Secure, Network-Centric Operations of a Space-Based Asset – an Abridged Report

William Ivancic, Phil Paulsen
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

Dave Stewart
Verizon Federal Network Systems
Cleveland, Ohio 44135

Dan Shell
Cisco Systems, Inc.
Richfield, Ohio 44286

Lloyd Wood
Cisco Systems, Inc.
Bedfont Lakes, London, United Kingdom

Chris Jackson, Dave Hodgson, James Northam, and Neville Bean
Surrey Satellite Technology Ltd.
Guildford, United Kingdom

Eric Miller
General Dynamics Advanced Information Systems
Vandenberg, California 93437

Mark Graves and Lance Kurisaki
General Dynamics Advanced Information Systems
Los Angeles, California 90045

***Abstract*— This paper describes the general communication network design and operations that resulted in a demonstration of the Office of the Secretary of Defense (OSD) space-based network-centric operations concepts and major elements of the National Reconnaissance Organization (NRO) Transformational Communication Architecture (TCA), using technology based around the Internet Protocol (IP). The broad functional intent of the Consultative Committee for Space Data Systems (CCSDS) Space Link Extension (SLE) was met. A key element of this demonstration was the ability to securely use networks and infrastructure owned and/or controlled by various parties.**

***Index Terms*—Network Centric Operations, Information Assurance, Satellites, Networks, Internet, Security**

I. Introduction

On 27 September 2003, a Cisco Internet router (Cisco Systems, Inc., San Jose, CA) was launched into low Earth orbit onboard the UK–DMC disaster-monitoring satellite built by Surrey Satellite Technology Limited (SSTL, Guildford, UK). This router has since been successfully tested and demonstrated by an international government and private sector collaboration, showing how IP can be used to communicate with satellite payloads in space.

In June 2004, after lying dormant while the satellite's primary payloads were used, the router successfully completed a number of tests that demonstrate the effectiveness of IP communication to satellites.

While the satellite's primary purpose is to provide images of the environment on Earth, its onboard router is the focal point of a secondary payload, an experiment that involves a wide range of organizations, including Cisco Systems, SSTL, the U.S. National Aeronautics and Space Administration (NASA), the U.S. Air Force, the U.S. Army, General Dynamics Advanced Information Systems (Arlington, VA), Universal Space Network, Inc. (Horsham, PA), Western DataCom (Westlake, OH), and others. The router was used as the IP-compliant, space-based asset for the OSD Rapid Acquisition Net Centricity "virtual mission operations center" demonstration (VMOC, discussed in section 2.0 "Background"). This initiative was executed as a collaborative experiment between the Air Force, the Army, and NASA

This work was made possible through combined funding of NASA's Earth Science Technology Office, the Office of Secretary of Defense's Rapid Acquisition Initiative – Net Centricity, Cisco Systems, Surrey Satellite Technology, Ltd., and General Dynamics.

Glenn Research Center (GRC) in Cleveland, Ohio. Nautilus Horizon, IP-based software by General Dynamics, was used to acquire satellite telemetry, request images from SSTL's satellite dynamically, and perform real-time access to on-orbit satellite equipment (the Cisco router).

The Army and Air Force Battle Labs provided support and performed the overall metrics collection and evaluation as part of the OSD-sponsored VMOC effort [1-5].

The VMOC experiments occurred at Vandenberg Air Force Base in California from June 1 to 13, 2004, and ended with a three-day demonstration there on June 14, 15, and 16. The users at the remote battlefield operations center at Vandenberg requested images of specific areas of the Earth, which were taken by the satellite and delivered from SSTL using standard IP. The General Dynamics VMOC application relied on mobile routing to communicate across the Internet via NASA GRC to SSTL's ground station and up to the Cisco router onboard the satellite. The VMOC application also monitored the health of the satellite using satellite telemetry information delivered over IP.

This VMOC demonstration serves as a blueprint for space-based network-centric operations and the Transformational Communication Architecture; VMOC is also intended for use with the TacSat-1 and TacSat-2 satellites. In addition, the interfaces developed to allow various organizations to share infrastructure (space and ground assets) meet all the functional requirements of the Consultative Committee for Space Data Systems (CCSDS) Space Link Extension (SLE), without relying upon the CCSDS protocol suite.

Cisco Systems' Global Defense, Space and Security group acted as a catalyst in bringing organizations in the defense, civil, and commercial worlds together to test and demonstrate its space-based router. NASA Glenn provided secure mobile networking expertise, was the network system integrator, and performed all preliminary tests leading to the successful router testing and VMOC experiments and demonstration. General Dynamics used Internal Research and Development funds to produce their VMOC software, Nautilus Horizon. Integral Systems, Inc. (Lanham, MD) also ran comparative testing of a pared-down VMOC in parallel with the General Dynamics VMOC.

Up until now, the space community has traditionally used purpose-built hardware. These tests represent a first demonstration of a generic commercial network device—a Cisco IP router—onboard a satellite in space. IP-based technologies and hardware can bring a number of benefits to satellite communications, including:

(1) Reducing the development/design time of satellite communication systems (both space- and ground-based)

(2) Increasing networking capabilities, thereby helping to enable secured remote access to cost-effective unmanned ground stations

(3) Improving satellites' ability to interoperate with ground stations and air and space systems by making satellites active nodes on the Internet.

