INET SYSTEM MANAGEMENT SCALING

Allison R. Bertrand[1], Todd A. Newton[1], Thomas B. Grace[2]
[1]Southwest Research Institute® **[2]Naval Air Systems Command (NAVAIR)**
San Antonio, Texas **Patuxent River, Maryland**
allison.bertrand@swri.org, todd.newton@swri.org,
thomas.grace@navy.mil

ABSTRACT

The integration of standard networking technologies into the test range allows for more capable and complex systems. As System Management provides the capability for dynamic allocation of resources, it is critical to support the level of network flexibility envisioned by the integrated Network-Enhanced Telemetry (iNET) project. This paper investigates the practical performance of managing the Telemetry Network System (TmNS) using the Simple Network Management Protocol (SNMP). It discusses the impacts and benefits of System Management as the size of the TmNS scales from small to large and as distributed and centralized management styles are applied.

To support dynamic network states, it is necessary to be able to both collect the current status of the network and command (or modify the configuration of) the network. The management data needs to travel both ways over the telemetry link (in limited bandwidth) without interfering with critical data streams. It is important that the TmNS's status is collected in a timely manner so that the engineers are aware of any equipment failures or other problems; it is also imperative that System Management does not adversely affect the real-time delivery of data.

This paper discusses measurements of SNMP traffic under various loading conditions. Statistics considered will include the performance of SNMP commands, queries, and events under various test article and telemetry network loads and the bandwidth consumed by SNMP commands, queries, and events under various conditions (e.g., pre-configuration, normal operation, and device error).

KEYWORDS

iNET, System Management, Performance, SNMP

INTRODUCTION

The Telemetry Network System (TmNS) is a system architected to enhance existing telemetry systems through the incorporation of networking technologies. The goal of incorporating these technologies is the ability to gain flexibility in conducting test operations. One of the key aspects is the addition of a two-way telemetry link that allows the test team in a control room to remotely manage the test system on a Test Article. This ability enables the test team to

dynamically modify certain parameters of the test system to maximize test efficiency. Additionally, a managed two-way telemetry link provides a test range the ability to dynamically manage the spectrum resources across test assets to maximize spectral usage. Furthermore, the two-way telemetry link provides the ability to remotely access the data recorder on board the Test Article. This capability allows the test team to retrieve data from the data recorder in order to maximize knowledge during test execution.

Providing the ability to remotely manage test resources increases the test team's capabilities to dynamically adjust the telemetry system for maximum test efficiency. This increase in flexibility creates challenges for test operations. These capabilities enable the team to re-configure selected parameters on the fly. Any re-configuration is likely to be conducted in between test points. One will have to understand the potential impacts of the changes and the time it takes to implement the changes. For example, changing the gain range on a single data acquisition channel can seem rather benign, but this changes the calibration that may require, as minimum, a post test re-calibration of that data channel. A more dramatic example is re-routing data on the Test Article. One will likely need to have a model in order to predict the potential impacts of the re-configuration. An increase in capabilities provides an increased level of flexibility that potentially leads to complexities in test execution.

The System Management Standard enables the capabilities to manage the TmNS. It provides the range of possibilities for a test range to implement via applications (managers). Each range will be able to establish their own constraints through range polices which can be identified in the test metadata. The test metadata structure is being defined in the Metadata standard. Additionally, the number managers can vary per range and potentially per test program. For example, a range is likely to have a single manager to manage the spectral resources. However, each test is likely to have a manager for managing the test instrumentation system on the Test Article. In addition, the Test Article can have its own manager to manage the resources on the Test Article.

PERFORMANCE CONSIDERATIONS

The goals of the assessment are to evaluate System Management and its impact on the performance of the TmNS. The application of System Management should enable improved system performance through monitoring and tuning. However, the addition of System Management to a system also adds additional network load. This creates the perception that (by adding network load) System Management decreases the performance of the network. This viewpoint downplays the potential benefits which may be gained by the use of a relatively small part of the network for System Management data. The amount and types of management data, the network geometry, and the amounts and criticality levels of other system data are all variables which are trade spaces which must be considered when using System Management to benefit the system.

