

Secure, Network-Centric Operations of a Space-Based Asset: Cisco Router in Low Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC)

William Ivancic
Glenn Research Center, Cleveland, Ohio

Dave Stewart
Verizon Federal Network Systems, Cleveland, Ohio

Dan Shell
Cisco Systems, Inc., Richfield, Ohio

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

Phil Paulsen
Glenn Research Center, Cleveland, Ohio

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

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

The NASA STI Program Office . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA Scientific and Technical Information (STI) Program Office plays a key part in helping NASA maintain this important role.

The NASA STI Program Office is operated by Langley Research Center, the Lead Center for NASA's scientific and technical information. The NASA STI Program Office provides access to the NASA STI Database, the largest collection of aeronautical and space science STI in the world. The Program Office is also NASA's institutional mechanism for disseminating the results of its research and development activities. These results are published by NASA in the NASA STI Report Series, which includes the following report types:

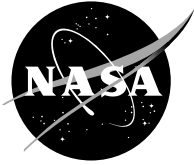
- **TECHNICAL PUBLICATION.** Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA's counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.
- **TECHNICAL MEMORANDUM.** Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.
- **CONTRACTOR REPORT.** Scientific and technical findings by NASA-sponsored contractors and grantees.

- **CONFERENCE PUBLICATION.** Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored by NASA.
- **SPECIAL PUBLICATION.** Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.
- **TECHNICAL TRANSLATION.** English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services that complement the STI Program Office's diverse offerings include creating custom thesauri, building customized databases, organizing and publishing research results . . . even providing videos.

For more information about the NASA STI Program Office, see the following:

- Access the NASA STI Program Home Page at <http://www.sti.nasa.gov>
- E-mail your question via the Internet to help@sti.nasa.gov
- Fax your question to the NASA Access Help Desk at 301-621-0134
- Telephone the NASA Access Help Desk at 301-621-0390
- Write to:
NASA Access Help Desk
NASA Center for AeroSpace Information
7121 Standard Drive
Hanover, MD 21076



Secure, Network-Centric Operations of a Space-Based Asset: Cisco Router in Low Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC)

William Ivancic
Glenn Research Center, Cleveland, Ohio

Dave Stewart
Verizon Federal Network Systems, Cleveland, Ohio

Dan Shell
Cisco Systems, Inc., Richfield, Ohio

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

Phil Paulsen
Glenn Research Center, Cleveland, Ohio

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

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

National Aeronautics and
Space Administration

Glenn Research Center

Acknowledgments

The primary authors would like to thank all the people who helped contribute to the success of this project and to the information contained within this report. Many portions of this report were taken from internal documents and documentation, test plans, e-mail correspondence, and papers.

Trade names or manufacturers' names are used in this report for identification only. This usage does not constitute an official endorsement, either expressed or implied, by the National Aeronautics and Space Administration.

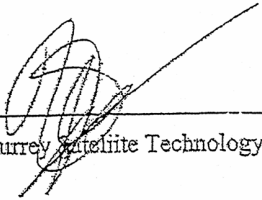
Available from

NASA Center for Aerospace Information
7121 Standard Drive
Hanover, MD 21076

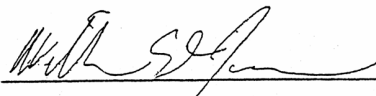
National Technical Information Service
5285 Port Royal Road
Springfield, VA 22100

Available electronically at <http://gltrs.grc.nasa.gov>

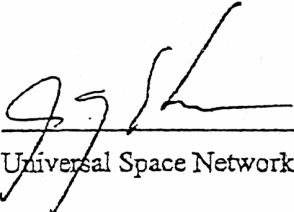
This report has been reviewed by Cisco Systems, NASA Glenn Research Center, Surrey Satellite Technology Ltd, General Dynamics, Universal Space Networks and Western DataCom to ensure all material is available for public release.



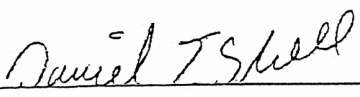
Surrey Satellite Technology Ltd. Date 14 MAR 05