NASA expects to save at least 25 percent of the cost of future spacecraft development by implementing architecture similar to the one tested with the VMOC [6-9]. The goal is to develop satellite systems that are as easy to integrate as networked printers, rather than to follow the difficult and different network paths encountered with today's non-IP-compliant systems. As the space and ground infrastructures merge, it becomes increasingly important that there is a common frame of reference—IP—to help enable end-to-end quality of service and a common framework for management. NASA also expects significant operations improvements with the full-scale adoption of IP, such as rapid adaptation to change, improved interoperability, and end-to-end security (where required).

II. Background

The Cisco router in low Earth orbit (CLEO) and the virtual mission operations center (VMOC) projects originated as two separate projects in two overlapping organizational groups, and remain separate. However, the projects are complementary in their shared use of the Internet Protocol (IP), and the groups have a mutually beneficial interest in working together towards the overall goal of network-centric operations.

Cisco Systems, Inc. (San Jose, CA), has been working with the U.S. National Aeronautics and Space Administration (NASA) for more than 6 years on joint research for aerospace networks. Cisco Systems eventually decided that it was in Cisco's best interests to demonstrate the ability of terrestrial IP routing technology to work in space. In order to secure a low-cost, high-performance space platform, Cisco turned to Surrey Satellite Technology Limited (SSTL, Guildford, UK). SSTL agreed to host Cisco's device as an experimental payload aboard one of their missions under construction, the UK–DMC satellite, the British contribution to the multinational Disaster Monitoring Constellation (DMC). Expenses related to the miniature router experiment, satellite modifications, testing, and operations were borne by Cisco.

Beginning in 1999, NASA Glenn Research Center (GRC) began looking at the operational implications of using IP in space. This was a first attempt to create a secure IP-based application for the remote command and control of space-based assets, and was called "virtual mission operations."

Working collaboratively with General Dynamics Advanced Information Systems[1] and operations specialists from the NASA Johnson Space Center's Mission Control Center, requirements for generic mission operations were developed. These generic requirements are:

- Enable system operators and data users to be remote
- Verify individual users and their authorizations

[1] General Dynamics Advanced Information Systems acquired Veridian Information Solutions, a leading network security vendor for the intelligence community, in August 2003, along with Veridian's Nautilus Horizon software.

- Establish a secure user session with the platform
- Perform user and command prioritization and contention control
- Apply mission rules and perform command appropriateness tests
- Relay data directly to the remote user without human intervention
- Provide a knowledge data base and be designed to allow interaction with other, similar systems
- Provide an encrypted gateway for "unsophisticated" user access (remote users of science data)

The Office of the Secretary of Defense (OSD) Rapid Acquisition Initiative—Net Centricity (RAI–NC) program awarded General Dynamics, the Air Force Battlelab, and the Army Space and Missile Defense Battle Lab a contract to document the assessment methodology for the proof-of-concept demonstration known as "virtual mission operations center" (VMOC). The VMOC group needed a platform to command and control, as three of its major goals were to, in a secure manner, have an unsophisticated user (1) remotely command a space asset, (2) remotely task a space asset for sensor data, and (3) remotely receive live telemetry.

SSTL's satellites were already using IP for communication between their onboard data recorder payloads and with their ground station network. Furthermore, Cisco had already invested in development and deployment of a space-based asset that fit into that network, the CLEO. In addition, Cisco has always been interested in further proving the utility of network-centric operations. Thus, combining VMOC and CLEO testing presented synergies and benefits to all parties.

Cisco Systems funded this onboard router work in its entirety. NASA worked with Cisco to implement the networking and test the router under a nonreimbursable NASA Space Act Agreement. At the request of NASA, the VMOC group was allowed to participate. Any work that was done by SSTL to support VMOC was above and beyond their commitments to Cisco. SSTL also used internal research and development funds to support VMOC and testing, as they saw long-term benefits to this approach and technology.

Note: The Cisco router was an experimental secondary payload onboard the UK–DMC. It was not the primary mission. As such, all network elements configured and used for the demonstration had to be changed in such a way as to not interfere with the operational network or the primary imaging mission of the UK–DMC satellite.

III. Virtual Mission Operations Center

A VMOC can be defined as a framework for providing secure, automated command and control, resource management, and access to an asset or assets by remote users using Internet technologies. These users may be operators or customers. Encompassed in this demonstration are actually three different entities that can be considered as VMOCs, developed separately and, initially, independently: SSTL's unmanned operations centers and their mission planning system, the Universal Space Network (USN) operations center and their pass scheduling system, and the General Dynamics master operations center and VMOC implementations using their Nautilus Horizon product.

A VMOC will always include the following: a security manager, system integrator and resource manager (scheduler). The security manager performs authentication of users and determines what level of privileges that user has for authorization purposes. The system integrator portion of the VMOC automates the interaction of subsystems such as antenna pointing and tracking, modem control, and radiofrequency and power-level control. The resource manager ensures that all subsystems are available prior to scheduling of their use. For example, when requesting an image from the UK–DMC, SSTL's mission planning system must ensure that a higher-priority user has not already requested an image near that time and that sufficient onboard power and storage are available to service the request.

A VMOC may also include the following features: intrusion detection, survivability and redundancy, accounting and data mining. Intrusion detection ensures that malicious users have not gained access to the system. Intrusion detection may also entail deployment of countermeasures to ensure system integrity. The VMOC may also be designed to ensure survivability and redundancy. There may be a number of VMOCs, geographically separated, networked so that if one VMOC goes off-line a secondary VMOC can immediately take over. Effectively, this is failover to a geographically-separated hot standby. Both the USN operations center and General Dynamics VMOC have this capability. The VMOC may implement an accounting mechanism in order to keep track of a customer's use of the resources for auditing or billing purposes. Finally, a VMOC may offer data-mining services. The General Dynamics VMOC was implemented to provide this data-mining service, and SSTL is planning to offer a similar database imagery service for images taken using its space assets, via its DMC International Imaging subsidiary. Ownership and privacy issues will have to be addressed regarding the access provided by any database service.

