for decision, incorporation, merging, or denial.

Likewise, a single reconnaissance mission will also receive a low number of allocated SLAs since, by design, each mission will be specific enough and the supporting SLA request should encompass the entire mission. “Mission” in this sense refers to the actual mission statement and not necessarily the insertion or extraction phase.

The amphibious landing operation will have a relatively high number of SLAs since this type of operation is perhaps the most complex, has the highest capacity for the “fog of war,” and is very difficult to command and control. Commanders at all levels will want to know as much as they can about the enemy situation, friendly situation, terrain, weather, and battlespace so they can keep the operational tempo high, reduce the number of casualties, and achieve mission success within the commander’s intent, as soon as practical.

MOUT operations will have several SLAs in effect as well, but not to the same degree as the amphibious operation. MOUT operations must be highly synchronized and therefore everyone must have the same level of battlespace knowledge in order to achieve a high degree of coordination. The high degree of synchronization calls for an equally high degree of coordination and centralization at higher command-and-control levels. SLAs will be determined by the senior level headquarters responsible for the MOUT operation; this accounts for a reduced number of SLAs in the network at any one time.

MEF-level sustained operations will have many SLAs in effect at any given time since the MEF encompasses a wide

variety of units and missions. A successful reconnaissance mission conducted by the force level reconnaissance unit can then lead to an upcoming offensive operation for the air wing and the ground division. Each unit will have SLAs in place for the success of their mission.

Operational phase shift is an important notion for proper SLA support and network QoS. For example, reconnaissance missions can either be conducted for general battlespace awareness, which can then lead to offensive operations should the situation warrant, or they can be conducted prior to planned combat operations in order to provide the needed intelligence support for mission success. In some instances, the reconnaissance mission is executed in conjunction with a larger operation. In this case, the reconnaissance unit will be the “main effort” as they insert and gather information critical to the success of the larger operation. Once that larger operation commences, the main effort will shift to the assaulting unit and the reconnaissance unit will shift to a “supporting effort.” This is an important distinction to make because when designating a unit the main effort is how the commander explicitly determines and “communicates” to the entire force which unit will get priority on all of the resources it needs for mission success. Priority of resources extends to the network as well, so when the operational phase shift occurs, the network needs to know this and understand what it means. The network will accommodate this shift and reprioritize the main effort units by manipulating the MEF-defined codepoints and PHBs. The amphibious landing phase shifts will occur in the same manner but on a larger, more complex scale.

It must be understood that the no one will have the perfect information from which to make the perfect decision. General George Patton was known to say that a good plan violently executed today is better than a perfect plan executed next week. In keeping with the model developed so far, the infantry battalion commander must realize that his unit is one of nine infantry battalions within the ground combat element of the MEF. In short, he may have to accept a less-than-perfect level of quality in his level of QoS when the entire MEF operational tempo and cycle of operations is considered. The battalion IMO must, therefore, be experienced enough to determine which other SLAs will be in effect, from which other relevant information can be pulled.

The information provided by the reconnaissance mission needs to be of high quality since pending operations and high-level decisions depend on the information developed from the recon. Amphibious landings need the best information possible that can be gleaned from the network, while both MOUT and MEF high-tempo operations require varying levels of information quality, which are dependent on the operations being conducted.

The Common Operating Picture (COP)/User Defined Operating Picture (UDOP) are the visual means for the commander and his staff to spatially view the information received from the sensor network (see Figure 26). The COP is presented in a standardized format with many different associated layers that show different degrees of detail. Each commander has his own vision of what he wants to see on a general, day-to-day basis and of what he needs to see for specific operations. It is up to the IMO and the Operations

section to configure the COP in a manner to meet the commander’s requirements. Likewise, the UDOP can be tailored so that each staff section can display the information they need to best accomplish their assigned tasks.

D. TACTICAL NETWORK SENSOR TAXONOMY

1. Taxonomy Development and Incorporation with IPv6

Table 8 and the associated discussion of the five example SLAs describe the tactical characteristics within each of the four layers of tactical sensor network QoS implementation. From top to bottom, these layers range from the vision the commander has when he describes his mission and how he wants to see his information requirements answered, to how the network will physically support the QoS needed to support the overall mission. After analyzing the sample SLAs within their respective unit sizes and mission types, both unique and similar tactical QoS considerations emerged; the number of sensor nodes, the transmission media, and the terrain were among these. While each SLA had unique aspects for each of these considerations, their physical layer generalities logically placed them together at the tactical sensor network physical layer. Similar considerations had a natural grouping as well and from this emerged the tactical network sensor taxonomy shown in Table 9.

Tactical Network Sensor Taxonomy	
Layers	Information Layer
	SLA Layer
	Data Flow Layer
	Physical Layer

Table 9. Tactical Network Sensor Taxonomy.

2. Tactical Network Sensor Taxonomy Described

a. Information Layer

The Information Layer is the layer at which the commander articulates how he wants his information requirements answered and what he intends to do with that information. These requirements can be captured in the SLA request template and supported at the lower layers of the taxonomy. The battalion staff supports the commander's efforts by working through the Marine Corps Planning Process (MCPP) to give him the best product under the circumstances which he can then use as a basis to operate his unit in the accomplishment of a mission statement. As a member of the staff, the IMO must determine if the sensor network's current configuration can support answering the developed information requirements, or if those requirements can be answered or provided in real-time by higher headquarters or other means. Taking the commander's guidance for what he needs to see and the products developed by the planning process, the IMO will draft and submit the battalion's SLA for review and incorporation into the MEF's SLA database.

The following scenario, which builds upon this thesis's opening scenario, illustrates the echelon and staff interactions that take place at this layer:

> A Marine Expeditionary Force (MEF) is forward deployed and is engaged in high tempo combat operations to secure a foothold from which to hand over sustained operations to a follow-on Army Corps. The MEF Commanding General (CG) desires to make use of recently fielded technology to support the high operations tempo by providing information to the requesting user at the appropriate time so that the MEF will operate on a compressed decision-making cycle.
>
> This shorter cycle will provide the CG the edge he needs to mass his combat power at the point of decision and to take advantage of his force's inherent speed, mobility, and lethality. Based on the CG's guidance, his staff recommends the increased use of intelligence, surveillance, and reconnaissance (ISR) assets in the form of UAV-born sensors, ground-deployed static sensors, ground-mobile sensors, and the battlesuit sensors worn by his reconnaissance and other selected units to feed real-time information to the respective Combat Operation Centers (COC). Each staff section at each level will have the ability to tailor a user-defined operating picture (UDOP) to display the feeds in the manner most appropriate for them in order to act on the information obtained and then provide recommendations based on their analysis. The CG

approved and the operation planning team (OPT) set to work incorporating this capability into their planning effort.

One of the MEF's operational assumptions was that the MEF's organic assets, supporting units, and higher headquarters would be spread all over the globe in order to mass whenever and wherever needed. The distances between units necessitate the use of the GIG, which provides the WAN/communications backbone for the MEF's higher, adjacent, and subordinate units. This global connectivity requires the use of IPv6 for its increased address space, end-to-end connectivity, and ease of auto-configuration.

To address these issues, develop the ISR asset employment plan, and determine how the network will support prioritizing the information flow, the MEF IMO and representatives from the operations (G3), intelligence (G2), and communications (G6) sections formed the IMO cell. The IMO's pre-established tactics, techniques, and procedures (TTP) in addition to standard operating procedures (SOP) guided the planning effort which resulted in the creation of the related sections of the IMO, Intelligence, Communications, and Operations annexes and appendices to the base MEF order.

The G3 reiterated the scheme of maneuver that the intelligence, communications, and information management plans needed to support. The G2 provided input about where the MEF-level sensors

should be located to support the intelligence gathering effort. The G6 provided input about how and where the sensors and gateways should be located in order to provide maximum connectivity. The IMO developed the MEF's information management plan, which would ensure that the information gained from every sensor located within the MEF's influence was properly managed and coordinated up, down, and laterally; a sensor network covering a MEF-sized battlespace can become quite congested and can restrict the ability for real-time information to reach its destination as intended. (One item included as an exhibit in the IMO's annex covers the use of SLAs for the MEF sensor network in order to deconflict potential sources of network congestion.) Standardization, submission procedures, and access to the management database are all addressed and cross coordination with the G3 is made to ensure that SLAs are included in the MEF's operational synchronization matrix (sync matrix). The G6, keeping in mind that communications supports operations, noted the overall scheme of maneuver and the types, locations, and availability of employed ISR assets that needed to connect with the network to provide the information required, and the IMO's plan to disseminate that information throughout the MEF. The G6's plan needed to include GIG connectivity, managing an IPv6 sensor network, and managing QoS assurance mechanisms to

ensure that the SLAs would be supported within the physical capabilities of the network.

Three levels down at an Infantry Battalion, a staff planned its part in a MEF-wide operation in which it is designated the MEF's main effort. As the designated main effort, the battalion enjoys the majority of the assets it requests. For this specific operation, significant real-time information is required for both the planning effort and the assault itself. The user in this case is the battalion commander who needs to pull sensor imagery and real-time sensor feeds from multiple sources through a network that is delivering different levels of traffic to various destinations, for a specific time interval, and at a specified QoS level. In this case, he needs more than one specific feed and needs to have a certain QoS level to guarantee at least the minimal network resources, and he needs this guarantee for a specified time to cover the projected length of his assigned task. This request would come in the form of a standardized SLA in accordance with unit TTP's, SOP's, and applicable operations orders. A suggested, single SLA request, to support this experiment's scenario, would be the following:

From 0445Z until 2200Z on 25 Oct 08, 2d Battalion, 3d Marines requests real-time feeds from the UAV's orbiting grids AZ123456, AZ234567, and AZ345678 – video resolution of 1 meter; the ground sensor cluster located in boxes X1Z, X2Y,

> and X3Y- video resolution of 1 meter; and TACON of one platoon from the ground mobile sensor company to be initially positioned at grid AY987654 and prepared to move in a northerly direction to provide streaming video of all action to the west of their direction of travel. One reinforced rifle company operating along Axis BLUE will need access to feeds in priority of UAVs; the ground sensor clusters X3Y, X2Y, and X1Z; and finally the ground mobile sensor platoon. This HQ requires access to all feeds during the time allotted and will have GW's located at grids AZ124578, AZ123987, and AZ987123. The main COC will be located at grid AY 987650.

Once reviewed by the Operations Officer and approved by the Commanding Officer, this SLA is the product of this layer of the taxonomy. Subsequent layers will take this "human readable language" and translate it into language that would support the operation by "informing" the network of the requesting unit's information requirements so that each packet can be tagged appropriately and subsequently prioritized throughout the network. Operating at the eighth layer, the SLA is then translated into application QoS by incorporating the specified or derived locations, distances, times, source nodes, destination nodes, information quality levels, and application bandwidth requirements from the SLA request in order to determine how to move the tagged packets through the network. This knowledge about the network puts

the QoS decision-making ability in the network, where it is much more responsive than a human operator located some distance away at the NOC.

b. SLA Layer

The Service Level Agreement Layer is the layer at which specific characteristics affecting the supportability of the Information Layer are captured and configured, thus supporting the information views that the commander and his staff need in order to answer the commander’s information requirements. The IMO must have an understanding of the data types that the commander and his staff wish to see that require the real-time QoS guarantee. Referring back to the UDOP/COP, configuration at the Information Layer will specify the information views. The IMO needs to then specify the data types and the specific requirements for each in order to pass each traffic flow from the sensors to the NOC/COC for display. Different data types have different bandwidth requirements, data formats, and security levels, which the IMO will need to know for QoS assurance. In conjunction with the data types, are the assigned classes of traffic, codepoints, and PHB’s for each traffic flow traveling in the DiffServ-enabled IPv6 network. The IPv6 header, shown in Figure 1, contains a 24-bit flow label starting at the eighth bit, which provides the routers a quick method of determining the packet’s QoS level. In IPv6, this flow label is marked with the appropriate Differentiated Service CodePoint (DSCP) value to differentiate one traffic class from another. This is the mechanism used by DiffServ to prioritize traffic as it flows through the network. At this layer, each traffic flow will

be assigned a traffic class and codepoint which map to specific PHBs, depending on which DS domain the traffic flow is travelling through.

