U.S. Department
of Transportation

**Federal Transit
Administration**

INDEPENDENT VERIFICATION AND VALIDATION OF WASHINGTON STATE FERRIES' WIRELESS HIGH SPEED DATA PROJECT

June 30, 2008
FINAL REPORT

http://www.fta.dot.gov/research

U.S. Department
of Transportation

**Federal Transit
Administration**

INDEPENDENT VERIFICATION AND VALIDATION OF WASHINGTON STATE FERRIES' WIRELESS HIGH SPEED DATA PROJECT

June 30, 2008

Prepared by:
Irving Popovetsky, A. Brandon Psmythe, Amber Pham
CASE Associates, Inc.
ProStructure Consulting LLC

FINAL REPORT
Report Number: FTA-WA-26-7001-2008.02

Sponsored by:
Federal Transit Administration
Office of Research, Demonstration, and Innovation
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, D.C. 20590

Available Online
[http://www.fta.dot.gov/research]

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE June 30, 2008	3. REPORT TYPE AND DATES COVERED Final Report November 2006 – June 2008

4. TITLE AND SUBTITLE
Independent Verification and Validation Report of
Washington State Ferries' Wireless High Speed Data Project
FINAL REPORT

5. FUNDING/GRANT NUMBER
FTA-WA-26-7001-2008.02

6. AUTHOR(S):
Irving Popovetsky, A. Brandon Psmythe, Amber Pham
FTA Project Manager: Charlene M. Wilder

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
CASE Associates, Inc.
ProStructure Consulting, LLC
14674 SE Sunnyside Road #148
Clackamas, Oregon 97015
http://www.caseassociates.com/

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Federal Transit Administration
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590 Website URL [http://www.fta.dot.gov/research]

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AD00013

11. SUPPLEMENTARY NOTES
Available Online [http://www.fta.dot.gov/research]

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Available from National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22161. NTIS Sales Desk 1-800-553-6847 or (703) 605-6000;
fax (703) 605-6900; TDD (703) 487-4639, Email [info@ntis.gov]

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

The following Independent Verification and Validation (IV&V) report documents and presents the results of a study of the Washington State Ferries Prototype Wireless High Speed Data Network. The purpose of the study was to evaluate and determine if real-time security monitoring applications could be consistently available from shore during the vessels' normal daily operations as well as in emergency situations.

The Washington State Ferries Prototype Wireless High Speed Data network project aims to demonstrate new technologies that may provide real-time surveillance capabilities and records for law enforcement agencies in the event of an emergency. Research methodologies included full-scale monitoring tests in combination with data collection phases over multiple weeks. These results were applied to track and evaluate high-speed wireless connections from the ferries to shore. It is the specific intent of this study to determine if the prototype network provides reliable connectivity, and protection against radio eavesdropping, network-based viruses, worms, and traffic floods. The findings of the study were a result of multiple weeks of data collection from communication equipment placed on board the Washington State Ferry vessels.

The intended audience of this report is government agencies wishing to implement secure high-speed mobile wireless data networks. The technical nature of the findings and recommendations in this report are intended to help technical teams make decisions regarding technology and implementation choices when building new wireless networks.

14. SUBJECT TERMS
wireless, ferries, security, verification, validation

15. NUMBER OF PAGES 83

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	

NSN 7540-01-280-5500 Prescribed by ANSI Std. 239-18298-102 Standard Form 298 (Rev. 2-89)

FOREWORD

The following Independent Verification and Validation (IV&V) report documents and presents the results of a study of the Washington State Ferries Prototype Wireless High Speed Data Network. The purpose of the study was to evaluate and determine if real-time security monitoring applications could be consistently available from shore during the vessels' normal daily operations as well as in emergency situations.

The Washington State Ferries Prototype Wireless High Speed Data network project aims to demonstrate new technologies that may provide real-time surveillance capabilities and records for law enforcement agencies in the event of an emergency. Research methodologies included full-scale monitoring tests in combination with data collection phases over multiple weeks. These results were applied to track and evaluate high-speed wireless connections from the ferries to shore.

It is the specific intent of this study to determine if the prototype network provides reliable connectivity, and protection against radio eavesdropping, network-based viruses, worms, and traffic floods. The findings of the study were a result of multiple weeks of data collection from communication equipment placed on board the Washington State Ferry vessels.

The intended audience of this report is government agencies wishing to implement secure high-speed mobile wireless data networks. The technical nature of the findings and recommendations in this report are intended to help technical teams make decisions regarding technology and implementation choices when building new wireless networks.

DISCLAIMER NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The United States Government does not endorse products of manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report.

TABLE OF CONTENTS

APPENDICES

FIGURES

TABLES

EXECUTIVE SUMMARY

BACKGROUND

The vessels of the Washington State Ferries system currently lack dedicated high-speed wireless connections to shore, which limits the real-time security monitoring applications such as video surveillance. In the event of an emergency or attack on a vessel, law enforcement authorities would have limited access to the real-time surveillance footage. An even greater security threat is that this footage would be lost and unavailable for forensic study if the on-board surveillance recording system was destroyed. The Washington State Ferries Prototype Wireless High Speed Data (HSD) network project aims to demonstrate new technologies with the goal of ultimately correcting this limitation and boosting the productivity of staff by providing enhanced network bandwidth for office applications.

The Washington State Ferries Prototype Wireless HSD Network was implemented by Washington-based Mobilisa, Inc., funded by a Federal Transit Administration cooperative agreement. Mobilisa's goal was to boost the available bandwidth to ferries above 25 Megabits per second, enough to allow the viewing of dozens of simultaneous video feeds from multiple ferries on each run. The prototype network aims to provide these speeds with 99 percent reliability, while also protecting against radio eavesdropping and network-based viruses, worms and, traffic floods. Many technical challenges exist in this project which had not been encountered before.

EVALUATION OVERVIEW

An independent team from ProStructure Consulting in conjunction with CASE Associates, Inc. (PSC/CAI) was hired to perform an Independent Verification and Validation (IV&V) of the Prototype. ProStructure and CASE each have decades of collective experience evaluating complex IT systems for government and Fortune 500 enterprises. The purpose of Verification and Validation testing is first to verify that the functionality of a system meets the design specifications, and then to create documented evidence that a system's desired characteristics are consistently maintained over time and adverse conditions.

This IV&V evaluated the Prototype Wireless HSD Network against key success criteria defined by WSF as well as Mobilisa. The success criteria included the following items:

Continuous Connectivity: The system's ability to maintain a connection from ship to shore with 99 percent or greater reliability.

Bandwidth: The system's ability to maintain 25 Megabits per second or greater of available throughput as well as facilitate at least 10 simultaneous video viewing sessions.

Security: The system's ability to protect the confidentiality and integrity of video data, as well as the system's ability to guard against network-based attacks such as viruses and worms.

Classification and Prioritization: The system's ability to ensure that video data traffic is delivered above all other types of traffic, as well as functionality to allow WSF to disable all non-essential data traffic in the event of an emergency.

Scalability and Feasibility: PSC/CAI was also tasked with analyzing the collected data and choices of technology, and to make a determination if the system can feasibly scale to encompass all of the ferries in the WSF fleet.

PSC/CAI's testing methodology utilized the Scientific Method by collecting results in an objective manner over a substantial period of time. In order to perform unprejudiced collection of data, PSC/CAI developed a fully self-contained Test and Measurement device akin to a Flight Recorder or Black Box. Two of these devices were installed as endpoints of the Prototype Wireless HSD network during each evaluation, one aboard the ship and one at the ferry terminal. These devices continually and automatically collected and recorded a wide variety of performance metrics throughout the entire test in a time-referenced and tamper-evident fashion. In order to provide a frame of reference around the results, automated collection of measurable external influences was simultaneously performed and stored within the same time-referenced database.

The evaluation was first performed using the M/V Klahowya vessel on the Southworth-Vashon-Fauntleroy Triangle run, known as evaluation test 1. The entire Prototype Wireless HSD network was then moved to the Steilacoom II vessel on the Port Townsend-Keystone run. Although the same equipment was used in both tests, the second test run demonstrated considerably improved results due to more favorable conditions for the radios.

RESULT OF THE CONTINUOUS CONNECTIVITY EVALUATION

PSC/CAI found that the Prototype Wireless HSD network did not meet all of the success criteria for Continuous Connectivity. The success rate for simulated video data streams in both tests was below the target success rate of 99 percent. In security-focused video streaming applications, missed data directly results in missing video frames. Network ping tests were used as a second measurement of connectivity. In both instances, these tests also fell below the required 99 percent success rate needed to meet WSF's requirements.

RESULT OF THE BANDWIDTH EVALUATION

PSC/CAI found that the Prototype Wireless HSD network did not meet all of the success criteria for Bandwidth performance. While the first phase tests showed that the Prototype Wireless HSD network performed poorly in the bandwidth category, the network performed well in the second phase, exceeding 25 Megabits per second of throughput over 99 percent of the time.

RESULT OF THE SECURITY EVALUATION

PSC/CAI found that the Prototype Wireless HSD network did not meet the success criteria for Security. PSC/CAI did not find any evidence of security measures for protecting the network from malicious activity or network-based attacks. Due to the sensitive and operationally important nature of the content that is intended to be transferred on this network, security will have to be a high consideration in the final Wireless HSD design. PSC/CAI also found some cases where wireless link encryption was not enabled, meaning that the confidentiality of the data was not fully protected.

RESULT OF THE CLASSIFICATION AND PRIORITIZATION EVALUATION

PSC/CAI found that the Prototype Wireless HSD network did not meet the success criteria for Classification and Prioritization. No Quality of Service measures were implemented on the network, resulting in all traffic on the network receiving equal priority. PSC/CAI noted that the success percentage for simulated video data streams was significantly reduced when forced to share the bandwidth with other types of data traffic. PSC/CAI also noted that network latency and jitter increased significantly during the same periods where other data traffic was sent across the network. This demonstrates that reliable video and voice traffic over the network would not be possible without Quality of Service measures. Furthermore, no evidence of functionality for disabling non-essential traffic was demonstrated on the network, as would be necessary in the event of an emergency.

RESULT OF THE SCALABILITY AND FEASIBILITY EVALUATION

PSC/CAI found that the Prototype Wireless HSD network did not meet the success criteria for Scalability and Feasibility. PSC/CAI observed that the choice of radio technology, non-ideal placement of antennas, and the use of unlicensed spectrum were the greatest limiting factors to successfully scaling up the project to include the entire WSF fleet.

CONCLUSION

ProStructure Consulting and CASE Associates, Inc. commend the FTA, WSF, and Mobilisa for setting high expectations and new precedents for high-speed wireless communications in mobile marine environments. However, after reviewing the results PSC/CAI is not confident that the system as designed will meet the project's success criteria in a wider scale deployment or under a wider variety of conditions and settings. PSC/CAI recommends that the Prototype Wireless High Speed Data network undergo a thorough review of the design and chosen technologies before proceeding to a wide-scale implementation of the system in the Puget Sound or any other mobile marine environment.

1 INTRODUCTION

1.1 PROJECT SUMMARY

ProStructure Consulting in conjunction with CASE Associates, Inc. (jointly referred to as "PSC/CAI") was engaged by Washington State Ferries (WSF) to provide Independent Verification and Validation (IV&V) of the Prototype Wireless High Speed Data (HSD) Network as implemented by Mobilisa. Mobilisa is implementing the Prototype Wireless HSD Network under contract to the Federal Transit Administration, in cooperation with WSDOT, in order to increase the available bandwidth to the Ferry vessels for security monitoring purposes.

Mobilisa's project, as outlined by its Implementation Plan document, is divided into seven (7) tasks which took place between August 2006 and May 2008.

1. Research and Development (120 days)
2. Third Party Evaluation Plan Development (30 days)
3. Design (150 days)
4. Demonstration of Promising Technologies (165 days)
5. Build Prototype and Testing (107 days)
6. Third Party Evaluation Period (22 days)
7. Release & Support (70 days)

Due to disruptions and complications during the Third Party Evaluation Period (Task 6) as well as changes in ferry service, a second Third Party Evaluation Period was performed several months later on a different run to validate and compare PSC/CAI's gathered evaluation data.

PSC/CAI's project deliverables were to develop an Evaluation Plan (Task 2), perform a complete IV&V of Mobilisa's finished product during the two Third Party Evaluation Periods (Task 6), review status reports submitted to WSF by Mobilisa for completeness and accuracy, and to assist in general Project Management oversight and provide feedback to WSF.

1.2 PURPOSE

Mobilisa’s Prototype Wireless HSD Network must meet criteria set forth by WSF in the categories of Available Throughput (Bandwidth), Network Delay, and Network Availability. The purpose of this project is to independently verify Mobilisa’s reported performance and availability numbers and to independently validate Mobilisa’s testing criteria and methodology.

1.3 SCOPE

The scope of PSC/CAI’s project was to provide a full Independent Verification and Validation of Mobilisa’s completed deliverable in the Wireless HSD project. It should be noted that the scope only allows for full IV&V of the completed deliverable, and not a full IV&V of the process and steps leading up to that deliverable. It was PSC/CAI’s responsibility to verify that the system as a whole satisfies the success criteria defined by WSDOT.

Two assessment phases are considered in this report. The first phase took place during the five working days of the week of October 8, 2007. During this time, the Prototype Wireless HSD Network equipment was located on the Southworth-Vashon-Fauntleroy Triangle Run. At the time of the first assessment period, the M/V Klahowya ferry housed the mobile portion of the network, while the stationary backhaul equipment was installed at the Fauntleroy and Southworth Ferry terminals.

The second assessment phase occurred from March 7 to March 17, 2008. Due to changes in the in-service ferry configuration during the time between the two assessment periods, the installation location was considerably different at the second assessment period. In the reconfiguration, Mobilisa placed the Prototype Wireless HSD Network equipment in the Port Townsend-Keystone run. The mobile portion of the network was installed on the Steilacoom II ferry, connecting to stationary backhaul equipment located at the Port Townsend and Keystone ferry terminals, as well as the Mobilisa offices.

1.4 REPORT ORGANIZATION

The first two chapters of this report provide an information overview of the Prototype Wireless HSD Network Project and the evaluation team. The second chapter also focuses on the success criteria for the project. Chapter 3 is the Background, containing information about the scope and methodology of PSC/CAI's evaluation of the Prototype Wireless HSD Network. The fourth chapter contains the results of the evaluation in terms of attainment of the success criteria. In the final chapter, Chapter 5, an analysis of the results and the evaluation of the system as a whole are provided. Following the report are appendices intended to provide further technical and background information. Appendices A and B contain detailed data collection design information and raw results data, while Appendix C contains the original Evaluation Plan written by PSC/CAI.

1.5 EVALUATION TEAM

Technical Lead: Irving Popovetsky, Principal Consultant, ProStructure Consulting
Irving Popovetsky leads ProStructure's Security and Systems Engineering practices. He brings over a decade of Information Security and large-scale network management from the Telecom sector, having worked for Sprint's IP Security team and MCI/WorldCom's global AOL dial network.

Project Manager: Brandon Psmythe, Principal Consultant, ProStructure Consulting
Brandon Psmythe leads ProStructure's Network Engineering, Data Center, and Operations Management practices. Brandon brings over a decade of large-scale network management and IT management experience from Webtrends/NetIQ and from Intel, where he oversaw the networks and data centers of the Desktop Processor design teams.

Project Oversight: David Sharon, Principal Consultant, CASE Associates Inc.
David Sharon specializes in providing Process Improvement, Project Management, Risk Management, and Quality Assurance Services to State Government Agencies. CAI has provided these services to more than 30 Agencies in Washington and Oregon and has over 18 years experience in providing these services.

2 BACKGROUND

2.1 OVERVIEW OF THE WIRELESS HSD NETWORK

Today WSF vessels are equipped with multiple security cameras connected to a Vigilos DVR (Digital Video Recorder) system that stores data locally. In case of a catastrophic event, the video data would be lost and unavailable for forensics and future reference. The primary purpose of the Prototype Wireless HSD network is to facilitate the real-time transfer of video data from the onboard Vigilos system to the shore, for real-time monitoring and storage for later retrieval.

The secondary use for this network is to provide connectivity for office applications used by WSF employees during the course of their normal workday on the ferry. This could consist of business data traffic including fax, Voice over IP (VoIP), email, and file transfer.

2.2 PROJECT GOALS

The fundamental criterion for success of the project is the successful demonstration of a working prototype that maintains continuous connectivity with sufficient bandwidth from the WSF Ferry to the Ferry terminal in a fully verifiable manner. Further details of the success criteria are defined in the Success Criteria section below.

Secondarily, the goal of this project is to thoroughly document the operation, external influences, and any performance failures of the Prototype Wireless HSD Network over a significant period of time. This information, when analyzed in a broad scope, should provide the planners of future projects with useful lessons.

2.3 THE FTA AND ITS STRATEGIC GOALS

The Prototype Wireless HSD Network project is part of a greater FTA initiative of Emergency Response Readiness. According to the FTA's Annual Performance Plan (FY 2007), it is the FTA's goal to increase preparedness to "*respond to emergencies that affect the viability of the transportation sector."* The prototype for the Wireless HSD Network supports this effort with its primary goal to supply a robust network backhaul from Washington State ferries to the shore that streams the data collected by security cameras. Having such a network in place would allow real-time monitoring from the shore of events happening on the ferries. It also improves the efficiency with which video data is relayed to off-ship storage.

A second goal of the FTA is its Project Management Oversight Strategy, to *"ensure that grant funds are spent efficiently and effectively."* CASE Associates, Inc. specializes in project quality assurance and risk assessment. By using an objective third party for project oversight, the FTA and WSF can provide project transparency to taxpayers. The FTA and WSF can clearly show whether its projects are completed on time, successfully, and within budget. Additionally, ProStructure Consulting brings technical expertise to help WSF fully understand the implementation of the prototype Wireless HSD Network

2.4 MOBILISA EVALUATION QUESTIONS

The Evaluation Questions created by Mobilisa and contained herein will guide the gathering and analysis of the Prototype Wireless HSD Network test data. Each question references a section, as noted, from Mobilisa's Implementation Plan.

- ☐ Does the final prototype demonstrate scalability, functionality, and feasibility? (6.1.1)
- ☐ Is the system robust enough to handle two-vessel traffic in an emergency, to include transmission to the terminal? (6.1.4)
- ☐ Is the hardware chosen for the system configured for optimal performance, and does it provide continuous and reliable performance in delivering high data throughput? (6.2.1)
- ☐ Does the system support upload bandwidth of 25Mbps during un-obstructed operations (e.g., there is a physical vessel blocking line-of-sight while traversing the route)? (6.2.2)
- ☐ Does the vessel provide virtually continuous connectivity, i.e., 99% data received during non-obstructed operations as the vessel traverses the route? (6.2.2)
- ☐ Does the system provide for a minimum of 10 video viewing sessions? (6.2.4)
- ☐ Is the system proactively designed with security considerations in mind to protect against viruses, worms, packet floods, data interception, or unauthorized system access? (6.2.5)
- ☐ Does Mobilisa provide evidence through documented process that video data received is actually transmitted off vessel? (6.2.5)
- ☐ Do the radios authenticate before connection is made? (6.2.5.1)
- ☐ Is the data encrypted during transmission? (6.2.5.2)
- ☐ How effective is the solution? (7.6)
- ☐ Does it meet all the above requirements? (7.5)

2.5 WSF SUCCESS CRITERIA

The following success criteria for the Wireless HSD project define the dimensions on which the prototype was measured. These criteria were defined by WSF, and CAI/PSC assisted in the clarification of the technical aspects of each criterion. These standards allow objective measurement of the prototype against WSF's requirements for the project.

2.5.1 CONTINUITY/RELIABILITY

The continuity of the ship-to-shore wireless connection was measured to ensure that data is reliably relayed to the onshore server that stores the video data. Mobilisa has defined this as greater than 99 percent of data transmitted from the Ferry to the Ferry Terminal successfully received. Successful transmission includes any packet that meets any specified bandwidth or latency requirement, and successfully reaches its intended destination. Any packet that is not received by the end station, or does not fall within the specified Quality of Service requirements is not counted as a successful transmission.

2.5.2 NON-INTERFERENCE

Mobilisa must ensure that the new wireless data network does not interfere with any ferry navigation and WSF-controlled communications systems. This would include any type of existing ship to shore voice communication systems, radar, GPS, and 800 Megahertz (MHz) radios.

2.5.3 SECURITY

The prototype was evaluated against federal standards for secure communications to protect the confidentiality and integrity of video data, and to ensure that security measures do not incur a considerable cost to performance. CAI/PSC was to verify that link-level encryption is used which meets the guidelines of the NIST publication FIPS 140-2. Additionally CAI/PSC was to verify that device-to-device authentication is in place.

2.5.4 CLASSIFICATION AND PRIORITIZATION

Quality of Service (QoS) policies should be employed to prioritize the transmission of data from appropriately tagged applications and/or protocols. This allows applications that have strict latency or bandwidth requirements (such as streaming video and voice) to perform correctly and provide an acceptable end-user experience.

WSF has stated that the wireless network will carry data that can be classified into two distinct groups. The high priority traffic will include any traffic that is related to the transmission of security-related video feeds. This traffic must be prioritized to meet the latency and bandwidth requirements specified by Vigilos. Vigilos has specified that its applications will tolerate a Round Trip Time no greater than 50ms.

The secondary class of traffic includes any traffic that is related to the WSF model of floating work offices for its employees. This includes employee-related business traffic such as email, intranet access, and Voice over IP (VoIP). This secondary class of traffic can be further subdivided into latency-sensitive traffic and non-latency-sensitive traffic. WSF may find that the requirement of VoIP will have different latency requirements than the Vigilos Application.

The working prototype must also include a mechanism to dynamically control the prioritization of traffic. In the event of an emergency, this mechanism would be used to limit the amount of resources non-emergency traffic would be allowed to access.

2.5.5 BANDWIDTH

Bandwidth was measured to ensure it would be sufficient to support live video feeds alongside business applications. Sufficient bandwidth should be available to support at least 10 streaming video feeds from two vessels simultaneously, limiting connectivity for all other applications. Sufficient bandwidth would also support secondary utilization of the wireless network without affecting the primary usage.

WSF has stated that the wireless network must be able to handle 25Mbps (Megabits per second) of network traffic. The Vigilos video data streams transmit 16 KB (Kilobytes) MJPEG video frames at a rate of 2 frames per second. Therefore, each video feed is estimated at 32 KB/s (Kilobytes per second), or 256 Kb/s (Kilobits per second). In order to transmit 10 simultaneous video feeds, an approximate 3.0 Mbps of bandwidth, including overhead, is required in order to transmit the feeds without congestion.