IV. Satellite Characteristics

The satellite used for this space-based network-centric demonstration was the UK–DMC. SSTL developed the UK–DMC satellite for the British National Space Centre (BNSC) under a grant from the BNSC's Microsatellite Applications in Collaboration (MOSAIC) program. Through UK–DMC, BNSC became the "anchor tenant" for the SSTL-led DMC,[2] accelerating the formation of a full international consortium. Other members of the consortium and their satellites include Algeria (AlSAT-1), Nigeria (NigeriaSAT-1), Turkey

[2]The DMC is the first Earth observation constellation of five to seven low-cost small satellites providing daily images for applications including global disaster monitoring. http://zenit.sstl.co.uk/index.php?loc=120.

(BILSAT-1) and China (the China-DMC satellite is currently under construction).

Each DMC satellite has similar physical characteristics:

- Capable of imaging anywhere on Earth every 24 hours as part of a shared service across all DMC satellites (compared to once every 10 to 20 days for a single Earth observation satellite)
- 686-km altitude, 98° inclination, sun-synchronous orbit
- 100-kg satellite
- 5-year target design life
- Multispectral imager (similar to LandSat 2, 3, and 4 thematic mapper bands)
    - 0.52 to 0.62 μm (green)
    - 0.63 to 0.69 μm (red)
    - 0.76 to 0.9 μm (near infrared)
    - 32-m ground resolution
    - 600-km push broom swath width
- 8.1-Mbps S-band downlink
- 9600-bps S-band uplink

UK–DMC is a satellite of the standard DMC design [10], with added research and development payloads (including the Cisco router and a Global Positioning System (GPS).

V. Cisco Router in Low Earth Orbit (CLEO)

The router deployed onboard the UK–DMC consists of two PC104 4-by-4-in. (90-by-96-mm) boards for this mission (fig. 1): a processor card, the Cisco 3251 Mobile Access Router (MAR), based on Motorola's MPC8250 PowerQUIC II microprocessor, and a serial communications card, a 4-port serial mobile interface card (SMIC) based on Infinion's PEB/F20534 communications device. Total power consumption of the combined unit is approximately 10 W at 5 V; power available on the UK–DMC is 30 W, and the high-speed 8.1-Mbps downlink also draws 10 W. The power draw limits router use across the downlink for extended periods of time, so the router is typically enabled for the 10 min of a pass over a ground station. Internally, the router can operate at up to 100 Mbps throughput for any Fast Ethernet ports, and a Fast Ethernet card with additional Fast Ethernet ports is optional. The serial cards are limited to 8 Mbps, which coincidently happens to be the speed limit of the downlink high-rate transmitters and the serial interface of the Cisco 2621 router in each ground station.

For purposes of the demonstration, the Cisco 3251 received the following flight modifications:

(1) The router was soldered with lead-based, rather than tin-based, solder. Although tin-based solder is environmentally friendlier than lead, it is particularly prone to growing "whiskers" in a vacuum which leads to shorted circuits.

(2) All terrestrial plastic connectors which would warp in temperature extremes were removed and replaced with point-to-point soldered wiring.

(3) All liquid-filled components (e.g., wet capacitors and clock battery) were removed and replaced with equivalent, non-liquid-filled parts.

(4) High-heat-rejection devices were provided a thermal path for heat rejection to the primary structure. A large heatsink was attached to the main processor, and a brace conducted heat away to the payload's aluminum chassis.

(5) The clock battery was removed to avoid explosion and leakage.

Figure 1.—Cisco router mounted in SSTL experiment tray.

The Cisco 3251 Mobile Access Router was NOT modified to provide any additional radiation tolerance. It successfully survived full system flight-level qualification testing (vibration, thermal vacuum, etc…) on the first attempt. This included a temperature range of –60 to +35 °C and a vacuum of less than 1×10^{-3} Pa (1×10^{-5} torr) [11]. To date, the Cisco 3251 has operated as expected on orbit (voltage and current readings are nominal). All data flow tests have been successful.

To accommodate Cisco's mobile access router card (MARC) and SMIC, an interface "motherboard" to supply power and provide an interface to the spacecraft, as well as providing physical mounting for the router cards, was required. The main features of the interface board are summarized below:

- Low voltage differential signal drivers and receivers for SSDR interfacing
- EIA-530 drivers and receiver for MARC and SMIC interfacing
- CAN interface for telecommand and telemetry data and payload configuration
- FPGA to hardwire interconnect spacecraft and payload P/L interfaces
- Provide isolated 3.3-, 5-, and 12-Vdc power supplies

The router can be communicated with and commanded using the onboard computer via the router's console interface, which is connected to the CAN bus. In this mode, the high-rate transmitters are not active. However, in this mode it is

only desirable and practical to perform simple configurations and interrogations as the buffering in the CAN bus link is insufficient to easily allow delivery of screenfuls of text—particularly when more sophisticated configurations can be easily performed via a telnet or ssh session. In order for the router to forward traffic between space and ground, an SSDR must be configured for "pass-through" mode so that frames are copied between the SSDR's physical interfaces to pass to and from the router and multiplexer. The high-rate transmitter must also be active for communication to the ground station.

Both the high-rate transmitters (there is a redundant transmitter) and the router are the main power drains. Thus, the router is only activated during passes over a ground station for connectivity and only if those passes can accommodate the combined power requirements of the high-rate transmitters and the router. This limits router passes to daylight.