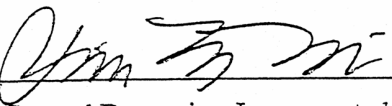
NASA Glenn Research Center Date 2/2/05



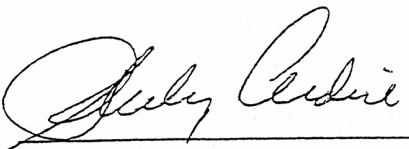
Universal Space Network Date 10 JAN 05



Cisco Systems, Incorporated Date 02/29/2005



General Dynamics, Incorporated Date 10 Jan 2005



Western DataCom Date 2-2-05

Contents

1.0 Executive Summary	1
2.0 Background	3
3.0 Surrey Satellite Technology Limited (SSTL)	5
3.1 Satellite Characteristics	6
3.2 RF Chain	7
3.3 Satellite and Ground IP Network	8
3.4 Operations	10
3.4.1 Resource management	10
3.4.2 Scheduling	10
3.5 UK–DMC Satellite Bus	10
3.5.1 Architecture	10
3.5.2 Spacecraft control	13
3.6 Firmware and Software	13
3.6.1 Pass-through firmware	13
3.6.2 SSSDR flight software description	13
3.6.3 Image transfer application	13
4.0 Cisco Router in Low Earth Orbit (CLEO)	15
5.0 Engineering Model Hardware	16
6.0 CLEO–SSTL Network Architecture	18
6.1 SSTL Normal Mode of Operation	19
6.2 CLEO Using Normal Operations	20
6.3 CLEO Using Mobile Networking	21
7.0 Secure Space-Based Network Architecture	22
7.1 Redirector	24
7.2 Ground Stations	25
7.2.1 SSTL ground network	25
7.2.2 Engineering model flatsat network	25
7.2.3 Virtual flatsat network	28
7.2.4 USN ground station network	29
7.2.5 Army Battle Labs ground station network	29
7.2.6 Remote user network	31
8.0 USN Ground Station Network	31
8.1 Network	32
8.2 Operations	32
8.2.1 Resource management	32
8.2.2 Scheduling	33
9.0 General Dynamics Nautilus Horizon	34
9.1 Security Manager	34
9.2 Redundancy and Survivability	35
9.3 Systems Integrator	35
9.4 Scheduler	35
9.5 Data Mining	36
10.0 Space Link Extensions—Functional Requirements	36
10.1 CCSDS Specification Summary	36
10.2 Shared Networks and Infrastructure	38
10.3 SSTL Constellation Mission Planning System (MPS)	38
10.4 VMOC–SSTL Interfaces	39
10.5 VMOC–USN Interfaces	41

10.6 SSTL–USN Interfaces	41
11.0 CLEO Testing	41
11.1 First Remote Access and Commanding of the CLEO	42
11.2 Mobile Routing Results	44
12.0 VMOC Test and Demonstration	47
13.0 Future Work	48
13.1 Onboard Routing Between Devices	48
13.2 Large File Transfers Using Multiple Ground Stations	49
13.3 SSTL Commanding Satellite Through USN Ground System	49
13.4 VMOC as Systems Coordinator and Security Manager	49
13.5 IPv6-Compliant Satellite	50
14.0 Recommendations and Lessons Learned	50
15.0 New Capabilities	51
16.0 Conclusions	51
References	51
Appendix A—Acronyms	53
Appendix B—Participating Organizations	57
Appendix C—Points of Contact	59
Appendix D—Cabling	61
D.1 Engineering Model Null Modem Serial Cable (Both Systems Supply Clocking).....	61
D.2 Ground Station Router-to-Modems Cable.....	62
Appendix E—VMOC Screen Shots.....	63
E.1 Log Screen	63
E.2 TT&C Screen	64
E.3 Tools Screen.....	65
E.4 Schedule Screen	66
E.5 Task Screen.....	67
E.6 Data Library Screen	67
Appendix F—Router Configurations.....	71
F.1 CLEO—Home Agent.....	71
F.2 Cisco Router in Low Earth Orbit—CLEO.....	75
F.3 Surrey Satellite Technology Limited (SSTL) Ground Router.....	78
F.4 Universal Space Network (USN) Ground Router	80
F.5 Virtual Flatsat Foreign Agent Ground Router.....	83
F.6 Virtual Flatsat Mobile Router	86
F.7 Engineering Model (EM) Flatsat Foreign Agent Ground Router	88
F.8 Engineering Model Flatsat Mobile Router (CLEO_EM).....	92
F.9 Engineering Model Flatsat Router—MR_Frame_Relay_Router.....	94
F.10 Engineering Model Flatsat Router—FA_Frame_Relay_Router	97
Appendix G—Mobile Router Debug Captures for First Space-Based Mobile Network Session.....	101

Secure, Network-Centric Operations of a Space-Based Asset: Cisco Router in Low Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC)

William Ivancic
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

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

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

1.0 Executive Summary

This report documents the detailed 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). This report also illustrates 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 use networks and infrastructure owned and/or controlled by various parties.

On 27 September 2003, a Cisco Internet router (Cisco Systems, Inc., San Jose, CA) was launched into low Earth orbit onboard the UK–DMC, the 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 Glenn Research Center (GRC) in Cleveland, OH. 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. See

- Unruh, Nicholas D.: Virtual Mission Operations Center (VMOC) After Initiative Report. Air Force Space Battlelab, 2004. Available from the Department of Defense.
- 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.
- Schmitt, C.: VMOC Metrics Collection Data Report. Prepared for Contract DASG62–01–D–0003, 2004.
- 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, FL, 2004.
- 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.

The VMOC experiments occurred at Vandenberg Air Force Base in California from June 1 to 13, 2004, and ended with a 3-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 CCSDS 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 and design time of satellite communication systems (both space-based 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. See

- Guo, G.: TRW: NASA Rapid II IP-Based Spacecraft Accommodation Study Final Report, 2000. Available from Phil Paulsen, NASA Glenn Research Center.
- Jackson, C.: SSTL: IP Accommodation Study Final Presentation, 2000. Available from Phil Paulsen, NASA Glenn Research Center.
- Laizbin, J.: Spectrum Astro: IP-Based Spacecraft Accommodation Study Final Presentation, 2000. Available from Phil Paulsen, NASA Glenn Research Center.
- Runge, H.: Orbital: Final Briefing IP-Based Spacecraft Accommodation Study, 2000. Available from Phil Paulsen, NASA Glenn Research Center.