3 OBJECTIVE AND METHODOLOGY

3.1 EVALUATION FRAMEWORK

PSC/CAI has been tasked with performing an unbiased and objective evaluation of the Prototype Wireless HSD network. PSC/CAI's evaluation of the network will be purely based on quantitative data. Due to the nature of the project, there are no qualitative aspects, such as user perception, that factor into the outcome of the evaluation.

3.1.1 EVALUATION SCOPE

PSC/CAI performed a full Independent Verification & Validation (IV&V) of the Prototype Wireless HSD Network after it had been completely implemented by Mobilisa. Mobilisa's completed deliverable, in brief, includes a fully functioning Wireless backhaul network from the target ferry vessel to shore stations located at the ferry terminals. Due to disruptions and complications during the first evaluation period, a second evaluation period was scheduled.

The first IV&V evaluation period began on October 9th, 2007 and ended on October 15th, 2007. During this period, the Prototype Wireless HSD Network equipment was installed on a ferry and at stationary points in the WSF Triangle run. The vessel in study was the M/V Klahowya, an Evergreen State Class Auto/Passenger Ferry that is bi-directional; it may travel in either direction. The M/V Klahowya traveled among the Fauntleroy, Vashon Island, and Southworth ferry terminals located in the southern end of the Puget Sound, before the ferry was removed from service.

The second IV&V evaluation period began on March 7 and continued for 10 days, ending on March 17, 2008. The location of the mobile Prototype Wireless HSD Network equipment during the second evaluation period was on the Steilacoom II, which is the only ferry in service on the WSF Port Townsend run at the time of writing. The two shore stations utilized in this run were located at the Port Townsend and Keystone ferry terminals. Additionally, the Port Townsend ferry terminal was backhauled to the Mobilisa offices where ProStructure's shore-side test equipment was located.

The primary testing focus during both evaluation periods was on the Bandwidth, Delay, and Reliability of the ship-to-shore communications via the Prototype Wireless HSD Network. Outside the scope of these evaluations were the design and installation phases of the Prototype Wireless HSD Network project. Only the final products were assessed.

3.1.2 EVALUATION OBJECTIVES

The objective of this evaluation was to independently verify that the Success Criteria (Section 2.5) have been met and that objective, verifiable answers could be provided to all of the Evaluation Questions stated in Section 2.4.

Because there is no connection between the Prototype Wireless HSD Network and the WSDOT network, there was no way to evaluate the performance of the Vigilos ship-to-shore streaming system directly. Therefore, the best avenue for evaluating the performance of the Network was to use synthetic network performance testing tools that simulate the behavior of the Vigilos system.

3.1.3 EXTERNAL INFLUENCES

In order to gather a complete picture of the Prototype Wireless HSD Network and any potential shortcomings, external factors that affect Wireless network performance must be taken into account. In this project, three factors have been identified that affect Wireless network performance:

Radio Antenna Misalignment: In order to achieve maximum throughput, Mobilisa has stated that it will use highly directional Sector antennas, rather than Omni-directional antennas. Directional antennas work by amplifying the radio signal in a pie or cone shape, rather than dispersing the signal in all directions as will an Omni-directional antenna. This technique works well for networks with stationary endpoints; however, in a mobile environment where non-stationary clients pitch, roll, and yaw, the concentrated signal can be sent in the wrong direction causing loss of connectivity.

Radio Interference due to loss of Line-of-Sight (LOS): Mobilisa chose to use the 5.8 Gigahertz (GHz) radio frequency range for the Prototype Wireless HSD Network for its high performance in point-to-point applications. The primary disadvantage of 5.8 GHz is that signal in this frequency range is greatly affected by physical objects, so much so that LOS is nearly always required for outdoor long-distance links. If any physical object, such as another vessel, travels between the antennas of the client and base station, the signal will be lost.

Radio Interference due to competing radio signals (noise): Another disadvantage of using the 5.8 GHz frequencies is that they are unlicensed, designated by the FCC for ISM (Industrial, Scientific and Medical) uses. This means that any other entity, private, public or personal, can acquire equipment that also transmits on this frequency, causing "noise," where a competing waveform cancels out the intended waveform. This can result in degraded performance or loss of connectivity for the wireless network.

PSC/CAI gathered several metrics in order to determine how often these external influences affected the Prototype Wireless HSD Network. First, PSC/CAI referenced GPS (Global Positioning System) data in order to determine the exact location, heading and speed of the M/V Klahowya and of the M/V Klickitat. If the vessel rotates or strays from its typical route, then the antennas may become misaligned. Second, PSC/CAI collected radio performance metrics directly from the wireless ship-to-shore radios, which includes information about the wireless link quality and noise. Finally, PSC/CAI collected weather condition information for the Puget Sound area, in order to provide additional clues about what causes the system to fail.

3.2 EVALUATION METHODOLOGY

PSC/CAI's testing methodology followed the Scientific Method by collecting results in an objective manner over a substantial period of time. PSC/CAI's tests accomplish this by providing a frame of reference around all results. This is achieved by recording all network performance test results and information about external factors in time series based database format.

PSC/CAI's hypothesis was that the outcome of its tests would be similar to those reported by Mobilisa, when gathered during favorable environmental conditions. PSC/CAI did expect some degree of performance degradation and failure when those conditions change. It was PSC/CAI's intention that by gathering data over a longer period of time that the successful functioning of the Prototype Wireless HSD Network could be verified, and some of these performance-degrading situations could be identified and better understood.

In order to perform unprejudiced collection of data, PSC/CAI developed a fully self-contained Test and Measurement device akin to a Flight Recorder or Black Box. Two of these devices were installed during each evaluation. In the first instance, one device was installed aboard the WSF test vessel (the M/V Klahowya), with the other located at the Fauntleroy Ferry Terminal where Mobilisa's equipment is housed. For the second instance, one unit was installed aboard the WSF test vessel (M/V Steilacoom II), and the other was located at the Mobilisa offices. In both scenarios the test devices were located inside of the network built by Mobilisa, but at logically opposite ends of the network in order to rule out other external factors that could influence the results. PSC/CAI prepared the devices to continually collect data over a time period of no less than 5 days and no more than 21 days.

These devices automatically collect and record a wide variety of performance metrics during one-minute intervals throughout the entire test. In order to ensure that the data is verifiable and easy to correlate, all results were stored in RRD (Round Robin Database) files along with the time interval of the data. These files were backed up hourly to the offices of ProStructure Consulting, and compared against the evaluation copies after each evaluation period. Some of the performance metrics collected include:

- Network availability status, including maximum and average throughput, delay, and jitter
- Wireless link status, speed, link quality, and noise (interference)
- Vessel location, heading, and speed

PSC/CAI established baselines with all utilized tools in a controlled environment. PSC/CAI also ensured the reproducibility of its test results by documenting all equipment, testing software, configurations, and tests for inspection in the final report. A thorough description of the equipment and tests utilized by PSC/CAI can be found in Appendix A of this report.

4 FINDINGS AND APPLICATIONS

4.1 OVERVIEW

After gathering and analyzing the test data, PSC/CAI has concluded that the Prototype Wireless HSD Network did not meet all of the requirements set out by WSF and Mobilisa prior to the implementation. In the first testing period on the Triangle Run, the prototype wireless network failed to meet the required success percentages for all of the tests (*see* Table 1). In the second testing period on the Port Townsend-Keystone Run, the prototype wireless network met its required success percentages for the throughput and latency tests, but not for the video stream success or network latency tests (*see* Table 1).

In the first testing period on the Triangle Run (Test1), the target success numbers for the TCP throughput test were achieved only 46 percent of the time, 36 percent of the time for the UDP Video stream tests, less than 29 percent for the network availability test, and less than 99 percent for the network latency test.

In the second testing period on the Port Townsend-Keystone Run (Test2), the target success numbers for the TCP throughput test were achieved greater than 99 percent of the time, but less than 96 percent of the time for the UDP Video stream tests, less than 99 percent for the network availability test, and greater than 99 percent for the network latency test.

Table 1: Quantitative Test Results for Test1 and Test2

	Test1	Test2
Throughput above 25Mbps Success Percentage	46%	99.63%
Video Stream Success Percentage	36%	95.85%
Network Availability Success Percentage	28.56%	98.18%
Latency	98.8%	99.52%

The data collected from the two test runs provide very different results. The evaluation reveals that the Prototype Wireless HSD Network did not meet all requirements defined by WSF and Mobilisa. Table 2 summarizes this outcome by displaying the outcome for each test period as well as the conclusion drawn based on the cumulative results. The outcome for each objective is described fully in the sections below.

Table 2: Attainment of Requirements

	Test1	Test2	Overall Result
Throughput above 25Mbps Success Percentage	No	Yes	No
Video Stream Success Percentage	No	No	No
Network Availability Success Percentage	No	No	No
Network Responsiveness Success Percentage	No	Yes	No
Quality of Service Effectiveness	No	No	No
Security Enforcement	No	No	No
Non-Interference	Yes	Yes	Yes

4.2 ATTAINMENT OF FUNCTIONAL REQUIREMENTS

The primary objective of the Prototype Wireless HSD Network Project was to successfully demonstrate a working prototype that maintains continuous connectivity with sufficient bandwidth from the WSF Ferry to the Ferry terminal in a fully verifiable manner. Mobilisa's Implementation Plan, section 6.2: Functional Requirements provides guidelines by which to measure the attainment of the project objectives. The present section summarizes those requirements and describes the level of success attained in meeting the objectives.

4.2.1 NETWORK AND HARDWARE PERFORMANCE

The implemented network as designed is expected to provide architectural robustness in the network that provides fail-over and redundancy. This is accomplished by having the vessel connected to both shore-side stations at the same time, with Mobilisa's router selecting the best path.

In terms of continuous and reliable performance that delivers a high level of data throughput, the prototype was not successful in Test1; although link speeds did reach 25 Mbps, this level of performance was not continuous and reliable. During Test2, performance did maintain the required level for over 99 percent of the testing periods.

4.2.2 HIGH DATA CAPACITY

The first test period showed that while throughput did average about 25 Mbps, it frequently dropped below the acceptable limit during normal operation, and availability was considerably below 99 percent. During the second testing period, sufficient data was gathered to show that the throughput objective was met; however, the availability success rate came in under 99 percent.

4.2.3 NETWORK RESPONSIVENESS SUCCESS PERCENTAGE

The prototype system was found to be sufficiently able to transfer data over the backhaul during normal operation. In objective tests and live demonstration, the prototype did meet the maximum 50ms latency requirement of the Vigilos system to stream the video feeds live during those times when the Prototype Wireless HSD Network was available in Test2. During Test1, the success rate for latency under 50ms fell just below 99 percent.

Line-of-sight issues did affect the off-board transmission of data. During periods where ferries were required to operate in an orientation opposite that for which the Network was designed, the backhaul connection was lost completely. The line-of-sight issue was more prevalent during the first testing period, as the final tested configuration involved a single-ferry run where the ferry did not change orientation. This problem would be a major issue for any large-scale implementation using the tested radios.

4.2.4 THROUGHPUT OPTIMIZATION OF LIVE VIDEO

PSC/CAI observed a demonstration of live video streaming by Mobilisa during the Demonstration of Promising Technologies on June 19th, 2007.

Because no live Vigilos system was available for the evaluation, PSC/CAI simulated the network traffic that would be created by 10 live Vigilos video streams for the purposes of testing the Prototype Wireless HSD Wireless Network.

PSC/CAI found that when the wireless network was available and there was no competing traffic, the bandwidth available during the test would allow for more than 10 simultaneous video streams. However, PSC/CAI found no evidence that the delivery of the video data was optimized or prioritized in any way. When competing traffic was introduced to the network, the additional load had a significant impact on video stream success rates. The delivery rates for the video streams did fall short of the target 99% delivery rate.

4.2.5 SECURITY

PSC/CAI did not find complete documentation and implementation of the security requirements stated in the Mobilisa Implementation Plan. 256-bit AES encryption is available on the radios used and would meet the security criteria defined for success. This encryption was found to be implemented on the radio links except during Test 2, where encryption was found to be disabled on two of the radio links: between the Port Townsend trestle and the Steilacoom II, as well as between the trestle and Mobilisa Headquarters. Without this encryption, these links were at risk of Man-in-the-Middle attacks, and the system during Test2 fails to meet the Success Criteria defined for secure communications. Other basic secure configurations were not completed, such as changing the SNMP community string to a value other than "public."

There is no evidence that protections were put in place to prevent disruption due to automated attacks such as viruses, worms, and packet floods. A Quality of Service (QoS) system could provide a great deal of protection against such network-based attacks, as well as ensure that video traffic is prioritized above office-related activities, but no such system was implemented.

4.2.6 NON-INTERFERENCE WITH EXISTING WSF SYSTEMS

Due to the choice by Mobilisa to use 5.8GHz radios, there was no interference with existing ship communications.

4.3 ANSWERS TO THE EVALUATION QUESTIONS

Does the final prototype demonstrate scalability, functionality, and feasibility?

No, the prototype is not highly feasible as designed. The scalability of the prototype is limited by the radio technology selected. The Motorola Canopy PTP 600 radios connect in a one-to-one directional pairing to form a network. When a ferry changes direction, the antenna loses connection with its mate; therefore, a second pair of radios is needed for the opposite direction. With every shore station and ferry added, an additional two pairs of radios are required to maintain a network. Radios that can form a point-to-multipoint connection would be more efficient for this mobile application.

Due to the use of the 5.8GHz frequency, direct line-of-sight is required for an acceptable level of functionality. This band is susceptible to interference from objects and competing radio signals. Since the 5.8GHz band is unlicensed and available for public use, there is a risk of interference from other wireless applications.

Is the system robust enough to handle two-vessel traffic in an emergency, to include transmission to the terminal?

Yes, as it is configured during the final testing period, the Prototype Wireless HSD network could perform as required by WSF at any given moment. In a real-life implementation, where there are multiple ferries on a run or one or more ferries require occasional turnarounds, or where competing network applications and radio equipment are enabled, the system as configured would not be robust enough to handle two-vessel traffic. During Test1, the latency was too great

for the reliable conveyance of video data. In addition, the system cannot be considered robust due to the lack of security controls to ensure the integrity of video data received at the shore.

Is the hardware chosen for the system configured for optimal performance, and does it provide continuous and reliable performance in delivering high data throughput?
No, the hardware chosen for the system has the capability of providing QoS optimizations; however, this feature was never configured by Mobilisa. Standard tests of continuous connectivity and connection reliability did not meet WSF's requirements during Test1 but did meet the requirements during Test2. If the prototype network were flooded with malicious traffic, the reliability of video and other UDP streams would be severely degraded.

Does the system support upload bandwidth of 25 Mbps during un-obstructed operations (e.g. there is a physical vessel blocking line-of-sight while traversing the route)?
Yes, the Prototype Wireless HSD network does support throughput of 25 Mbps when all conditions are ideal. During Test1, the prototype network did not maintain 25 Mbps during 99 percent of the testing times; however, in the second deployment and system configuration during Test2 the bandwidth achieved did meet WSF's requirement.

Does the vessel provide virtually continuous connectivity, i.e. 99% data received during non-obstructed operations as the vessel traverses the route?
No, the prototype network provided less than 99 percent availability. Test1 showed the system could maintain 99 percent availability for only 28.5 percent of the time, while the system in Test2 was able to meet the availability criteria for only 98.18 percent of the time.

Does the system provide for a minimum of 10 video viewing sessions?
No. While Mobilisa's live demonstration showed 10 video viewing sessions, objective automated testing of UDP stream success and network latency showed that the reliability of the network was not sufficient to meet WSF's criteria. Test1 showed a success rate of 66.25 percent, while the second test's success rate was 95.85 percent. The percentage of time periods with acceptable latency was 98.8 during Test1 and 99.52 in Test2.

Is the system proactively designed with security considerations in mind to protect against viruses, worms, packet floods, data interception or unauthorized system access?
No, the system design does not show any indication of security controls. During Test1, PSC/CAI verified that link-level encryption used in the Prototype Wireless HSD network met the security guidelines of the NIST publication FIPS 140-2; however, this encryption was not used consistently in Test2. The use of device-to-device authentication was confirmed. The firewall installed between the Prototype Wireless HSD Network and the Internet is not configured to block any traffic. This leaves the Prototype Wireless HSD network susceptible to the modes of attack listed above. The equipment chosen contains QoS capabilities, but Mobilisa has not implemented these features. During a network flood, the quality of any video or other UDP streams would not be sufficient to meet WSF's requirements.

Can the system classify and prioritize to guarantee the delivery of video surveillance traffic?
No, Mobilisa did not include in its final design any method of prioritizing traffic groups differently on the network. As a result, all packets on the network are treated with the same urgency. As a result, the latency-sensitive camera streams will perform poorly, losing data, during times of network congestion.

In the case of an emergency is there a mechanism to disable all non-essential communications?
No such control was included in the final design of the Prototype Wireless HSD Network. Non-essential network traffic can disrupt emergency-related network traffic without this throttling control in place.

Does Mobilisa provide evidence through documented process that video data received is actually transmitted off vessel?
No, a live demonstration was witnessed by WSF and PSC/CAI that successfully convinced all parties that the video data was successfully transmitted off vessel, but no documentation has been received to date to confirm the process. PSC/CAI did demonstrate that its own simulated video traffic was successfully received off the vessel without any modifications.

Do the radios authenticate before connection is made?
Yes, the Motorola Canopy PTP 600 radios authenticate before the connection is made.

Is the data encrypted during transmission?
No, the Prototype Wireless HSD network equipment is capable of using 256-AES to encrypt data that is passed between the radios; however, this was not enabled on two of the radio links during Test2. A single radio with unencrypted communications compromises the security of the entire network.

How effective is the solution?
In a carefully controlled environment, the solution can be effective. Once line-of-sight is lost due to turnabouts or crossing paths with other ships, or when interference is introduced from competing wireless broadcasting equipment, the solution loses effectiveness.

Does it meet all the above requirements?
No, the Prototype Wireless HSD Network met some but not all of the requirements above.

4.4 REVIEW OF THE DATA COLLECTION RESULTS

The data collected during both tests has been compiled into graphs to provide a visual view into the data.

4.4.1 BASELINE DATA

The following figures are presented for comparison with the test data. These were generated with the same testing suite that was used for Test1 and Test2 of this IV&V. The two test systems were attached via a single controlled network switch. The data collected and presented show the expected test results when performed under ideal network conditions. Baseline data was collected prior to the test to ensure the correct operation of the testing suite, and again after Tests 1 and 2 to ensure that no changes to the testing suites had happened that could have affected the results during the tests.

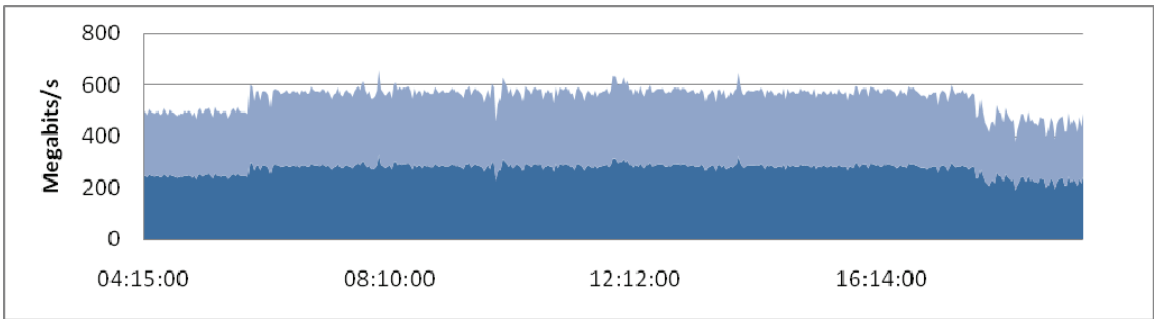

Figure 1: Baseline TCP Throughput Test Results in Megabits per Second – 3/6/2008

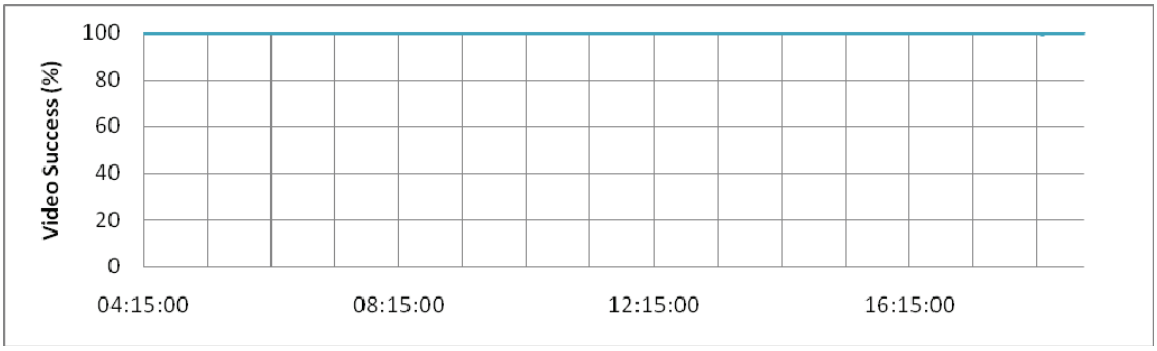

Figure 2: Baseline UDP Video Stream Test Results – 3/6/2008

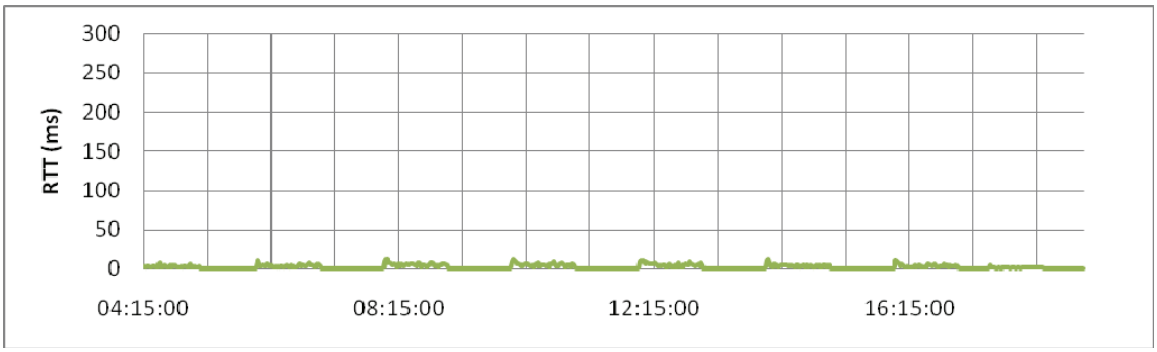

Figure 3: Baseline ICMP Network Latency Test Results – 3/6/2008

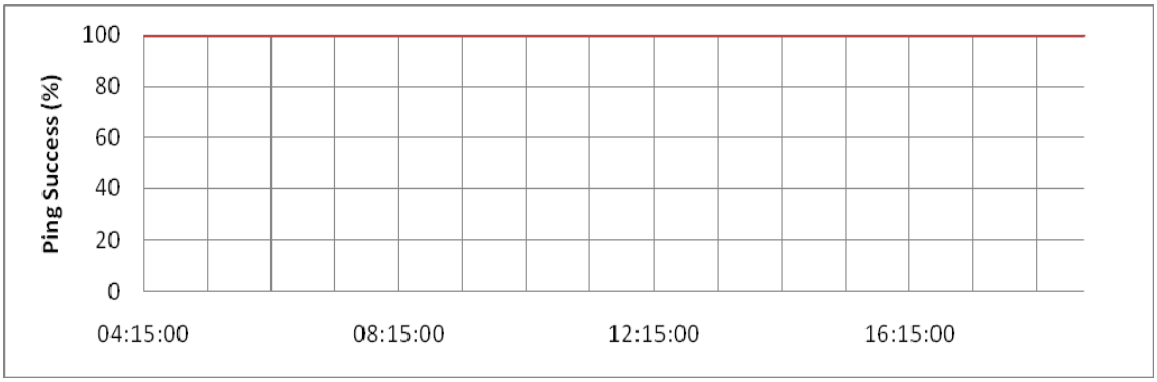

Figure 4: Baseline ICMP Network Availability Test Results – 3/6/2008

4.4.2 REPRESENTATIVE TEST 1 RESULTS

The following figures show daily results in graphical format for each day of the first evaluation test on the Triangle Run.