VI. Engineering Model Hardware

Cisco financed the construction of an engineering model containing a mobile router along with an SSTL SSDR in order for Cisco and NASA GRC to become familiar with SSDR configuration and allow testing of network configurations on the ground at leisure prior to transporting those configurations to the onboard router for in-space validation. This engineering model was built after launch and delivered to Cisco in February of 2004. Cisco and NASA GRC found this engineering model to be invaluable. Without it, the program would not have been a success, as pass times consisted of two to three passes per week with each pass lasting between 5 to 10 minutes, heavily restricting experimentation with the onboard router. The testing and configuration was done at NASA Glenn Research Center.

In order to reasonably accommodate the NASA GRC working day five time zones away, SSTL scheduled router passes over their Guildford ground station between 9:30 and 12:00 UTC (5:30 and 8:00 EDT). Without repeated execution and testing on the engineering model, the ability of NASA GRC to configure and test the onboard router would have been greatly impaired due to the limited amount of passes, the duration of the passes, and quite seriously, the ability to think coherently when having to get up at 4:00 or 4:30 in the morning for arrival in the laboratory with colleagues in time for a scheduled pass over a remote ground station. (A virtue of VMOC and IP is that you don't have to get out of bed – just use your networked laptop…) The USN Alaska ground station at North Pole, Alaska, was later configured to duplicate SSTL's ground station links. Coincidently, this allowed for router passes over Alaska to be conducted at the more comfortable times of 17:00 and 18:00 UTC.

VII. CLEO–SSTL Network Architecture

The overall goal of the CLEO project was to put a COTS Cisco router in space and determine if the router could withstand the effects of launch and radiation in a low Earth orbit and still operate in the way that its terrestrial counterparts did.

The two goals of the CLEO network design were (1) to ensure that the router was functioning and routing properly and (2) to implement mobile network and demonstrate its usefulness for space-based applications. Since the UK–DMC is an operational system, a major constraint placed on the network design was that any network changes could not impact the current operational network. This basically resulted in two networks being implemented and maintained simultaneously: a network design that worked directly with SSTL's normal mode of operation and a slightly more complex mobile network design. The detailed network design is explained in the full technical report [12].

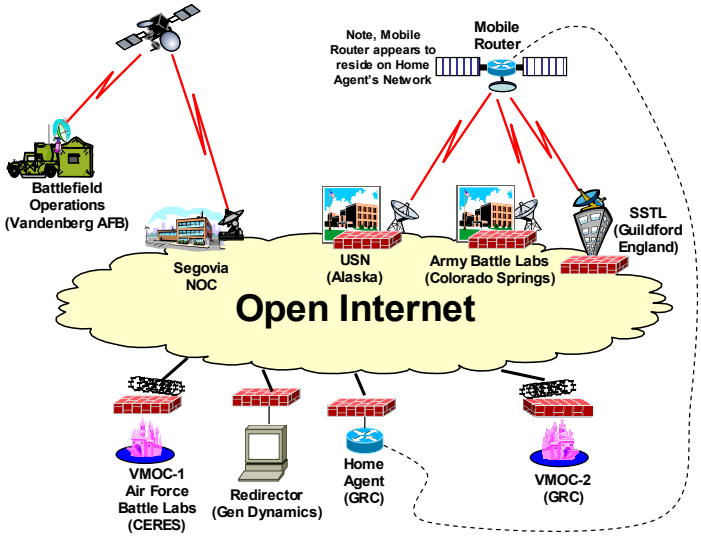

Figure 2.— Secure space-based network.

VIII. Secure Space-Based Network Architecture

The secure space-based network architecture used the open Internet to tie together networks owned and operated by five independent organizations: NASA, the U.S. Air Force Center for Research Support (CERES, Schriever Air Force Base, Colorado Springs, CO), General Dynamics, USN, and SSTL (fig. 2). The purpose of this network configuration was to enable a remote user to securely access and command a space-based asset via a space-command VMOC. Two space-command VMOCs were implemented by General Dynamics using their Nautilus Horizon product. The two space-command VMOCs provided mirroring and redundancy features that enable automatic fail-over capability. SSTL and USN also have similar mission operation implementations dedicated to operations of the SSTL assets and USN ground station infrastructure, respectively. Detailed router configurations are presented in the full technical report [12].

General connections to the Internet occurred throughout the world. Connection points included:

- Home agent router: NASA Glenn Research Center in Cleveland, Ohio
- Primary VMOC: Air Force Space Battlelab Center for Research Support (CERES) in Colorado Springs

- Secondary VMOC: NASA Glenn Research Center in Cleveland, Ohio
- Redirector: General Dynamics in Los Angeles, California
- SSTL ground station: Guildford, England
- USN ground station: North Pole, Alaska
- Army Battle Labs ground station: Colorado Springs, Colorado (low-rate telemetry, receive only)
- Remote battlefield operations: Vandenberg Air Force Base, California, connected through the Segovia, Inc. (Hemdon, VA) IP satellite-based network3
- Remote user: anywhere in the world. Examples include router passes accessed via the home agent, conducted by Will Ivancic while in a Minneapolis hotel room during the March 2005 IETF meeting.