Traffic class and codepoints are selected from a common database maintained by the IMO hierarchy. For example, an SLA criterion for one-meter resolution from a certain sensor node or cluster of nodes will be assigned a PHB, which ensures that the packet carrying video data relating to a particular sensor, source, and destination IP gets the QoS it requires. Knowing that one-meter resolution requires a certain minimum bandwidth to ensure that it will stream properly, forced routing may need to be invoked at the application layer. Having an understanding of the level of network control is important to ensuring QoS from the sensor node to the NOC/COC. Information which is traveling through several DS domains with several SLAs already in effect or in the queue could suffer higher congestion levels and poorer QoS than information travelling through one DS domain with none or fewer SLAs. Knowing this network information ahead of time gives the IMOs several options. Static routing, which forces certain traffic flows to take certain routes, can be requested to provide for better QoS; likewise, the IMO annex to the OPORD could direct adjacent DS domains to provide a certain level of QoS through their domains for specific operations. In cases where the sensor nodes themselves are not in a position to transmit data through the sensor network, the IMO needs to understand the degree of maneuverability of the mobile sensors and must know how easily the static sensors can either be moved or new sensors placed in a more advantageous position. The IMO also needs to make recommendations for initial sensor

placement with respect to QoS assurances during the MCPP, taking into account that deployed static sensors can be used for more than one mission and for general battlespace awareness.

c. Data Flow Layer

The Data Flow Layer defines the quality level of the data flows from the sensor nodes to the NOC/COC and serves as the bridge between the physical layer and the SLA layer. During the planning phase, this layer can help the IMO and the communicators determine if the physical sensor layout and data paths will provide the QoS needed for proper functioning in the upper two layers. During execution, the metrics gathered from this layer will help both the network and the network operators determine if the current configuration is meeting the minimal QoS requirements, as defined in the SLA Information Layer requirements section. It is crucial that the three categories (average sensor to AO size ratio, ratio of nodes to gateways, and traffic flow data rates) are determined as accurately as possible during the planning phase, since the upper two layers depend on the accuracy of these figures to provide the necessary QoS for the commander and his staff. A failure at this level will cause a lag in the network’s ability to provide the needed QoS. Of the three categories, data rates are the easiest to reconfigure on the fly. Gateways can be added and new sensors can be implanted but this effort could siphon resources away from the supported operation.

d. Physical Layer

The Physical Layer defines the physical implementation of the sensor network with respect to the expected QoS levels needed in the above three layers to fully provide the commander and his staff with the level of QoS needed to support mission accomplishment. Knowing the sensor types, the potential number of sensors in the network, and their locations will provide the IMO with an idea of potential congestion points and an estimate of the number of network gateways and aggregate bandwidth needed to move the sensor information to the NOC/COC. This layer is the most dynamic since with IPv6, sensor nodes can enter and leave the network without human intervention through autoconfiguration. While the network itself will need to dynamically reconfigure itself to provide the best paths through the network, the planning effort must take this into account and the initial sensor network laydown must be designed to accommodate it. Referring back to Table 8, it is obvious that different missions and different-sized units will have different physical layer characteristics which are unique to each situation and which are based on the differences between each SLA in the other layers. Because terrain affects communication among nodes, it is easier to communicate across open terrain than it is in an urban environment.

Network size and density will also have an impact because a denser network offers more links to communicate across. While specific sensor node locations cannot always be determined, their general locations will be known, based on the OPORD’s scheme of maneuver. Gateway locations and

transmission media can then be planned accordingly. The NOC/COC's locations need to be determined as well, since all sensor node communications need to terminate in these facilities. It should be noted that any other users who need the information from these nodes should be able to access it through the unit's LAN rather than having to pull it from the sensor network.

Figure 31 is a summation of the sensor network taxonomy discussion as it applies to the IPv6 networking protocol. It is a "snapshot in time" on D-Day, at L-Hour, which is the date and time an amphibious landing begins. The upper third of the figure depicts a MEF conducting an additional three supporting simultaneous operations to ultimately ensure a successful amphibious landing. The landing has been deemed the main effort, while the remaining three operations are in support of it and are labeled as such. The arrows on the left side show how each level flows into the next.

In the SLA Layer, the data types supporting each operation are shown. These data types correspond to sensor types that will support the unit commander's information requirements. The classes of traffic field depicts how each operation will each have different quantities of traffic class. The flow label field emphasizes the fact that DiffServ is enabled in the tactical sensor network. DiffServ uses the flow label in the IPv6 header to set codepoints and Per Hop Behaviors (PHBs) that correspond to different units in the network. Assigned by the IMOs and monitored by the communications units, this information is loaded into the DiffServ-enabled network and is updated as operational needs

dictate. Routers read these flow labels and queue packets according to their priority, based on the pre-set codepoints and PHBs. The bottom third layer shows the IPv6 packet header, which facilitates the settings made in the SLA layer in order to support operational requirements by providing a means of answering the commander's information requirements.

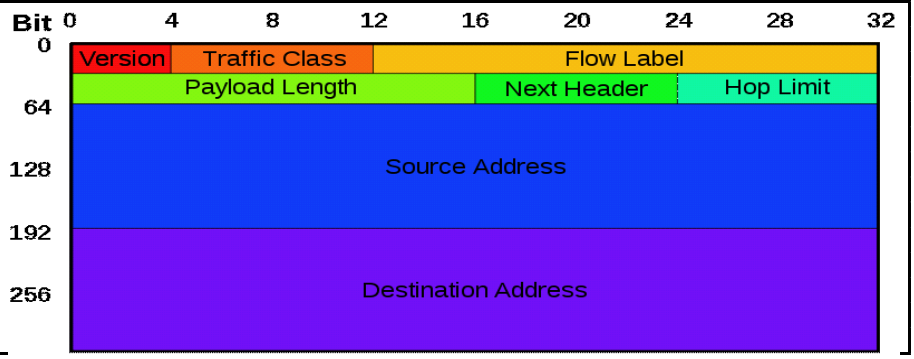
Supported Operations		**MEF-level Sustained High-tempo Operations at D-Day, L-Hour**			
	Unit/Mission	Infantry Battalion on the Offense	Air/Ground Reconnaissance	**Amphibious Landing**	MOUT
	Effort	Supporting	Supporting	**Main**	Supporting
↓		**Sensors employed to answer the Unit Commander's Information Requirements in support of the Operational Mission**			
SLA Layer	Data Types	Video, voice, application data (NBC, seismic, weather, blue force tracker), real-time data	Video, voice, application data (NBC, seismic, weather, blue force tracker), real-time data	**Video, voice, application data (NBC, seismic, weather, blue force tracker), real-time data**	Video, voice, application data (NBC, seismic, weather, blue force tracker), real-time data
	Classes of Traffic	Low	Medium	**Increasing**	High
	Flow Label (DiffServ enabled)	SUPPORTING EFFORT#3 Unit assigned Codepoints/PHBs have BEST EFFORT delivery priority	SUPPORTING EFFORT#1 Unit assigned Codepoints/PHBs have BEST EFFORT delivery priority after the MAIN EFFORT	**MAIN EFFORT: Unit assigned Codepoints/PHBs have OVERALL priority in the DiffServ enabled IPv6 sensor network**	SUPPORTING EFFORT#2 Unit assigned Codepoints/PHBs have BEST EFFORT delivery after SUPPORTING EFFORT#1
↓		**IPv6 packet header (Figure 2) showing the Flow Label used by DiffServ to prioritize packets in the tactical sensor network**			
IPv6 Protocol Header	Flow Labels are assigned a Codepoint/DHCP based on the destination address. The network will read the flow labels and queue and forward packets based on the assigned level of priority.				

Figure 31. Operational Application of the IPv6 Protocol in a Tactical Sensor Network.

V. CAMPAIGN OF EXPERIMENTS FOR IPV6 SENSOR NETWORKING STUDIES

A. INTRODUCTION

The Command-and-Control Research Program (CCRP) publishes a series of books aimed at researching and defining how the DoD can take advantage of and apply emerging technologies in the Information Age. Concepts such as Network-Centric Warfare and Agile Organizations have been the subjects of much research and subsequent publication. Another area that the CCRP addresses as part of its Information Age Transformation Series is how experimentation can be applied to the DoD to build synergy between the needs of the DoD and the technology being researched. Experimentation is considered to consist of three separate, distinct, yet related purposes: Discovery, Hypothesis Testing, and Demonstration. Experimentation begins as vague, immature ideas and evolves to useful knowledge from which doctrine; tactics, techniques, and procedures (TTPs); and standard operating procedures (SOPs) are developed, or which adds to more abstract theory. These three purposes have since evolved to produce the four phases of an experiment campaign: formulation, concept definition, refinement, and demonstration (Alberts & Hayes, 2005).

Formulation is the seed of an idea and can originate from multiple sources. Ideas from journals, ideas tried during field exercises, or the latest hardware devices or software applications can serve as the genesis of discovery

experiments. At this stage, the campaign is scoped, the initial problem is stated, and the planning effort is started.

Concept definition, the next step, produces the conceptual model, resulting from considerable research and several design iterations; the rest of the campaign is based on these. This step requires so much research and so many design iterations and research method specifications because the goal is to produce a quality, robust model worthy of the time and resources dedicated to the campaign.

The refinement stage consists of “robust, rigorous hypothesis testing on both the concept itself and how the concept will be applied” (Alberts & Hayes, 2005). Testing at this phase must show broad concept application in addition to the innovative use of the application, or the experiment risks being labeled as “stove-piped” or too narrowly defined. Both the concepts of command and control (C^2) and information technology are very broad in scope and have many, many different applications in DoD alone. C^2 can cover the range of military operations from two-man teams to theater-wide commands. Information technology applications, such as the TCP/IP protocol, are designed for use in all manner of networking applications. The breadth and depth of the application must be determined at this stage.

The final stage, demonstrations, displays the newfound concepts to users who will either incorporate the concept as is, or further develop it for their own unique purposes. Three experiments for the refinement phase are briefly proposed while Experiment Four, the capstone, is explained in greater detail.

Figure 32 depicts the overarching structure used to design this particular experiment campaign. Shown as a networking adaptation model, the familiar seven-layer OSI model is incorporated in a large feedback loop with two "control entries" at the application and physical layer and three "measurement entries" at the transport, network, and data link layer.