4.4.2.1 OCTOBER 11, 2007 RESULTS

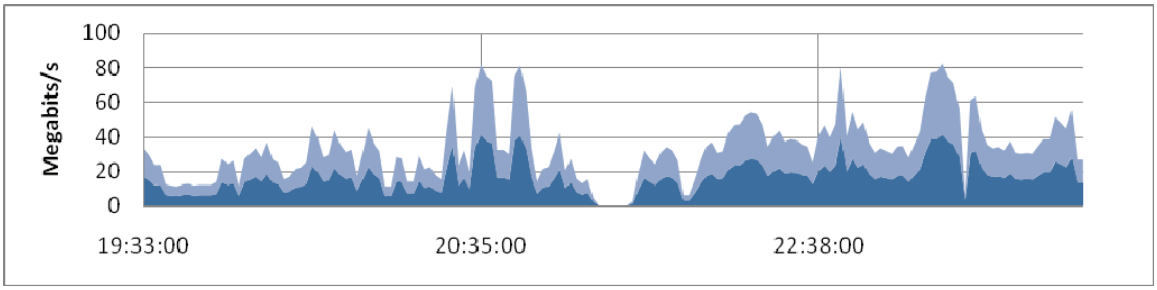

Figure 5: TCP Throughput Test Results in Megabits per Second – 10/11/2007

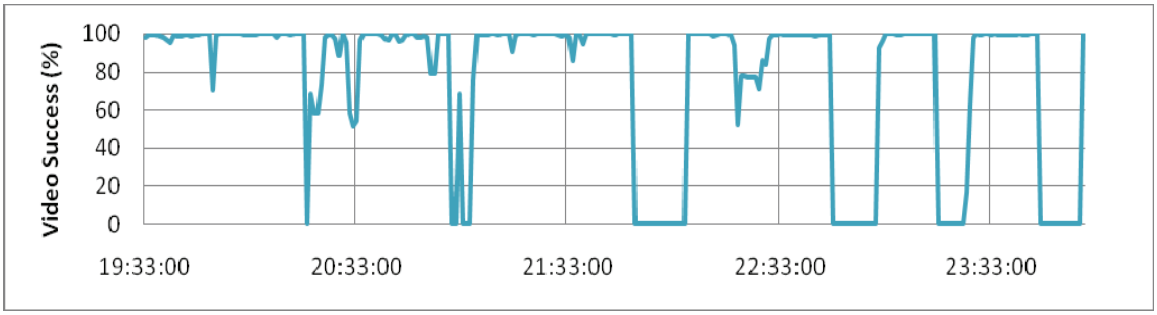

Figure 6: UDP Video Stream Test Results – 10/11/2007

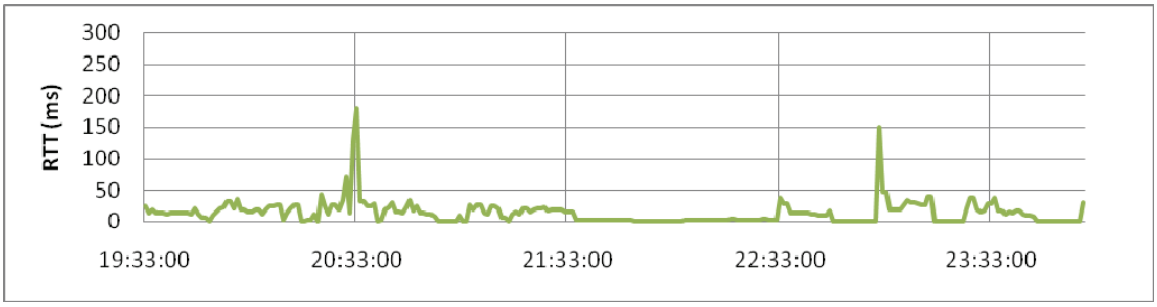

Figure 7: ICMP Network Latency Test Results – 10/11/2007

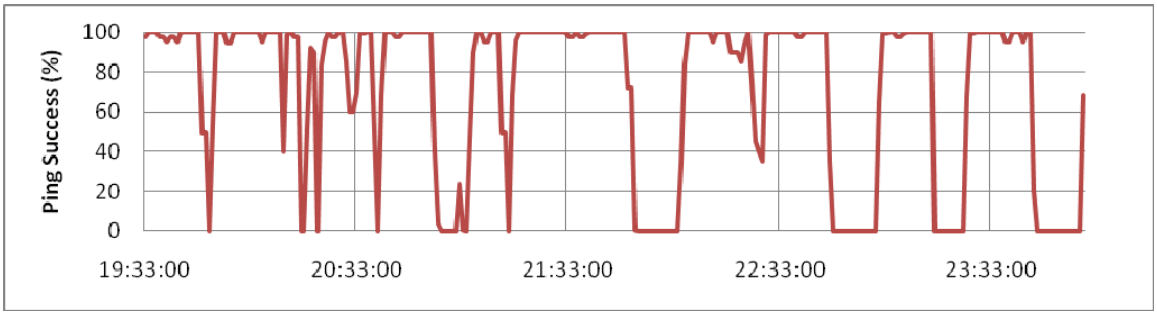

Figure 8: ICMP Network Availability Test Results – 10/11/2007

4.4.2.2 OCTOBER 12, 2007 RESULTS

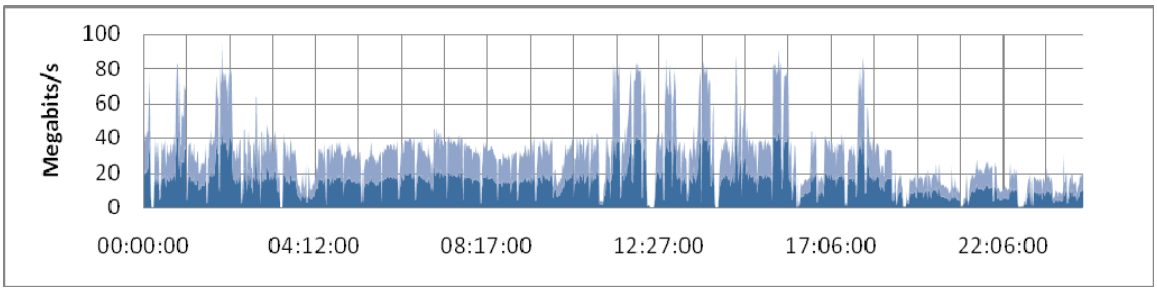

Figure 9: TCP Throughput Test Results in Megabits per Second – 10/12/2007

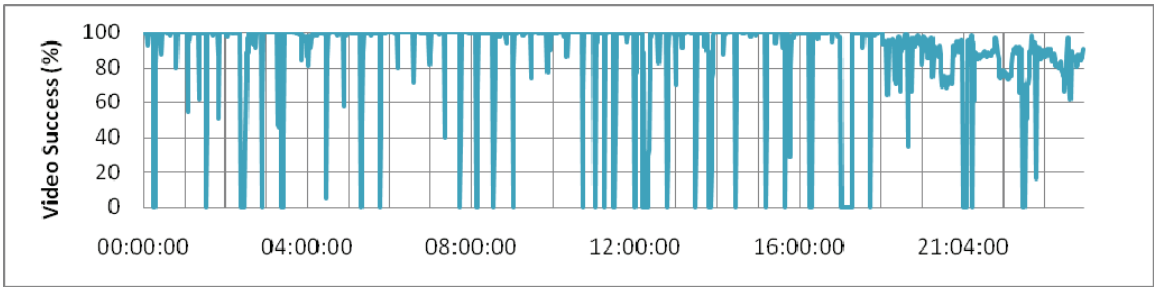

Figure 10: UDP Video Stream Test Results – 10/12/2007

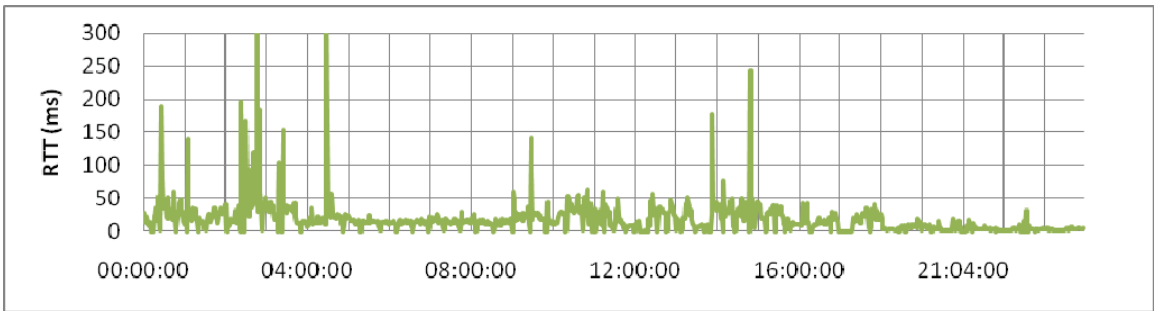

Figure 11: ICMP Network Latency Test Results – 10/12/2007

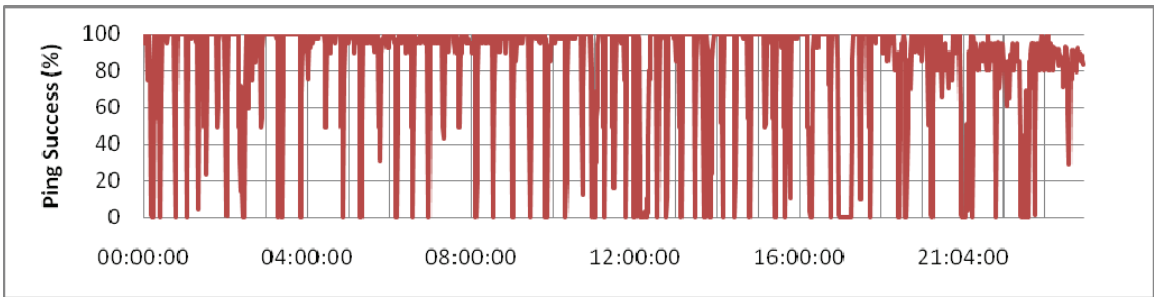

Figure 12: ICMP Network Availability Test Results – 10/12/2007

4.4.2.3 OCTOBER 13, 2007 RESULTS

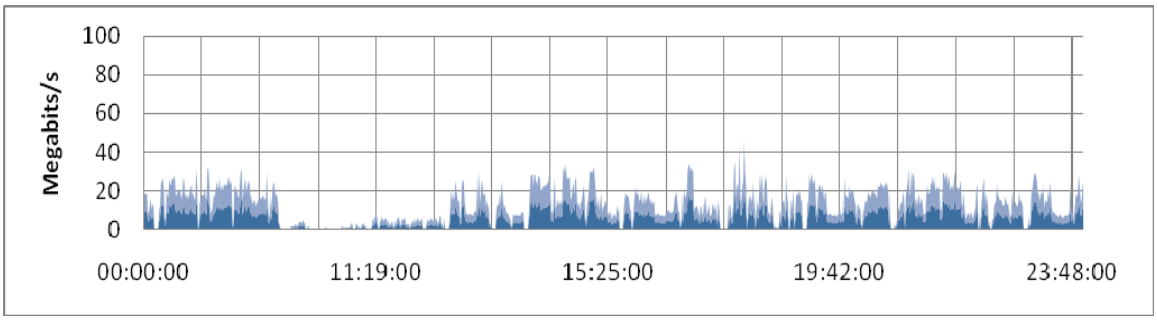

Figure 13: TCP Throughput Test Results in Megabits per Second – 10/13/2007

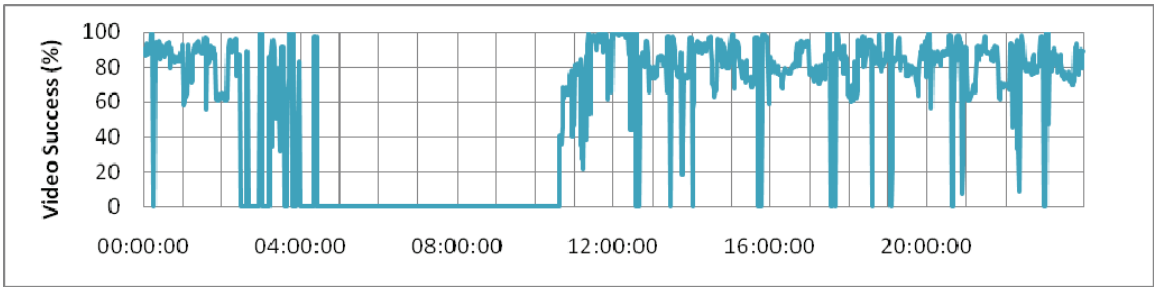

Figure 14: UDP Video Stream Test Results – 10/13/2007

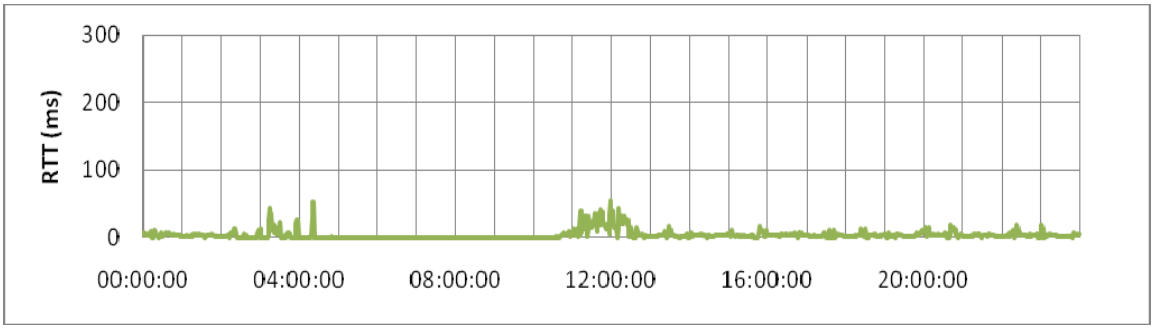

Figure 15: ICMP Network Latency Test Results – 10/13/2007

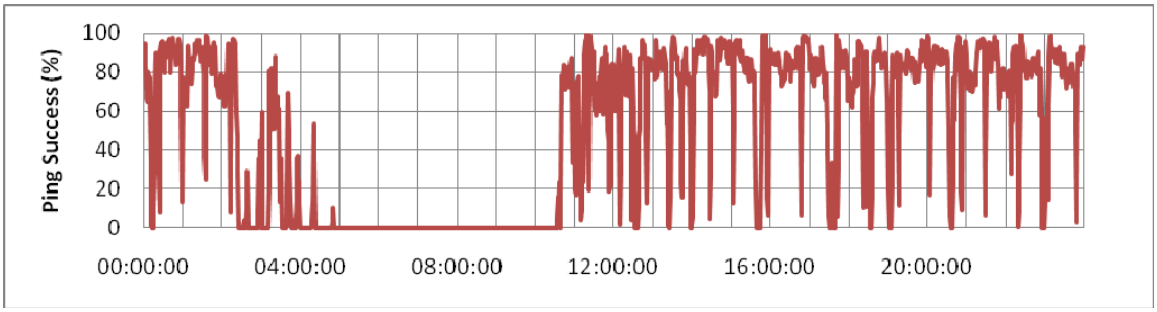

Figure 16: ICMP Network Availability Test Results – 10/13/2007

4.4.2.4 OCTOBER 14, 2007 RESULTS

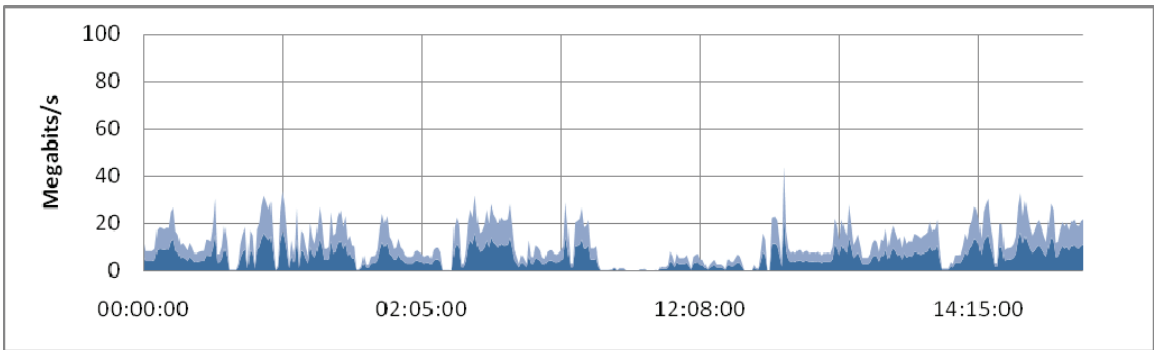

Figure 17: TCP Throughput Test Results in Megabits per Second – 10/14/2007

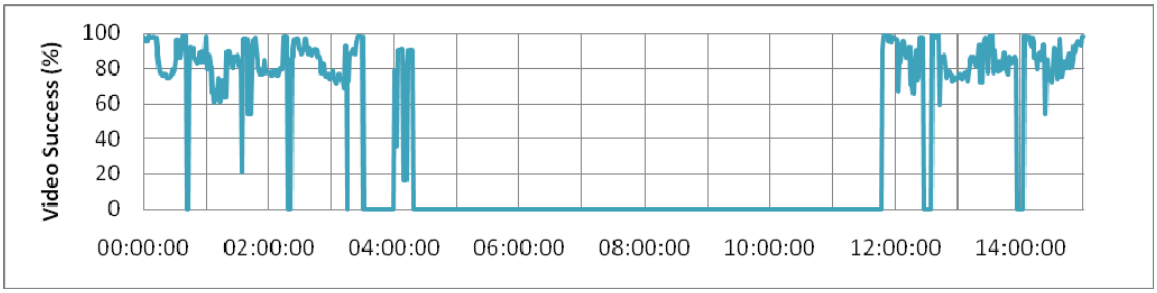

Figure 18: UDP Video Stream Test Results – 10/14/2007

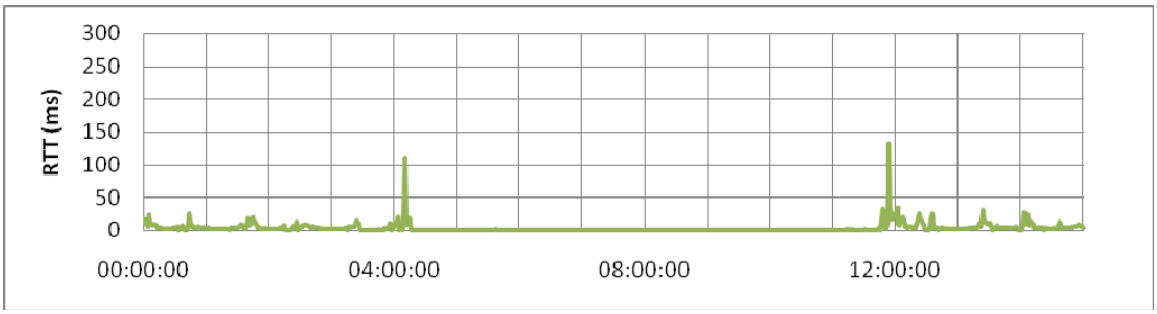

Figure 19: ICMP Network Latency Test Results – 10/14/2007

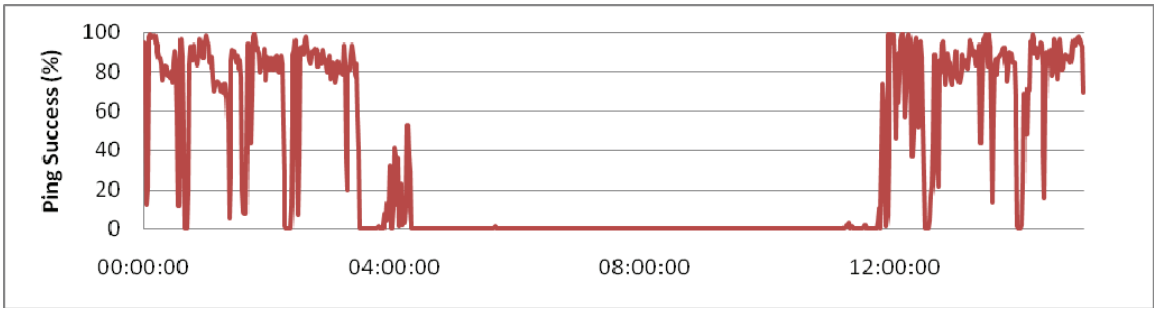

Figure 20: ICMP Network Availability Test Results – 10/14/2007

4.4.3 REPRESENTATIVE TEST 2 RESULTS

4.4.3.1 MAY 9, 2008 RESULTS

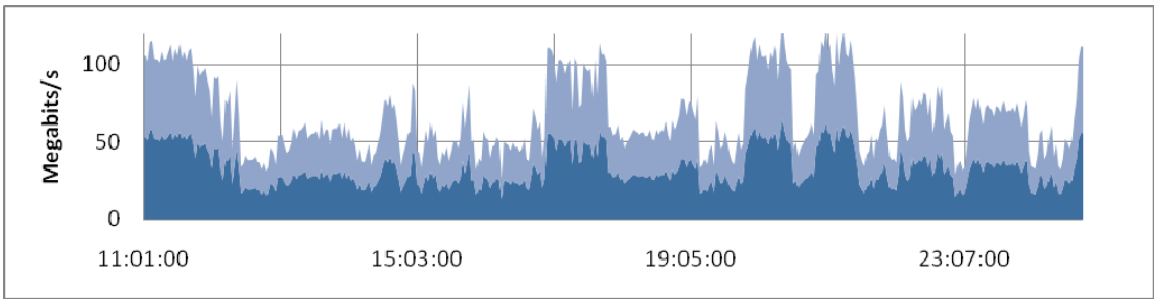

Figure 21: TCP Throughput Test Results in Megabits per Second – 3/9/2008

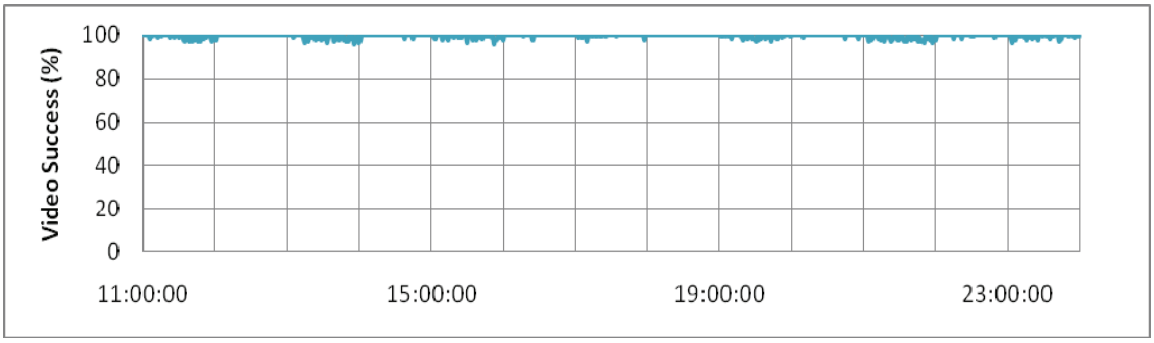

Figure 22: UDP Video Stream Test Results – 3/9/2008

