Expanding DoD Network Management

Secure Multi-web Remoting Tool (SMRT)

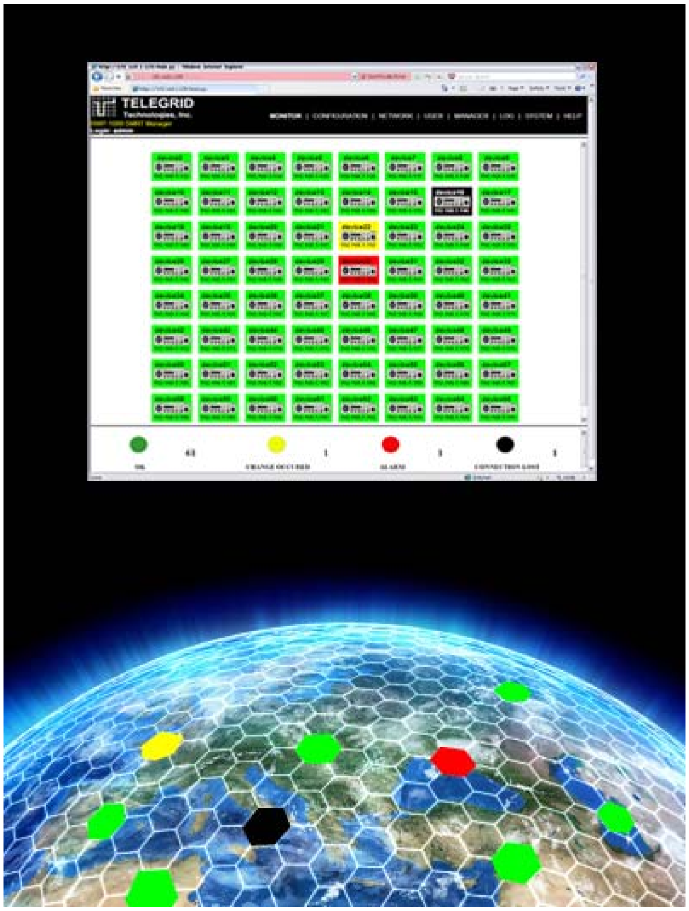
TELEGRID
www.telegrid.com

1 Abstract

The needs of the Department of Defense (DoD) have not changed. Supporting the warfighter by providing the best technology available is still the DoD's main goal. The economic realities, however, are drastically different today than they were five years ago. The troop drawdown and threat of sequestration have put the budgets of many organizations in jeopardy. If carried out, sequestration will force the DoD to operate on a skeleton budget threatening the level of operational readiness. In short, the DoD today is looking for ways to do more with less. To increase productivity and cut costs the DoD has implemented innovative technologies including data center consolidation, cloud computing, and enterprise software. In addition to these solutions the DoD has turned to Network Management Systems (NMS) to ensure the US Military retains its superiority despite the diminished budget. This paper will present the benefits of utilizing a NMS, pitfalls the DoD faces in deploying a NMS, and an innovate solution to expanding the scope of a NMS.

2 Network Management Systems

Network Management Systems help government and commercial organizations improve operational efficiency and reduce cost. At its most basic level a NMS consists of a hardware monitoring unit and a software manager that provides a user with remote monitoring and control capabilities. At its most expansive it is a highly intuitive system that provides an administrator with centralized control over a network and all its components. With a NMS administrators can remotely monitor equipment and processes without the requirement for hands on monitoring. The increase in uptime and reduction in labor translate into large economic incentives.


TELEGRID
Technologies, Inc.
MONITOR | CONFIGURATION | NETWORK | USER | MANAGER | LOG | SYSTEM | HELP
OK
61
CHANGE OCCURED
1
ALARM
1
CONNECTION LOST
1

To increase interoperability the Simple Network Management Protocol (SNMP) was developed by the Internet Engineering Task Force (IETF) as a common language for NMS communications. SNMP is an application layer protocol coupled with a database scheme that allows a NMS to interpret signals from a device by cross referencing them with a database or Management Information Base (MIB). SNMP versions range from the open signals of Version 1 (SNMPv1) to the encrypted signals of Version 3 (SNMPv3). SNMP message types include queries and traps. Queries are sent by the application to a device to request status information. Traps are relayed to the application from a device based upon a predetermined signal. With SNMP traps a device can automatically notify a system administrator when a change occurs or an alarm is triggered.