Management data may be used at many different levels. The use may be as basic as the collection of statistics from the system or as complex as dynamic modifications to the system. Some examples of statistics include the rates of network traffic moving through the network or the power level of a Data Acquisition Unit (DAU). Dynamic management passes commands and

configuration information across the telemetry link to allow on-the-fly modifications. One use case for dynamic management would be the ability to change to a new test configuration between maneuvers without requiring the Test Article to land. The selection of system statistics to monitor and the amount of dynamic management utilized will vary according to the needs of the range.

The convenience of having more live visibility and interaction capabilities with the test system must be weighed against the constraints of the system. All Test Article networks are constrained by the physical limits of their links; the telemetry link is constrained even more so. The TmNS objective is a 20 Mbps downlink and a 2 Mbps uplink [2]. When such a telemetry link is coupled with a common Ethernet 1 Gbps or even 100 Mbps network bandwidth, there is a clear requirement to down-select the data which travels the telemetry link. The choice of which data to transmit is already difficult because human nature demands all the data all the time. Users may chafe at the idea of losing yet another portion of their telemetry bandwidth to System Management data.

Another consideration is the balance between the preservation of critical data streams and the preservation of management data streams. Depending on system usage, either may require near-real-time delivery of data. While attention is most easily drawn to the needs of critical data streams such as key test data, the ability to ensure delivery of management data may also be highly important. An over-temperature notification from a sensor may indicate a problem which could be alleviated if discovered in a timely manner. A control message could be sent to enable a recorder neglected at pre-flight checkout. In situations like these, System Management data might also be considered critical.

While the benefits of System Management are fairly well known, the questions yet to be fully answered are, “How much is System Management going to cost in my system?” and “Can I trust System Management to get the job done in a timely manner?” The considerations in applying System Management must weigh the size of System Management messages, management bandwidth on the Test Article, management bandwidth across the telemetry link, and the amount of time it takes to retrieve System Management information. Other factors which impact the design trades include the size of the system (the number of devices being managed) and where the management information is being gathered (locally by consolidation or centralized). For instance, consolidating non-critical management information on the Test Article is one method of reducing the amount of downlink bandwidth. Quantifying these types of costs will allow ranges to make informed choices on the ratio of System Management to test data.

STANDARDS ASSESSMENTS METHODS

The management of the TmNS has been standardized by the iNET System Management Working Group using the Simple Network Management Protocol (SNMP). The TmNS System Management Standard defines a collection of management information through an SNMP Management Information Base (MIB). The SNMP protocol defines methods for requesting the MIB information (queries, or snmpgets), sending MIB information (commands, or snmpsets), or receiving asynchronous MIB information (notifications). SNMP agents on each TmNS device

use this MIB to exchange management information with a System Manager application. At the highest level, the System Manager is the Mission Control Center Test Manager. This gives the Mission Control Center the capability to monitor statistics and faults and (if appropriate) control or configure some pieces of the TmNS across the network. The management of the TmNS using SNMP and the management information prescribed by the TmNS System Management Standard will be the platform for this assessment.

Using SNMP for System Management has a long track record in the network world [7] and has more recently been employed in the Flight Test environment [8]. By their very design, networks are flexible and extensible. Perhaps because it is difficult to describe a typical network (and hence a typical network management system) few direct studies of SNMP System Management effects have been undertaken. We will present information from one study which surveyed an extensive collection of vendor and standardized MIBs to characterize the typical management information packet size. We also glean data from studies aimed at comparing the network characteristics of different versions of SNMP or those comparing SNMP to other System Management protocols. The limited amount of information available in the literature points to the need for our assessment to illustrate how ranges can best benefit from System Management.

Methodologies of Historical SNMP Studies

A study by Schonwalder analyzed 824 standard and vendor MIB modules to characterize the typical management information packet size [1]. This study was a statistical analysis based solely on the MIB structures and did not include any live network measurements. Among the calculations in the study, one measure was the average size of the SNMP packets. While this study did not perform empirical measurements on a network system, it did show a likely range of sizes with which we can use to bound the measurements in the TmNS study.