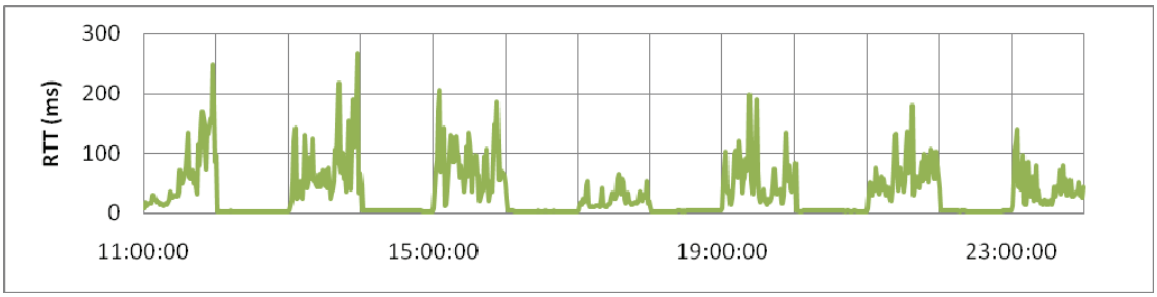

Figure 23: ICMP Network Latency Test Results – 3/9/2008

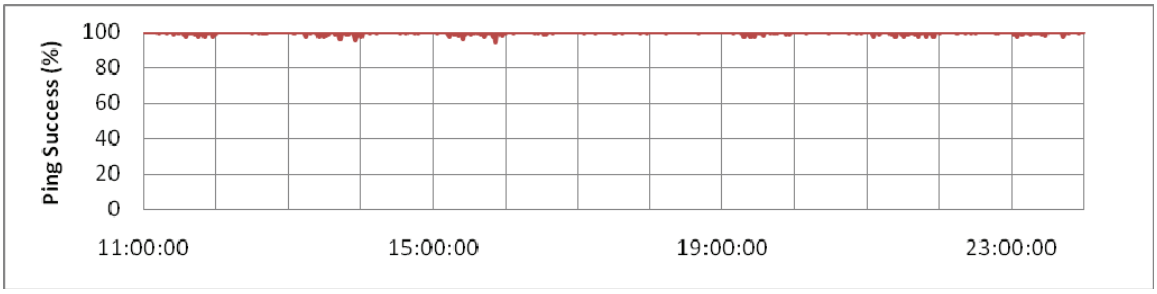

Figure 24: ICMP Network Availability Test Results – 3/9/2008

4.4.3.2 MAY 10, 2008 RESULTS

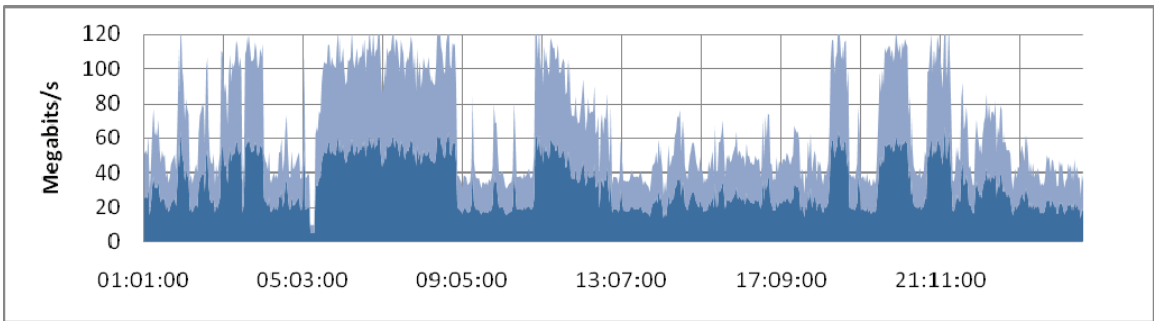

Figure 25: TCP Throughput Test Results in Megabits per Second – 3/10/2008

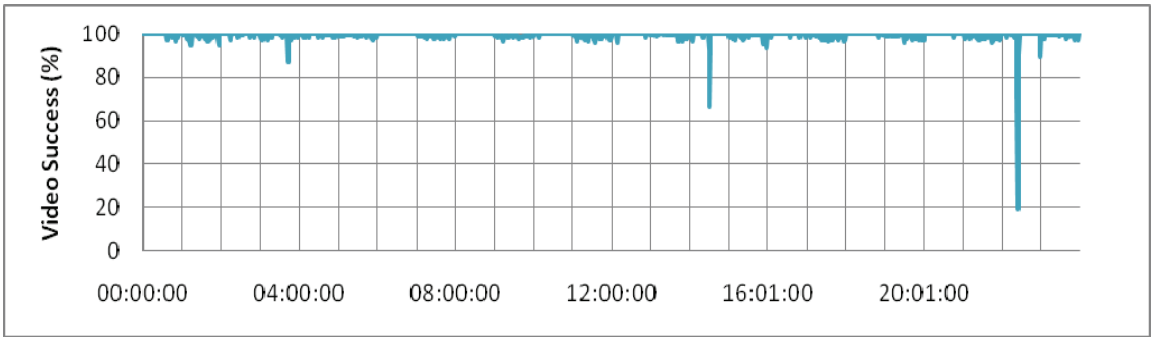

Figure 26: UDP Video Stream Test Results – 3/10/2008

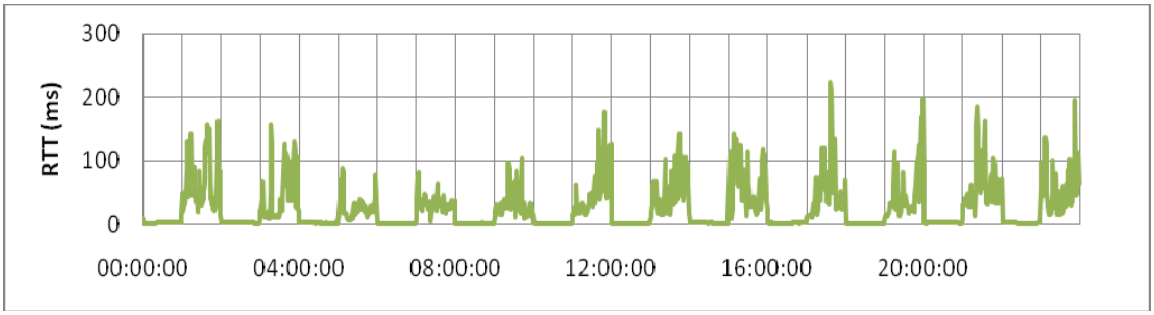

Figure 27: ICMP Network Latency Test Results – 3/10/2008

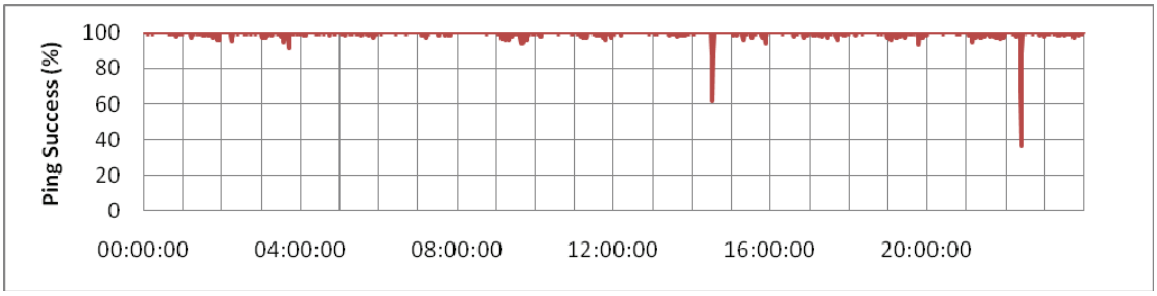

Figure 28: ICMP Network Availability Test Results – 3/10/2008

4.4.3.3 MAY 11, 2008 RESULTS

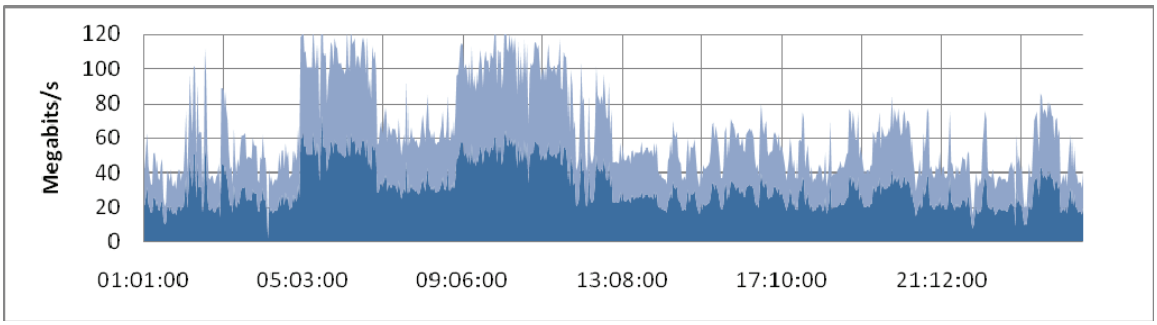

Figure 29: TCP Throughput Test Results in Megabits per Second – 3/11/2008

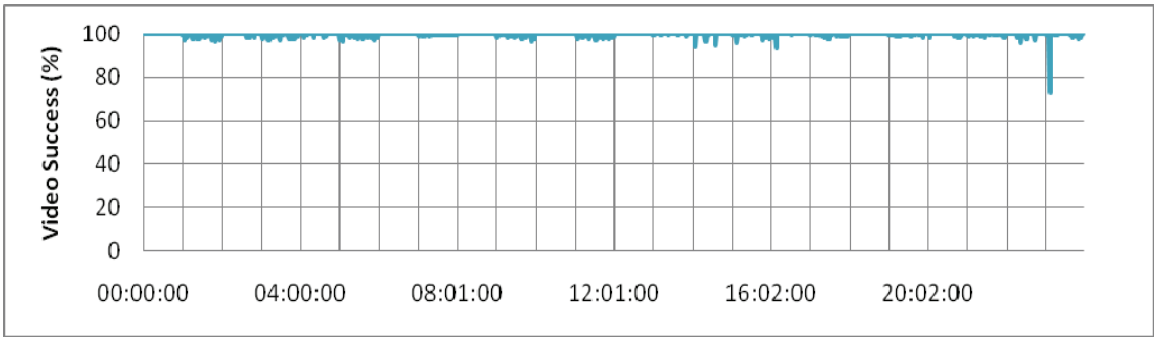

Figure 30: UDP Video Stream Test Results – 3/11/2008

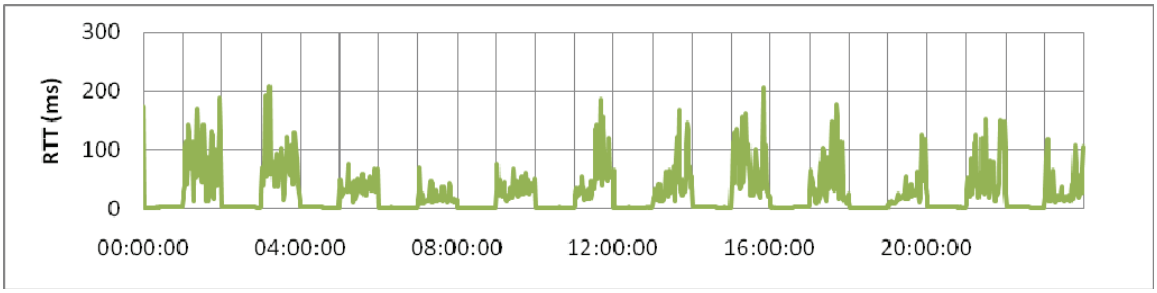

Figure 31: ICMP Network Latency Test Results – 3/11/2008

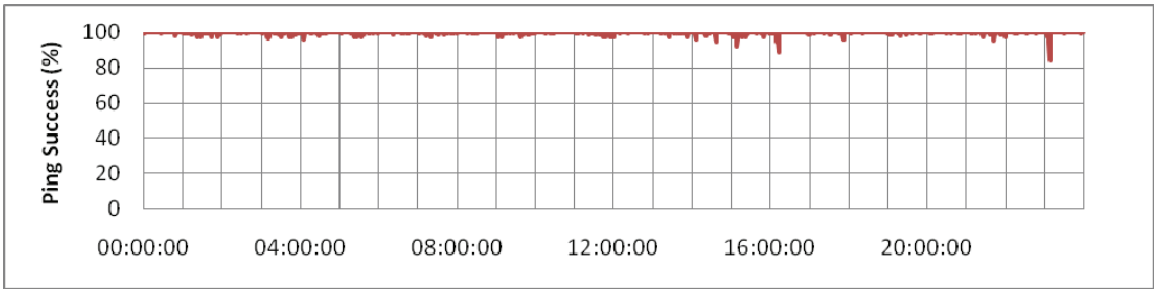

Figure 32: ICMP Network Availability Test Results – 3/11/2008

4.4.3.4 MAY 12, 2008 RESULTS

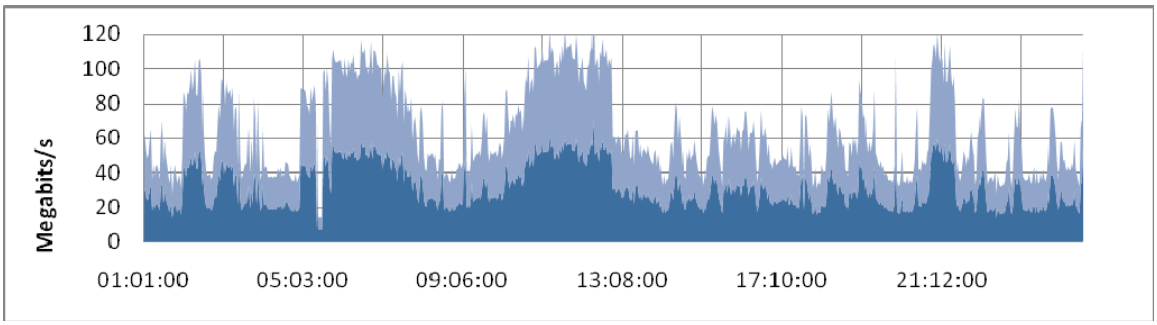

Figure 33: TCP Throughput Test Results in Megabits per Second – 3/12/2008

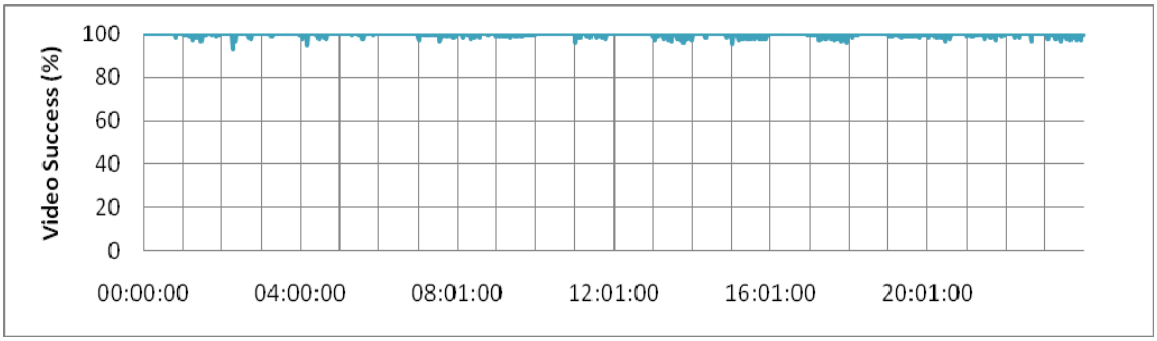

Figure 34: UDP Video Stream Test Results – 3/12/2008

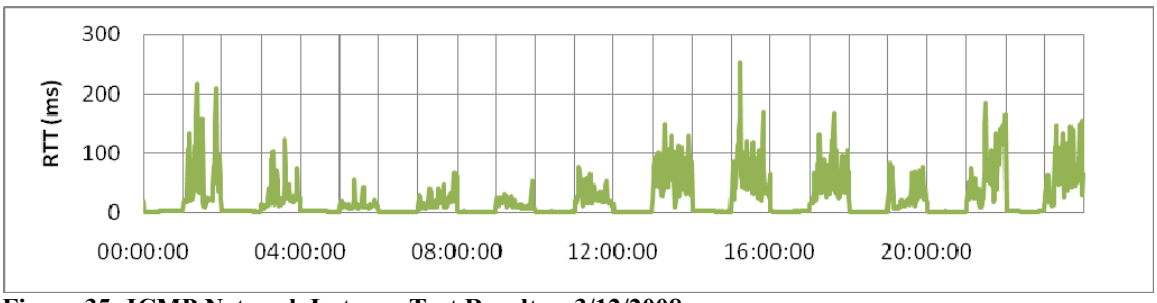

Figure 35: ICMP Network Latency Test Results – 3/12/2008

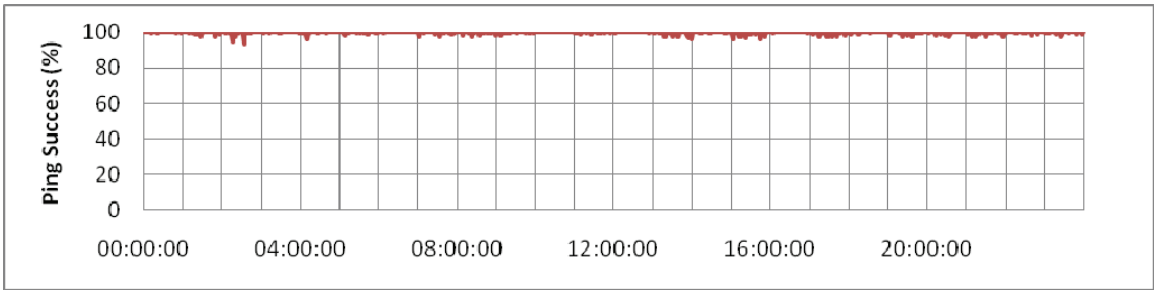

Figure 36: ICMP Network Availability Test Results – 3/12/2008

4.4.3.5 MAY 13, 2008 RESULTS

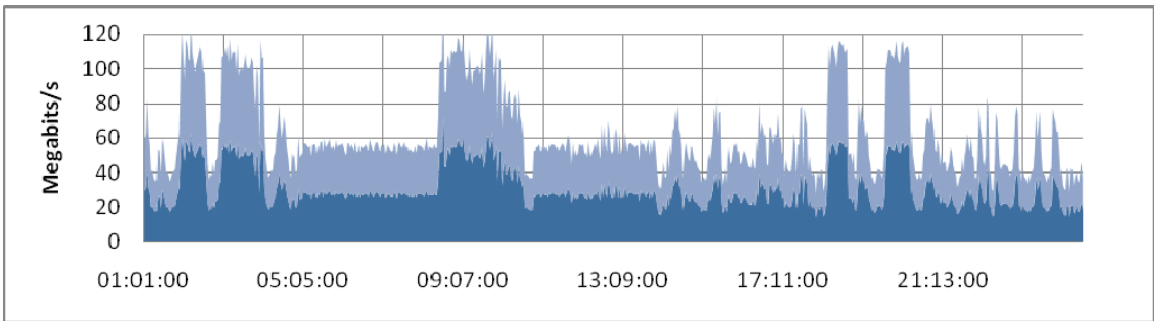

Figure 37: TCP Throughput Test Results in Megabits per Second – 3/13/2008

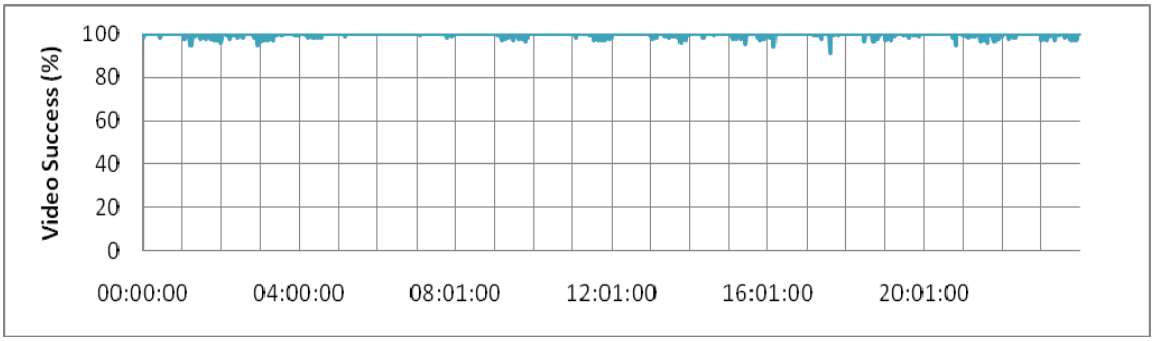

Figure 38: UDP Video Stream Test Results – 3/13/2008

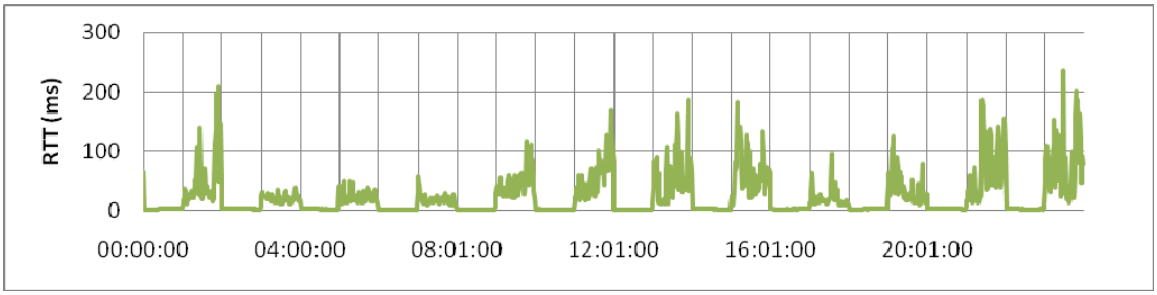

Figure 39: ICMP Network Latency Test Results – 3/13/2008

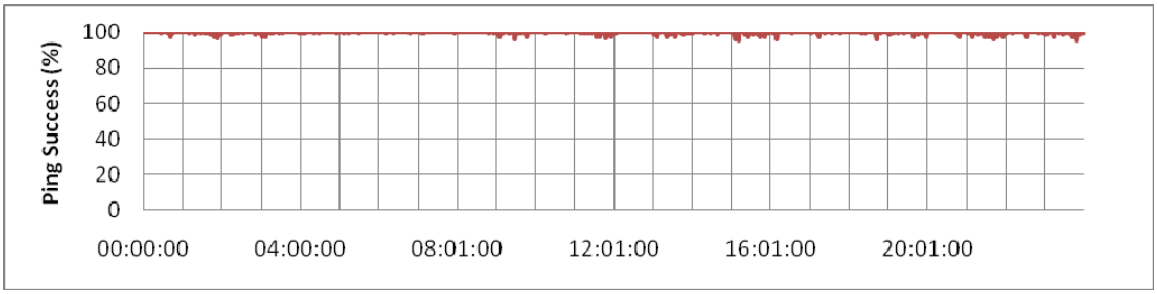

Figure 40: ICMP Network Availability Test Results – 3/13/2008

4.4.3.6 MAY 14, 2008 RESULTS

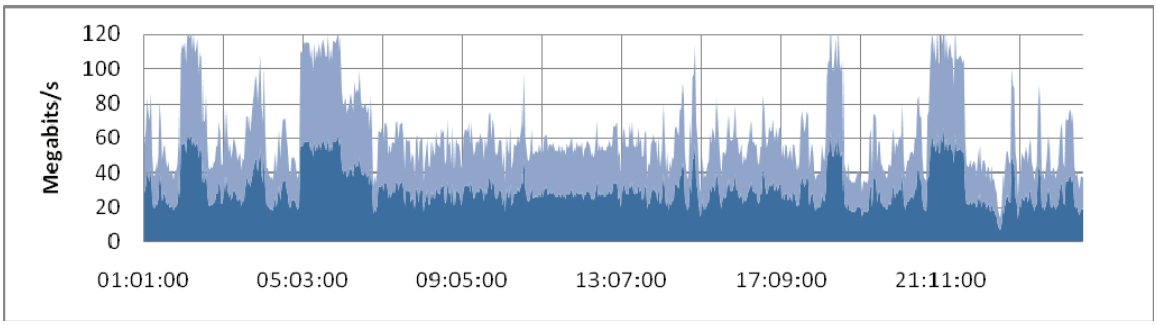

Figure 41: TCP Throughput Test Results in Megabits per Second – 3/14/2008