3 Obstacles to Network Management

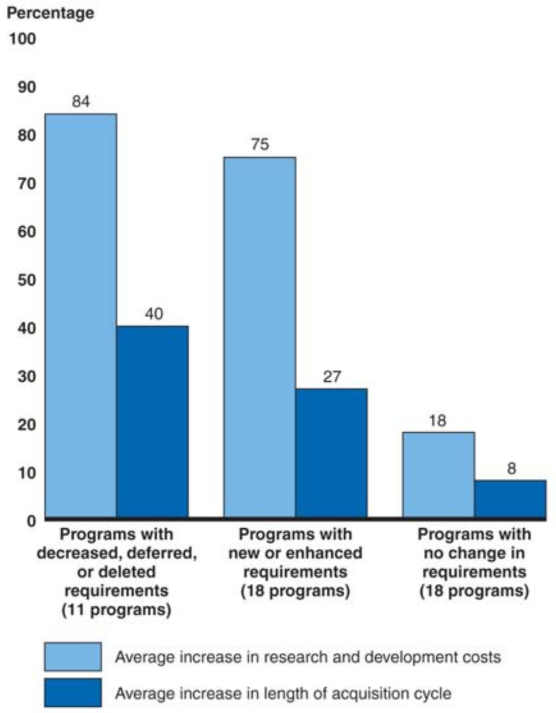
There are many obstacles to the widespread deployment of a NMS specifically within the DoD. For instance, many devices being utilized by the DoD are proprietary; designed to “lock-in” customers and force users to pay higher fees while stunting competition and innovation. Attempting to incorporate proprietary devices into a non-proprietary system, like a SNMP based NMS, can lead to integration problems and higher costs.

Additionally the decrease in budgets means equipment modernization programs are being halted or delayed. This is forcing commands to rely on legacy equipment which often does not include SNMP based monitoring and control.

Finally, while most modern devices include SNMP capability others do not, restricting inclusion into a NMS. The reasons for non-inclusion of SNMP in modern devices are abundant but for the DoD the main culprit has been the intense testing and certification requirements of military equipment. With equipment taking years to reach appropriate Technology Readiness Level for deployment (TRL 8-9) SNMP was either not considered or was included with the unsecure SNMPv1. Once SNMPv3 was available many manufacturers or commands decided that repeating the certification process was not worthwhile. This is particularly true for encryption equipment which must undergo years of NSA security testing in addition to DoD specific certifications.

The Government Accountability Office (GAO) confirmed this in a report from March 2011 (GAO-11-233SP) where they reviewed 40 individual weapons programs in the DoD’s 2010 portfolio. The GAO found that for programs with new requirements both research and development costs and length of acquisition cycle increased roughly 3.5 times more than for programs with no changes in requirements. The average increase from original estimates of research and development costs was 18% when there were no changes and 75% when there was a new requirement. The average increase in acquisition life cycle was 8% when there were no changes and 27% when there was a new requirement. Interestingly the increase was even larger when requirements were deferred or deleted.

Figure 3: Relationship between Key Performance Parameter Changes, Research and Development Cost Growth, and Delays in Achieving Initial Operational Capabilities



Source: GAO analysis of DOD data.

Notes: Programs that had both increases and decreases in key performance parameters are included in both categories. Cost and schedule data were not available for the Joint Air-to-Surface Standoff Missile Extended Range variant, which had a new or enhanced requirement.

4 KIV-7M Link Encryptor

One example of a critical DoD device that does not include SNMP is the KIV-7M Link Encryptor. The KIV-7M is a NSA Type 1 certified device that is approved for use at the highest level of assurance. It is widely implemented across all branches of the DoD and is pervasive in data centers. Despite the fact that it is typically deployed in remote data centers, far away from a system administrator, it does not include SNMP. To counteract this fault the manufacturer of the equipment includes a web configuration tool to monitor and control the device. While effective, the design requires an individual internet tab for each KIV-7M which can cause confusion in sites with ten or more units. The web configuration screen is also a standalone monitoring tool which cannot be integrated into an overall NMS. A simple solution is required to include these disparate systems into a NMS while still maintaining security and flexibility.