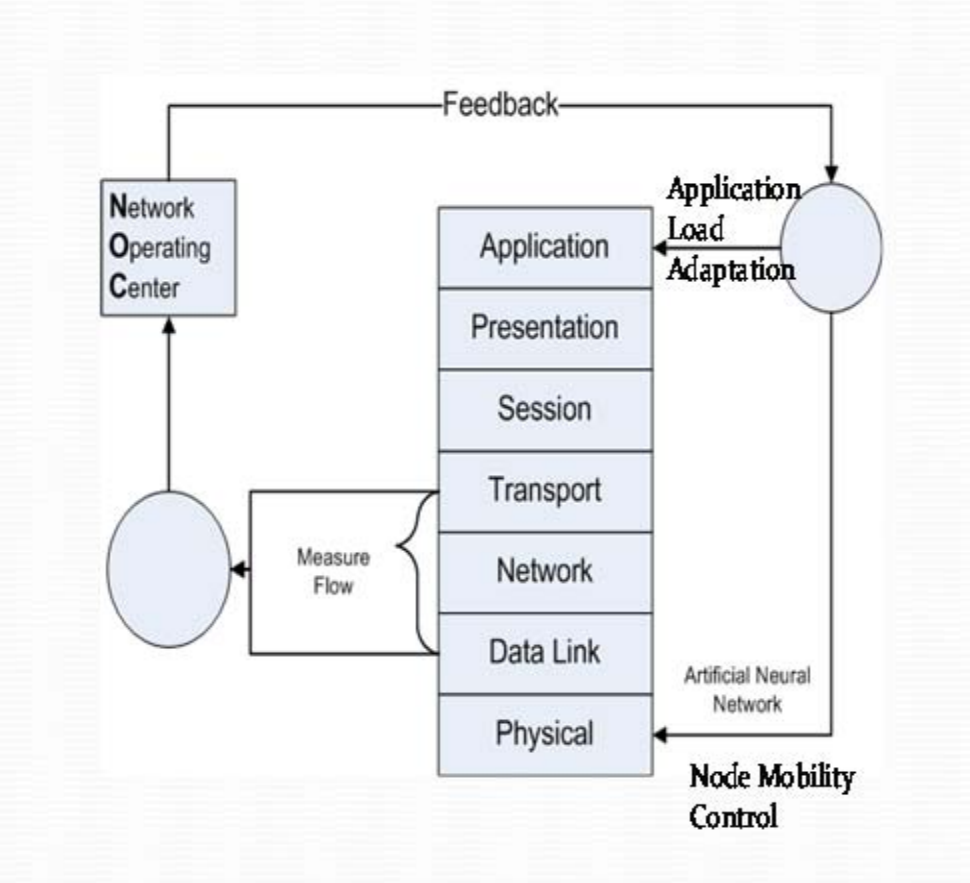


Figure 32. Layers of Adaptation in the TNT Testbed: the Adaptive Management Interface (From Bordetsky & Netzer, 2009).

Bordetsky and Netzer (2009) in "TNT Testbed for Self-Organizing Tactical Networking and Collaboration" developed this model to show how networks can adapt to their environments, as well as allow users to "have [a] unique

capability of exploring possible adaption patterns, i.e., management of their resources by experimenting with applications load or physically moving and re-aligning their assets". The design of the sensor networking experiment campaign that follows was based on this unique thought process and subsequent model. The experiment control variables were derived from the application and physical layers while measurable parameters were selected from the three measurable layers. The selected variables and parameters follow in subsequent sections.

IPv6 sensor networks that are based on an adaptive networking model, such as the adaptive management interface shown in Figure 32, will provide users with a network that can operate in a more robust and survivable manner especially during fluid, unpredictable combat operations. The TNT testbed introduced in Chapter II provides a unique opportunity to explore networking applications using the adaptive management interface model in a plug-and-play environment to define the boundaries of this model and of applications based on it.

B. EXPERIMENT ONE: DETERMINE THE SENSOR NETWORK TESTBED'S BEST-EFFORT CHARACTERISTICS WITH INCREASING LEVELS OF TCP AND UDP NETWORK TRAFFIC

1. Purpose

A baseline for network best-effort performance only needs to be established in order to determine the network's performance characteristics. The network testbed adapted from Bouras et al.'s (2009) work in "QoS Issues in al Large-scale IPv6 Network" is a native IPv6 network with foreground

traffic generators (both OSI layer four TCP and UDP data) passing data through an IPv6 exercise network and then ultimately to a traffic receiver. The traffic generators could be augmented with a combination of live or recorded UAV feeds, ground sensor feeds, and mobile sensor feeds. Adjacently, a background traffic generator passes background data through the same network to its own receiver, bypassing the IPv6 exercise network. QoS mechanisms such as DiffServ are implemented on several routers inserted between the traffic generators.

These routers are connected through a link to a bandwidth appropriate to that of a sensor network. TCP traffic and UDP streaming traffic is then passed through the network at increasing levels while several parameters are measured by means of a packet analyzer sitting astride the network at the receiver end. For the purposes of this experiment, the QoS features will be turned off so as to measure the best-effort performance. The QoS experiments to follow will be compared against this network baseline to analyze what techniques are working and how well they are working.

2. Parameters Measured

Table 10 is a compilation of the parameters to be measured by Experiment One.

Name	Model Layer	Description	Units
Congestion	Network	A measure of packet loss and throughput	Bits/second
Jitter	Network	Fluctuation in source to destination delivery within the same data stream – UDP traffic	Microseconds
Average Throughput	Network	The quantity of traffic that passes a point on the network in one second.	Bits/second
Packet loss	Network	The overall number of packets lost compared to the total number of packets transmitted.	Bits
Packet reordering	Network	Measured as a ratio of the number of packets that are delivered out of order to the total number of packets	Bits
Flow Retransmit Cost	Network	The percentage of traffic that must be resent for a given application	Percent

Table 10. Experiment One Parameters Measured.

3. Parameters Controlled

Table 11 is a compilation of the controlled variables for this experiment. The traffic will be steadily increased as the parameters in Table 10 are measured or derived through the use of a packet analyzer.

Name	Model Layer	Description	Units
Foreground Traffic (UDP and TCP)	Application	MTU's transmitted over the network to simulate various levels of network use. Both TCP and UDP are common transport layer protocols.	Bits per second
Background Traffic (UDP and TCP)	Application	MTU's transmitted over the network to simulate various levels of network use. Both TCP and UDP are common transport layer protocols.	Bits per second

Table 11. Experiment One Control Variables.

4. Performance Criteria

This experiment will be conducted to establish a best-effort delivery network baseline.

C. EXPERIMENT TWO: DETERMINE THE SENSOR NETWORK'S QOS CHARACTERISTICS WITH ONE APPLICATION ON A NETWORK WITH INCREASING AND VARIABLE LEVELS OF NETWORK CONGESTION

1. Purpose

The scenario applicable to this experiment is a military, law enforcement, or emergency services commander or staff officer, a user, who needs to pull sensor imagery or a real-time sensor feed from a single source through a network that is delivering different levels of best-effort delivery traffic to various destinations. That single source could be a single UAV feed, a single ground video camera, or a single cluster of homogenous sensors. In this case, the user wants one specific feed and needs to have a specific QoS to maintain a certain level of performance guarantee. This performance level is affected by several factors

outside the application’s control. The network’s resource availability is increased or decreased based on other users pulling their own feeds, the state of the network, and the performance of the sensor nodes themselves. These issues are transparent to the user, who is not only unaware of the network’s state, but does not need to know or care. Application performance and getting the needed information is the priority.

This experiment expands on Experiment One by implementing the QoS mechanism in the router and then measuring the performance variables as one real-time application is streamed from one end of the testbed to the other. The application will be streamed from the foreground traffic generator from a real-time feed such as UAV, ground sensor, or a mobile sensor feed as background network traffic will be generated to simulate varying network conditions. One method of ensuring QoS in streaming real-time data is the use of the flow label in the layer three header.

The 24-bit flow label, marked with the appropriate Differentiated Service CodePoint (DSCP) value to differentiate one traffic class from another traffic class, provides the routers with a quick method of determining the packet’s QoS level. The real-time streaming data will have one pre-set DSCP value while the background traffic will have another. This experiment uses the same mechanism to differentiate the foreground streaming traffic from the background-simulated traffic. As these packets traversed the network, the intervening network devices queued the traffic based on these values. As part of this experiment, the background traffic will be steadily increased until the

network becomes too congested to easily pass the streaming real-time traffic. The foreground traffic will be then increased and the background traffic measurements will be repeated until network congestion again precludes the minimum application performance requirements. The foreground traffic will be increased until the bandwidth exceeds the capacity of the sensor network maximum bandwidth.

2. Parameters Measured

Table 12 is a compilation of the parameters to be measured during Experiment Two.

Name	Model Layer	Description	Units
Congestion	Network	A measure of packet loss and throughput	Bits/second
Jitter	Network	Fluctuation in source to destination delivery within the same data stream	Microseconds
Average Throughput	Network	The quantity of traffic that passes a point on the network in one second.	Bits/second
Packet loss	Network	The overall number of packets lost compared to the total number of packets transmitted	Bits
Packet reordering	Network	Measured as a ratio of the number of packets that are delivered out of order to the total number of packets	Ratio
Flow Label Traffic	Network	Percentage of different DSCP values contained in the IPv6 header for DiffServ architectures compared to total packets sent	Percentage

Name	Model Layer	Description	Units
Flow Retransmit Cost	Network	The percentage of traffic that must be resent for a given application	Percent

Table 12. Experiment Two Parameters Measured.

3. Parameters Controlled

Table 13 is a compilation of the controlled variables for this experiment. The traffic will be steadily increased as the parameters in Table 12 are measured or derived through the use of a packet analyzer.

Name	Model Layer	Description	Units
Foreground Traffic (UDP and TCP)	Application	MTU's transmitted over the network to simulate various levels of network use. Both TCP and UDP are common transport layer protocols. Streamed generated traffic or real-time traffic	Bits per second
Background Traffic (UDP and TCP)	Application	MTU's transmitted over the network to simulate various levels of network use. Both TCP and UDP are common transport layer protocols.	Bits per second
Total Available Bandwidth	Physical	Maximum network bandwidth available	Bits per second

Table 13. Experiment Two Control Variables.

4. Performance Criteria

The following criteria will be used as a measure of streaming data performance and can be viewed on a level

higher than those monitoring network performance characteristics in the NOC; this is what users see and are interested in. Optimal performance for voice is a clear, intelligible sound from the distant end devoid of “pops,” delay, or broken/inaudible sound. Likewise, optimal performance for streaming video is a clear screen devoid of latency and jitter. While it should be noted that video is more flexible than voice, video also requires more bandwidth than voice does.

Name	Description	Max/Min
Uninterrupted, high quality, real-time data streaming	Streaming data will not suffer from latency or jitter and will be viewed in real-time from any source in the network	Max (0% latency or jitter)
High-value information delivery	Critical information from any source in the network will be delivered to its destination without delay	Max (0% delay)

Table 14. Experiment Two Performance Criteria.

D. EXPERIMENT THREE: DETERMINE THE SENSOR NETWORK’S QOS WITH MULTIPLE REAL-TIME APPLICATIONS WITH INCREASING AND VARIABLE LEVELS OF NETWORK CONGESTION

1. Purpose

The applicable scenario is a commander or staff officer, a user, who needs to pull sensor imagery or real-time sensor feeds from multiple sources through a network that is delivering different levels of traffic to various destinations. In this case, the user wants more than one specific feed and needs to have a certain QoS level to

guarantee at least the minimal network resources. The network's demand will be increased or decreased based on other users pulling their own feeds, the state of the network, and the performance of the sensor nodes themselves. This experiment expands on Experiment Two by adding real-time feeds to the testbed architecture in order to determine how the network will deliver multiple real-time applications and support associated performance criteria. The foreground traffic generator will add alternate real-time traffic as the background network traffic is generated to simulate varying network conditions. The background traffic will initially be set to a low level. The foreground traffic will start with one streaming application and will then be increased as more and more real-time applications are streamed across the testbed via the foreground traffic generator until the network becomes too congested to easily pass the streaming real-time traffic. The background traffic will then be increased and the foreground traffic experiment will then be repeated. When the background traffic generator produces too much network congestion to pass more than one application the experiment concluded.

2. Parameters Measured

Table 15 is a compilation of the parameters to be measured during Experiment Three.

Name	Model Layer	Description	Units
Congestion	Network	A measure of packet loss and throughput	Bits/second
Jitter	Network	Fluctuation in source to destination delivery within the same data stream	Microseconds

Name	Model Layer	Description	Units
Average Throughput	Network	The quantity of traffic that passes a point on the network in one second	Bits/second
Packet loss	Network	The overall number of packets lost compared to the total number of packets transmitted.	Bits
Packet reordering	Network	Measured as a ratio of the number of packets that are delivered out of order to the total number of packets	Ratio
Flow Label Traffic	Network	Percentage of different DSCP values contained in the IPv6 header for DiffServ architectures compared to total packets sent	Percentage
Flow Retransmit Cost	Network	The percentage of traffic that must be resent for a given application	Percent

Table 15. Experiment Three Parameters Measured.