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).

2.0 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 their best interest 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 Systems¹ 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
- 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 database 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—Network Centric (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 computer 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.

The remainder of the report is organized as follows: It first discusses, in general, what is meant by the phrase “virtual mission operations center.” It then presents a detailed description of the SSTL UK–DMC satellite and network designs. A discussion of the operation of the CLEO follows, after which the detailed network design is presented, including the detailed operation of the General Dynamics implementation of the master VMOC. A list of the acronyms used in this report is given in appendix A. A list of the

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.

organizations that participated in this demonstration is given in appendix B, and a list of the project's points of contact is given in appendix C.

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, Inc. (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 (RF) 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 offline 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, Ltd., subsidiary. Ownership and privacy issues will have to be addressed regarding the access provided by any database service.

3.0 Surrey Satellite Technology Limited (SSTL)

SSTL is the world leader in low-cost, rapid-response small satellites. SSTL, a spinoff company of the University of Surrey in the United Kingdom, pioneered low-cost, rapid-response small satellites. From its inception, SSTL has produced reliable, high-quality, low-cost satellites using advanced terrestrial commercial-off-the-shelf (COTS) technologies that are adapted for use in the harsher conditions of space. SSTL now employs over 250 staff and has designed, built, and launched 23 small satellites, making it the most successful and experienced small satellite supplier in the world (refs. 1 and 2).

Most recently, SSTL has built and launched the DMC—four satellites in orbit that have been of extensive use in disasters throughout the world, including taking daily images of the 2004 tsunami-hit regions in South East Asia. SSTL has also designed and built satellites for international customers, including the first frequency-testing Galileo satellite for the European Space Agency and two high-resolution Earth observation microsattellites: one for the United Kingdom Ministry of Defence (UK-MoD) for its Tactical Optical Satellite, TopSAT, and one for the China Ministry of Science and Technology (MoST) as the Chinese contribution to the DMC. SSTL is also contracted to build five microsattellites for the first commercial Earth observation constellation for RapidEye AG (Munich, Germany) and a microsattellite for the Los Alamos National Laboratory, part of the National Nuclear Security Administration (NNSA) of the U.S. Department of Energy.

3.1 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 (AISAT-1), Nigeria (NigeriaSat-1, see ref. 3), Turkey (BILSAT–1, see ref. 4) 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-synxynchronous 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 (fig. 1 and ref. 5), with added research and development payloads (including the Cisco router and a Global Positioning System (GPS) reflectometry experiment). In comparison to the other DMC satellites in orbit, UK–DMC features increased onboard data storage, with 1.5 GB capacity across two solid-state data recorders (SSDRs). Images are returned to the SSTL mission operations centre via an 8.1-Mbps (8 140 800-bps) S-band downlink.

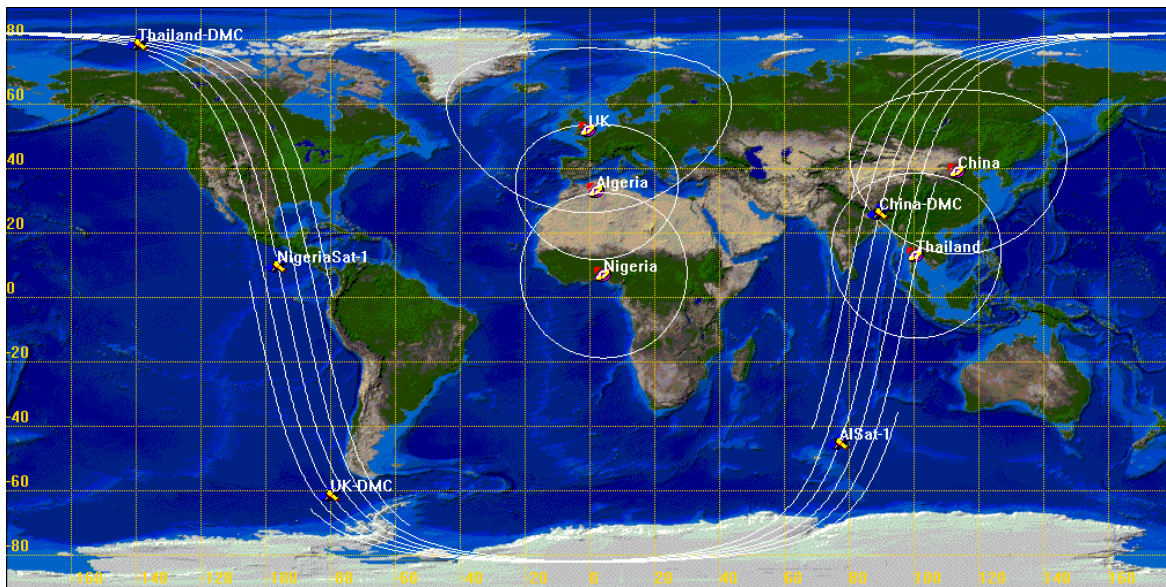


Figure 1.—DMC constellation ground trace.