A comparison of SNMPv2c versus the various authentication levels allowed by SNMPv3 [3] illustrated the differences between the SNMP versions using measurements including protocol overhead (bytes in the packet due to features like authentication, over and above the data being requested) and network capacity consumed. This study was performed on a small, non-realistic system with two management stations connected by a switch to an SNMP agent on a 10 Mbps network. The SNMP agent was based on Agent++ software. A packet-sniffing station using Ethereal (the predecessor to Wireshark) was connected inline through a hub on the same side of the switch as the SNMP agent.

SNMPv3 and SNMPv2c were also compared as part of an evaluation of options for secure SNMP [5]. Network capacity and processing time were measured on a 10 Mbps network using Ethereal. The network consisted of a System Manager attached to a Net-SNMP agent across a secure tunnel.

An extensive study of different SNMP agents was performed as part of a comparison to Web Services [4]. Bandwidth and round-trip delay were measured for agents from 3Com, Cisco, HP, IBM, Nortel, Net-SNMP, Microsoft Windows XP, NuDesign, SNMP Research, Cabletron, and Xircom. The study was conducted with SNMPv1 and SNMPv2c. Measurements were made with the tcpdump utility sampling messages on the manager side of the network.

TmNS Standards Assessment Testbed

To investigate the choices necessary when applying System Management to a telemetry network, we have designed a series of assessments based on a simulated test range [6]. The test range has two Test Articles. One Test Article has ten managed devices (those capable of interacting through SNMP System Management messages); the second Test Article may be configured with seven to fifteen managed devices. The Test Articles are equipped with a variety of common test instrumentation including recorders, data acquisition units, Serial Streaming Telemetry (SST) transmitters, switches, and routers (Figure 1). Each of these devices has an SNMP interface used to send and receive System Management messages.