3. Parameters Controlled

Table 16 is a compilation of the controlled variables for this experiment. The traffic will be steadily increased by the number of streaming data applications, as the parameters in Table 15 are measured or derived through the use of a packet analyzer.

Name	Model Layer	Description	Units
Foreground Traffic (UDP and TCP)	Application	MTU's transmitted over the network to simulate various levels of network use. Both TCP and UDP are common transport layer protocols. Streamed generated traffic or real-time traffic	Bits per second
Background Traffic (UDP and TCP)	Application	MTU's transmitted over the network to simulate various levels of network use. Both TCP and UDP are common transport layer protocols.	Bits per second

Table 16. Experiment Three Control Variables.

4. Performance Criteria

The following criteria will be used as a measure of streaming data performance. Optimal performance for voice is a clear, intelligible sound from the distant end devoid of "pops," delay, or broken/inaudible sound. Likewise, optimal performance for streaming video is a clear screen devoid of latency and jitter. Here again, while it should noted that video is more flexible than voice, video also requires more bandwidth than voice does. For the purposes of Experiment Three, more than one application will be monitored for QoS.

Name	Description	Max/Min
Stream multiple high image feeds from various sources	The commander and staff can view one or more data streams from multiple sources without having to shut down one or more sources to ensure “best effort delivery”	Max
Uninterrupted, high quality, real-time data streaming	Streaming data will not suffer from latency or jitter and will be viewed in real-time from any source in the network	Max
High-value information delivery	Critical information from any source in the network will be delivered to its destination without delay	Max

Table 17. Experiment Three Performance Criteria.

E. EXPERIMENT FOUR: DETERMINE THE SENSOR NETWORK’S QOS CHARACTERISTICS WITH MULTIPLE-USERS AND MULTIPLE SLAS WITH INCREASING AND VARIABLE LEVELS OF NETWORK CONGESTION. THIS IS THE CAPSTONE EXPERIMENT FOR THIS CAMPAIGN

1. Purpose

The applicable scenario builds on this paper’s opening scenario and can be found in Chapter IV, Section D, Paragraph 2a. This experiment expands and builds on the three previous experiments by adding more granularity to the levels of QoS in order to determine how the IPv6 sensor network will support SLAs. Experiments Two and Three differentiated network traffic levels by dividing traffic into best effort and priority by manipulating the DSCP values in the IPv6 header. All priority traffic cannot be considered equal or with equal queuing considerations, since different data types have different bandwidth requirements

and users may wish to prioritize one data type or one set of mission-related data streams over another. This experiment will explore this further classification of priority traffic by manipulating location, node density, time, source and destination nodes, information quality level, and application bandwidth requirements to determine how those manipulations are affected by a dynamic network simulated by the background traffic generator and competing SLAs.

2. Baseline SLA

A baseline SLA incorporating all of the parameters in Table 18 will be established based on Experiments One through Three and will be the cornerstone to which all other SLAs modified in this experiment will be compared.

Name	Model	Description	Setting
Sensor Node Location	Physical	The node's distance from the gateway as measured by the number of sensor node hops	Hops
Sensor Node Density	Physical	The ratio of sensor nodes to gateways	Ratio
Information Requirements	8th Layer	Information priority level, determined by appropriate tags	Scale
Bandwidth requirement of communication service	8th Layer	Video, voice, imagery, or file transfer for the specific SLA	Bits/second
Information Quality Level	8th Layer	Dependent on the type of communication	Video: pixels, bits of color,

Name	Model	Description	Setting
		service contained in the SLA	latency in seconds Voice: Bits/second, latency Imagery, File Transfer: Bits/second
Time interval	8th Layer	The time the SLA is in effect	Seconds
SLAs	8th Layer	The number of SLAs in effect on the network	Number

Table 18. BSLA Settings.

This baseline SLA (BSLA) will be tested in the same manner as Experiment Two. Foreground traffic with the BSLA will be streamed as the background traffic is systematically stepped up until the SLA cannot support the user's QoS requirement. Once that threshold has been achieved, the bandwidth level of foreground traffic is stepped up and the experiment with the increasing background traffic is repeated. From this data, a threshold curve will develop which will show QoS of steamed data at the BSLA as a function of the level of background traffic.

3. Experiment

The experiment will then continue by using the live feeds contained in the scenario to determine which control parameters should be manipulated to increase the threshold and thereby to provide the user with the requisite QoS in

the face of increasing background traffic for each level (bandwidth) of foreground traffic. For example, if the key sensor nodes were moved, the bandwidth could increase because of a better line of sight (LOS) to the gateway. Reducing the SLA latency or the image resolution request by a fraction could increase the overall throughput and therefore maximize uninterrupted, high quality, real-time data streaming performance overall. A relationship may develop between increasing the density of sensor nodes and/or gateways, network load balancing, and QoS. Better SLA management may prove to be useful as well. If separate SLAs are overlapping, and therefore competing for the same network resources, they could be combined to share sensor information with several requesting users. An online collaborative tool would be useful for this purpose. A user could query an SLA database and see all pending and active SLAs to determine if he could “piggyback” on one of these, request an extension to an SLA, or use one as a template from which to build a new one.

Likewise, the SLAs could be linked to the database where information/knowledge gained from expired SLAs could be pulled. Finally, SLA network metrics could be obtained for QoS performance analysis. The goal is to determine what parameters can be manipulated to fulfill the QoS requirement in light of the dynamic network and is also to attempt to shift the improved SLA (ISLA) curve to the right, in effect, providing more QoS per level of background traffic as compared to the generic BSLA curve.

The culmination of this experiment campaign is to determine how to support multiple ISLAs streaming through the network at the same time. The experiment will then

continue by determining which design parameters should be manipulated in order to increase the performance threshold. These discovered parameters will then provide more resources to the separate SLAs, at the requisite QoS, in the face of increasing background traffic for each level (bandwidth) of foreground traffic and with other SLAs in competition for the same network resources

4. Parameters Measured

Table 19 is a compilation of the parameters to be measured during Experiment Four.

Name	Model Layer	Description	Units
Congestion	Network	A measure of packet loss and throughput	Bits/second
Jitter	Network	Fluctuation in source to destination delivery within the same data stream	Microseconds
Average Throughput	Network	The quantity of traffic that passes a point on the network in one second.	Bits/second
Packet loss	Network	The overall number of packets lost compared to the total number of packets transmitted.	Bits
Packet reordering	Network	Measured as a ratio of the number of packets that are delivered out of order to the total number of packets	Ratio
Flow Label Traffic	Network	Percentage of different DSCP values contained in the IPv6 header for	Percentage

Name	Model Layer	Description	Units
		DiffServ architectures compared to total packets sent	
Flow Retransmit Cost	Network	The percentage of traffic that must be resent for a given application	Percent

Table 19. Experiment Four Parameters Measured.

5. Parameters Controlled

Table 20 is a compilation of the controlled variables for this experiment. Each variable is assigned a controlling entity or a role player who is responsible for manipulating or stipulating the conditions to cause SLA success and to thus meet the performance criteria outlined in Table 21.

Name	Model Layer	Description	Units	Roles
Sensor Node Location	Physical	The node's distance from the gateway as measured by the number of sensor node hops	Hops	Sensor Operating Unit, IMO, G3
Sensor Node Density	Physical	The ratio of sensor nodes to gateways	Ratio	G6
Information Requirements	8th Layer	Information priority level, determined by appropriate tags	Scale	Requesting Unit/IMO/G6
Bandwidth	8th Layer	Video, voice,	Bits/second	Requesting

Name	Model Layer	Description	Units	Roles
requirement of communication service		imagery, or file transfer for the specific SLA		Unit
Information Quality Level	8th Layer	Dependent on the type of communication service contained in the SLA	Video: pixels, bits of color, latency in seconds Voice: Bits/second, latency Imagery, File Transfer: Bits/second	Requesting Unit/IMO/G6
Time interval	8th Layer	The time the SLA is in effect	Seconds	Requesting Unit
SLAs	8th Layer	The number of SLAs in effect on the network	Number	IMO,G3,G6
Foreground Traffic (UDP and TCP)	Application	MTU's transmitted over the network to simulate various levels of network use. Both TCP and UDP are common transport layer protocols. Streamed generated traffic or	Bits per second	Exercise Controller

Name	Model Layer	Description	Units	Roles
		real-time traffic		
Background Traffic (UDP and TCP)	Application	MTU's transmitted over the network to simulate various levels of network use. Both TCP and UDP are common transport layer protocols.	Bits per second	Exercise Controller

Table 20. Experiment Four Control Variables.

The roles are defined as follows:

- Sensor Operating Unit: A generic term for the individual unit responsible for initially placing the static nodes, moving the mobile ground sensors, flying the UAV, or wearing sensor-adorned battlesuits. Units, such as reconnaissance and sniper teams, or VMU's can be tasked by the higher headquarters COC, on the advice of the G6 and IMO, with placing sensors or moving sensors in accordance with TTPs, SOPs, the operations order, and the current situation as dictated by Mission, Enemy, Time, Terrain and Weather, Troops and Fire Support Available, Space, and Logistics (METT-TSL).

- IMO: The Information Management Officer sets the Information Management policy in accordance with the MEF operations order, TTPs, SOPs, and the current situation.

- The IMO at each level can make recommendations to their respective operations section and higher and adjacent IMOs to move sensors to best support the ISR plan within their area of operations (AOR).
- SLA approval and management: The IMO collects, evaluates, manages, and forwards SLAs submitted by subordinate units. The IMO also resolves conflicts with competing SLAs within the G3’s scheme of maneuver with the advice of the G6.

- G3: The MEF operations section responsible for the conduct of all MEF operations. This is the supported section which the communications, ISR, and IMO plan must support. The IMO and G6 need G3 approval to make any changes to their operations.
  - The G3 is responsible for ensuring that the SLAs are synchronized with ongoing operations and are included as part of the operational sync matrix.
- G6: The MEF communications section is responsible for planning, installing, operating, and maintaining the MEF communications network.
  - The G6 has responsibility for the network and must support the G3 and the IMO’s plan within the physical limits of network capabilities. Network changes that will affect operations need approval from the G3.
  - G6 support to SLA approval and management: The G6 advises the IMO on the network’s status and ability to support submitted SLAs.

- SLA execution: The G6 is responsible for monitoring SLA execution and will advise the IMO when QoS levels fall outside of the expected level of service.

- IMO cell: A group headed by the IMO and consisting of a G3 representative, a G6 representative, and a G2 (MEF Intelligence Section) representative, which makes decisions concerning the MEF's information flow in support of operations.

- Requesting Unit: The unit requesting the SLA for uninterrupted, real-time data in support of an operational task. A battalion is the lowest level unit authorized to submit an SLA to higher headquarters for action and approval.

  - The battalion operations officer, S3, in conjunction with the battalion communications officer, S6, and in the context of the higher headquarter's operation order consolidates the battalion's requirements, drafts, and submits the battalion's SLA request(s).

  - The battalion monitors the feed for SLA QoS performance feedback.

- Exercise Controller: The exercise controller controls the level of traffic generated by the foreground and background traffic generators. They are also responsible for monitoring, recording, and deriving the parameters detailed in Table 19 with the use of a packet analyzer, such as Wireshark.

6. Conduct of the Experiment

Combining this experiment's technologically oriented purpose with the tactical scenario, a notional construct of a MEF staff, subordinate commands, and the sensor network will be used to determine two things. First, it will determine how the IPv6 sensor network will support multiple SLAs by adding more granularity to the QoS levels. Second, it will determine how the sensor network's QoS characteristics including multiple-users and multiple SLAs with increasing and variable levels of network congestion will provide the MEF IMO cell with the ability to support multiple SLAs over an extended period.