²The 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>.

3.2 RF Chain

The RF communication path for the uplink and downlink (ref. 6) are shown in figures 2 and 3. On the uplink, the ground station router serial interface, transmit portion is connected to the 9600-bps continuous phase frequency shift keying (CPFSK) baseband modem (ref. 7). Note that the modem provides the clock to the router. The router's serial interface is configured as data terminal equipment (DTE). The baseband modem is then VHF-modulated with appropriate computer control to compensate for Doppler. This signal is then upconverted to S-band, amplified, and transmitted.

The power amplifier amplifies the signal to an output power of 40 W. This is the power level that, when taking into account filter- and transmission-line losses, is required to produce sufficient E_b/N_0 at the SSTL satellites for reliable satellite commanding. The transmit filter improves ground station emissions and prevents ground station receive desensitization.

An orthogonal mode transducer, which is part of the feed, separates the uplink right-hand circular polarized (RHCP) and downlink left-hand circular polarized (LHCP) signals and provides isolation between the antenna's transmit and receive ports.

On the downlink, the LHCP S-band signal is downconverted and demodulated using a Comtech EF Data CDM-600 modem (ref. 8, Comtech EF Data Corp. (Tempe, AZ)). The modulation scheme used is quadrature phase shift keying (QPSK) with half-rate Viterbi encoding and International Telecommunication Union (ITU) V.35 scrambling.³ Downlink rates are 38.4 kbps for telemetry only and 8.1 Mbps for high-rate transmission and when the spacecraft is configured for router operation using the high-speed downlink.

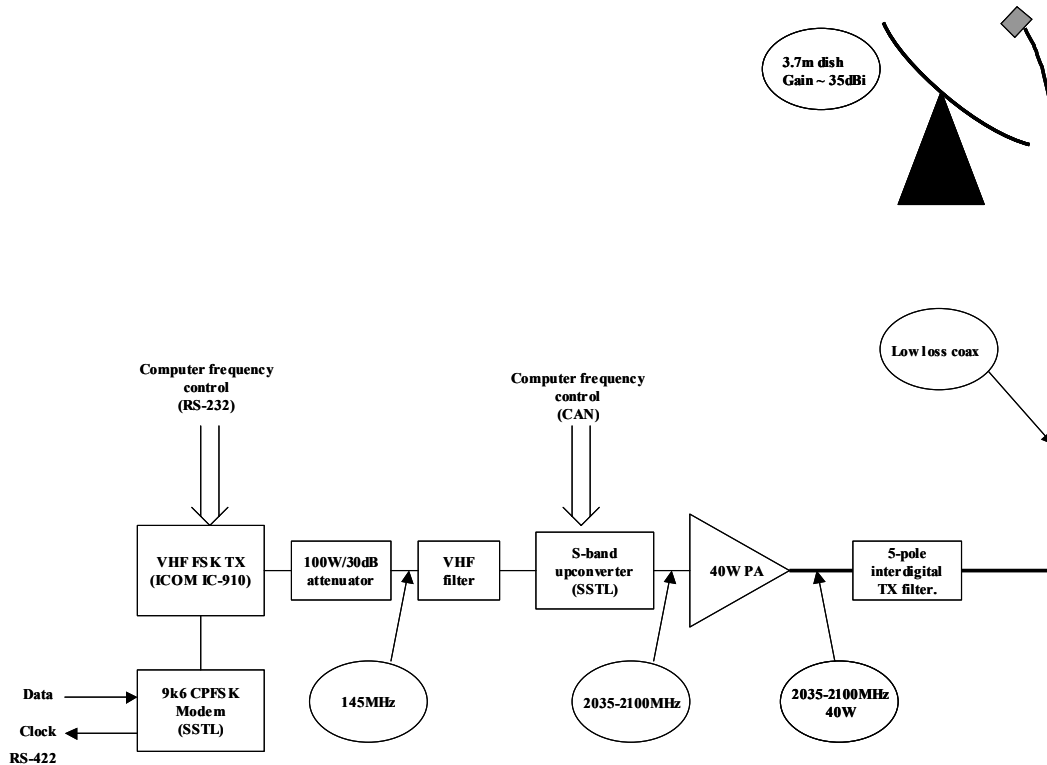


Figure 2.—Ground station S-band uplink path.

³ Both USN and Integral Systems use IN-SNEC CORTEX Series products (IN-SNEC, Paris, France) in their LEO tracking stations. CORTEX is a line of fully digital and highly integrated PC-based products that perform signal processing for ground station and system applications. The CORTEX unit currently operates at up to 10 Mbps. It does not, however, perform ITU V.35 descrambling. Thus both USN and Integral Systems used the CDM-600 modem. This did, however, result in additional hardware integration.