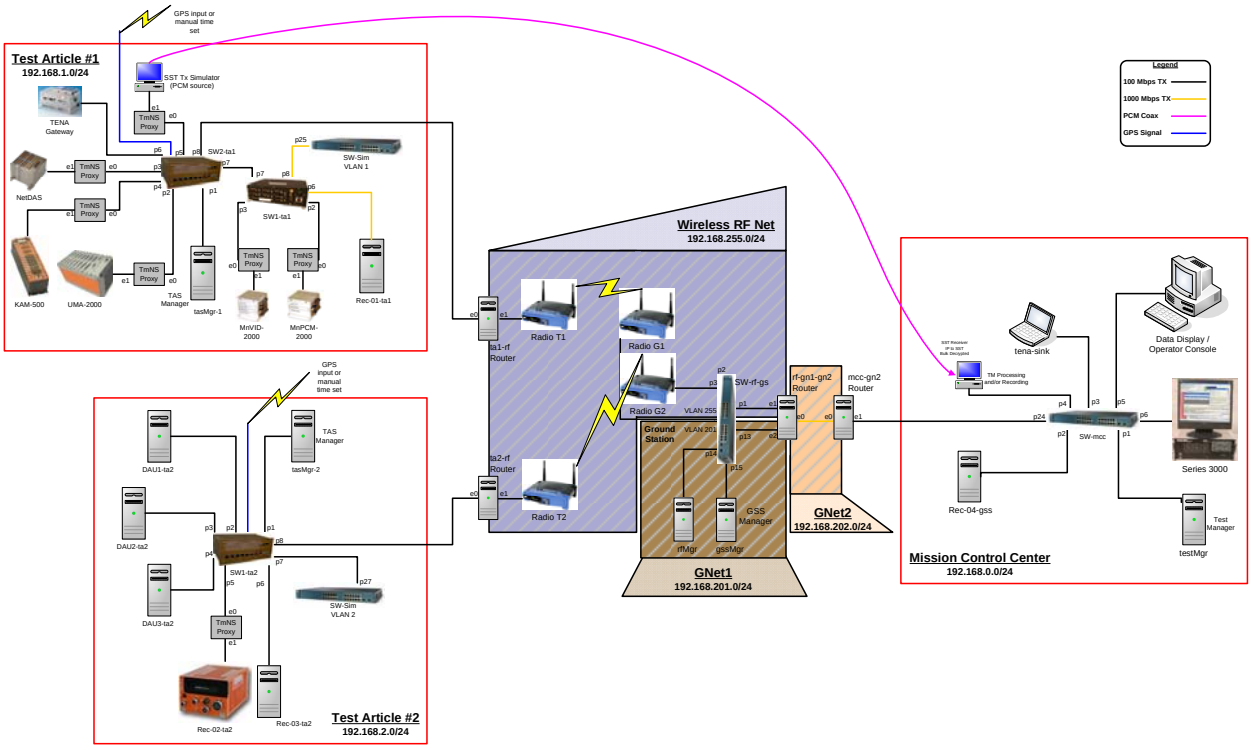

Figure 1. TmNS Test Bed Network

The test range Mission Control Center has a Test Manager application which acts as the interface for sending and receiving management information to and from the Test Articles. The Mission Control Center can manage devices on the Test Articles directly or may communicate with a "Test Article Manager" (a technique known as "centralized management"). The Test Article Manager is an application which can perform management on the local Test Article devices. The Test Article Manager can be configured to collect MIB statistics from the Test Article devices at varying intervals. The Test Article Managers can also perform "Consolidated Management"; they can consolidate statistics from the Test Article devices and distribute commands and configuration to the Test Article devices. Figure 2 shows consolidated management messages (striped blue arrow) which are distributed by the Test Article Manager to Test Article #1 and centralized management messages (yellow arrows) that go directly from a manager to the device being managed. The Test Article Manager may use this consolidated management technique to

communicate with the Mission Control Center through a Net-SNMP Test Agent (part of the Test Article Manager). This allows for the reduction of management data bandwidth across the telemetry link. The presence of the Test Article Manager also allows management information to be collected and logged when the telemetry link is down.

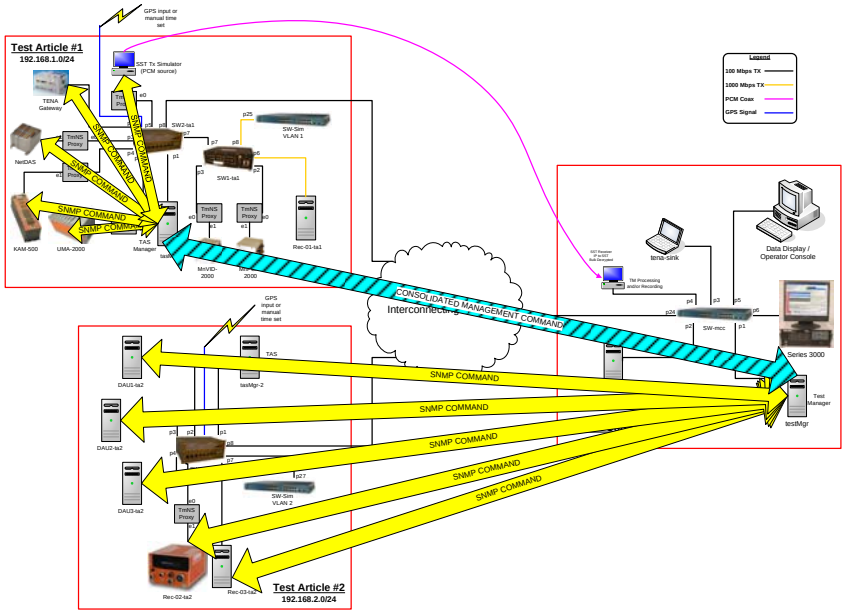

Figure 2. Centralized and Consolidated Management

Ideally, all equipment would be actual flight test hardware. However, this is not a practical approach due to the immediate need for proving TmNS technologies and unavailability of actual flight test hardware that complies with the TmNS standards. As a way to move forward, device emulators have been deployed in the networks; some as end devices and others as TmNS proxies. These emulators may be used in the place of the actual flight test hardware until the real hardware becomes available. For flight test hardware that is currently in the test bed but not fully TmNS-compliant, the device emulator will serve as a TmNS proxy device. The proxies will support the TmNS MIB through Net-SNMP agents. The SNMP agents on the flight test hardware will be developed by the vendors.