This experiment incorporates additional tactical role players to simulate one MEF staff (G2, G3, G6, and IMO), one division staff (G2, G3, G6, and IMO), one ACE staff (1 person), one FSSG staff (1 person), 2 regimental staffs (S2, S3, S6, and IMO), and four battalion staffs (CO, S2, S3, S6, and IMO); real-time sensor feeds from several static locations, several ground mobile sensors, and two UAV feeds in addition to the foreground and background traffic generators; and a change in location to an exercise area such as Camp Roberts, California. This location allows the sensor network to be set up over a wide area and has use of airspace for UAV flights. Over the course of seven days, staffs subordinate to the MEF will be given a partial operations order at the beginning of the experiment and fragmentary orders thereafter. From these orders, they must derive their own concept of operations and their information management plan. Part of this plan requires supporting the ISR effort and building SLAs that will support crucial parts

of the operation. The IMO cells at intervening levels will attempt to sync the SLAs with operations and the MEF IMO cell will do the same in addition to sequencing the requests.

During this process, the exercise controllers are independently manipulating foreground and background traffic to simulate network variability and a common network rhythm that syncs the normal flow of best-effort delivery traffic with ongoing operations. For example, if the MEF is heavily engaged in combat operations all over its AOR, the network would be heavily used if not actually approaching high levels of congestion. At the other end of the spectrum, if very little action were occurring the network would be relatively “quiet.” The exercise controller adjusts the level of traffic generated by the foreground and background traffic generators and will use a packet analyzer to monitor the parameters in Table 19.

Keeping within the play of the scenario, combat operations will start off slowly as the MEF develops and secures its footprint, and will then rapidly increase combat operations to achieve the increased operations tempo desired by the CG. Network traffic will therefore be minimal in the beginning, with few active SLAs. As operations continue, the network will become more taxed, SLA requests will increase proportionally, and performance will begin to suffer as a result. If at any point in the experiment the network cannot support the SLAs as requested, the role models, with the exception of the exercise controllers, will adjust the variables under their control detailed in Table 20 so as to provide the optimal performance levels as shown in Table 21.

7. Performance Criteria

The following criteria provide a measure of streaming data performance. Optimal performance for voice is a clear, intelligible sound from the distant end that is devoid of “pops,” delay, or broken/inaudible sound. Likewise, optimal performance for streaming video is a clear screen devoid of latency and jitter. As above, while it should be noted that video is more flexible than voice, video also requires more bandwidth than voice. Each SLA will need to meet all of the requirements outlined in Table 21 and will need to meet the expectations of the requesting Infantry Battalion(s) in order to be considered successful. The evaluators are defined as follows:

- Battalion Commander (CO): The officer ultimately responsible for everything the battalion does and fails to do. All correspondence and requests, to include SLAs, are submitted in his name. As the “SLA customer” it is his opinion, backed up by facts, on whether or not the SLA meets its intended performance criteria. The Battalion Commander is a consumer of the information that is obtained and derived from the networked sensors and from the analysis conducted from his staff.

- Battalion Staff: The principle officers responsible to the CO for their individual staff sections. The battalion staff is three abstractions below that of the MEF staff. The staff uses the information obtained and derived from the networked sensor to then update the situational status within their AOR.

- Subordinate Commanders: The officers commanding companies within the battalion. They work directly for the CO and will be consumers of the products from the battalion staff and possibly from the sensor feeds themselves.

Name	Description	Max/Min	Evaluator
Stream multiple high image feeds from various sources	The commander and staff can view one or more data streams from multiple sources without having to shut down one or more sources to ensure “best effort delivery”	Max	Battalion Commander, Staff, and subordinate Commanders
Uninterrupted, high quality, real-time data streaming	Streaming data will not suffer from latency or jitter and will be viewed in real-time from any source in the network	Max	Battalion Commander, Staff, and subordinate Commanders
High-value information delivery	Critical information from any source in the network will be delivered to its destination without delay	Max	Battalion Commander, Staff, and subordinate Commanders

Table 21. Experiment Four Performance Criteria.

VI. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

Large-scale, dynamic sensor networks provide a wealth of information to users who need that information to plan, execute, and monitor the full range of military operations. Real-time information collected and forwarded from UAVs, ground sensors, battlesuits, mobile video sensors, and other environmental collection devices to traditional NOCs and COCs provides commanders and their staffs with a virtual picture of the battlespace and surrounding areas of interest. This view thus provides an information advantage from which rapid-tempo combat operations can be generated. When those same sensor networks operate within the IPv6 domain, the increased capabilities of increased globally-unique addresses, end-to-end connectivity, autoconfiguration, and inherent security provide the commander with the ability to achieve a significantly more robust view of the battlespace and gain a significantly increased knowledge advantage from which a proportionate level of combat power can be generated.

Perhaps the most promising aspect of structuring sensor networks within the IPv6 domain is that QoS is an inherent functionality contained in the IPv6 header and can be used in conjunction with the proper QoS protocol architecture. QoS techniques, such as Differentiated Services, which are implemented in the native IPv6 network are able to label packets accordingly, examine the IPv6 headers as the packets move throughout the network, queue if needed, and then forward traffic flows based on preset levels of priority.

The SLA taxonomy developed in Chapter IV describes the hierarchical relationship between the commander's vision of how he wants his information requirements answered and how the traffic flows associated with those requirements can be given QoS priorities in a large-scale sensor network. SLAs developed from this vision and then implemented at the NOC provide the network the knowledge about which data streams have performance guarantees and, therefore, pre-set levels of QoS.

An IPv6 sensor network experiment conducted as part of the battlefield medical IPv6 sensor network experiment series during TNT 09-2 demonstrated the feasibility of operating sensors in a native IPv6 network. Throughout the course of preparation for the experiment, and during the experiment itself, the IPv6 protocol proved to be compatible with network sensor operations. No noticeable performance degradation between the IPv4 and IPv6 was detected which is qualitatively important from the commander's view. The huge IPv6 address space is ideal for networking sensors which can be accessed from anywhere in the world. Autoconfiguration is beneficial because it allows sensors to autonomously enter and leave the IPv6 network with little to no human intervention.

The following sections outline two separate but related approaches to continue studying the IPv6 QoS boundaries. The first proposal is a continuation of the battlefield medical experiment series, which seeks to determine the ranges at which critical messages begin to experience latency and then are no longer received at their intended destination. The second proposal uses the systems approach to explore the QoS boundary.

B. FUTURE CONSIDERATIONS: PROPOSED TNT IPV6 SENSOR NETWORK BATTLESUIT QOS EXPERIMENT

1. Purpose

This Battlefield Medical IPv6 Sensor Network field experiment is a feasibility study that leverages the architecture and successful discovery and constraints analysis step conducted during TNT 09-1 and -2 aboard Camp Roberts, California. The details and results of the 09-2 experiment can be found in Chapter III. The next logical step in the battlefield network sensor series is to begin to show how QoS techniques can be applied to sensor traffic flows. To do so, the boundary of traffic latency and packet loss must be explored.

2. Research Question

Given a selection of operational messages with levels of prioritization from routine through priority, immediate, and flash, a specified level of mission-critical streaming data, a native IPv6 network, a unit's specified number of battlesuits of a specified type of sensors, and an available level of aggregate bandwidth, at what point does priority traffic experience packet loss as mission-critical streaming traffic increases over the transmission link of a specified available bandwidth?

3. Discussion

A six-man reconnaissance team will wear battlesuits with different biometric sensors and a capability to transmit and receive data. These battlesuits will have intra-team connectivity with the other teams' battlesuits

and will rely on an aggregate pipe emanating from a local gateway for reachback and connection to the GIG. For the reasons stated in the Introduction to this thesis, the IPv6 protocol will be used for layer three Internet routing. Depending on a sensor's function, each will transmit messages to other battlesuits, a Network Operations Center (NOC), a battlefield medical collaboration team, or any other interested parties (see Figure 33). For example, one set of sensors can measure the battlesuit wearer's core temperature and transmit periodic messages. These messages can be routine for general-force health awareness, priority for an incident such as an increase in body temperature above an environmentally-driven threshold, immediate when the temperature has been above a threshold for a certain period of time, or flash when the battlesuit wearer's temperature indicates an immediate danger that requires immediate action or risks losing life and limb.

The message priority dictates which Quality of Service (QoS) level the message will have as it travels through the network. A message marked "immediate" will have a higher QoS level than a message marked "routine" and will therefore have priority of network resources to ensure that it gets to the destination node first. This makes sense. A battlesuit wearer with a dangerously high temperature needs to ensure that his message is not delayed, due to excessive TCP retransmissions or dropped altogether in the network by routine messages sent by the battlesuits of wearers who are "well." A second example of the necessity to differentiate QoS among common function sensors is the need to identify wearers who have suffered the effect of NBC contaminants. Those wearers need medical attention as soon as possible and

would need the flash precedence set so that their information is not waiting for less urgent traffic.

In addition to messages originating from battlesuit sensors, priority-marked messages also have to compete for bandwidth on the aggregate link with any other transmissions the recon team is transmitting. Voice communications, streaming video, static sensors placed by the team, and other units who may need use of the gateway will all contend for space on the aggregate pipe. Providing QoS by marking the priority messages originating from the battlesuits, both wearers and higher headquarters personnel can be assured that critical messages will not be delayed or lost.

The team will also have connectivity via their battlesuit sensors and single-channel voice radios to rear echelon units in addition to the video imagery. Table 1 displays a list of the type, frequency, and the QoS levels of the messages that the battlesuit can send. A majority of the messages sent from the team’s battlesuits will be considered routine so long as everything remains within the mission parameters that were developed during the team’s mission planning. The notes for Table 23 show that routine messages are sent with a low QoS rating, therefore, routine messages will not have any interference with streaming video data.

In cases of immediate or flash messages with a high or critical QoS, video streaming will no longer be the priority traffic. At some level, video streaming will begin to degrade in order for the network to route additional traffic.

4. Operational Topology

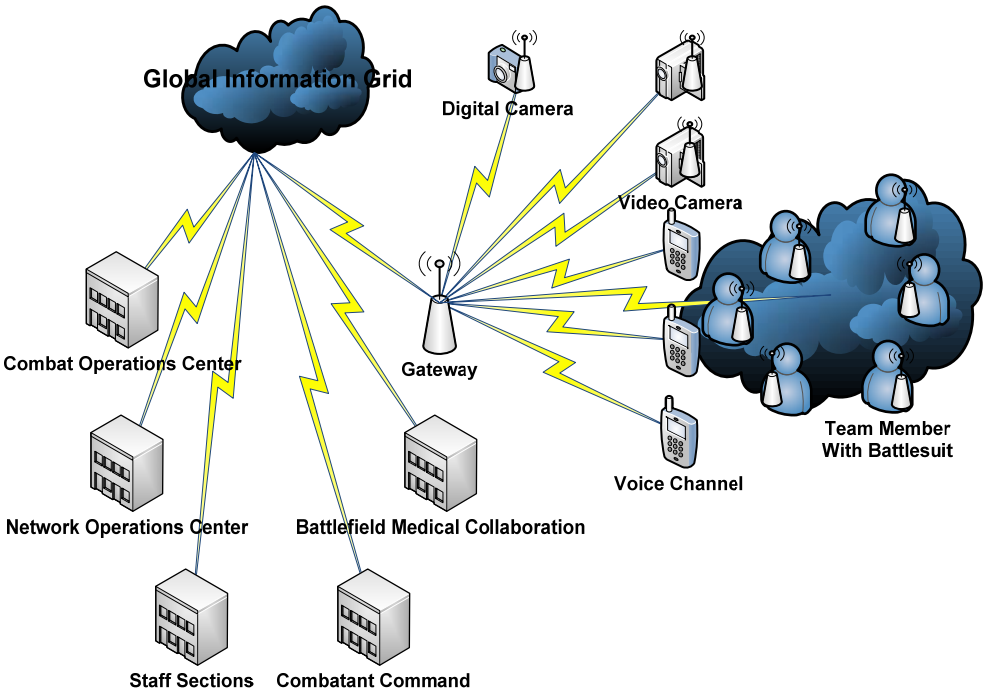


Figure 33. Operational Topology for Battlesuits.

a. Information Produced from the Communications Devices External to the Battlesuit

Message Type	Frequency	Latency Tolerance	QoS Level
Video	Streaming	High	Mission Dependent (High for this scenario)
Voice	Periodic	Low	Medium
Text Chat	Burst	High	Low
Image	Burst	High	Low

Table 22. External Communication Messages.

b. Information Produced from the Battlesuit Sensors

Type	Category	Frequency	Tolerance	QoS	Precedence
Core body temperature	Medical	Periodic		As noted	1,2,3,4
Hydration level		Periodic		As noted	1,2,3,4
O_2 level		Periodic		As noted	1,2,3,4
Perspiration level		Periodic		As noted	1,2,3,4
Heart rate		Periodic		As noted	1,2,3,4
Blood pressure		Periodic		As noted	1,2,3,4
NBC Contaminant and level	NBC	Periodic		High	2,3,4
NBC contaminant ingested and level		Periodic		Critical	4
Ambient Temperature	Environment	Periodic		As noted	1,2,3,4
Position/GPS		Periodic	High	As noted	1,2,3,4
Wind Speed		Periodic		As noted	1,2,3,4
Humidity		Periodic		As noted	1,2,3,4

Table 23. Battlesuit Messages.