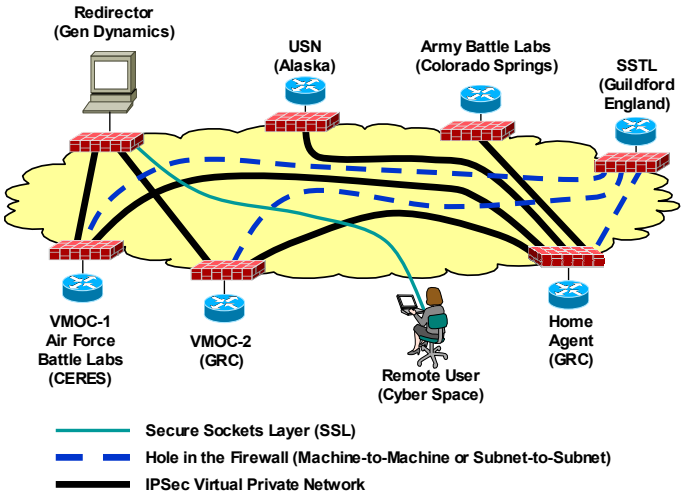

Figure 3.— Network Security Implementation

Network security was performed using a number of techniques and technologies to fulfill the overall needs and requirements of the various users (fig. 3). Virtual private networks (VPNs) using IP security (IPsec) tunnels were implemented between the General Dynamics' redirector and the two VMOCs. IPSec VPNs were also implemented between the two VMOCs and the home agent router as well as between the home agent router and the USN and Army Battle Labs ground stations. Originally, a VPN IPSec tunnel was also created between the remote user and the redirector. This was later replaced with Secure Sockets Layer (SSL) security. There was a strong desire to create an IPsec tunnel between SSTL and the home agent with all communication between the VMOC sites and the SSTL ground station occurring by way of the existing IPSec VPN tunnels between the home agent and two VMOCs. However, since SSTL's network is supporting live operations, placing a new firewall into SSTL's network was not possible without affecting SSTL operations. This is because SSTL's internal network topologies required some redesign to implement the necessary subnetwork configurations. To reasonably secure the network and demonstrate secure space-based network-centric operations, a decision was agreed upon by all parties to open restricted holes in SSTL's existing firewall to allow some machine-to-machine and subnetwork-to-subnetwork communications. These holes have since been plugged and a Cisco PIX firewall put in place as an SSTL corporate firewall.

A. *Redirector*

The redirector is in the General Dynamics facility in Los Angeles, behind the General Dynamics VPN/firewall. The redirector at one time used a VPN client to allow remote users to access the VMOC. That technique has since been replaced with SSL connections. Both CERES and NASA GRC VMOCs have VPNs to the redirector. The redirector "proxies" the current "primary" VMOC to the user, and has an inbound proxy rule that statically NATs the Internet address **http://Portal.VMOC.dummy_name** to the internal address of the redirector. There is no direct access from the Internet to the actual VMOCs as the redirector is actually a reverse proxy. With tunnels between the VMOCs and the redirector and the use of SSL, there is no more vulnerability than when using VPN tunnels from remote clients.

Note: The redirector is currently a potential single point of failure, but that issue is being investigated.

B. *Ground Stations*

Five ground station networks were implemented consisting of three physical ground stations, the flat satellite (flatsat[4]) engineering model emulated ground station at NASA Glenn, and the "virtual flatsat installation at NASA Glenn, where a Cisco mobile access router was always available for remote configuration and experimentation in parallel to the dedicated "flatsat" engineering testbed. The three physical ground stations with links to the UK–DMC were SSTL, Army Battle Labs, and USN (Alaska). Both SSTL and USN-Alaska sites had bidirectional links with a 9600-bps uplink and an 8.1-Mbps downlink and could therefore be used for complete command and control of the UK–DMC if desirable. The Army Battle Labs site only had a low-rate downlink that could capture and retransmit real-time telemetry. In addition, the Army Battle Labs site implemented a third-party VMOC to perform comparative testing with General Dynamic's space-control VMOC implementation.

IX. CLEO TESTING

The Cisco router in low Earth orbit (CLEO) is a major component of these network-centric operations. Future near-planetary space systems are likely to use IP routing in space for access to onboard networks and for cross-link and downlink communications over a variety of wireless interfaces.

[3] Segovia's network operations center is in Ashburn, Virgina with teleports in Laurel, Maryland; Napa, California; and Amsterdam, Netherlands. http://www.segoviaip.com/global_network/index.htm.

[4] Hardware emulation of relevant components of a satellite.

There were two major goals regarding test and demonstration of the CLEO. The first was to demonstrate useful routing. The second was to demonstrate mobile IP and mobile routing. Static routing was used as a fallback as that was all that was required to ensure minimal interoperation between the CLEO and the SSTL ground station network.

Prior to testing of the CLEO, SSTL had to develop and upload the pass-through software to configure an SSDR to allow CLEO to interface to the uplink and downlink transmitters, by copying frames between physical interfaces in software. This was completed and fully tested by NASA and SSTL on May 6, 2004, after the first console access to CLEO on April 29, 2004. NASA and Cisco access to CLEO for configuration and testing was not available until May 11, 2004. Also, since CLEO was not the primary mission of the UK–DMC, and since the router and high-speed transmitter use much of the power budget of the UK–DMC (the router uses ~10 W, and the high-speed downlink uses ~10 W, yet the power budget for the whole satellite is only 30 W), router passes were limited. Usually scheduled passes testing the router consisted of three per week, one per day for approximately 8 to 10 min, depending on elevation of the pass, over the SSTL ground station in Guildford.