TmNS System Management Scaling Assessments

The TmNS System Management Standard will be assessed using several different criteria:

- Size of the system

The number of devices being managed will be scaled from one to twenty-five. The number of Test Articles will be scaled from one to two.

- Geometry of the management system

A comparison of centralized management and consolidated management will be performed.

- Loading of the network

Variations of the TmNS data message load and variations of the System Management load (number and frequency of variable queries) will be applied. The System Management loading will reflect typical test phases and events such as configuration before the test, normal test conditions, and device error during the test.

The measurements performed on these different assessment conditions will include network load (all network traffic, SNMP traffic, TmNS traffic), number of SNMP packets and bytes sent and SNMP message latency. The measurements will be accumulated between the Test Article Manager and the Test Article devices; between the Test Article Manager and the Mission Control Test Manager; and between the Test Article devices and the Mission Control Test Manager. The network traffic will be recorded under these conditions with an inline Absolute Analysis Model AA-3300-010 and analyzed for statistics using Wireshark.

RESULTS

Results of Historical SNMP Studies

The SNMP message size study [1] analyzed 824 standard and vendor MIB modules. The study concentrated on the size of the raw SNMP protocol headers and data. The 28 bytes for User Datagram Protocol (UDP) and IPv4 headers were not included in the packet sizes. The study found that 70-90% of the encoded SNMP messages analyzed would be smaller than 484 bytes (a historical SNMP packet size limit). Approximately 90% of encoded SNMP messages in the study would be smaller than 1500 bytes (the typical Ethernet “maximum transmission unit” or maximum packet size).

The comparison of SNMPv2c and SNMPv3 protocols [3] illustrated that in most cases SNMPv3 puts a heavier load on the system in terms of bandwidth. This should not be a great surprise considering the additional features provided by SNMPv3. The protocol overhead added by the use of SNMPv3 was about 10% for SNMP gets and sets even without use of the authentication features (SNMPv3 noAuthnoPriv). An additional (small) 1% average overhead was accumulated with the enabling of the SNMPv3 features (authNoPriv or authPriv). The network bandwidth measurements showed SNMPv3 messages consuming nearly twice as many bytes as SNMPv2c for the SNMP set and SNMP get operations. Again in the bandwidth study, the difference between SNMPv3 varieties (noAuthnoPriv, authNoPriv, or authPriv) was minimal.

The security alternatives study of SNMPv2c and SNMPv3 [5] showed similar results to the previously described SNMPv2c and SNMPv3 protocol study. An SNMPv2c request for the sysContact variable (IETF RFC 3418) required 79 bytes and generated a 101 byte response for a total round-trip packet expenditure of 180 bytes. The same operation in SNMPv3 required 306 to 358 bytes for the request and response SNMP messages. It was not clear whether these

measurements included the UDP and IPv4 headers. Processing time included the time between when the in-line network analyzer saw the SNMP get message and when it saw the SNMP response message. In this network, the mean processing time for an SNMPv2c message was 310 microseconds; the SNMPv3 processing time varied from 500-700 microseconds, depending on the SNMPv3 features enabled.

In the extensive survey of many vendor SNMP agents [4], it was shown that the bandwidth for one SNMP message transporting one object was likely to be under 100 bytes (neglecting UDP and IPv4 headers). These calculations were verified by retrieving "hundreds of MIB objects" from a variety of SNMP agents. Measurements of the round-trip delay for an SNMP get (or SNMP getbulk where available) were presented for 23 SNMP agents from various vendors. Measurements of the time required to retrieve one and 22 objects (SNMP variables) in one message were measured ten times on each agent with the lowest values tabulated. Additional measurements of 66 and 270 objects were made on agents which supported large SNMP messages (only six of the 23 agents supported the largest request size). The median round-trip time for one object request was 1.25ms, with 15 agents under 2ms. The median round-trip time for 22 objects in one SNMP request was 3.55ms (0.16ms per variable requested). No information was given about the size or geometry of the network, so it is difficult to know the scale of this data.