Notes:

1. Precedence: Routine	QoS: Low
2. Precedence: Priority	QoS: Medium
3. Precedence: Immediate	QoS: High
4. Precedence: Flash	QoS: Critical

c. Communication Path

Each battlesuit has a communication path to every other battlesuit in the unit, as well as to the gateway to the GIG. The bandwidth to the gateway is determined by the unit that is conducting the mission; however, the available bandwidth of the link(s) from the gateway to the GIG point of entry will determine the aggregate data rate. This available bandwidth is mission-dependent.

d. Scenario

A six-man reconnaissance team has been inserted into a denied area for the purposes of surveillance and gathering intelligence on a target that is suspected to be in the area. A set of targets is suspected of planting IEDs in and among protected areas such as mosques, hospitals, and other areas deemed neutral zones. The team needs to record the target’s actions both in wide-view for general situational awareness and close-up view for identification purposes and then transmit that imagery for real-time viewing. In addition to the real-time intelligence evaluation carried out by intelligence analysts in a separate location, a legal team in yet another location needs to validate the target’s actions as illegal before action can be taken against the target. The imagery from the

two camera views and still images from the digital camera needs to be within certain parameters in order to provide irrefutable proof, and therefore a basis for follow-on action, of the target's activities. Likewise, the follow-on action needs to be documented to show that the appropriate actions were taken. Hence, the video quality needs be protected as it streams through the network by use of QoS mechanisms in the IPv6 protocol.

The team has set up their video imaging systems and has ensured that the imagery is being received in the manner needed. They have also received assurance that their battlesuits are communicating normally with each other and with the gateway to their higher headquarters. The team has received several reports indicating that the medical and environmental messages received show that everything is within normal parameters.

After a period of time, the target has appeared in the recon team's area of observation. The video and still image cameras pick up the imagery and are transmitting as required. Radio chatter with the intelligence and legal teams begins to increase as the activity level increases. The VHF nets are relaying through the gateway as well, using the Radio over IP network (RIPRNET), which requires a QoS level to maintain an intelligible conversation. The battlesuits begin to relay signs of increasing stress as heart rates begin to quicken. Some of the heartrates exceed what is considered normal, which elevates the QoS level of the packets associated with those messages. Confirmation comes from the legal team that the target's activity does warrant appropriate action. The recon team leader then calls

in air support to attack the target as it leaves the protected area. The attack must be video recorded as well as narrated by the recon team to provide proof that the protected area was not harmed. It is most critical at this point that the video and voice stream levels of QoS not suffer. At this point, a section of attack helicopters attack the fleeing targets, which causes the video imagery to increase its needed bandwidth in order to capture rapid movement and changes. The narration is quicker, which again stresses the data and voice streams that are transmitting to the higher headquarters viewing the video and hearing the narration. At that moment, two battlesuits begin sending medical alarms. The suits' wearers have been wounded in an ensuing small arms fight that has erupted in the vicinity of their position.

The recon team then returns fire on a previously unknown enemy security team that was providing cover for the target's IED activity. The battlefield medical collaboration team (BMCT) begins to evaluate the alarms from the battlesuits, project possible outcomes based on the situation, and collaborate among themselves regarding possible medical courses of action that could be taken should they need to intervene. One item that the BMCT can work on is alerting the hospital staff to injuries that they will have to treat when the team returns. This then allows the ER team to prepare, and to begin working faster. As this occurs, the wounded team members radio back that they are okay for the time being and will extract with the team.

The recon team leader has successfully serviced the fleeing target with the section of attack helicopters

and now asks for them to return and attack the enemy security team. The gunships do so which allows the recon team to maneuver and assault the enemy position. As that happens, an IED explodes and subsequently sets off other IED-making material that the enemy security team left behind. Because the IED exploded in the vicinity of a marketplace, there is a mass casualty situation. Secondary explosions have also severely wounded two more recon team members. The BMCT now has to go to work.

Following this event, voice messaging increases and video recording must continue; wounded team members also need medical attention that can be provided through their suits from the battlefield medical team. A UAV has just checked in on-station that needs to relay its video feed of the ensuing gunfight through the same gateway. In addition to these concerns, mission-critical video, audio, and messages with high precedence from the battlesuits must be delivered in the manner expected.

5. Experiment

a. Experimental Topology

The experimental topology is shown in Figure 34, below. The PelcoNet video system will stream video to the Video PC. This data stream will traverse the link between the two switches, which will have a data rate limit of X Mbps. The traffic generator will simulate varying levels of voice traffic traversing the link. The IPv6 Laptop with the Medical E-Tag will simulate the battlesuit by sending high priority messages with a QoS level; this will ensure that it

has priority while traversing the link. This experiment will make use of the IPv6 traffic class header and DiffServ to provide QoS in the network.

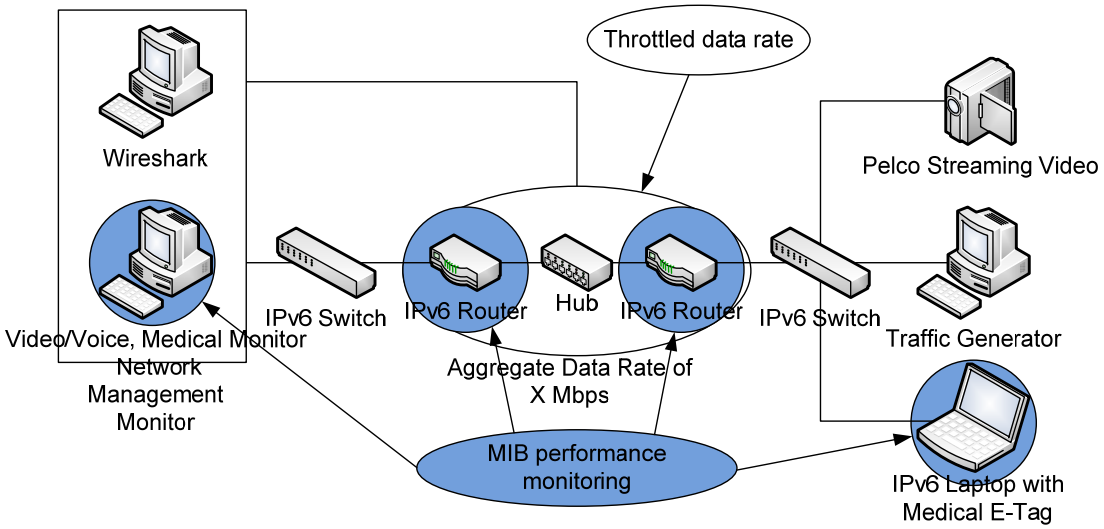


Figure 34. Experimental Topology.

b. Experiment

(1) Stream a given video data rate from the streaming video source and receive on the Video/Voice PC. Observe packet flow via Wireshark and on NMS.

(2) Stream a given level of background traffic via the traffic generator to simulate voice traffic (use XXX protocol) and receive on the Video/Voice PC. Observe packet flow on Wireshark and on NMS.

(3) Send messages with differing priority from the Medical E-Tag laptop to the Medical Monitor laptop and observe the video streaming and priority message performance parameters.

(4) Increase the voice traffic and then send the same differing priority messages as in (3), while observing the video streaming and priority message performance parameters.

(5) Repeat step (4) until the priority message traffic begins to experience latency in the form of dropped packets and requested re-transmissions.

(6) Repeat step (5) until the link is saturated in generated voice traffic and no priority messages are received at the distant end.

6. Expected Results

The research question was posed to determine the point at which priority traffic experiences packet loss as mission critical streaming traffic increases over a transmission link of a fixed bandwidth. Packet latency and loss can be considered acceptable in some sensor applications, such as routine building security surveillance, where a video image of someone approaching an unauthorized area is enough reason to warrant further investigation. High-quality network service is not necessary in this case. On the other hand, sensor applications such as those as described in this experiment, which require a high degree of granularity and fidelity for legal decisions, cannot accept packet latency or loss, because they can introduce doubt into the minds of those rendering a legal opinion based on what they see. For this application, it is of primary importance that the network support the operational needs to the extent that it can.

In this experiment, streaming video was defined as priority traffic, and battlesuit medical sensor information that passed predefined levels was defined as critical traffic. High-quality priority traffic is an operational necessity. The legal team needs to watch the streaming video in real-time in order to determine if the operation can proceed, as well as to preserve the video as evidence that the operation was legal, should it be challenged at a later time. In the scenario, critical traffic increases in response to the recon team’s health status. The experiment simulates this by increasing the generated traffic and observing both the streaming video and, later on, the aggregated results from the packet-capturing application. It is expected that priority traffic will begin to degrade both quantitatively and qualitatively once TCP-transported critical messages begin to “drop” and the TCP protocol begins requesting retransmissions. These retransmission requests will place an additional burden on a network which is already experiencing stress. Each retransmission request will require an answer from the source, which must now resend “old information” in addition to continually sending priority traffic and additional critical traffic. The experiment will reveal the point at which video quality degrades, qualitatively in the form of jitter as seen on the display screen, and quantitatively with the number of TCP retransmission requests sent and the number of packets dropped in the network. The operational personnel will be interested in the video quality, while the network operators will be interested in retransmission levels and in the point at which the network begins to drop packets and request retransmissions. It is possible that a meaningful

relationship exists among fixed bandwidth, priority and critical traffic data rates, and number of retransmission requests and packets dropped, which will aid network operators in developing network QoS applications.

C. FUTURE CONSIDERATIONS: SYSTEMS APPROACH TO QUALITY OF SERVICE

1. Sensor Network Topology

Adapting a large-scale sensor network so that it will function properly within the IPv6 address space requires a new application of QoS mechanisms. In this way, users can scope their view to a particular set or sets of sensor clusters and can pull real-time information, all while contending with a dynamic, continually-adapting network topology and with other demands that may be made on the network. While relatively untested, IPv6 appears to be the protocol of choice, as it inherently supports QoS with its “designed from the ground up” traffic class and the flow label fields which are contained in the IPv6 header; this is a functionality which was not practically implemented in IPv4.

This section will develop the experiment framework by using the multivariable analysis method, as described by Bordetsky et al. (2004), to determine the necessary design variables that bound a large-scale sensor network within the IPv6 domain, to determine the relationships that define QoS within a dynamic and adapting network, and to determine the performance criteria, which will then lead to optimizing QoS solutions in the dynamic environment.