During the initial contact times of May 11 and 12, the SSDR was not in pass-through mode. Rather, the router received configuration commands via the console port by way of the onboard computer where serial frames were carried over the parallel CAN bus. The console port provided a poor link in that the CAN bus only provides limited buffering while control codes were not handled well in virtual terminals, making it difficult to show router status. However, this imperfect connectivity was sufficient to allow configuration that enables telnet access to the router. An SSDR was then placed in pass-through mode and the remaining configuration of the router, including implementation of ssh and password-secured Web interfaces, was performed via telnet sessions directly to the router. CLEO's initial configuration was for simple static routing. Once the static routing configuration was completed, file transfer from a SSDR through the router was tested successfully.

Secure shell (ssh) was added, as was HyperText Transfer Protocol (HTTP) command access and multi-layer security. This allowed the VMOC team direct access the space-based router and direct commanding, but only allowed VMOC users access to "show commands" thereby ensuring the safety of the space-based asset. This was successfully tested on May 26.

Next, configurations were added to enable mobile IP and mobile networking. On Wednesday, May 26, 2004, CLEO was successfully configured for mobile networking. This was confirmed during a May 28 pass.

Network services that have been demonstrated to date include:

- Console port access via the CAN bus
- Telnet
- Static routing
- Mobile-IP mobile networks
- Router access via http
- ssh access
- Secure Web access
- Trivial File Transfer Protocol (TFTP) copying of configuration files to ground
- FTP copying of configuration files to ground
- Cisco Internetworking Operating System (IOS) command line functionality
- Earth image file transfer from an SSDR to ground through CLEO using static routing
- Network Time Protocol (NTP). The CLEO router is powered down after each experimental pass, and there is no battery to maintain the clock, so all timing information is lost. Running NTP at the start of each pass and syncing router time with the ground compensates for loss of known time when the router is turned off.

Applications that are desirable but have yet to be completed:

(1) File transfer from an SSDR to ground through CLEO using mobile routing. This requires configuration of the SSDR address to be in the mobile network address space.

(2) Simple Network Management Protocol to provide information on router performance and performance metrics

(3) Distributed file transfer across multiple ground stations. This would require new file transfer application in both SSDR and in terrestrial systems [13].

(4) Uploading new IOS firmware to the router. This would be one of the end-of-life experiments because of the risk of corruption. An IOS upload requires numerous passes due to large file size in the 6-Mbyte range and low uplink rate of 9600 bps, and would require onboard SSDR software to reassemble the uploaded segments into a single file for onboard transfer to the router. Because of the large number of passes required, the need for file transfer development, and the impact on other uses of the satellite, this is extremely unlikely to be carried out.

X. VMOC Test and Demonstration

The VMOC concept demonstration showed the utility of the TCP/IP Internet Protocol suite to acquire satellite data, dynamically task a satellite payload, and perform TT&C of an on-orbit satellite asset. In addition, remote access to meaningful information by military personnel was demonstrated, showing that the VMOC can support the warfighter. The user can pull needed data rather than relying on product centers pushing data that is not of interest to him.

For this demonstration, General Dynamics' Nautilus Horizon VMOC software was used to perform the following tasks:

- Demonstrate secure operations across the open Internet
- Incorporate active intrusion testing
- Validate multiple users and perform contention control
- Obtain real-time data from the SSTL UK–DMC satellite
- Schedule access time to the spacecraft
- Identify appropriate ground station for routing command / telemetry
- Communicate with the NASA GRC VMOC to provide shadow operations
- Demonstrate fail-over between Battle Lab and NASA VMOCs

The VMOC demonstration evaluated five categories to assess the feasibility of the VMOC to provide access to payload information, knowledge data bases, and receive TT &C data:

(1) Does VMOC provide access to payload information for the warfighter?

(2) Can the field users request information from a platform or sensor?

(3) Can field users request information from existing databases?

(4) Can the VMOC demonstrate rapid response and reconfiguration of an IP based platform?

(5) Can the VMOC task platforms as required to get necessary information to the warfighter?

All five categories were successfully met.

XI. Space Link Extensions—Functional Requirements

As part of the secure space-based network-centric operations demonstration, the functional requirements outlined in the CCSDS SLE documents have been met [14-16]. The overall goal of moving spacecraft telemetry around beyond the confines of the space-ground link, which is the purpose of the CCSDS SLE, becomes possible and even easy with the use of IP in the space-ground link and in the terrestrial network for a merged space-ground architecture. A key element of these demonstrations was the ability to securely use IP-enabled networks and infrastructure owned and/or controlled by various parties.

We believe that the network-centric operations and command and control of space-based assets concept that was implemented for this demonstration met the overall intent of the CCSDS interoperability standards and in particular the Space Link Extension. See the full technical report for a detailed description [12].

Note: This secure net-centric operations implementation asset differs from the initial assumptions for SLE Cross Support in that the net-centric architecture is, by design, scalable to meet the needs of multiple missions, multiple spacecraft, and multiple mission-managers.

This demonstration currently uses only a single IP-compliant satellite, the UK–DMC. SSTL, has, however, developed a general Web-based interface to its mission planning system for end users to request services across multiple IP-based satellites and payloads; the DMC mission planning system (MPS) has become distributed across multiple satellites and across multiple ground stations. USN has already developed an interface for users to request service from any USN ground station and for the particular modulation and coding required. General Dynamics' VMOC implementation, acting as the master controller, can task the SSTL assets via a common Web interface and could also perform autonomous scheduling of the USN assets (although the latter task has not been accomplished as of the time of this writing).

XII. Future Work

Some major concepts that should be pursued in the near future are described in this section.