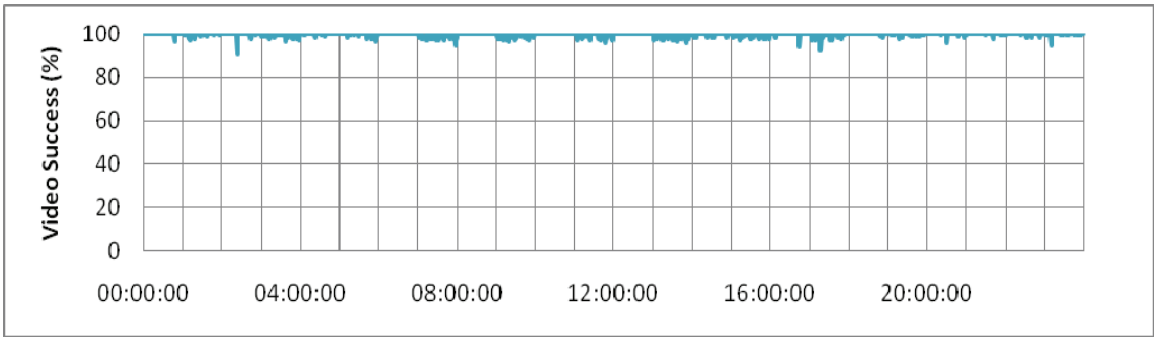

Figure 42: UDP Video Stream Test Results – 3/14/2008

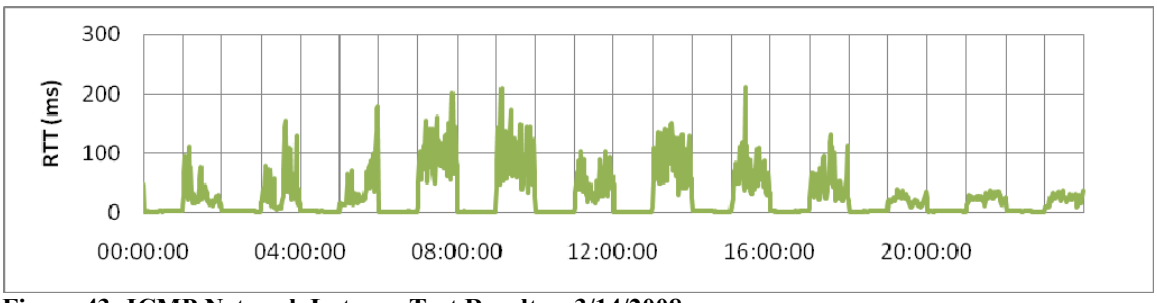

Figure 43: ICMP Network Latency Test Results – 3/14/2008

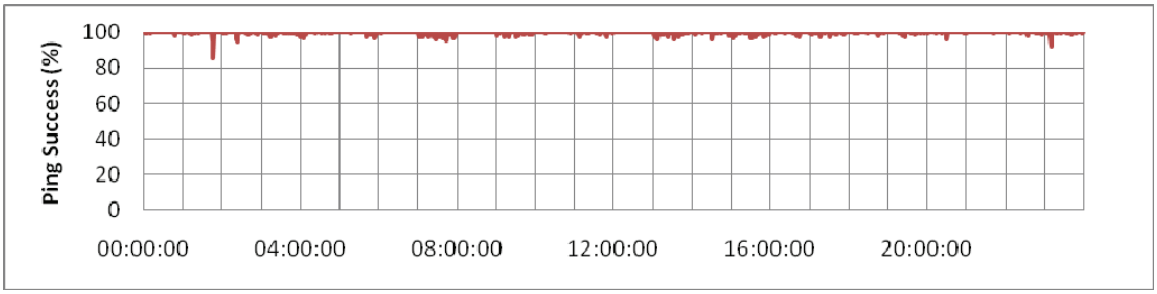

Figure 44: ICMP Network Availability Test Results – 3/14/2008

4.4.3.7 MAY 15, 2008 RESULTS

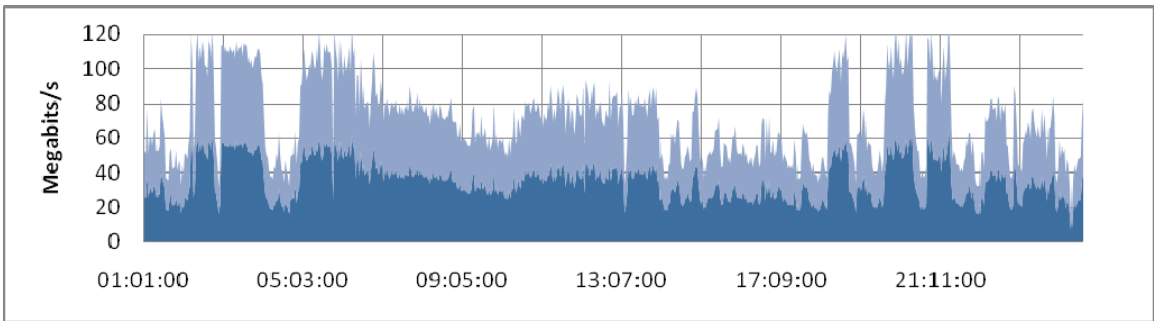

Figure 45: TCP Throughput Test Results in Megabits per Second – 3/15/2008

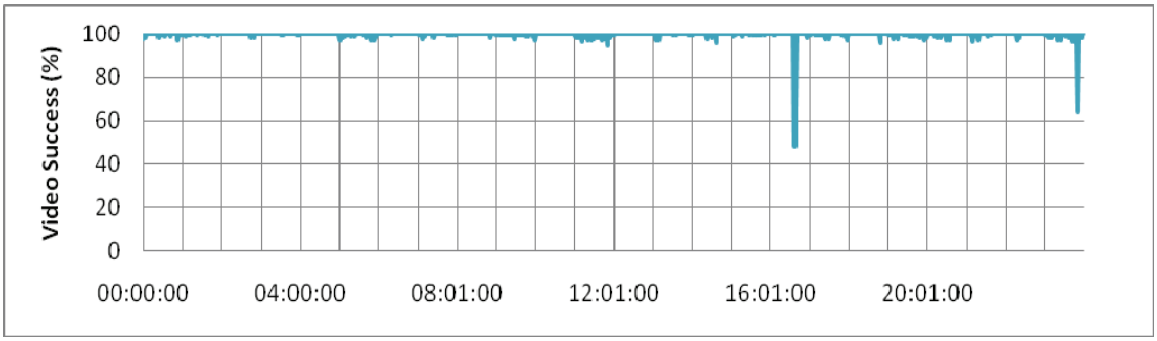

Figure 46: UDP Video Stream Test Results – 3/15/2008

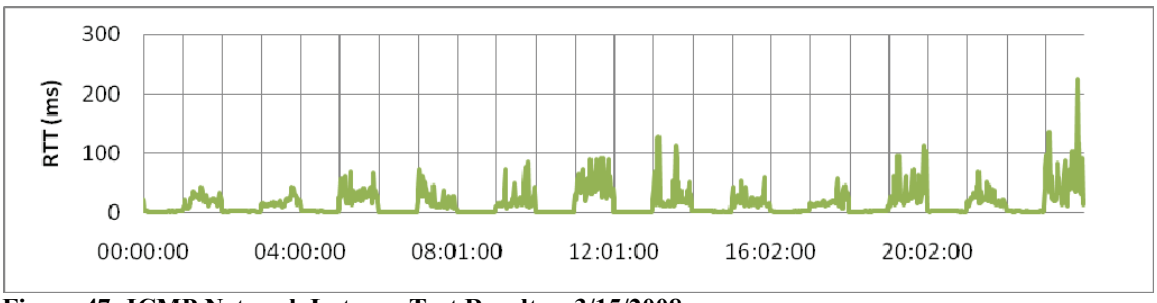

Figure 47: ICMP Network Latency Test Results – 3/15/2008

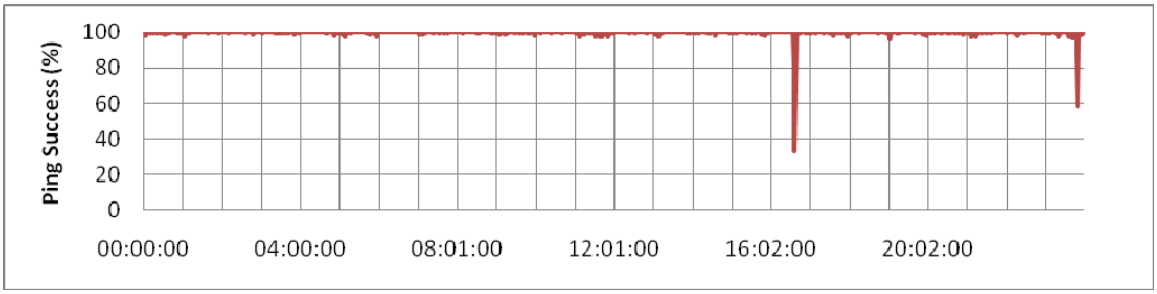

Figure 48: ICMP Network Availability Test Results – 3/15/2008

4.4.3.8 MAY 16, 2008 RESULTS

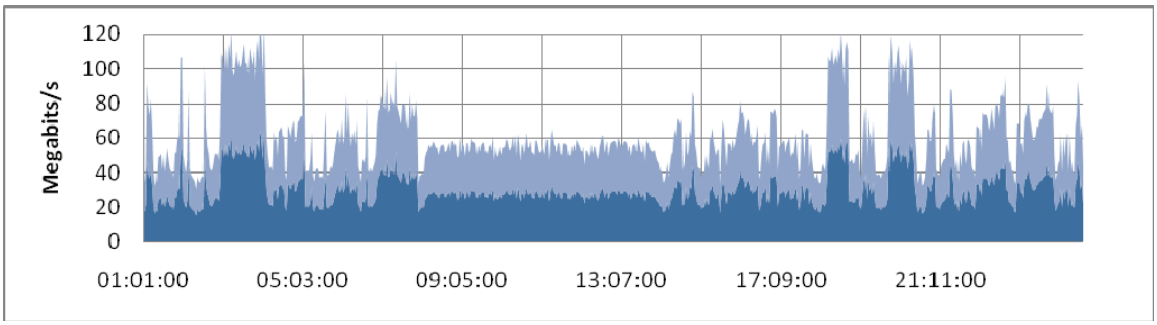

Figure 49: TCP Throughput Test Results in Megabits per Second – 3/16/2008

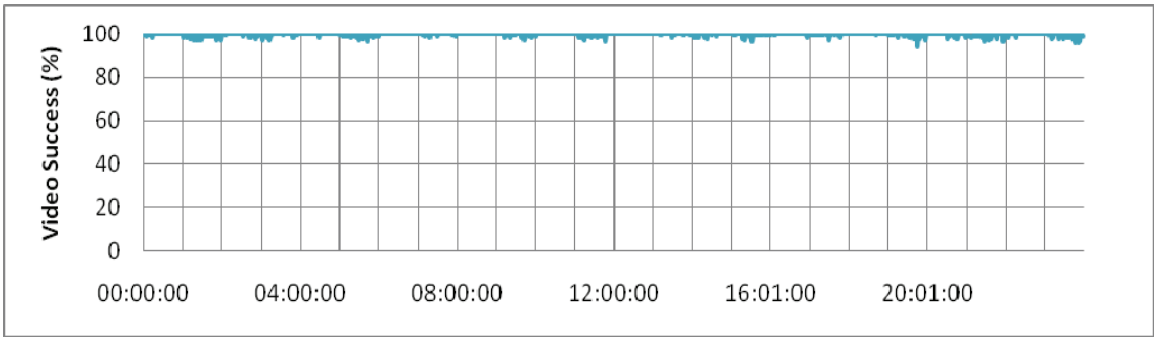

Figure 50: UDP Video Stream Test Results – 3/16/2008

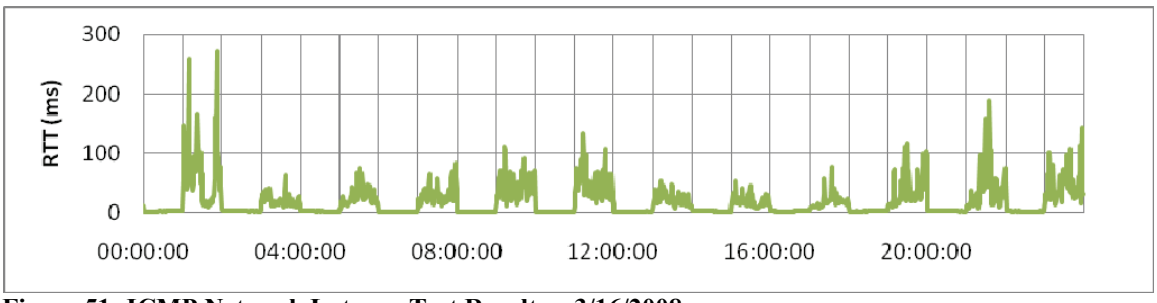

Figure 51: ICMP Network Latency Test Results – 3/16/2008

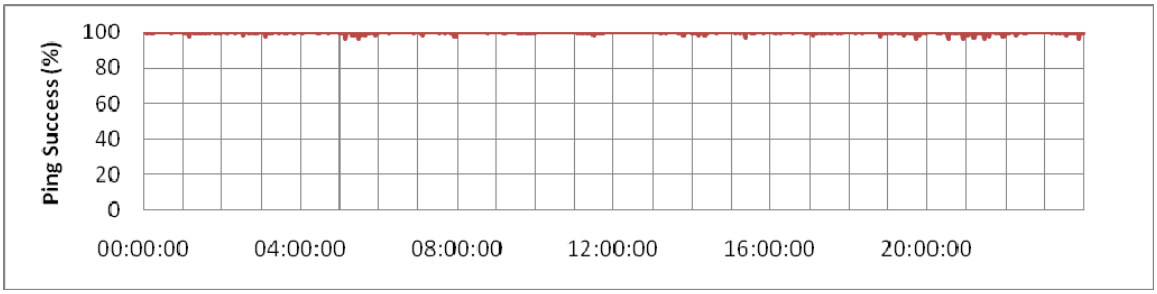

Figure 52: ICMP Network Availability Test Results – 3/16/2008

4.4.3.9 MAY 17, 2008 RESULTS

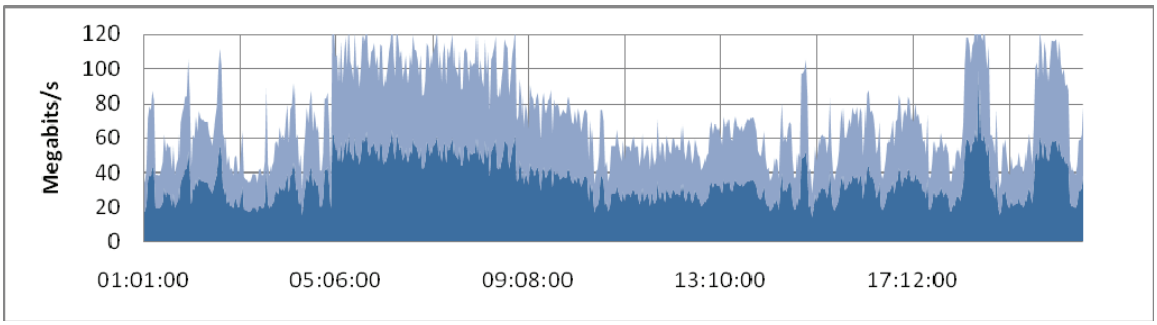

Figure 53: TCP Throughput Test Results in Megabits per Second – 3/17/2008

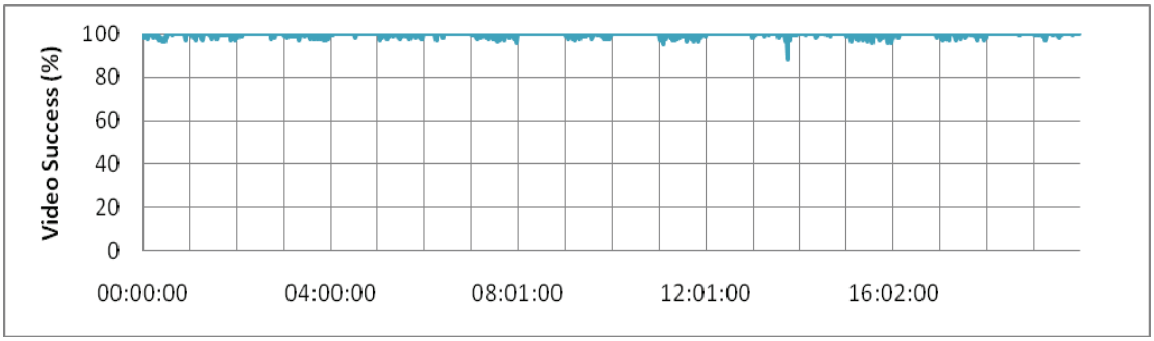

Figure 54: UDP Video Stream Test Results – 3/17/2008

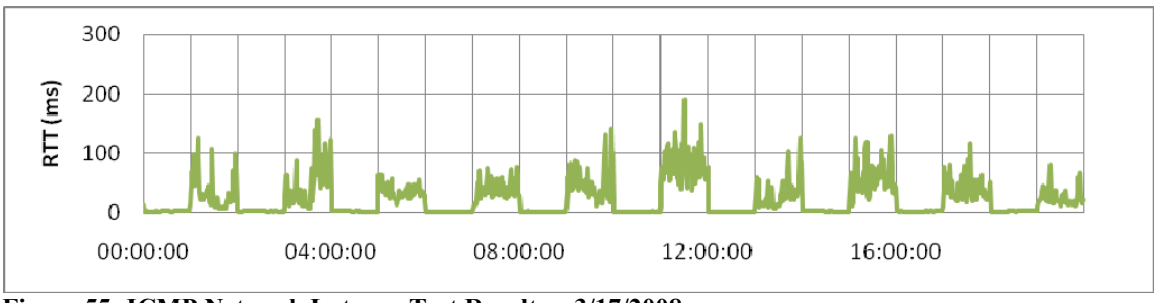

Figure 55: ICMP Network Latency Test Results – 3/17/2008

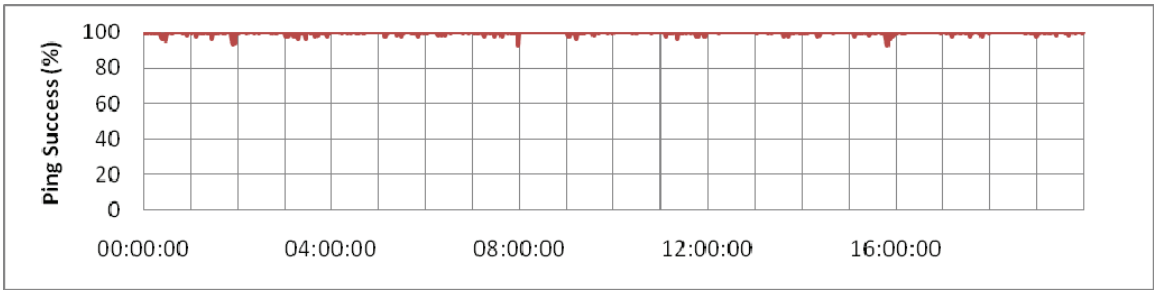

Figure 56: ICMP Network Availability Test Results – 3/17/2008

4.4.4 RADIO STATISTICS

The following tables display the radio statistics collected via SNMP from the ship-to-shore radio links during both tests. The home (primary) ferry terminal was considered to be the terminal where PSC/CAI and Mobilisa located most of their shore-based equipment. In Test 1, the home terminal was considered to be the Fauntleroy ferry terminal, and in Test 2 it was the Port Townsend terminal.