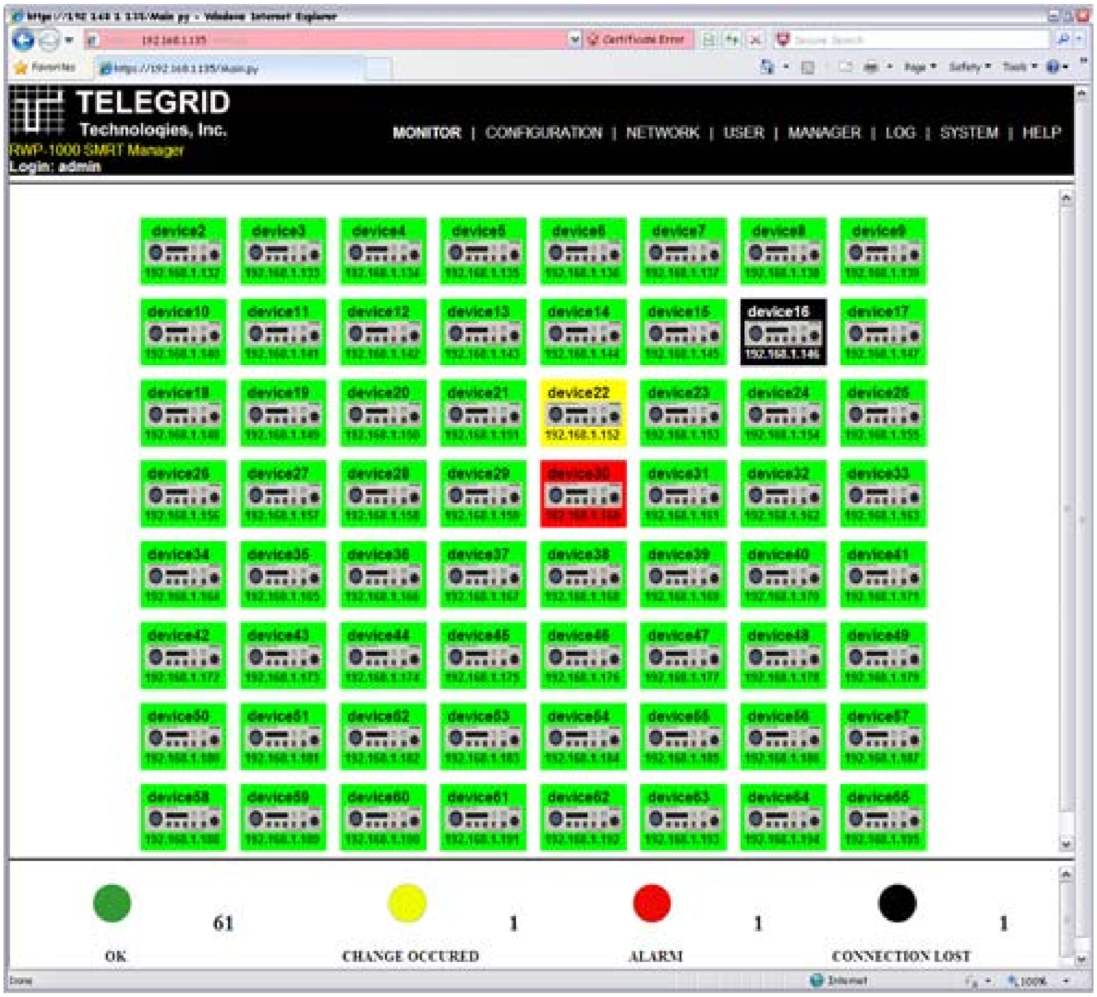
5 Secure Multi-web Remoting Tool (SMRT)

The SMRT, developed by TELEGRID Technologies, Inc., is the ideal solution for integration of the KIV-7M into the DoD's NMS. The SMRT utilizes a reverse web proxy that automatically monitors the web configuration tools of managed equipment for changes or alarms. It is a standalone hardware device that is co-located with the managed equipment and can be accessed remotely. SMRT provides management information in multiple formats and can be easily deployed. It was designed to comply with the DoD's high level of security and provides flexibility for the integration of numerous devices beyond the KIV-7M. SMRT bridges the gap between non-SNMP based devices and a NMS providing near plug and play network management.