A. *Onboard Routing Between Devices*

The UK–DMC satellite also has a GPS reflectometry experiment onboard. A third onboard SSDR controls the GPS reflectometry experiment and stores the data from that experiment. To download the data, that SSDR has to be given access to the multiplexer, and packetized data has to be pumped out over the wireless link to ground during a pass. That third SSDR is an older design based on an older Intel StrongARM-based processor, and cannot output data faster than ~3 Mbps, so downlink and pass time is not used efficiently. Moving data from the slower StrongARM-based SSDR controlling that experiment to ground requires dedicating passes to that SSDR. Data can be moved through the router to be stored on a primary imaging SSDR while the satellite is not passing a ground station. This would use CLEO without using the high-speed downlink and take advantage of the router being connected to all SSDRs, each on a different subnet.

Transferring the data offline to the faster PowerPC-based SSDR–1 or SSDR–2 (controlling the imagers) means less pass time is wasted during transfers, that the SSDR-3 does not have to be powered up storing data until a pass or at the same time as the high-speed downlink, and that SSDR–1 or 2 can downlink images as well as the GPS data much faster, increasing overall power and time efficiency for the satellite and simplifying scheduling during a pass. It also permits on-orbit use of the router without the high-speed downlink being on, and demonstrates use of the router as a good onboard citizen doing something useful.

B. *Large File Transfers Using Multiple Ground Stations*

By using mobile routing and developing a special file

transfer application that splits delivery end-to-end and caches files locally in the ground station, it is possible to fully use each space-to-ground downlink at maximum capacity, even with lower rate terrestrial links between the ground stations and the the end user [13].

One could conceivably use USN's and SSTL's ground stations to perform this multi-ground station file transfer, providing the ability to split downloads across multiple ground stations and recombine files afterwards. This effort would require USN to implement the required ground station modifications necessary for operation with the DMC satellites and for SSTL to write the application software to run a file transfer over multiple ground stations.

C. SSTL Commanding Satellite Through the USN Ground System

SSTL could send commands to the DMC satellites or other SSTL space assets via a USN ground station. This would require SSTL to modify its MPS to automatically check availability of USN assets (published list) and request available assets. This could be performed via machine-to-machine e-mail transactions – see full technical report for details of USN Operations [12].

D. VMOC as Systems Coordinator and Security Manager

A master VMOC could be the security manager and system of systems coordinator over a number of VMOCs. The master VMOC would receive a request from a user for an image and then coordinate between SSTL and USN to determine what ground station(s) would receive the image and at what time. In addition, it would be advantageous to consider adding an Army Battle Labs ground station and a NASA ground station. The goal would be to show the utility of VMOC as security and systems coordinator of various assets that are owned by various entities and to demonstrate the ability of IP technology to flexibly perform the equivalent functionality of the CCSDS SLE.

E. IPv6-Compliant Satellite

Recommendations for a next-generation IP-compliant experimental satellite would include use of an onboard router and HAIPIS encryptor that utilizes the next-generation IP protocol, IPv6. This would be highly beneficial as the US DOD has mandated IPv6 for all Global Information Grid—Broadband Extension (GIG–BE) elements.

XIII. Recommendations and Lessons Learned

Following is a list of lessons learned and recommendations:

(1) The ability to have all the tools available in a full IOS on the onboard router proved invaluable. Some discussions have taken place to consider a slimmed-down IOS. The thought is that an IOS-lite may be more robust or easier to qualify rigorously for the space environment. The users and network administrators of the CLEO router and associated network question this concept for the following reasons: first, removing functionality may result in less stable code rather than more stable code, as any change in software can affect the robustness of software and second, it is quite probable the functionality taken out will end up being the functionality one needs for some later, unforeseen configuration need. Case in point: because of the hardware implementation of the UK–DMC, the serial interface was physically connected to both the onboard controller (OBC) and CLEO. Thus, when both entities were activated, messages bound for the OBC were heard by CLEO. An access list had to be put into the CLEO configuration to prevent circular routes. With a lot of forethought and discussion between SSTL's hardware designers and NASA GRC's routing team beforehand, this might have been identified as a problem earlier and remediation steps taken in design. Fortunately, this unique problem was able to be simply addressed by a single command in the router configuration once the problem manifested itself, as the router IOS permitted this.

(2) Mobile networking greatly simplifies network configurations at the ground stations and adds an extremely insignificant amount of overhead (three small packets per session for binding setup).

(3) Triangular routing is preferred if the rate on the terrestrial links cannot meet or exceed the rate of the downlink. Triangular routing along with new file transfer applications enables full utilization of the downlink [13].

(4) When sharing infrastructure such as ground terminals, space assets, air traffic control systems, radars, or databases, the interface between asset owners will have to be identified and some special software written for each to share this infrastructure and use it for the purpose for which it is intended. The use of Internet standard protocols and applications, such as the TCP/IP protocol suite and SOAP (simple object access protocol) for exchanging information in XML (extensible markup language) over http, make implementing these interfaces much quicker and easier than if noncommercial standard protocols and applications were used.

(5) The engineering model of the onboard and ground assets is a necessity. The engineering model on the ground was invaluable for testing configurations and scenarios prior to uploading to the actual flight router—particularly when considering the limited available contact time.

(6) According to commercial ground terminal service providers, USN and Integral Systems, there are products available for ground station TT&C that have become de facto industry standards. IN–SNEC's CORTEX series product family is one such example. It would be highly desirable for the spacecraft operators to work with the ground-station service providers in order to use existing hardware or establish some new common space-ground conventions. This would ease integration of the ground systems with the space systems. In the case of the UK–DMC, the uplink is 9600 bps using an amateur radio standard G3RUH modem whereas the downlink is 8 Mbps using a commercial convention for geostationary satellites (i.e., Viterbi: r = ½ k = 7, IESS 308/309, and ITU

V.35 scrambling). Since the CORTEX products could not provide this descrambling, a geostationary satellite modem had to be incorporated into the ground systems, adding cost and complexity to the ground systems.