One scenario contained in Chapter IV, a battalion in the offense, outlines a tactical application of sensor

networks in which the information collected by the sensor nodes and subsequently relayed back through the network to a command-and-control node, such as the Combat Operations Center (COC). This application was also used to speed up the initial observation, orientation, and decision-making cycle for a company commander (CO) who was preparing to conduct a deliberate assault on an objective through by using UDOPs. While in the attack and assault phases, the CO and supporting battalion staff have the ability to monitor changes in the environment, which allows the CO to adapt and act accordingly. These dispersed sensor nodes, the network they are part of, the information they collect and transmit, and the address space and capabilities provided by IPv6 all provide an exploitable tactical advantage for the CO in the conduct of his mission.

Different mission requirements, data types, and categories of streamed data all necessitate IPv6 compatible QoS mechanisms integrated within the network to provide acceptable levels of service. In the cases where various sensor nodes are clustered together to form multiple mission-specific or mission-tailored packages to provide real-time information, the network can become extremely congested due to these operational demands being placed on a dynamic network that is already attempting to adapt to provide best-effort service. Voice, imagery, data, and sensor data types require increasing degrees of QoS in order to sustain acceptable service. Time-sensitive, time-insensitive, and operational-level support are the three categories of streamed data in descending order. Routine voice data may be considered operational level support, since it does not have direct mission impact, while sensor

data is considered time-sensitive due to the necessity to properly time stamp sensor readings. Common QoS metrics to support mission information flow include the following: loss of data, regardless of the cause; latency; delay from source to destination; jitter or fluctuation in source to destination delivery; and throughput/bits per second (Wilson et al., 2005).

2. Sensor Network Model

There have been various types of protocols, approaches, and research connected to QoS in sensor networks in the IPv4 domain; however, this is less often the case in the IPv6 domain, due to its relative lack of widespread use. The QoS model described by Dohler (2007), the “adaptive network stack,” outlines a means of mapping from the familiar OSI model to the layered QoS model shown in Table 24.

OSI Model	QoS Stack	Metrics
8th Layer Hyper-Nodes	Telecommunications Management Network (TMN)	Self-diagnosis, sub-network view, QoS requirements response, SLA negotiation
Application Layer	Application/QoS functions	Node CPU speed, Node Buffer size, Flow size/delay/loss, Flow buffer, Flow Retransmit Cost
Network Layer	Network Performance Metrics	Node NIC Buffer size, Flow Path, Connectivity, Link MTU size, Link Reliability, Jitter, Packet Loss
Data Link Layer	Data Link Performance Metrics	Connectivity, Link Congestion
Physical Layer	Physical Layer Performance Metrics	Connectivity, Node NIC Speed, Link Quality, Link Speed

Table 24. The adaptive network stack (After Bordetsky, 2006; Clement, 2006; Wilson et al., 2005).

This model supports the application's QoS requirements by providing, at the uppermost layer, information about the state of the network so as to then determine the best way to adapt to the network's changing conditions. Through polling, each layer determines its metrics and then communicates with its adjacent layers to ultimately derive the state of the network, thus providing a path for an appropriate level of QoS. This "eighth layer" provides each sensor node with Network Operation Center (NOC) capabilities that can

effectively assure the network performance required. In other words, the eighth layer puts the network management function into the network one node at a time. Because large-scale sensor networks are complex, reducing latency caused by the human network operator's decision cycle through automating portions of the network-management function will improve overall QoS. Bordetsky and Hayes-Roth (2007) identified two limitations, and, thus, two areas on which to focus in order to ensure that the correct information reaches the correct destination, at the correct time: (1), limitations in bandwidth and (2), limitations in the ability of human decision makers to quickly process complex information and make decisions that will have the desired effect on the network. Therefore, as a result of its management function, the eighth layer, along with the physical layer, are the two layers that have controllable variables from which QoS can be achieved and maintained. The layers in between are governed by protocols that facilitate network operation and provide metrics via SNMP polling.

At the bottom of the stack is the physical layer, which transmits the frames received from the data link layer; this layer also sends frames to the data link layer after having received them from another node or nodes in the network. Mobile sensor nodes that are not able to communicate with the network can be repositioned in order to gain a better signal with other sensor nodes or the gateway. In the case of static nodes or mobile nodes not easily moved, the gateway can be moved to a more advantageous position or another gateway could be inserted. For this reason, the sensor node insertion-planning phase is important.

Because nodes can enter and leave the network due to recent implantation or destruction, variations can occur in signal propagation. Power fluctuations or losses can also occur, and mobility can change the data link and network layer topology. Sensors must continually determine new routes to the gateway and back to the destination node. In this regard, interlayer communication is especially important between the data link and network layer, particularly as the level of mobility increases, and as these layers relay their performance metrics to the upper-most layer. The function of the sensor node application layer is to gather the mission-specific data and push it down the stack for eventual transmission. When combined with the application layer QoS requirements, the information gathered from the model's performance metrics will provide the eighth layer with the input it needs to support the application's minimum QoS. The top layers' use of SLAs, as briefly discussed and used in the opening scenario of "Sensor Network QoS in an IPv6 Environment," provides a user or a group of users with a particular level of guaranteed service, for a specific time duration, over a specific area of the network (Dobrydney, 2008). These QoS assurances, managed from the NOC at the eighth layer, provide QoS configurations for mission-specific requirements such as real-time information flow from specific sensors or entire clusters of sensors. The information from all three layers within the QoS stack, as shown in Table 25, is thus polled to provide the level of support desired within a large-scale dynamic sensor network.

When combined with IPv6 QoS capabilities and operated with the Differentiated Services (DiffServ) architecture,

the eighth layer concept provides the stool's proverbial third leg. One key of the eighth layer is that the network "must know the information requirements of each recipient" (Nichols et al., 2009) and, therefore, must tag each packet appropriately. IPv6 has both the Traffic Class and Flow Label fields in its header, which are intended to provide QoS in a network configured to interpret these fields in intervening network devices. DiffServ makes use of the one-byte Traffic Class field to map a set of behavior to routines contained in the network routers. The routers, in reading the traffic class field, then determine how to handle the specific packet, based on the contents of the field (Nichols et al., 2009). This functionality in the DiffServ architecture and the IPv6 header provides the means to support the eighth layer's efforts to communicate the level of QoS required for each packet as part of a greater information flow.

3. Multiple Criteria Design Variables

In complex systems where many opposing variables must be considered, multiple-criteria decision techniques are used to find the optimal solution per the given criteria within numerous evaluations. As described by Bordetsky et al. (2004), all too often decision makers do not correctly frame the engineering problem within the confines of the variables. It is often difficult to properly define a model, which may optimize one variable at the expense of another, ultimately reducing the entire system's optimality. As a result, a badly-posed question will result in an equally badly-derived solution. The Parameter Space Investigation (PSI) method was developed in order to aid in correctly

defining the large-scale engineering problem by defining a criteria space from which optimal Pareto solutions, or the feasible solution set, can be determined. Large-scale system solution sets can be derived because PSI can determine results with “thousands of design variables and dozens of criteria constraints” (Bordetsky, 2004). Like other optimization methods, such as nonlinear programming and genetic algorithms, PSI determines the system’s criteria-defined optimal solution by using the system’s inputs and outputs, and the relationships between the two, to correctly formulate the problem. However, PSI implicitly provides the mechanism for stating the problem correctly. In formulating the problem, the decision maker must study the system and determine the relevant design variables which will describe the system behavior, and from which will determine the system’s optimal solution set (Clement, 2006). The design variables in Table 25 are proposed. Those in bold face are the proposed control variables.

Name	Model Layer	Description	Units
Sensor Node Location	**Physical**	**The node’s distance from the gateway as measured by the number of sensor node hops**	**Hops**
Sensor Node Density	**Physical**	**The ratio of sensor nodes to gateways**	**Ratio**
Connectivity	Physical	Determine if the node is or is not connected to the network	Boolean
Active nodes	Physical	Number of active nodes on the network at any given time (Active nodes/Total nodes)	Percent

Name	Model Layer	Description	Units
Link Quality	Physical	The quality of a physical link, defined as the signal to noise ratio	dB
Link Delay (One way and round trip)	Physical	The delay inherent in a link as it propagates through its transmission medium	Microseconds
Link Congestion	Data Link	The amount of traffic on a particular link	Bits/second
Jitter	Network	Fluctuation in source to destination delivery within the same data stream	Microseconds
One-way delay	Network	The delay inherent in a link as it propagates through its transmission medium	Microseconds
Packet loss	Network	The overall number of packets lost compared to the total number of packets transmitted.	Bits
Packet reordering	Network	Measured as a ratio of the number of packets that are delivered out of order to the total number of packets	Bits
Flow Label Traffic	Network	Percentage of different DSCP values contained in the IPv6 header for DiffServ architectures compared to total packets sent	Percentage
Flow Retransmit Cost	Network	The percentage of traffic that must be resent for a given	Percent

Name	Model Layer	Description	Units
		application	
Information Requirements	**8th Layer**	**Information priority level, determined by appropriate tags**	**Scale**
Bandwidth requirement of communication service	**8th Layer**	**Video, voice, imagery, or file transfer for the specific SLA**	**Bits/second**
Information Quality Level	**8th Layer**	**Dependent on the type of communication service contained in the SLA**	**Video: pixels, bits of color, latency in seconds Voice: Bits/second, latency Imagery, File Transfer: Bits/second**
Time interval	**8th Layer**	**The time the SLA is in effect**	**Seconds**
SLA	**8th Layer**	**The number of SLAs in effect on the network**	**Number**

Table 25. Design Variables (After Clement, 2006 and Dobrydney, 2008).

Note: Control Variables in bold

a. Design Variable Constraints

Tactical sensor networks must be compatible with the TCP/IP protocol suite, in order to seamlessly interoperate with the DoD GIG and other commercial off-the-shelf (COTS) equipment. The network layer must use the IPv6 protocol natively in order to take advantage of inherent capabilities that are not present in IPv4, such as end-to-

end connectivity, standard MTU size, IPSec, the increased address space previously mentioned, the reduced overhead of running two network layer protocols on the same network devices, and the IPv6 flow labels. Although IPv4 is more mature at this point in networking development, it is limited in its use for global connectivity and sensor monitoring. QoS mechanisms must provide better service than the current best-effort service that the current network standard provides; “better service” is defined as minimal QoS application requirements.

b. Performance Criteria

At this stage, the decision maker seeks to optimize the design variables through derived relationships among the system design variables, and between the design variables and a set of system performance criteria. In the case of dynamic sensor networks, the performance criteria in Table 27 are derived to optimize QoS for the applications that are traversing the network. The point of view of the performance criteria is that of the commander and his staff, who need the information for mission purposes. These criteria revolve around the eighth layer functionalities.

Name	Description	Max/Min
Stream multiple high image feeds from various sources	The commander and staff can view one or more data streams from multiple sources without having to shut down one or more sources to ensure “best effort delivery”	Max
Uninterrupted, high quality, real-time data streaming	Streaming data will not suffer from latency or jitter and will be viewed in real-time from any source in the network	Max
High-value information delivery	Critical information from any source in the network will be delivered to its destination without delay	Max

Table 26. Performance Criteria.

c. Design Variable Relationships

The design variables listed in Table 26 will be considered as inputs to the Pareto set solution described below. However, the relationships between the variables, at this point, can only be theorized and require the PSI problem and the subsequent campaign of experiments in order to be fully developed and executed. From the results, the relationships among the variables in this dynamic, continually adapting network can be determined, from which the eighth layer can then manage QoS for the information delivered over the network.

d. Pareto Set Solution

By design, the Pareto set offers many optimal solutions along a curve, each of which cannot be improved upon without negatively impacting one or more design criteria. The best Pareto solution is determined by the

decision maker, who will find the solution that best matches his prioritized criteria (Bordetsky, 2004). Several of the design variables were chosen to simulate a network under various conditions, such as low use/low congestion, low use/high congestion, high use/low congestion, and high use/high congestion. The results of the subsequent campaign of experiments will be used to find the Pareto set of solutions for the eighth layer, that is to say, the network management function contained in the uppermost layer in each sensor node. By determining the optimal solution based on the design variables and on the observed relationships between the relevant design variables, the sensor node's management layer will be able to properly support SLAs and thus to maximize the performance criteria listed in Table 26. The human operator will still determine the information requirements of the commander and his staff by developing appropriate SLAs, but the sensor node's eighth layer will have responsibility for using the relevant feedback mechanisms developed by the Pareto set solution so as to adapt to the dynamic network.