5.1 Management Formats

The SMRT provides system administrators with multiple formats for remote management. This increases flexibility and provides users with information in a familiar form. The first format is visual notification via the SMRT Management Screen. The SMRT combines the web configuration tools of multiple devices and displays each as an icon on a single page. It automatically monitors the underlying pages for changes and notifies the system administrator by changing the icon's color (red-alarm, yellow-change in status, black-device offline, green-no change detected). The second format is using encrypted SNMPv3 traps to capture changes or alarms and then sending them to an overall NMS. By utilizing existing software to view events the network manager can increase the value of an existing NMS. The final format is email notifications which can automatically send any change in status to a system administrator.

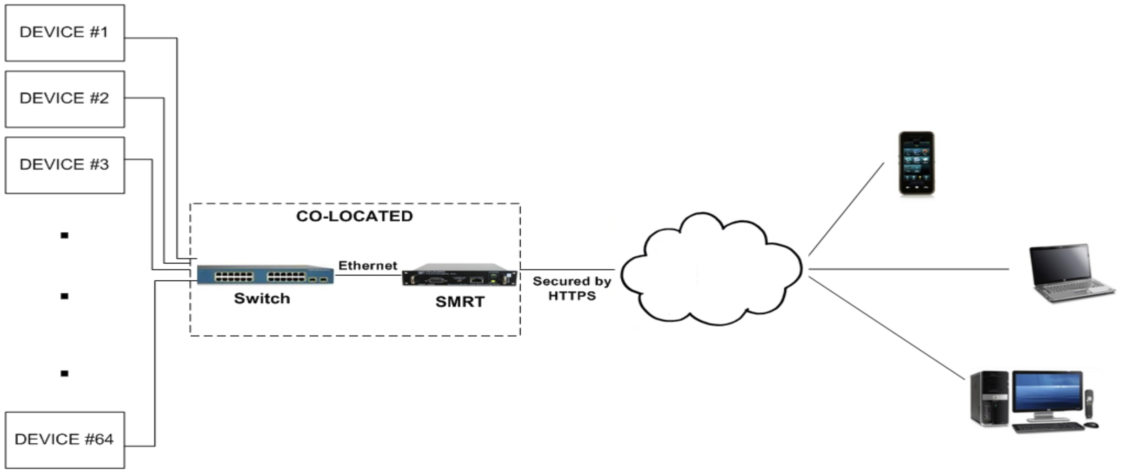
- Visual Notification
- SNMP Traps
- Email Alerts



SMRT Management Screen

5.2 Ease of Deployment

Since the SMRT is a hardware based device it does not require the installation of software which can interfere with processes running on other servers. Simply plug the device into a switch that is co-located with the managed equipment. By communicating through a switch a network manager only needs one external IP address to remotely manage an unlimited number of devices. This feature greatly reduces the time associated with assigning individual external IP addresses to each device. As a side benefit this reduces security risks associated with management of multiple external IP addresses. Finally, because SMRT functions as a reverse web proxy its management screen can be viewed on any browser or smart device with an internet connection.



SMRT Concept of Operations

5.3 Security Features

SMRT was designed with five main security features. The SMRT utilizes SNMPv3 to send only encrypted traps to the NMS. Second, SMRT's Apache web server was designed in compliance with NSA type 1 standards. The Apache web server also creates a firewall between the local area network (LAN) and external networks. Third, the SMRT gives the network administrator the ability to assign levels of user access. Fourth, access protection is in the form of username and password authentication with multiple failed login attempts resulting in a user being permanently locked out. Finally, the SMRT utilizes SSL certification by verifying a user's certificate with a certificate saved on file by the system administrator.

- SNMP version 3
- Apache web server
- Multi-level user access
- User lock-out
- SSL certification

5.4 Flexibility

Although designed for the KIV-7M the SMRT is an adaptable solution which can monitor any device with a web configuration tool including simple devices like Uninterruptible Power Supplies (UPS). With such a wide range of applications the SMRT provides a unique answer to managing non-SNMP based devices.

6 Conclusion

In order to provide the best support to the warfighter while cutting costs the DoD is implementing network management solutions. A NMS increases the DoD's operational efficiency while providing economic benefits. Due to the long development cycles there are hurdles that must be overcome in order to integrate non-SNMP enabled devices into a NMS. The SMRT was designed to increase the functionality of a NMS by allowing integration of these devices. The SMRT provides system administrators with management information in a simple and familiar format. It is simple to deploy and was designed with a focus on security. To discuss how the SMRT can be used to monitor your KIV-7M or any other non-SNMP enabled equipment call 973-994-4440 or email sales@telegrid.com.