Table 3: Motorola PTP600 Radio Statistics to Home (Primary) Ferry Terminal

	Test1	Test2
Average ship-to-shore signal strength	16.46	99.44
Average Receive Data Rate (Kilobits per second)	18,641	29,576
Average Transmit Data Rate (Kilobits per second)	27,560	50,198

Table 4: Motorola PTP600 Radio Statistics to Secondary Ferry Terminal

	Test1	Test2
Average ship-to-shore signal strength	61.95	32.74
Average Receive Data Rate (Kilobits per second)	21,869	8,140
Average Transmit Data Rate (Kilobits per second)	31,480	11,974

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 OVERVIEW

This section provides a detailed explanation of the raw data collected during the two evaluation periods. Results from the two intervals will be treated separately since there were significant changes to the Prototype Wireless HSD Network prior to the second evaluation period.

5.1.1 TCP THROUGHPUT TEST EXPLANATION

The goal of the TCP throughput tests was to determine whether the Prototype met the success criterion of maintaining at least 25 Megabits per second of available bandwidth at least 99% of the time during the course of the test. TCP is the Transmit Control Protocol, which is the most commonly used Layer 4 protocol used on IP networks. The TCP Throughput test was designed by PSC/CAI to measure the available throughput of Mobilisa's Prototype network as a whole, by sending TCP traffic at the maximum allowable speed from PSC/CAI's Test and Measurement device located aboard the ship to the identical device located at the shore-side terminal.

TCP has several features that make it ideal for taking advantage of dynamic IP networks such as Mobilisa's Prototype network: First, TCP automatically enforces reliability, because every data packet must be confirmed with an acknowledgement packet, or else re-transmitted until it is successfully received. Secondly, TCP automatically handles congestion control using methods called "slow start" and "congestion avoidance," where the congestion window size (and transfer speed) is increased exponentially until a packet is lost, and then backed off until a level is achieved where no congestion is observed. Visually this appears as an equilibrium graph, with many increasingly smaller waves of ramp-up and back-off, until an optimal configuration is found that maximizes throughput while minimizing loss.

Therefore, TCP is an ideal protocol for measuring throughput because it automatically finds the fastest reliable transfer speed for a single TCP stream or multiple TCP streams, despite ongoing changes in available bandwidth and latency on a network.

PSC/CAI utilized an Open Source TCP throughput testing tool called Thrulay, which was developed by researchers from the Internet2 project to measure throughput, delay and jitter on the Internet and Internet2 networks. Thrulay was configured to run two simultaneous TCP streams between ProStructure's two Test and Measurement devices for 52 seconds during every one-minute period. The individual TCP stream throughput as well as aggregated TCP throughput was stored in RRD format (a database format for storing historical data indexed over time) along with the time the test was run. The test duration was specifically chosen to ensure that all delayed packets could be flushed and all data could be recorded before the next minute's test was scheduled.

5.1.2 UDP VIDEO STREAM SIMULATION TEST EXPLANATION

The goal of the UDP video stream simulation test was to determine whether the Prototype network met its success criterion in reliably transmitting video camera traffic at least 99% of the time during the course of the test. UDP is the User Datagram Protocol, which is most commonly used by video streaming applications and is specifically used by WSF's Vigilos surveillance camera system. This test was designed by PSC/CAI by simulate the traffic patterns of 10 simultaneous video streams from 10 individual Vigilos surveillance cameras in order to measure

what percentage of data was successfully received. The 10 simultaneous UDP streams were sent from PSC/CAI's Test and Measurement device located aboard the ship to the identical device located at the shore-side terminal using pre-calculated repeating patterns of data, which can be easily verified unlike real video data.

UDP is sometimes referred to as the *Unreliable Datagram Protocol* by network engineers because it lacks the reliability and congestion controls of TCP. The advantage of UDP is its extremely low overhead and speed, UDP's packet header is only 8 bytes compared to TCP's 20 byte packet header. Because of this, UDP is often used for video streaming applications which can tolerate lost packets (resulting in dropped video frames), which are tolerable to the human eye when viewing 24 frame-per-second or higher video. Because of the lack of reliability and congestion controls, UDP streams are sent at a fixed data rate that cannot adapt to network changes, and lost datagrams are not retransmitted.

PSC/CAI configured Thrulay for the UDP tests to transmit 10 simultaneous 256 Kilobit per second UDP streams, based on information received from Vigilos that its surveillance cameras transmit 16 KB (Kilobytes) size Motion-JPEG video frames at a rate of two (2) frames per second. Therefore, each video feed is estimated at 32 KB/s (Kilobytes per second), or 256 Kb/s (Kilobits per second). Similar to the TCP tests, the UDP video simulation tests were run every minute for 52-second durations, and the results were stored in RRD format.

5.1.3 ICMP NETWORK AVAILABILITY TEST EXPLANATION

The goal of the ICMP network availability test (sometimes referred to as a "ping test") was to determine whether the Prototype network met its success criteria of being continuously connected at least 99% of the time during the test as well as demonstrating network latency of less than 50 milliseconds at least 99% of the time.

ICMP is the Internet Control Message Protocol, it is used by computers on IP networks to send various control and error messages. The Ping program is found in every modern Operating System and is the most widely used utility for testing network availability. Ping works by sending an ICMP echo request to another network device, and waits for a corresponding echo response. By timing the response window, ping is able to report RTT (Round Trip Time) which is the way all network latency is measured.

PSC/CAI designed the test to work by having the two Test and Measurement devices transmit 52 ICMP echo packets using the ping utility during every minute and to record if the response was successfully received. RTT data was received with the ICMP data and was stored in an RRD format.

5.1.4 QOS AND PRIORITIZATION TEST EXPLANATION

The goal of the QoS (Quality of Service) and Prioritization test was to determine whether the Prototype network met its success criteria of being able to guarantee the delivery of the UDP-based video streams at the expense of other traffic as well as to allow WSF staff the ability to disable all non-essential traffic during emergency situations.

An inherent property of modern IP networks is that TCP streams, as described in section 5.1.1 of this report, are continuously testing the maximum available bandwidth before packets are lost. Because of this, all other traffic (such as UDP) which does not have reliability and flow control capabilities registers lost packets. As a result, modern networks which regularly face congestion

must be able to prioritize and guarantee delivery to all protocols that cannot handle flow control but serve critical functions, such as video and voice streams. This is why most modern network routers and wireless bridges support some level of QoS features.

In the first evaluation period, on the M/V Klahowya, PSC/CAI relied on the aforementioned inherent property of networks to demonstrate the effectiveness of any QoS system which may be in place. In the second evaluation period, PSC/CAI changed its testing methodology to better highlight the effects the TCP streams have upon the UDP streams. In this evaluation period, the TCP tests were only run on alternative (odd) hours of the day, to demonstrate the contrast between the odd and even hours of the UDP and ICMP tests.

5.1.5 TCP THROUGHPUT TEST ANALYSIS

During Test1, PSC/CAI observed that throughput from M/V Klahowya to the Fauntleroy terminal was at or above the 25 Mbps threshold 46 percent of the time, although the average bandwidth across the entire test was 25.26 Megabits per second. Figure 57 displays the period October 10, 2007 11:00:00 to October 14, 2007 8:00:00, excluding three periods of time during which connectivity was lost for extended lengths of time due to power disruptions aboard the M/V Klahowya.

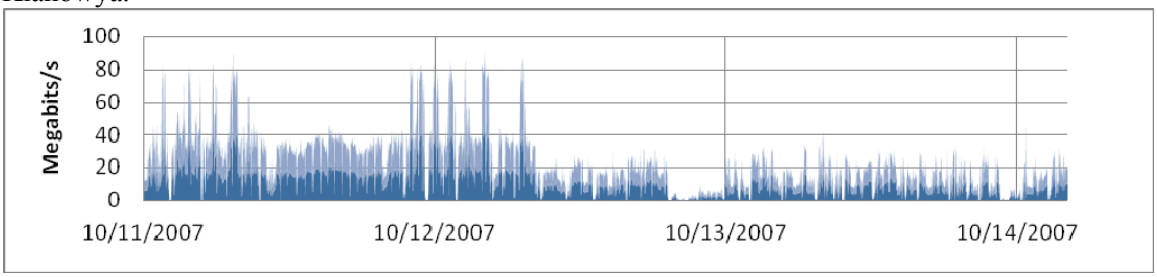

Figure 57: TCP Throughput Test Results – Entire Test Period 1

The above data from the first set of test results has been recalculated removing the throughput numbers from all times where connectivity was lost completely. This is to account for problems reported by Mobilisa during this first testing period.

As is clear from Figure 58, Test2 showed more favorable results than Test1 for the throughput test. The Prototype Wireless HSD Network maintained at least 25 Mbps throughput for over 99 percent of the testing period, with an average throughput across the entire test of 65.20 Megabits per second.

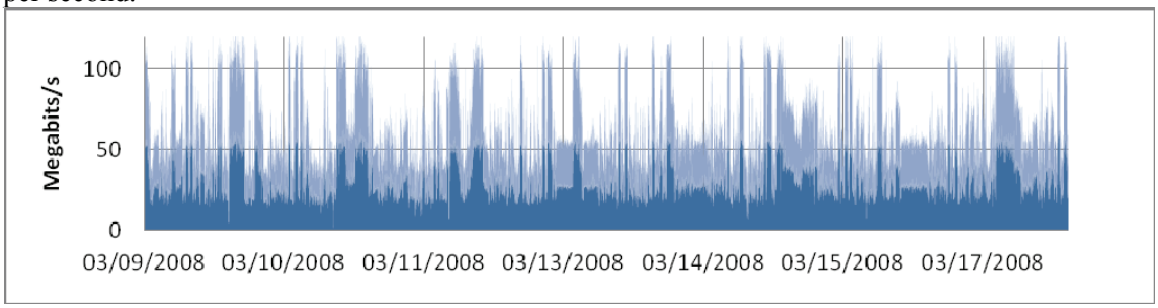

Figure 58: TCP Throughput Test Results – Entire Test Period 2

The difference between the two tests can be explained primarily by the radio statistics from the previous section. The signal strength and negotiated data rates were considerably lower in Test 1 than in Test 2.

5.1.6 UDP VIDEO STREAM SIMULATION TEST ANALYSIS

Camera feed traffic was simulated using UDP streams. This test needed to show a 99 percent success rate of the UDP streams to meet WSF's success criteria.

Figure 59 shows the Test1 results of a UDP stream from M/V Klahowya to the Fauntleroy terminal. In Test1, from October 10, 2007 11:00:00 to October 14, 2007 8:00:00, again excluding times of complete connectivity loss, the video stream test was successful for 36 percent of the testing periods.

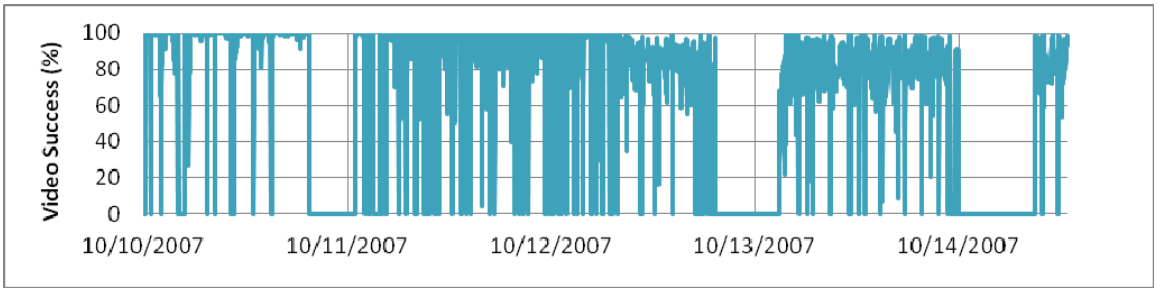

Figure 59: UDP Video Stream Success Test Results – Entire Test Period 1

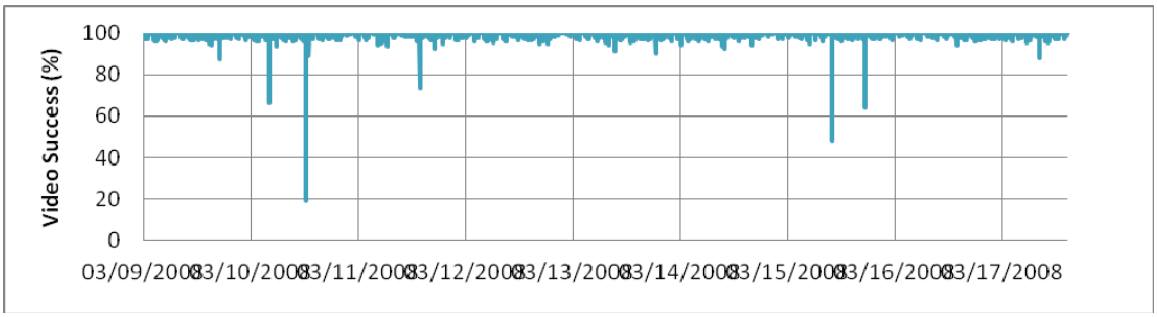

Figure 60: UDP Video Stream Success Test Results – Entire Test Period 2

As with the TCP tests, the greatest observable difference between the two tests is the radio link quality. There were times during which the M/V Klahowya was tied up at night in a location where it had no signal whatsoever, as observed by the GPS data. No such issues were observed during the second test.

5.1.7 ICMP AVAILABILITY AND LATENCY TEST ANALYSIS

Ping is one of the most straightforward methods to verify network availability and latency. In PSC/CAI's tests, a 64-byte packet is sent to a destination IP address, and the sender either receives a response in a timely manner or not. Ping also reports the round trip time.

During the first testing period, from October 10, 2007 11:00:00 to October 14, 2007 8:00:00, excluding three periods during which connectivity was lost entirely, the availability average was 61.37 percent over 5441 data points. This average fell well below the desired 99 percent benchmark.

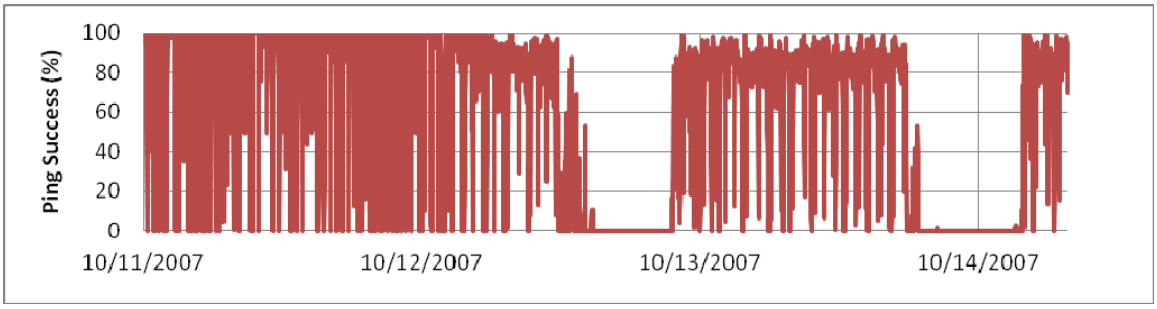

Figure 61: ICMP Network Availability Results – Entire Test 1

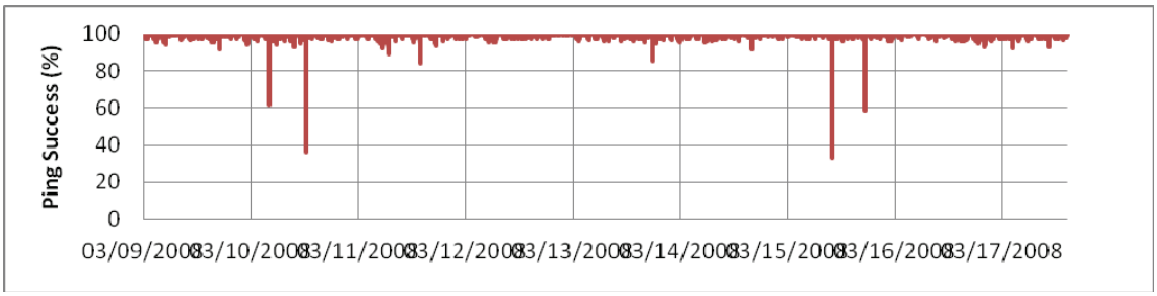

Figure 62: ICMP Network Availability Results – Entire Test 2

Using the same dataset described for the first testing period for ICMP Availability, network latency averaged 11.33ms over 3916 data points. The network delay average fell well within the Vigilos requirement of 50ms for proper video streaming.

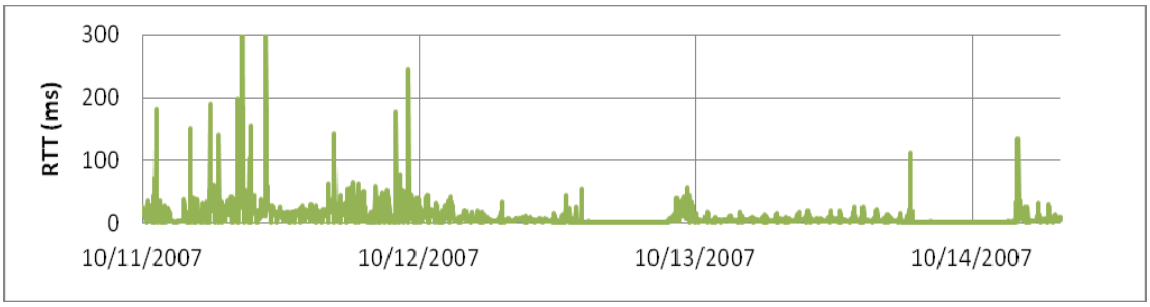

Figure 63: ICMP Network Latency Results – Entire Test 1

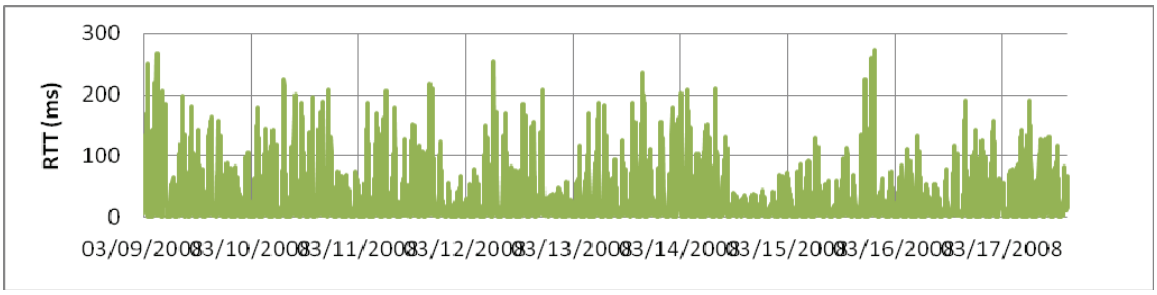

Figure 64: ICMP Network Latency Results – Entire Test 2

As with the TCP and UDP tests, the primary factor for poor network availability in Test 1 was due to poor radio signal strength or lost signal. However, it cannot be explained why the Round Trip Time (latency) is consistently higher in Test 2. This should be studied in detail if and when a larger scale network is planned, as the higher latency and latency variance (jitter) would have a great impact on latency-sensitive applications such as VoIP (Voice over IP).

5.2 LESSONS LEARNED

Part of the usefulness of providing a comprehensive assessment of a transportation project is that issues encountered during the project can be reported, and suggestions can be made to improve the outcome of future projects. Here are outlined suggestions for implementers and overseers of similar projects.

5.2.1 OVERSIGHT ANALYSIS OF PROJECT MANAGEMENT

In the case of this project, the contractor (Mobilisa) scoped both the project and the project oversight. Mobilisa's Implementation Plan specifically dictates the mission, goals, and limitations of the "3rd party evaluator" (PSC/CAI) in a way that would prevent a completely independent verification and validation of its work product. For true third-party oversight, the contractor should have limited influence in this regard. In this case, checks and balances were missing from the project, such that critical questions were not being asked.

In order to improve the oversight of the project, WSF and PSC/CAI reached a compromise agreement by expanding PSC/CAI's role to that of an Independent Verification and Validation (IV&V). However, the IV&V scope was limited to cover only Mobilisa's final work product and excluded the planning, development, and decision making processes of Mobilisa's project.

The changes to scope have not fully rectified PSC/CAI's concerns, because many decisions have been made by Mobilisa which are not fully explained and some of those decisions have resulted in the negative marks noted in section 4 of this report.

5.2.2 TRANSFERABILITY OF RESULTS

The Prototype Wireless HSD Network is transferable, as evidenced by the equipment move during the course of the project. The new environment had a simpler configuration, which resulted in better performance. A few factors influence the transferability, however. First, due to the type of radio equipment selected, which only connects one point to one point, the Prototype Wireless HSD Network would be better suited to an environment where both endpoints are stationary. Secondly, a portion of the Prototype Wireless HSD Network equipment requires a

secured dry closet with power and an uninterruptible power supply (UPS) available. Some smaller vessels may not provide adequate protection for the equipment.