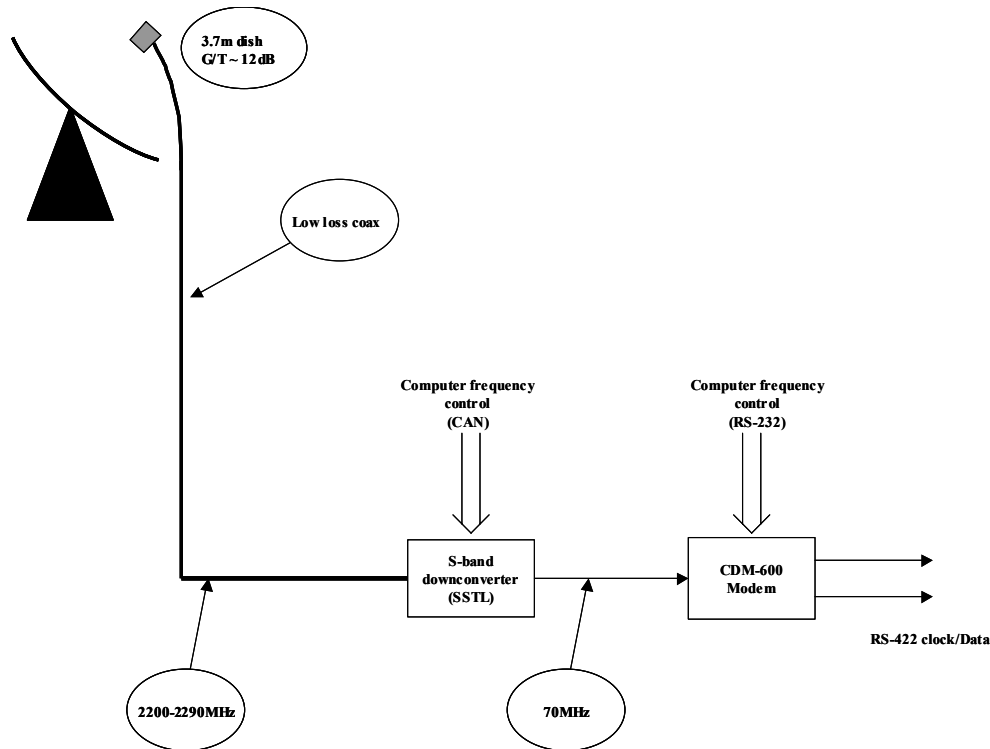


Figure 3.—Ground station S-band downlink path.

The modem provides the clock to the router serial interface, receive portion. As such, the router's serial interface is configured as DTE.

3.3 Satellite and Ground IP Network

SSTL's current satellite network concept evolved from SSTL's early days as an experimental spacecraft developer. In the early stages, it was highly desirable to keep the satellite ground station IP network as simple as possible. Scalability was not an issue or concern. As such, the current DMC network encountered and built on at the start of the CLEO work is a direct result of evolving that simplicity. However, with the advent of the DMC, SSTL is considering evolving the current network topology to a more scalable topology. The current DMC IP network is designed as a flat network. All satellite onboard networks and the ground station networks are effectively on the same private, class C subnetwork, the SSTL.Private.0 subnetwork.

The current network configuration (fig. 4) has served SSTL quite well and has some elegant features. SSTL uses IP more for layer-3 switching on the private subnetwork than for actual IP routing. Thus, IP is used as an effective and simple tool to get the necessary functions performed. The ground station router receiving the downlink serial stream has three interfaces: an Ethernet interface to the private network of SSTL.Private.0 with a 24-bit mask, an Ethernet interface to the local infrastructure and eventually the global Internet, and an unnumbered serial interface to the satellite via a satellite modulator and demodulator pair. Anything going from the private Ethernet local area network (LAN) to the satellite has a corresponding static router configuration entered in the ground station router (thus, it really acts as a layer-3 switch here). In SSTL's current operations profile, any information from the satellite is always destined to the private LAN, allowing the use of User Datagram Protocol (UDP) broadcast for telemetry so that all computers on the ground station network can receive those broadcasts. Once the packets are received from the spacecraft, normal routing will place them on the private Ethernet LAN. Network address translation (NAT) was used to map machines on the private network to corresponding publicly routable address space for remote access purposes.