Of the four studies discussed here, two compared SNMPv2c and SNMPv3; most made various measurements of bandwidth or packet size; and some measured message transmission or response time. SNMPv3 was shown to take roughly double the network resources of SNMPv2c. It should be noted that groups which compared SNMPv2c and SNMPv3 [3, 4, 5] emphasized that since the SNMPv3 costs are related to authentication, there are configurations in which the SNMPv3 differences are reduced when the management connections are persistent over a long duration. The studies pointed to an SNMP message size that is often near one hundred to a few hundred bytes, enabling someone implementing System Management in a constrained environment to make educated guesses about the required bandwidth for a given set of SNMP variables. Finally, two studies showed radically different time scales for acquiring SNMP information (one in the millisecond range and one in the microsecond range) reminding us that network geometry plays a big role in the timeliness of System Management messages.

As noted earlier, it is difficult to collect a cohesive picture of the costs and trades related to SNMP management based on the current literature. This is due in part to the variety of ways in which management can be used. Some areas of investigation (such as SNMPv2c versus SNMPv3) have been sufficiently evaluated to provide the reader with a basic understanding of the trades involved. These studies provide some basic guidance to ranges, but point strongly to the need for additional, focused investigation.

Results of TmNS System Management Scaling Assessments

The results of the TmNS System Management Scaling Assessments will be presented at ITC. The analysis of System Management latencies, packets, and bytes sent during various loading conditions will give guidance for the development of future TmNS ranges. The results of the TmNS System Management Assessment should help indicate how to design a system where

SNMP messages are successfully transmitted under heavy data loads and where TmNS data messages do not get dropped because of heavy SNMP traffic.

CONCLUSION

We have presented a framework for a System Management Scaling Assessment for the Telemetry Network System. The results of this work will not only help to prove out the capabilities of the TmNS System Management Standard, but will also provide guidance to ranges adopting the TmNS. Several SNMP studies were presented showing performance trades involved in choosing SNMPv2c or SNMPv3 for a System Management implementation. These studies also give the reader a general feeling for the bandwidth required when managing a system. The TmNS System Management Scaling Assessment will build on these studies and use the TmNS System Management Standard to illustrate how System Management can best be applied to the telemetry environment.

ACKNOWLEDGEMENTS

The work described in this paper would not have been possible if not for the contributions from the many members of the iNET Standards Working Groups. We gratefully acknowledge this effort and the funding and guidance provided by the iNET program.

REFERENCES

1. Schonwalder, J., Characterization of SNMP MIB Modules, 9th IFIP/IEEE International Symposium on Integrated Network Management, May 2005 Page(s): 615 – 628.

2. https://www.inetprogram.org/Documents/TCRD_Objectives_and_Thresholds/TCRD_chart_on_objectives_and_threshold_technical_parameters.pdf.

3. Corrente, A, Tura, L., Security Performance Analysis of SNMPv3 with Respect to SNMPv2c, 2004 IEEE/IFIP Network Operations and Management Symposium, Vol. 1, 2004, p.p. 729-742.

4. Pras, A., Drevers, T., van de Meent, R., Quartel, D., Comparing the Performance of SNMP and Web Services-Based Management, IEEE Etransactions on Network and Service Management, Fall 2004.

5. Hia, H. E., Secure SNMP-Based Network Management in Low Bandwidth Networks, Thesis Virginia Polytechnic Institute, 2001.

6. Newton, T. A., Kenney, J. D., Moodie, M. L., Grace, T. B., iNET Networking Standards Test Bed, International Telemetering Conference, Las Vegas, Nevada, October 2009.

7. Case, J., Fedor, M., Schoffstall, M., Davin, J., A Simple Network Management Protocol, IETF RFC 1067, http://tools.ietf.org/html/rfc1067, 1988.

8. Moodie, Myron, Newton, Todd, and Abbott, Ben, "Development of a Network-Centric Data Acquisition, Recording, and Telemetry System," Proceedings of the International Telemetering Conference, Las Vegas, Nevada, October 2007.