4. Expected Results

At the conclusion of this unique approach to determining optimal network QoS in light of multi-variable interaction in a dynamic environment, proper design variable selection and performance criteria will be validated, in addition to determining the relationships among the variables in this dynamic, continually adapting network. The curve developed from the Pareto Set Solution will show the optimal solution along the problem space boundary and, therefore, the optimal relationships among the design

variables within the problem space. From this boundary (i.e., the variables and the relationships between them), eighth layer network management logic can be developed and incorporated into the network to manage QoS for the information delivered. This eighth layer logic will then provide a model for incorporating more agile SLAs that will support the operational and information layers in providing information through a dynamic sensor network. In cases such as an amphibious landing or an active operation in a contested MOUT environment, perhaps two of the most dynamic tactical situations described in Chapter IV, agile eighth layer SLA management logic based on appropriate design variables and performance criteria will greatly aid in QoS performance in the network. This performance increase is due to the ability to continually adapt to environmental changes that occur. Sensors will enter and leave the network, others will be destroyed, electromagnetic interference will block some paths, and changes at the informational and SLA layers will occur. The tactical network that has optimized SLA management logic based upon multiple criteria decision techniques will be the network most able to support operational needs.

LIST OF REFERENCES

Adame, A. & Kong, B. (2008, June). *Performance Management an Analysis of an IPv6 Sensor on the Move Using Commercial Network Management Software*. Master's Thesis, Naval Postgraduate School, Monterey, California.

Akyildiz, I.F., et al. (2002). A survey on sensor networks. *IEEE Communications Magazine*, v. 40, 102-114.

Alberts, D. & Hayes, R. (2005). *Code of Best Practice: Campaigns of Experimentation.* Washington, DC: CCRP Press.

Alberts, D.S., Garstka, J.J., & Stein, F.P. (1999). *Network Centric Warfare,* (2nd Edition, Revised). Washington, DC: CCRP Press.

Bechler, M., Ritter, H., & Schiller, J. (2000). Quality of Service in Mobile and Wireless Networks: The Need for Proactive and Adaptive Applications. *33rd Hawaii International Conference on System Sciences-Volume 8, Maui, Hawaii, 4-7 January 2000.*

Bordetsky, A., et al. (2004) Network Aware Tactical Collaborative Environments. *Proceedings of 9th International Command and Control Systems and Technology Symposium, Copenhagen, 2004.*

Bordetsky, A., et al. (2003). Adaptive management of QoS requirements for wireless multimedia communications. *Journal of Information Technology and Management*, v.4, 9–31.

Bordetsky, A., Statnikov, A., and Statnikov, R. (2004). Multicriteria analysis of real-life engineering optimization problems: Statement and solution, *Proceedings of the 4th World Congress of Nonlinear Analysts, Orlando, Florida, 30 June-7 July 2004*., 685–696.

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

Bordetsky, A. & Netzer, D. (2009). TNT Testbed for Self-Organizing Tactical Networking and Collaboration. *14th International Command and Control Research and Technology Symposia (ICCRTS), Washington, DC, 15-17 June 2009.*

Bouras, C., et al. (2009). *QoS Issues in a Large-scale IPv6 Network* Retrieved July 2009 from http://ru6.cti.gr/ru6/publications/41271178.pdf.

Bouras, C., et al. (2004). Quality of Service aspects in an IPv6 domain. *2004 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS' 04), San Jose, California, 25–29 July 2004.*

Bowden, M. (1999) *Black Hawk Down*. New York: Atlantic Monthly Press.

Brosh, E., et al. *The Delay Friendliness of TCP.* Retrieved July 2009 from http://dna-pubs.cs.columbia.edu/citation/paperfile/163/CUCS-014-08.pdf.

Capra, Fritjof (1996). *The Web of Life*. New York: Anchor.

Clement, M.R. (2006, September). *Adaptive Network Resource Management.* Master's Thesis, Naval Postgraduate School, Monterey, California.

Clement, M.R. (2008, December). *CENETIX Lab brief*. Naval Postgraduate School, Monterey, California.

Culler, D., Estrin, D., & Srivistava, M. *Overview of Sensor Networks.* Retrieved July 2009 from http://www.archrock.com/downloads/resources/IEEE-overview-2004.pdf.

Department of Defense (DoD) (2002). *Directive 8100.1: Global Information Grid (GIG) Overarching Policy.* Washington D.C.: Department of Defense.

Dobrydney, J.F. (2008, August). "Sensor Network QoS in an IPv6 Environment." Course paper, Naval Postgraduate School, Monterey, California.

Dohler, M. (2007). Wireless Sensor Networks: The Biggest Cross-Community Design Exercise To-Date. *Recent Patents on Computer Science 2008,* v. 1, 9-25.

Eschenauer, L. & Gligor, V.D. (2002) A key-management scheme for distributed sensor networks. *Proceedings of the 9th ACM conference on Computer and communications security,* Washington, DC, 18-22 November 2002. 2314-2341.

Estrin, D., et al. (1999) Next Century Challenges: Scalable Coordination in Sensor Networks. *Proceedings of the ACM MobiCom '99*, *August 1999.* 263–270.

Ferrell, M. (2006, September). *Expansion of the Center for Network Innovation and Experimentation (CENETIX) Network to a Worldwide Presence.* Master's Thesis, Naval Postgraduate School, Monterey, California.

Fineberg, V. (2005). IPv6 Features for Enhancing QoS in the GIG. *MILCOM-2005, Atlantic City, New Jersey, October 2005*.

Fiuczynski, M.E., Lam, V.K., & Bershad, B.N. *The Design and Implementation of an IPv6/IPv4 Network Address and Protocol Translator.* Retrieved July 2009 from, http://images.google.com/imgres?imgurl=http://www.usenix.org/publications/library/proceedings/usenix98/full_papers/fiuczynski/fiuczynski_html/figure3.gif&imgrefurl=http://www.usenix.org/publications/library/proceedings/usenix98/full_papers/fiuczynski/fiuczynski_html/fiuczynski.html&usg=__yuBF0o7HyTheUFbJag-IxOm_2oA=&h=359&w=299&sz=5&hl=en&start=5&sig2=d0QvZ75fXhcL-R73kP799Q&um=1&tbnid=qbu30eXbprtcCM:&tbnh=121&tbnw=101&ei=4l0wSZXFB5-0sQPatpXtCA&prev=/images%3Fq%3Dipv4%2Band%2Bipv6%2Bheader%26um%3D1%26hl%3Den%26rlz%3D1C1GGLS_en-USUS291%26sa%3DN.

Hagen, S. (2006). *IPv6 Essentials*, 2nd ed. Sebastopol: O'Reilly.

He, T., et al. (2003) SPEED: A Stateless Protocol for Real-Time Communication in Sensor Networks. *23rd IEEE International Conference on Distributed Computing Systems (ICDCS'03),* Providence, Rhode Island, 19–22 May 2003.

Intaero. *An image of a Common Operating Picture.* Retrieved July, 2009, from, http://www.intaero.com/images/Air.jpg.

JTF-GNO. *Global Information Grid Operational View-1.* Retrieved July 2009 from, http://en.wikipedia.org/wiki/File:Gig_ov1.jpg.

Kalepu, S., Krishnaswamy, S., & Loke, S.W. (2003) Verity: A QoS Metric for Selecting Web Services and Providers. *Proceedings of the First Web Services Quality Workshop, Rome, Italy, December 2003.*

Kim, J. & Shin, J. (2002) Dynamic network adaptation framework employing layered relative priority index for adaptive video delivery. *Proceedings of the IEEE Pacific-Rim Conference on Multimedia,* December 2002. 936-943.

Marilly, E., et al. *Service Level Agreements: a Main Challenge for Next Generation Networks.* Retrieved July 2009 from http://www-rp.lip6.fr/adanets/PublicDoc/Papers/001_ECUMN02-SLA-NGN.pdf.

U.S. Marine Corps (2001). *Marine Corps Operations*, MCDP 1-0.

Mikm. *Diagram of the IPv6 packet header.* Retrieved July 2009 from http://images.google.com/imgres?imgurl=http://upload.wikimedia.org/wikipedia/commons/thumb/3/32/IPv6_header_rv1.svg/800px-IPv6_header_rv1.svg.png&imgrefurl=http://commons.wikimedia.org/wiki/File:IPv6_header_rv1.svg&usg=__m0SkAxv_FUgQxbEPPUyTS8eNhg0=&h=388&w=800&sz=25&hl=en&start=17&sig2=GISjXJuOFoJbIBDQw7oDuQ&um=1&tbnid=SCYndVqFuieO8M:&tbnh=69&tbnw=143&prev=/images%3Fq%3DIPv6%2Bheader%26hl%3Den%26rlz%3D1C1GGLS_en-USUS295US303%26sa%3DN%26um%3D1&ei=ycJbSqWdPJnitQOIqpSiCg].

NAI Labs Technical Report #00-010D, *Constraints and Approaches for Distributed Sensor Network Security* by Carman, P., et al., September 2000.

National Institute of Standards and Technology (NIST), Special Publication 500-267, A Profile for IPv6 in the US Government –Version 1.0, by Montgomery, D., and others, July 2008.

Office of ASD (NII)/DoD CIO (2006). *The Department of Defense (DoD) internet protocol version 6 (IPv6) Transition Plan*. Version 2, Unclassified\\For Official Use Only. Washington, D.C.: Department of Defense (DoD).

Nichols, K., et al. Definition of the Differentiated Services field (DS field) in the IPv4 and IPv6 headers, RFC 2474. Retrieved July 2009 from ftp://ftp.ietf.org/rfc/rfc2474.txt.

Office of ASD (NII)/DoD CIO (2007) *DoD IPv6 Standard Profile for IPv6 Capable Products v 2.0.* Washington, D.C.: Department of Defense (DoD).

Perkins, D.T. (1996). *Understanding SNMP MIBs*. Santa Clara: Prentice Hall.

Routhier, E. *RFC 4293, Management Information Base for the Internet Protocol (IP).* Retrieved July 2009 from http://www.ietf.org/rfc/rfc4293.txt.

Sohrabi, K., et al. (2002). Protocols for Self-Organization of a Wireless Sensor Network. *Personal Communications, IEEE*, v. 7, 16-27.

University of California, Los Angeles, UCLA/CSD-TR-01-0023, *Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks* by Yu, Y., Govindan, R., and Estrin, D., 14 August 2001.

VieSurIP. *Tiny6 - IPv6 in sensor networks.* Retrieved July 2009 from [http://www.viesurip.fr/wp-content/uploads/2008/09/network.png]

Wilson, J.W., et al. (2005). Capacity Planning to Meet QoS Requirements of Joint Battle Management and Command and Control (BMC2) Applications. *Military Communications Conference, 2005.*

Yu, Q., et al. (2002). Fair Intelligent Congestion Control Resource Discovery Protocol on TCP Based Network. *Proceedings of the IFIP 6th Internetworking 2002 Symposium*, *October 2002,* 145-159.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

7. Dr. Alex Bordetsky
   Naval Postgraduate School
   Monterey, California

8. Dr. Dan Boger
   Naval Postgraduate School
   Monterey, California

9. Mr. Mike Clement
   Naval Postgraduate School
   Monterey, California