DMC IP Network Topology

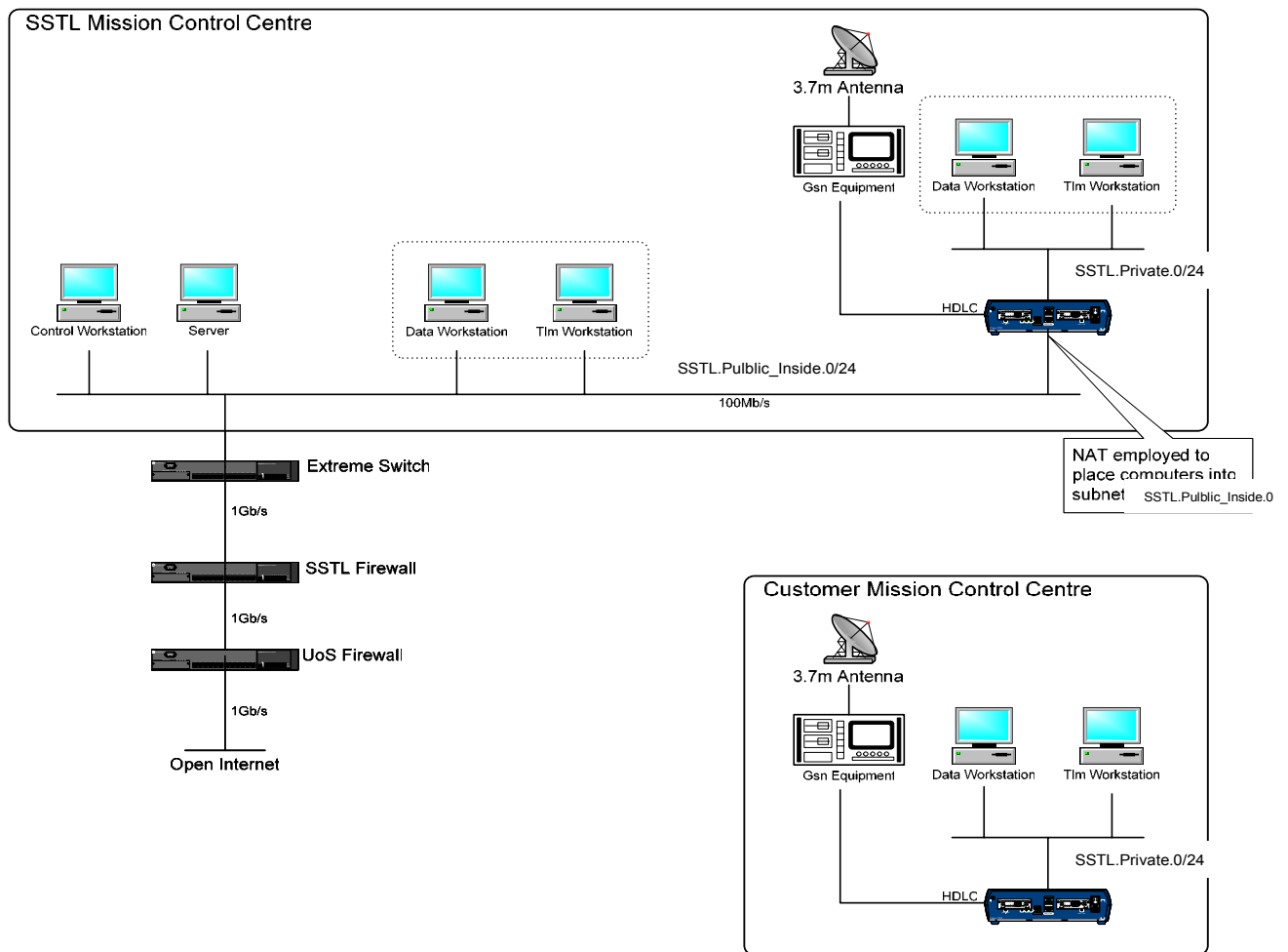
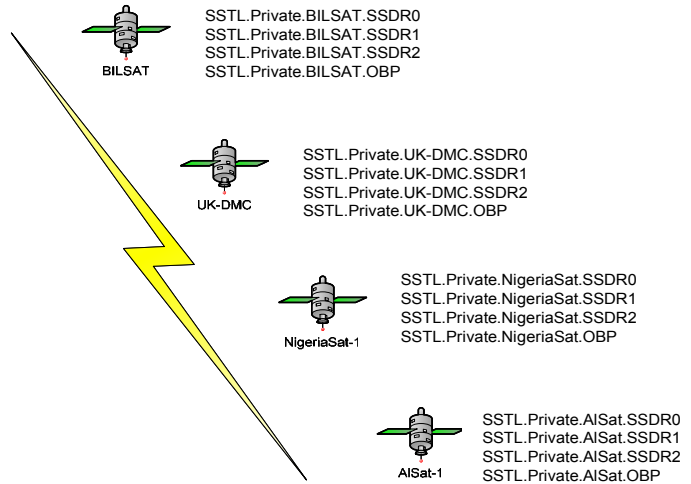


Figure 4.—SSSL ground and satellite network.

SSSL developed an elegant solution for determining when to correspond with a satellite. The satellite periodically sends UDP broadcast messages down the serial link. The ground router expands these broadcasts and places them on the private LAN via use of the “ip directed-broadcast” command in the Cisco routers. Once the workstations on the private LAN hear these broadcasts, applications such as file

retrieval can automatically begin. Although this technique has served SSTL well in the past, it is not scalable to a large number of ground stations, as operations like NAT configuration and address coordination to preserve the address space used for UDP broadcast become increasingly painful. Future systems may use a similar strategy by using multicast instead—particularly when considering migration to Internet Protocol 6 (IPv6). In this way, any subscribing hosts on any network can receive the telemetry corresponding to that multicast group.