XIV. New Capabilities

An onboard router or embedded onboard routing functionality helps enable standard payloads to be placed on an onboard local area network and be commanded and controlled using commercial standard Internet Protocols.

The VMOC's distributed architecture provides for survivability and rapid reconfiguration needed in the battlefield, science, and business environments. This enables new and exciting mission architectures that will advance military and NASA air and space core competencies by laying the groundwork for the use of IP and desktop browsers for command and control of spacecraft, sensors, and manned and unmanned aerial vehicles.

By using commercial standard equipment and commercially available standard protocols, such as the TCP/IP protocol suite, to communicate with the space and ground systems, the service provider—here, the VMOC – has many more ground assets to draw upon. In addition, these ground assets may be available from multiple commercial ground service providers. This competition and standardization results in significant cost savings. In addition, the ability to use multiple assets results in more available contacts, greater contact time, and quicker response time. For example, a request to take an image over Japan may be received. The spacecraft may have its next available contact time over a ground station owned by company A in Australia. The VMOC could send the commands to take an image of Japan through company A's ground station in Australia. The image would be taken and stored. The image could then be transmitted to the ground through company B's ground station in Alaska. By being able to use multiple ground stations and ground station providers, and perhaps multiple spacecraft providers, one will increase the contact time and responsesiveness of the system significantly.

This use of common standards and interfaces may enable new markets for space and ground system providers and encourage competition.

The ability to use multiple ground stations enables large file transfers to take place over multiple ground stations' contact times. This architecture allows system implementers tremendous flexibility in the design of the space system. It would be possible to reduce the downlink transmit rate and corresponding transmit power because of the increased contact time. One no longer has to transmit an entire file in a single contact time. Potentially, this enables systems with longer life expectancies, lower battery power, and less spacecraft mass to reduce launch costs.

XV. Conclusions

The successful demonstrations of secure command and control of a space-based asset, CLEO, proves the concept for network centric operations using space-based assets and could easily be extended to other assets (e.g., air, ground, and sea). These demonstrations showcased major elements of the National Reconnaissance Organization (NRO) Transformal Communication Architecture (TCA), using Internet Protocol (IP) technology. These demonstrations also showed that the broad functional intent of the Consultative Committee for Space Data Systems (CCSDS) Space Link Extension (SLE) was met. A key element of this demonstration was the ability to securely using networks and infrastructure owned and/or controlled by various parties.

References

[1] Unruh, Nicholas D.: Virtual Mission Operations Center (VMOC) After Initiative Report. Air Force Space Battlelab, 2004. Available from the Department of Defense.

[2] Unruh, Nicholas D.: Opportunity Analysis for Virtual Mission Operations Center Web-Based Interface (VMOC WBi). Department of the Navy Business Innovation Team and Air Force Space Battlelab/Army Space and Missile Defense Battle Lab, 2004. Available from the Department of Defense.

[3] Schmitt, C.: VMOC Metrics Collection Data Report. Prepared for Contract DASG62–01–D–0003, 2004.

[4] Schmitt, C.L.; Groves, S.R.; and Tomasino, T.: Net-centric C2 in Near and Far Space. Proceedings of the 24th Army Science Conference, Orlando, Florida, 2004.

[5] Conner, B.P., et al.: Bringing Space Capabilities to the Warfighter: Virtual Mission Operations Center (VMOC). Proceedings of the 18th Annual AIAA/USU Small Satellite Conference, VMOC Paper SSC0–II–7, 2004.

[6] Guo, G.: TRW: NASA Rapid II IP-Based Spacecraft Accommodation Study Final Report, 2000. Available from Phil Paulsen, NASA Glenn Research Center.

[7] Jackson, C.: SSTL: IP Accommodation Study Final Presentation, 2000. Available from Phil Paulsen, NASA Glenn Research Center.

[8] Laizbin, J.: Spectrum Astro: IP-Based Spacecraft Accommodation Study Final Presentation, 2000. Available from Phil Paulsen, NASA Glenn Research Center.

[9] Runge, H.: Orbital: Final Briefing IP-Based Spacecraft Accommodation Study, 2000. Available from Phil Paulsen, NASA Glenn Research Center.

[10] da Silva, Curiel, et al.: Second Generation Disaster-Monitoring Microsatellite Platform. Acta Astronaut., vol. 51, nos. 1–9, 2002, pp. 191–197

[11] van der Zel, V.: Nigeria and UK–DMC Thermal Vacuum Test Procedure. SSTL Internal Technical Document, 2003.

[12] Ivancic, W., et al.: Secure, Network-Centric Operations of a Space-Based Asset: Cisco Router in Low-Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC), NASA/TM-2005-213556, May, 2005

[13] Ivancic, W.: Secure, Network-Centric Operations of a Space-Based Asset: Cisco Router in Low-Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC)" Net-Centric Operations 2005, May 10-11, 2005 Washington, DC. http://roland.grc.nasa.gov/~ivancic/papers_presentations/AFEI_NCO_presentation.ppt Accessed May. 13, 2005.

[14] Space Link Extension Services—Executive Summary. Yellow Book, CCSDS 910.0–Y–1, 2002.

[15] Cross Support Concept—Part 1. Space Link Extension Services, Green Book, CCSDS 910.3–G–2, 2002.

[16] Cross Support Reference Model—Part 1. Space Link Extension Services, Blue Book, CCSDS 910.4–B–1, 1996