5.3 SCALABILITY AND FEASIBILITY

PSC/CAI believes that several factors affect the scalability and feasibility of this project, these factors are detailed below.

5.3.1 RADIO EQUIPMENT CHOICE

For the Prototype Wireless HSD project, Mobilisa chose to use the Motorola PTP600 point-to-point radio. Mobilisa demonstrated, after the decision process had been completed, CDRL A002 (Technology Analysis Report), a detailed document with tables comparing all of the radio models that it had tested, and sections explaining why it believed the Motorola PTP600 was the best choice for the project.

CDRL A002 did not evaluate all possible vendors and radios, only equipment from vendors which were able to *"provide adequate information or a product demonstration"* in an unspecified timeframe. These radios were evaluated for throughput, RF characteristics, security capabilities, management, and operating capabilities. The chart in CDRL A002 contained some errors.

Unfortunately, CDRL A002 does not state if the question was asked "How feasible are these radios in a large scale deployment of mobile marine vessels?" If this question had been considered, PSC/CAI believes that the Motorola PTP600 would have been eliminated from the evaluation. This is because the Motorola PTP600 is a pure point-to-point radio designed to work in pairs in fixed operation. A "base station" will not allow multiple clients to associate, nor will clients re-associate to a stronger base station as with Point-to-Multipoint wireless systems. In fact, the Motorola PTP600 must be manually re-configured and rebooted to associate with a different unit.

This point-to-point behavior has caused large problems throughout the entire test, for example when the M/V Klahowya, a bi-directional vessel, would have to "flip" to operate opposite its usual direction. In these cases, neither ship-to-shore radio aboard the M/V Klahowya would be pointing at the usual base station, causing the vessel to have no connectivity. A point-to-multipoint system would gracefully re-associate all client radios to the strongest base station with minimal loss of connectivity.

From a scalability perspective, the point-to-point nature of the PTP600 radio makes it infeasible. In order to maintain above 99% coverage for the Triangle run, where 3 vessels operate simultaneously between 3 ferry terminals, a total of 6 Motorola PTP 600 radios would be required at each location (1 radio for regular operation, and 1 for "flipped" operation), resulting in the need for 32 radio pairs. These 32 radio pairs would not be able to share the limited number of channels available in the 5.8 GHz spectrum frequency.

5.3.2 RADIO FREQUENCY CHOICE

For the Wireless HSD project, as stated in CDRL A002, Mobilisa chose to use the 5.8 GHz ISM (Industrial, Scientific and Medical) band because of the large number of available non-overlapping channels, relatively high maximum transmit power, and the convenience of using

unlicensed frequency. Unfortunately, by definition the unlicensed ISM can be used for private, public, and personal use with no mediation or arbitration from the FCC.

The primary danger of using the ISM band is that it will continually grow more crowded over time, as new non-WSF systems are brought online that will interfere with the Prototype Wireless HSD system, affecting available bandwidth and reliability. Another danger is equipment designed to transmit at very high power in the 5 GHz band is extremely inexpensive. Malicious parties which choose to attack the ferries could build an effective portable jamming system with considerably less effort and resources than would be required if WSF was using specialized public safety bands.

5.4 APPRAISAL OF EVALUATION PROCEDURES AND RECOMMENDATIONS FOR IMPROVEMENT

As explained in Section 5.2 above, the quality assurance and oversight processes were initiated in a way that was not in WSF's best interest. PSC/CAI recommends that WSF strictly enforce the State of Washington's own IV&V and project oversight requirements for all future projects, rather than allowing the contract to define or limit oversight. In this way, the interests of Washington taxpayers will be better served in future projects.

5.5 POSSIBLE USES OF THE TECHNOLOGY

Lessons learned through the Prototype Wireless HSD Network project could be applied to other networking situations. For instance, the technology presented in this project could be used to provide a wireless backhaul for WSF customer wireless access. The results are applicable even better, perhaps, for providing a very high bandwidth and shorter distance network links between stationary bases, such as between two office buildings.

APPENDIX A DETAILED DATA COLLECTION DESIGN

A.1 THE SELF-CONTAINED TESTING PLATFORM

PSC/CAI has developed a platform for performing autonomous testing and measurement of IP-based networks. The system is designed to require no human intervention after installation in order to minimize variance and human error. The testing and measurement platform continually collects a pre-defined set of metrics and logs all data to a time-based database. At the end of the test, all of the collected data may be viewed and graphed across any relevant time period.

PSC/CAI's testing platform is both secure and rugged, yet built using entirely COTS (Commercial off the Shelf) components in order to maximize its value and interoperability. The systems are designed to handle both hostile network environments as well as a wide range of inhospitable weather conditions.

Figure 65: ProStructure Principal Irving Popovetsky performing a final check of the Test and Measurement device aboard the Steilacoom II

A.1.1 HARDWARE

At the heart of PSC/CAI's testing and measurement platform lays a VIA-based SBC (Single Board Computer) designed for embedded applications. The Jetway Versa J7F4K1G5D board was chosen for its high performance in networking and cryptographic applications. It features a crypto acceleration module and dual Gigabit Ethernet network interfaces. The board is installed in a chassis with an LCD-based information display, which PSC/CAI uses to display critical system statistics.

The system is enclosed in a weatherproof Pelican 1440 Top Loader Case. These cases will withstand temperatures from -10°F (-23.3°C) to +210°F (98.9°C). All Pelican cases have been tested to MIL-C-4150J, ATA 300, Def Stan 81-41/STANAG 4280 and Ingress Protection (IP) 67. For power and network ports, PSC/CAI is utilizing Bulgin Buccaneer IP68-rated BNC-style plugs and sockets. For shock and vibration proofing, the system has almost no moving parts, and is shock mounted inside of the Pelican case.

Figure 66: PSC/CAI Test and Measurement Device (Closed)

Figure 67: PSC/CAI Test and Measurement Device (Open)

A.1.2 OPERATING ENVIRONMENT

Redhat Enterprise Linux 5 was chosen because it is well suited for assured computing in government and enterprise environments, and it is also well suited for embedded deployments. RHEL5 has achieved Common Criteria EAL4+/CAPP/RBAC/LSPP certification by the National Information Assurance Partnership (NIAP), which is operated by the NSA. This makes RHEL5 suitable for any situation that requires Director of Central Intelligence Directive (DCID) 6/3 at Protection Level 3, which specifies intelligence-related information security measures.

In addition to using a certified Operating System, PSC/CAI also applies ProStructure's proprietary system hardening procedure to the systems. PSC/CAI utilizes this process in Information Security audit and assessment engagements for large business and government clients.

A.2 TEST AND COLLECTION TOOLS

PSC/CAI utilizes Open Source testing tools in order to maximize interoperability and reproducibility. None of the source code for the tools has been modified and all of the configuration options are listed in this plan. This allows any party to verify PSC/CAI's test results with minimal resources and expenditure. The tools used in the present evaluation are listed below.

A.2.1 THRULAY

Thrulay 0.9, once named Iperf2, was developed by Internet 2 researchers that wished to measure Throughput, Delay and Jitter. Thrulay 0.9 was obtained from SourceForge.net.

A.2.2 PING

PSC/CAI will be using the standard Linux ping command (/bin/ping), from the RHEL5 iputils-20020927-43.el5 package.

A.2.3 RRD

RRD is the Round Robin Database, the Open Source industry standard high performance data logging and graphing system for time series data. Tobias Oetiker, the author of MRTG, developed RRD. MRTG and RRD are used in almost every commercial and public network for collecting and graphing network performance statistics.

A.2.4 A NOTE ABOUT VIDEO STREAMING

PSC/CAI has chosen not to use a video streaming tool for its evaluation. This is because most video streaming platforms are not designed for test and measurement, and most are not designed to log dropped frames, lost or retransmitted data, etc. in a bi-directional fashion. Therefore, PSC/CAI believes that it is better to use true network test and measurement tools to benchmark the network and then to predict how the video platforms will perform.

A.3 TESTS

PSC/CAI ran several continuous and one period test. These tests all run in parallel, and all results are available in RRD for correlation.

A.3.1 THRULAY BANDWIDTH TEST

Two separate Thrulay instances were operated. The first Thrulay instance simulates high-priority Vigilos security camera traffic by sending 10 simultaneous streams of UDP (User

Datagram Protocol) traffic of 256 Kilobits per second each, totaling 2.56 Megabits per second. This test was initiated every minute, and operated for 52 seconds.

The second Thrulay instance simulated non-priority office traffic. Two simultaneous TCP (Transmit Control Protocol) streams operated on a non-priority port. Unlike the UDP tests, which send traffic at a fixed level, the Thrulay TCP test allows the system's TCP/IP network stack to determine the best possible transmit speed. This test was initiated every minute, and operated for 52 seconds.

A.3.2 ICMP ECHO/RESPONSE (PING)

ICMP echo/response packets were continuously sent between the two Network Test and Measurement devices. The ping command was initiated every minute to send 52 ICMP echo requests of standard size (64 bytes).

A.3.3 DISRUPTIVE NETWORK TESTS

In addition to the continuous tests detailed above, PSC/CAI periodically initiated a suite of disruptive network tests meant to simulate malicious traffic. Every three hours, beginning at Midnight, this suite of tests operated for 10 minutes.

A.4 PERFORMANCE METRICS

PSC/CAI will collect the following metrics every minute and log them into RRD.

A.4.1 THRULAY HIGH-PRIORITY (UDP)

- Average Round-trip Delay (ms)
- Packet Loss (%)
- Average Jitter (ms)
- Packet Duplication (%)
- Packet Reordering (%)

A.4.2 THRULAY LOW-PRIORITY (TCP)

- Average Throughput (Megabits/sec)
- Average Round-trip Delay (ms)
- Jitter (ms)

A.4.3 ICMP

- Packet loss (%)
- Round-trip time (Average)
- Round-trip time (Minimum)
- Round-trip time (maximum)
- Round-trip time (Mean deviation)

A.4.4 GPS DATA

- Latitude/Longitude
- Heading
- Speed

A.4.5 MOTOROLA PTP600 RADIO DATA

- SNMP Object Group motorola.ptp.phyStatus
  - receivePower (Receive power expressed in tenths of a dBm)
  - transmitPower (Transmit power expressed in tenths of a dBm)
  - range (Distance between the two peer wireless units expressed in tenths of a kilometer)
  - linkLoss (The wireless link loss expressed in tenths of a dB)
  - receiveChannel (Current active receive channel)
  - transmitChannel (Current active transmit channel)
  - receiveModulationMode (Current active receive modulation mode)
  - transmitModulationMode (Current active transmit modulation mode)
  - receiveFreq (Current receive frequency expressed in MHz)
  - transmitFreq (Current transmit frequency expressed in MHz)
  - signalStrengthRatio (Signal strength ratio (Vertical / Horizontal) expressed in tenths of a DB)
- SNMP Object Group motorola.ptp.PubStats
  - receiveDataRate (Average data rate over the last one second interval expressed in kbps)
  - transmitDataRate (Average data rate over the last one second interval expressed in kbps)
  - aggregateDataRate (Average data rate over the last one second interval expressed in kbps)
- SNMP Object Group motorola.ptp.Encryption
  - encryptionAlgorithm (The encryption algorithm used by the wireless link)

A.4.6 NOTE 1: REPORTING OF TEST AVERAGES

On all tests above where "Average" is noted, the average is calculated only over the 1-minute time period of the test. Aggregate averages are extrapolated from RRD and calculated after the tests are complete.

A.4.7 NOTE 2: DIFFERENCES IN TCP VS. UDP

Due to the nature of TCP, errors such as packet loss, duplication, and reordering are automatically handled by the system's TCP/IP network stack and are therefore not reported by Thrulay.

A.5 PLANS FOR VERIFIABILITY

PSC/CAI will take several measures to ensure the integrity of the collected data.

A.5.1 PHYSICAL SECURITY MEASURES

Although it is impossible to prevent tampering or intrusion on the console, PSC/CAI has implemented the following measures in order to detect if a system has been compromised:

- Tamper evident strips were installed inside of the Pelican 1440 case in order to detect unauthorized opening of the case.
- The systems were monitored for physical link failure in order to detect unplugging or tampering with the network links. Any network link failures were treated as unplanned and were investigated by PSC/CAI personnel.
- The systems were monitored for reboots during the tests in order to detect potential intrusion on the console. Any reboots were treated as unplanned and were investigated by PSC/CAI personnel.

A.5.2 INFORMATION SECURITY MEASURES

- The testing systems continuously transmit key system data to each other, including system logs and health information. This data was also transmitted off-site when possible.
- On a periodic basis, the systems back up and checksum the RRD database. This backup was transmitted off-site when possible.
- On a periodic basis, the systems perform a suite of automated system security checks including the file and configuration modification detection tool AIDE, a Rootkit scanner, as well as additional security verification checks used by ProStructure Consulting during Forensic Investigations and Security Assessments.
- The systems are hardened using ProStructure's proprietary system hardening techniques.
- The systems are time synchronized using NTP (the Network Time Protocol).

A.5.3 PRE-DEPLOYMENT BASELINES

PSC/CAI performed thorough baseline testing of the systems and all testing tools in controlled laboratory environments before they were deployed in the field. When the tests were complete, ProStructure performed all of the baseline tests again to ensure that they are consistent with one another. This consistency of results ensures the integrity and reproducibility of the testing infrastructure.

APPENDIX B TECHNICAL GLOSSARY

Line-of-Sight (LOS): Line-of-Sight is an RF (Radio Frequency) Engineering term referring to the fact that radio signals travel in a straight line, and that radio signals are strongest when they have travelled in a straight line from the point of transmission to the receiver. Radio signals are degraded when they are reflected, refracted, or absorbed by physical objects.

Omni-directional Antenna: An Omni-directional antenna is one which radiates signal evenly along one plane. Omni-directional antennas are typically vertically oriented and pole-shaped, allowing for transmission and reception of signal in 360 degrees. The radiation pattern of a typical Omni-directional antenna can be described as "donut shaped."

Sector Antenna: A Sector Antenna is a type of directional antenna. Unlike an Omni-directional antenna, a directional antenna concentrates the signal power in a specific pattern. The more the signal is concentrated, the narrower the radiated beam becomes. Sector antennas typically create a "pie shaped" radiation pattern and are most commonly used for point-to-multipoint base stations such as cellular phone towers.

Signal Strength: Signal strength refers to the power of the received signal, expressed in dBm (decibels with a reference quantity of one milliwatt). dBm is expressed by a base-10 logarithmic scale. For example, a signal strength of 36 dBm is equal to 4 watts, which is the maximum transmit power allowed by the FCC in the ISM band. 0 dBm is equivalent to 1 milliwatt. -90 dBm is equal to 0.000000001 milliwatts, which is generally the lowest strength usable by most WLAN device.

Point-to-Point (wireless): In wireless applications, point-to-point systems are typically ones where pairs of stationary (fixed) radios communicate solely with each other using highly directional antennas.

Point-to-Multipoint: Point-to-multipoint wireless applications involve a single or multiple common Base Stations and multiple clients. The base stations will typically use Omni-directional or sector antennas, while fixed clients will use highly directional antennas and mobile clients will use Omni-directional antennas. It is usually up to the client to select the strongest base station among a common system.

Quality of Service (QoS): Quality of Service is utilized in modern packet-switched networks to guarantee or reserve a set amount of bandwidth and priority to certain types of traffic by delaying the packets of other types of traffic. For example, VoIP (Voice over IP) traffic requires a fixed amount of bandwidth and latency or else the caller's voice will become disrupted. In this case QoS is used to prevent other applications, such as file downloads, from disrupting the call. This is in contrast to classic circuit-switched networks, where each application has a dedicated physical circuit between two points.

Bandwidth: Bandwidth refers to a maximum data rate typically expressed in bits per second. Bandwidth is a term that is usually used metaphorically to mean throughput, which is the maximum achievable data rate possible on a network. Originally bandwidth was an analog communications term.

Stream: In TCP communications, a stream is a stateful connection made by two applications consisting of many packets. Each stream is usually identified by a known destination port or a server with a unique source port from a client. Although UDP is stateless, a stream can still be created and maintained by the applications involved.

Real-time: Real-time is a computing term referring to data that must be delivered immediately, as opposed to batch or delayed data transmission. Real-time delivery of data is most important when there are humans viewing the data at one or both ends of the communication.

Latency: Latency is a measure of how much time is required for packets to travel across a network. Latency is usually expressed as Round Trip Time (RTT), which is a measure of time taken for a packet to travel to its destination plus the time required for the acknowledgement packet to travel back.

Jitter: Jitter is *"a metric for variation in delay of packets across Internet paths. The metric is based on the difference in the One-Way-Delay of selected packets"* according to IETF RFC 3393. Jitter is particularly important to some applications such as VoIP, which can adapt to handle a fixed level of delay on a network, but are more greatly affected by varying levels of delay.

AES: AES is the Advanced Encryption Standard, which was adopted as an encryption standard by the U.S. Government in 2002. It has been thoroughly reviewed and tested by cryptologists worldwide and is considered to be the most effective encryption cipher for use in securing communications.

FIPS 140-2: FIPS 140 is Federal Information Processing Standard 140, a publication from the U.S National Institute of Standards and Technology (NIST). FIPS 140-2 defines security levels and acceptable encryption technologies and configurations deemed suitable for U.S. Government agencies.

INDEPENDENT VERIFICATION AND VALIDATION OF WASHINGTON STATE FERRIES' WIRELESS HIGH SPEED DATA PROJECT

EVALUATION PLAN

Contract # AD00013

October 3, 2007

Prepared by:
CASE Associates Inc.
in conjunction with ProStructure LLC
14674 SE Sunnyside Road #148
Clackamas, Oregon 97015
(503) 658-0727

Table of Contents

1 INTRODUCTION

1.1 PROJECT SUMMARY

CASE Associates, Inc. (CAI) in conjunction with ProStructure Consulting (PSC) has been engaged by Washington State Ferries (WSF) to provide Independent Verification and Validation (IV&V) of the Prototype Wireless High Speed Data (HSD) Network as implemented by Mobilisa. Mobilisa is implementing the Prototype Wireless HSD Network under contract to the Federal Transportation Administration, in cooperation with WSDOT, in order to increase the available bandwidth to the Ferry vessels for security and monitoring purposes.

1.2 PURPOSE

Mobilisa's Prototype Wireless HSD Network must meet criteria set forth by WSF in the categories of Available Throughput (Bandwidth), Network Delay, and Network Availability. The purpose of this project is to independently verify Mobilisa's reported performance and availability numbers and to independently validate Mobilisa's testing criteria and methodology.

1.3 SCOPE

Originally, PSC/CAI was engaged by WSF to perform Project Management analysis and passive technical analysis of the HSD Wireless Network project. Since the project's commencement, several changes were made to the scope of PSC/CAI's project with WSF. The scope of PSC/CAI's project was expanded to include full Independent Verification and Validation (IV&V) of Mobilisa's completed deliverable in the HSD Wireless project. It should be noted that the new scope only allows for full IV&V of the completed deliverable, and not a full IV&V of the process and steps leading up to that deliverable. PSC/CAI will be verifying that the system as a whole satisfies the success criteria defined by WSDOT.

1.4 ORGANIZATION

This Evaluation Plan is organized into chapters for the Project Background, the Success Criteria for the project, the Evaluation Framework and Methodology, and the Outline of the Final Report. Section 2 consists of subsections that detail the background of the HSD network project, the project's goals, the evaluation questions, and a description of the participants in the evaluation and their roles. Section 3 provides the technical details of the criteria that will be measured. Section 4 describes the framework and methodology used for the evaluation, while Section 5 lists PSC/CAI's technical and access requirements. Section 6 details the proposed Data Collection Design and Section 7 provides a suggested outline for the Final Report.

1.5 ENGAGEMENT TEAM

Technical Lead: Irving Popovetsky, Principal Consultant, ProStructure Consulting
Irving Popovetsky leads ProStructure's Security and Systems Engineering practices. He brings over a decade of Information Security and large-scale network management from the Telecom sector, having worked for Sprint's IP Security team and MCI/WorldCom's global AOL dial network.

Project Manager: Brandon Psmythe, Principal Consultant, ProStructure Consulting
Brandon Psmythe leads ProStructure's Network Engineering, Data Center, and Project Management practices. Brandon brings over a decade of large-scale network management and IT management experience from Webtrends/NetIQ and from Intel, where he oversaw the networks and data centers of the Desktop Processor design teams.

Project Oversight: David Sharon, Principal Consultant, CASE Associates Inc.
David Sharon specializes in providing Process Improvement, Project Management, Risk Management, and Quality Assurance Services to State Government Agencies. CAI has provided these services to more than 30 Agencies in Washington and Oregon and has over 18 years experience in providing these services.

2 BACKGROUND

2.1 OVERVIEW OF THE HSD WIRELESS NETWORK

Today WSF vessels are equipped with multiple security cameras connected to a Vigilos DVR (Digital Video Recorder) system that stores data locally. The video is transferred to shore-based storage once the ferry docks to unload passengers. In case of a catastrophic event, the video data would be lost and unavailable for forensics and future reference. The primary purpose of the HSD Wireless network is to facilitate the real-time transfer of video data from the onboard Vigilos system to the shore, for real-time monitoring and storage for later retrieval.

The secondary use for this network is to provide connectivity for office applications used by WSF employees during the course of their normal workday. This could consist of business data traffic including fax, Voice over IP (VoIP), email, and file transfer. Appropriate technologies will be used in order to prioritize the various types of traffic traversing this new network.

2.2 PROJECT GOALS

The fundamental Criteria for Success of the project will be the successful demonstration of a working prototype that maintains continuous connectivity with sufficient bandwidth from the WSF Ferry to the Ferry terminal in a fully verifiable manner. Further details of the success criteria are defined in the Success Criteria section below.

Secondarily, the goal of this project is to thoroughly document the operation, external influences and any performance failures of the HSD Wireless Network over a significant period of time. This information, when analyzed in a broad scope, will hopefully provide the planners of future projects with useful lessons.

2.3 EVALUATION QUESTIONS

The Evaluation Questions created by Mobilisa and contained herein will guide the gathering and analysis of the HSD Wireless Network test data. Each question references a section, as noted, from Mobilisa's Implementation Plan.