The link-layer framing, set in the router serial interface configuration and onboard the spacecraft, is frame relay using the IETF (Internet Engineering Task Force) specification for encapsulation. Frame relay encapsulation of IP packets carried across the satellite serial links uses the synchronous high-level data link control (HDLC) frame format.

3.4 Operations

3.4.1 Resource management.—The SSTL’s ground station control room typically monitors 15 satellites and actively controls 9 using 3 independent antennae. Software is used extensively to monitor and interact with the space vehicles (human intervention is typically not required for routine operations; the room is often unmanned and unlit). SSTL automatically monitors the onboard devices, power, battery life, and health status of all active missions. As such, SSTL has developed its own automated mission operations center, which could well be considered SSTL’s own VMOC.

Anomalies in satellite or payload operation are also detected through software, and notifications are made to the appropriate flight personnel via pager or mobile phone. Satellite recovery operations can be conducted locally or through a generic Internet connection. The responsible parties can log into the system from remote locations and take appropriate action. Operators do not have to be physically present in the control room.

3.4.2 Scheduling.—Scheduling of spacecraft assets occurs approximately once per week by convention with a face-to-face planning meeting, but can be preempted if the need occurs. Requests are generally submitted to SSTL’s operational staff via e-mail, fax, or phone; a Web interface to SSTL’s distributed mission planning system for DMC owners to request and schedule images has recently been deployed. Requests are entered into SSTL’s resource scheduler, which determines that the spacecraft can meet the request and flags any conflicts with suggested alternatives. Once the scheduling routines are complete, a list of scheduling commands is queued up for transmission to the appropriate spacecraft. All commands are encapsulated into UDP/IP packets and transmitted at the appropriate time.

3.5 UK–DMC Satellite Bus

3.5.1 Architecture.—The UK–DMC satellite is of a modular design that was easily extended to incorporate a module containing a Cisco 3251 router and corresponding serial interface card (ref. 9), along with microcontroller-based circuitry to interface the router’s console and serial links to the internal low-speed Controller Area Network (CAN) bus, 8.1-Mbps serial buses, and power management. Figure 5 illustrates the general bus configuration and shows the low-rate point-to-point links for the transmitters and receivers. Low-rate transmission from the satellite is at 38.4 kbps. This is the configuration used when broadcasting only telemetry messages (UDP packets) to the ground; UDP telemetry is sent down the high-rate downlink when that is available.

Notice that the UK–DMC satellite has redundant receivers, onboard computers, transmitters, cameras, and SSDRs. Redundancy at all levels is a key part of SSTL’s approach to ensuring reliability and mission success.

Figure 6 shows the high-rate connections. The imagers transmit data to the SSDRs at 40 Mbps. The SSDRs transmit stored images to the ground station at the common serial link speed of 8.1 Mbps. Redundant paths are available for all connections.

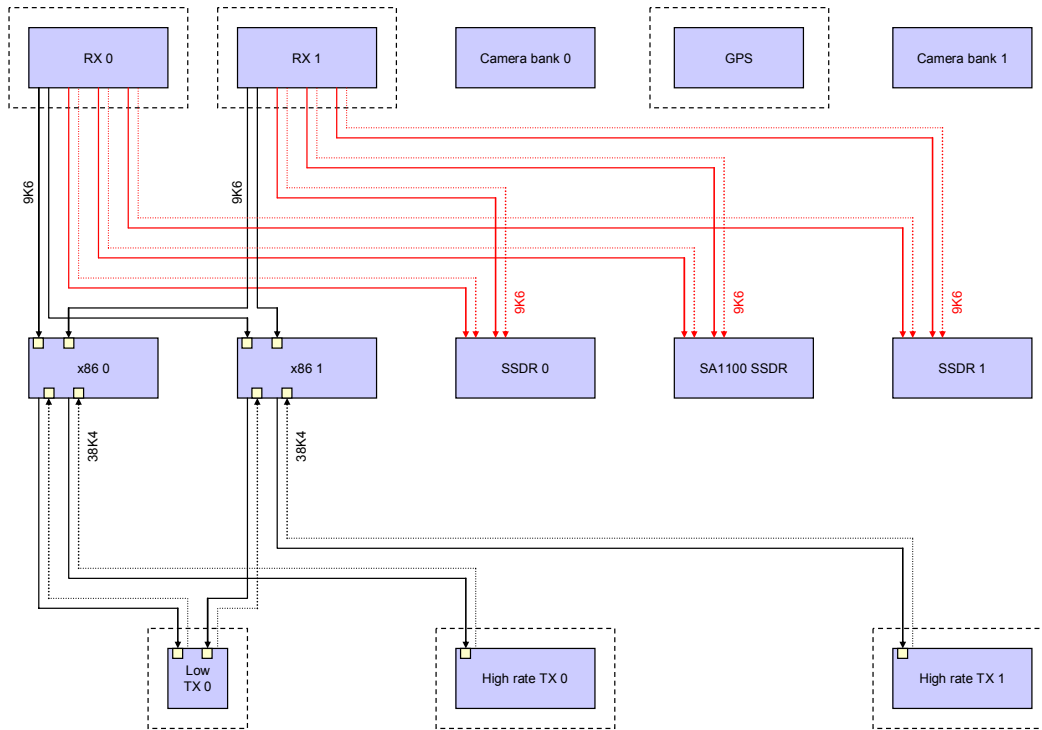


Figure 5.—UK-DMC transmitter and receiver low-rate point-to-point links.