- ☐ Does the final prototype demonstrate scalability, functionality, and feasibility? (6.1.1)
- ☐ Is the system robust enough to handle two-vessel traffic in an emergency, to include transmission to the terminal? (6.1.4)
- ☐ Is the hardware chosen for the system configured for optimal performance, and does it provide continuous and reliable performance in delivering high data throughput? (6.2.1)
- ☐ Does the system support upload bandwidth of 25Mbps during un-obstructed operations (e.g., there is a physical vessel blocking line-of-sight while traversing the route)? (6.2.2)
- ☐ Does the vessel provide virtually continuous connectivity, i.e., 99% data received during non-obstructed operations as the vessel traverses the route? (6.2.2)
- ☐ Does the system provide for a minimum of 10 video viewing sessions? (6.2.4)

- ☐ Is the system proactively designed with security considerations in mind to protect against viruses, worms, packet floods, data interception, or unauthorized system access? (6.2.5)
- ☐ Does Mobilisa provide evidence through documented process that video data received is actually transmitted off vessel? (6.2.5)
- ☐ Do the radios authenticate before connection is made? (6.2.5.1)
- ☐ Is the data encrypted during transmission? (6.2.5.2)
- ☐ How effective is the solution? (7.6)
- ☐ Does it meet all the above requirements? (7.5)

2.4 EVALUATION PARTICIPANTS AND ROLES

There are three groups involved in the evaluation of the HSD network: the implementing contractor, the independent evaluator, and the sponsor. The role of the implementing contractor, Mobilisa, is to design and build a prototype HSD network for a single ferry on one run. The independent evaluator, CAI/PSC, is responsible for designing and conducting an evaluation of the prototype network. The outcome of the evaluation is to be formatted in a final report that will provide the project sponsor data to determine whether the prototype meets its criteria. The role of the sponsor of this project, WSF, is to facilitate the communication of requirements and other information between the implementer and the evaluator.

3 SUCCESS CRITERIA

3.1 CONTINUITY/RELIABILITY

The continuity of the ship-to-shore wireless connection shall be measured to ensure that data is reliably relayed to the onshore server that will store the video data. Mobilisa has defined this as greater than 99 percent of data transmitted from the Ferry to the Ferry Terminal is successfully received. Successful transmission will include any packet that meets any specified bandwidth or latency requirement, and successfully reaches its intended destination. Any packet that is not received by the end station, or does not fall within the specified Quality of Service requirements will not be counted as a successful transmission.

3.2 NON-INTERFERENCE

Mobilisa must ensure that the new wireless data network does not interfere with any ferry navigation and communications systems. This would include any type of existing ship to shore voice communication systems, radar, GPS, and 800Mghz radios.

3.3 SECURITY

The prototype will be evaluated against federal standards for secure communications to protect the confidentiality and integrity of video data, and to ensure that security measures do not incur a considerable cost to performance. CAI/PSC will verify that link-level encryption is used which meets the guidelines of the NIST publication FIPS 140-2. Additionally CAI/PSC will verify that device-to-device authentication is in place.

3.4 CLASSIFICATION AND PRIORITIZATION

Quality of Service (QoS) policies will be employed to prioritize the transmission of data from appropriately tagged applications and/or protocols. This will allow applications that have strict latency or bandwidth requirements (such as streaming video and voice) to perform correctly and provide an acceptable end-user experience.

WSF has stated that the wireless network will carry data that can be classified into two distinct groups. The high priority traffic will include any traffic that is related to the transmission of security-related video feeds. This traffic must be prioritized in such a way as to meet the latency and bandwidth requirements specified by Vigilos. Vigilos has specified that its applications will tolerate a Round Trip Time no greater than 50ms.

The secondary class of traffic will include any traffic that is related to the WSF model of floating work offices for its employees. This would include employee-related business traffic such as email, intranet access, and Voice over IP (VoIP). This secondary class of traffic can be further subdivided into latency-sensitive traffic and non-latency-sensitive traffic. WSF may find that the requirement of VoIP will have different latency requirements than the Vigilos Application.

The working prototype must also include a mechanism to dynamically control the prioritization of traffic. In the event of an emergency, this mechanism would be used to limit the amount of resources non-emergency traffic would be allowed to access.

3.5 BANDWIDTH

Bandwidth shall be measured to ensure it will be sufficient to support live video feeds alongside business applications. Sufficient bandwidth should be available to support at least 10 streaming video feeds from two vessels simultaneously, limiting connectivity for all other applications. Sufficient bandwidth will also support secondary utilization of the wireless network without affecting the primary usage.

WSF has stated that the wireless network must be able to handle 25Mbps of network traffic. The Vigilos video data streams transmit 16 KB (Kilobytes) MJPEG video frames at a rate of 2 frames per second. Therefore, each video feed is estimated at 32 KB/s (Kilobytes per second), or 256 Kb/s (Kilobits per second). In order to transmit 10 simultaneous video feeds, an approximate 3.0 Mb/s (Megabits per second) of bandwidth, including overhead, is required in order to transmit the feeds without congestion.

4 EVALUATION OF THE HSD WIRELESS NETWORK

4.1 EVALUATION FRAMEWORK

PSC/CAI has been tasked with performing an unbiased and objective evaluation of the Prototype HSD Wireless network. PSC/CAI's evaluation of the network will be purely based on quantitative data; there are no qualitative factors, such as perception, that make sense to measure.

4.1.1 EVALUATION SCOPE

PSC/CAI will perform a full Independent Verification & Validation (IV&V) of the Prototype HSD Wireless Network after it has been completely implemented by Mobilisa. Mobilisa's completed deliverable, in brief, includes a fully functioning Wireless backhaul network installed on one vessel on the WSF Triangle Run. The vessel in question is the M/V Klahowya, an Evergreen State Class Auto/Passenger Ferry that is bi-directional; it may travel in either direction. The M/V Klahowya travels among the Fauntleroy, Vashon Island, and Southworth ferry terminals located in the southern end of the Puget Sound.

The IV&V evaluation period will begin on October 9th, 2007 and will end on October 15th, 2007. During this period, the primary testing focus will be on the Bandwidth, Delay, and Reliability of the ship-to-shore communications via the HSD Wireless Network.

4.1.2 EVALUATION OBJECTIVES

The objective of this evaluation is to independently verify that the Success Criteria (Section 3) have been met and that objective, verifiable answers can be provided to all of the Evaluation Questions stated in Section 2.3.

Because there is no connection between the HSD Wireless Network and the WSDOT network, there will be no way to evaluate the performance of the Vigilos ship-to-shore streaming system directly. Therefore, the best avenue for evaluating the performance of the Network is to use synthetic network performance testing tools.

4.1.3 EXTERNAL INFLUENCES

In order to gather a complete picture of the HSD Wireless Network and its potential failings, external factors that affect Wireless network performance must be taken into account. In this project, three factors have been identified that affect Wireless network performance:

1. **Radio Antenna mis-alignment:** In order to achieve maximum throughput, Mobilisa has stated that it will use highly directional Sector antennas, rather than omni-directional antennas. Directional antennas work by amplifying the radio signal in a pie or cone shape, rather than dispersing the signal in all directions. Although this technique has many advantages, the primary disadvantage is in Mobile environments where non-stationary clients pitch, roll, and yaw, thus causing the concentrated signal to be sent in the wrong direction.

2. Radio Interference due to loss of Line of Site (LOS): Mobilisa chose to use the 5.8 Gigahertz radio frequency range for the Prototype Wireless HSD Network for its high performance in point-to-point applications. The primary disadvantage of 5.8 GHz is that signal in this frequency range is greatly affected by physical objects, so much so that Line of Site is nearly always required for outdoor long-distance links. If any physical object, such as another vessel, travels between the antennas of the client and base station, the signal will be lost.

3. Radio Interference due to noise: Another disadvantage of using the 5.8 GHz frequencies is that they are unlicensed, designated by the FCC for ISM (Industrial, Scientific, and Medical) uses. This means that any other entity, private, public, or personal, can acquire equipment that also transmits on this frequency, causing "noise," where a competing waveform cancels out the intended waveform.

PSC/CAI will gather several metrics in order to determine how often these external influences come into play. First, PSC/CAI will collect GPS (Global Positioning System) data in order to determine the exact location, heading and speed of the M/V Klahowya. If the vessel strays from its typical route or rotates, then the antennas may become mis-aligned. Second, PSC/CAI will collect radio performance metrics directly from the wireless ship-to-shore radios, which will include information about the wireless link quality and noise. Finally, PSC/CAI will collect weather conditions information for the Puget Sound area, in order to provide additional clues about what causes the system to fail.

4.2 EVALUATION METHODOLOGY

PSC/CAI's testing methodology will follow the Scientific Method by collecting results in an objective manner over a substantial period of time. PSC/CAI's tests will accomplish this by providing a frame of reference around all results by recording all network performance test results and information about external factors in time series based database format.

PSC/CAI's hypothesis is that the outcome of its tests will be similar to those reported by Mobilisa, when gathered during favorable environmental conditions. PSC/CAI does expect some degree of performance degradation and failure when those conditions change. It is PSC/CAI's intention that by gathering data over a longer period of time that some of these performance-degrading situations can be identified and better understood.

In order to perform unprejudiced collection of data in the spirit of the Scientific Method, PSC/CAI is developing a fully self-contained Test and Measurement device akin to a Flight Recorder or Black Box. Two of these devices will be installed for the evaluation. One device will be installed aboard the WSF test vessel (the M/V Klahowya), and the other one will be located at the Fauntleroy Ferry Terminal, where Mobilisa's equipment is housed. PSC/CAI will prepare the devices to continually collect data over a time period of no less than 5 days and no more than 21 days, depending on WSF-imposed restrictions.

These devices will automatically collect and record a wide variety of performance metrics during regular intervals in a verifiable way. Some of the performance metrics collected will include:

- Network availability status, including maximum and average throughput, delay, and jitter
- Wireless link status, speed, link quality, and noise (interference)
- Vessel location, heading, and speed
- Weather conditions.

PSC/CAI will establish baselines with all utilized tools in a variety of controlled environments. PSC/CAI will also ensure reproducibility by documenting all equipment, testing software, configurations, and tests for inspection in the final report.

5 TECHNICAL & ACCESS REQUIREMENTS

5.1 PSC/CAI REQUIREMENTS FOR MOBILISA

PSC/CAI will require Mobilisa's cooperation on several key factors in order to ensure that the tests are successful and fair. PSC/CAI expects the following items to be provided by Mobilisa:

- **Device Configurations:** In order to thoroughly evaluate the security configuration as required by the Success Criteria, PSC/CAI must view the configuration settings and passwords. These configuration settings and passwords will be evaluated against Federal Government standards for Information Security.
- **Network Access:** In order for PSC/CAI's Test and Measurement devices to pass standard IP traffic between each other, they will require standard Gigabit Copper Ethernet (1000base-T) access to Mobilisa's Proof of Concept HSD Wireless Network.
- **Network Details:** Mobilisa will provide PSC/CAI with the following technical details about its Proof of Concept network.
- **Type of Network Access Device:** Will PSC/CAI's Test and Measurement devices be plugging in to a switch, or directly into a router? Details must be provided about Ethernet speed, auto-negotiation support, and auto-MDIX support.
- **Firewall Rules:** If any types of traffic are blocked by Mobilisa's network, they must be clearly specified in writing. Any relevant Network Address Translation rules must also be detailed.
- **QoS Rules:** All QoS (Quality of Services) rules must be specified in writing.
- **Host Addresses:** IP Addresses and Network ranges for equipment on the network, including pre-assigned addresses for PSC/CAI's Test and Measurement devices.
- **Remote Access:** If any Remote Access of the network is available, PSC/CAI will use this access to manage its Test and Measurement devices.
- **Device Access:** PSC/CAI will require, at a minimum, read-only SNMP access to all of the Motorola PTP-600 wireless bridges as well as a recent copy of the Motorola PTP-600 SNMP MIB. This is in order to gather statistics about the wireless link quality, speed, etc. PSC/CAI would also like to have read-only access to the routers and switches on this network, in order to verify and validate the network topology.

5.2 PSC/CAI REQUIREMENTS FOR WSF

PSC/CAI will need several basic things from WSF in order to properly collocate the devices. The device located at the Fauntleroy terminal will require reliable 120V 15A power, and must be within 100 meters of Mobilisa's equipment. The Test and Measurement device aboard the M/V Klahowya has the same requirements as the first device.

6 DATA COLLECTION DESIGN

6.1 THE SELF-CONTAINED TESTING PLATFORM

PSC/CAI has developed a platform for performing autonomous testing and measurement of IP-based networks. The system is designed to require no human intervention after installation in order to minimize variance and human error. The testing and measurement platform continually collects a pre-defined set of metrics and logs all data to a time-based database. At the end of the test, all of the collected data may be viewed and graphed across any relevant time period.

PSC/CAI's testing platform is both secure and rugged, yet built using entirely COTS (Commercial Off The Shelf) components in order to maximize its value and interoperability. The systems are designed to handle both hostile network environments as well as a wide range of inhospitable weather conditions.

6.1.1 HARDWARE

At the heart of PSC/CAI's testing and measurement platform lies a VIA-based SBC (Single Board Computer) designed for embedded applications. The Jetway Versa J7F4K1G5D board was chosen for its high performance in networking and cryptographic applications. It features a crypto acceleration module and dual Gigabit Ethernet network interfaces. The board is installed in a chassis with an LCD-based information display, which PSC/CAI uses to display critical system statistics.

The system is enclosed in a weatherproof Pelican 1440 Top Loader Case. These cases will withstand temperatures from -10°F (-23.3°C) to +210°F (98.9°C). All Pelican cases have been tested to MIL-C-4150J, ATA 300, Def Stan 81-41/STANAG 4280 and Ingress Protection (IP) 67. For power and network ports, PSC/CAI is utilizing Bulgin Buccaneer IP68-rated BNC-style plugs and sockets.

6.1.2 OPERATING ENVIRONMENT

Redhat Enterprise Linux 5 was chosen because it is well suited for assured computing in government and enterprise environments, and it is also well suited for embedded deployments. RHEL5 has achieved Common Criteria EAL4+/CAPP/RBAC/LSPP certification by the National Information Assurance Partnership (NIAP), which is operated by the NSA. This makes RHEL5 suitable for any situation that requires Director of Central Intelligence Directive (DCID) 6/3 at Protection Level 3, which specifies intelligence-related information security measures.

In addition to using a certified Operating System, PSC/CAI also applies ProStructure's proprietary system hardening procedure to the systems. PSC/CAI utilizes this process in Information Security audit and assessment engagements for large business and government clients.

6.2 TEST AND COLLECTION TOOLS

PSC/CAI utilizes Open Source testing tools in order to maximize interoperability and reproducibility. None of the source code for the tools has been modified and all of the configuration options are listed in this plan. This allows any party to verify PSC/CAI's test results with minimal resources and expenditure.

6.2.1 THRULAY

Thrulay 0.9, once named Iperf2, was developed by Internet 2 researchers that wished to measure Throughput, Delay, and Jitter. Thrulay 0.9 was obtained from SourceForge.net.

6.2.2 PING

PSC/CAI will be using the standard Linux ping command (/bin/ping), from the RHEL5 iputils-20020927-43.el5 package.

6.2.3 RRD

RRD is the Round Robin Database, the Open Source industry standard high performance data logging and graphing system for time series data. It was developed by Tobias Oetiker, the author of MRTG. MRTG and RRD are used in almost every commercial and public network for collecting and graphing network performance statistics.

6.2.4 A NOTE ABOUT VIDEO STREAMING

PSC/CAI has chosen not to use a video streaming tool for its evaluation. This is because most video streaming platforms are not designed for test and measurement, and most are not designed to log dropped frames, lost or retransmitted data, etc. in a bi-directional fashion. Therefore, PSC/CAI believes that it is better to use true network test and measurement tools to benchmark the network and then to predict how the video platforms will perform.

6.3 PLANNED TESTS

PSC/CAI plans to run several continuous and one period test. These tests will all run in parallel, and all results will be available in RRD for correlation.

6.3.1 THRULAY BANDWIDTH TEST

Two separate Thrulay instances will be operated. The first Thrulay instance will simulate high-priority Vigilos security camera traffic by sending 10 simultaneous streams of UDP (User Datagram Protocol) traffic of 256 Kilobits per second each, totaling 2.56 Megabits per second. This test will be initiated every minute, and will operate for 59 seconds.

The second Thrulay instance will simulate non-priority office traffic. Two simultaneous TCP (Transmit Control Protocol) streams will operate on a non-priority port. Unlike the UDP tests, which send traffic at a fixed level, the Thrulay TCP test allows the system's TCP/IP network stack to determine the best possible transmit speed. This test will be initiated every minute and will operate for 59 seconds.

6.3.2 ICMP ECHO/RESPONSE (PING)

ICMP echo/response packets will be continuously sent between the two Network Test and Measurement devices. The ping command will be initiated every minute to send 59 ICMP echo requests of standard size (64 bytes).

6.3.3 DISRUPTIVE NETWORK TESTS

In addition to the continuous tests detailed above, PSC/CAI will periodically initiate a suite of disruptive network tests meant to simulate malicious traffic. Every three hours, beginning at Midnight, this suite of tests will operate for 10 minutes.

6.4 PERFORMANCE METRICS

PSC/CAI will collect the following metrics every minute and log them into RRD.

6.4.1 THRULAY HIGH-PRIORITY (UDP)

- Average Round-trip Delay (ms)
- Packet Loss (%)
- Average Jitter (ms)
- Packet Duplication (%)
- Packet Reordering (%)

6.4.2 THRULAY LOW-PRIORITY (TCP)

- Average Throughput (Megabits/sec)
- Average Round-trip Delay (ms)
- Jitter (ms)

6.4.3 ICMP

- Packet loss (%)
- Round-trip time (Average)
- Round-trip time (Minimum)
- Round-trip time (maximum)
- Round-trip time (Mean deviation)

6.4.4 DISRUPTIVE TEST

- Test running (Boolean)

6.4.5 GPS DATA

- Latitude/Longitude
- Heading
- Speed

6.4.6 MOTOROLA PTP600 RADIO DATA

- SNMP Object Group motorola.ptp.phyStatus
  - receivePower (Receive power expressed in tenths of a dBm)
  - transmitPower (Transmit power expressed in tenths of a dBm)
  - range (Distance between the two peer wireless units expressed in tenths of a kilometer)
  - linkLoss (The wireless link loss expressed in tenths of a dB)
  - receiveChannel (Current active receive channel)
  - transmitChannel (Current active transmit channel)
  - receiveModulationMode (Current active receive modulation mode)
  - transmitModulationMode (Current active transmit modulation mode)
  - receiveFreq (Current receive frequency expressed in MHz)
  - transmitFreq (Current transmit frequency expressed in MHz)
  - signalStrengthRatio (Signal strength ratio (Vertical / Horizontal) expressed in tenths of a DB)
- SNMP Object Group motorola.ptp.PubStats
  - receiveDataRate (Average data rate over the last one second interval expressed in kbps)
  - transmitDataRate (Average data rate over the last one second interval expressed in kbps)
  - aggregateDataRate (Average data rate over the last one second interval expressed in kbps)
- SNMP Object Group motorola.ptp.Encryption
  - encryptionAlgorithm (The encryption algorithm used by the wireless link)

6.4.7 NOTE 1: REPORTING OF TEST AVERAGES

On all tests above where "Average" is noted, the average is calculated only over the 1-minute time period of the test. Aggregate averages will be extrapolated from RRD and calculated once the tests are complete.

6.4.8 NOTE 2: DIFFERENCES IN TCP VS. UDP

Due to the nature of TCP, errors such as packet loss, duplication, and reordering are automatically handled by the system's TCP/IP network stack and are therefore not reported by Thrulay.

6.5 PLANS FOR VERIFIABILITY

PSC/CAI will take several measures to ensure the integrity of the collected data.

6.5.1 PHYSICAL SECURITY MEASURES

Although it is impossible to prevent tampering or intrusion on the console, PSC/CAI has implemented the following measures in order to detect if a system has been compromised:

- Tamper evident strips will be installed inside of the Pelican 1440 case in order to detect unauthorized opening of the case.
- The systems will be monitored for physical link failure in order to detect unplugging or tampering with the network links. Any network link failures will be treated as unplanned and will be investigated by PSC/CAI personnel.
- The systems will be monitored for reboots during the test in order to detect potential intrusion on the console. Any reboots will be treated as unplanned and will be investigated by PSC/CAI personnel.

6.5.2 INFORMATION SECURITY MEASURES

- The systems will continuously transmit key system data to each other, including system logs and health information. This data will also be transmitted off-site if possible.
- On a periodic basis, the systems will back-up and checksum the RRD database. This backup will be transmitted off-site if possible.
- On a periodic basis, the systems will perform a suite of automated system security checks including the file and configuration modification detection tool AIDE, a Rootkit scanner, as well as additional security verification checks used by ProStructure Consulting during Forensic Investigations and Security Assessments.
- The systems are hardened using ProStructure's proprietary system hardening techniques.
- The systems will be time synchronized using NTP (the Network Time Protocol).

6.5.3 PRE-DEPLOYMENT BASELINES

PSC/CAI will perform thorough baseline testing of the systems and all testing tools in controlled laboratory environments before they are deployed in the field. When the tests are complete, ProStructure will perform all of the baseline tests again to ensure that they are consistent. The details of the tests will be enumerated in the Final Report.

7 FINAL REPORT OUTLINE

1. Introduction
   - 1.1. Executive Summary
   - 1.2. Project Summary
   - 1.3. Purpose
   - 1.4. Scope
   - 1.5. Organization
   - 1.6. Evaluation Team
2. Background
   - 2.1. Overview of the HSD Wireless Network
   - 2.2. Project Goals
   - 2.3. The FTA and its Strategic Goals
   - 2.4. Evaluation Questions
   - 2.5. Success Criteria
3. Evaluation Overview
   - 3.1. Evaluation Framework
   - 3.2. Evaluation Methodology
4. Evaluation Results
   - 4.1. Overview
   - 4.2. Attainment of Objectives
     - 4.2.1. Answers to the Evaluation Questions
     - 4.2.2. Comparison of the Success Criteria to the Evaluation Results
   - 4.3. Review of the Data Collection Results
5. Analysis
   - 5.1. Technical Analysis
   - 5.2. Analysis of Project Management
   - 5.3. Lessons Learned
   - 5.4. Possible Uses of the Technology
6. Appendix A: Detailed Data Collection Design
7. Appendix B: Detailed Data Collection Results

Office of Research, Demonstration and Innovation
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Washington, DC 20590

www.fta.dot.gov/research

Report Number FTA-WA-26-7001-2008.02