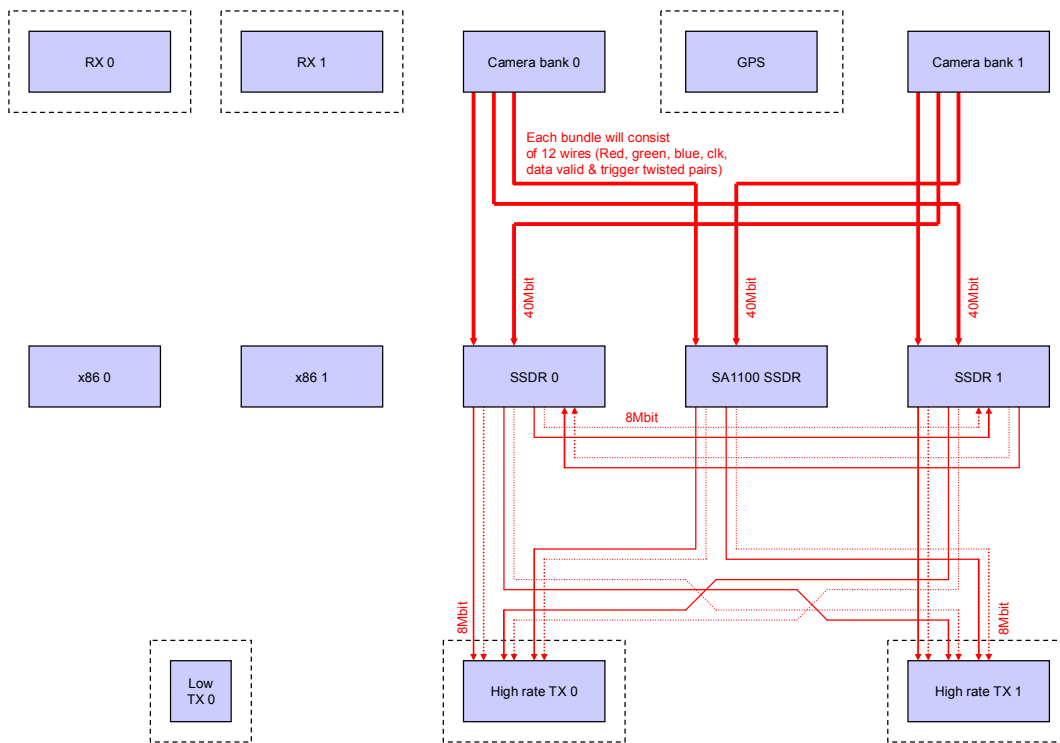


Figure 6.—UK-DMC transmitter high-rate point-to-point links.

The Cisco router was integrated into the satellite in such a manner as to enable complete isolation as this is an experimental secondary package and is not the primary mission of the UK–DMC. The satellite was already using 8.1-Mbps serial links to talk to the serial interface on the Cisco 2621 router in the ground stations, and onboard devices were connected using 8.1Mbps serial links, allowing full use of the 8.1-Mbps serial downlink by any one scheduled device at a time. Integrating the mobile access router and its serial card interfaces to the UK–DMC serial links into this environment was therefore straightforward.

The Cisco router obtains connection to the transmitter and receiver via its serial connections to either SSSDR0 or SSSDR1 (fig. 7). Either of these SSSDRs can be configured into “pass-through” mode in order to connect the Cisco router to the transmitters and receivers by copying frames from an input interface to an output interface via a program stored in the SSSDR firmware. When an SSSDR is in pass-through mode, it is dedicated to that task and cannot be used to capture new imaging data. However, a stored image can remain intact in random access memory (RAM) while the SSSDR is in pass-through mode. The other two SSSDRs can be used for data storage and file transfers. It is particularly important to note that telemetry data is also passed through the SSSDR and multiplexed in with imaging data; IP telemetry can be sent via any available downlink, and there are no dedicated separate control links.

The onboard computer that commands the spacecraft can provide console access to the router when the satellite is configured for low-rate transmit operation. The CAN bus, carrying serial information across it, is used for this communication. Buffering is very limited when communicating via the CAN bus. Therefore, after initial configuration using console access, the majority of router configuration was performed via telnet, secure shell (ssh) and Web interface sessions while communicating through an SSSDR in pass-through mode.

When in pass-through mode, the high-rate transmitters are operational. In this mode, bidirectional connection to the onboard computer (OBC) that runs the satellite platform may not be available, depending on the uploaded configuration. Both the high-rate transmitters and the router require substantial power; of the available 30-W power budget for the satellite, the router requires 10 W, and the high-speed downlink requires 10 W. Therefore, this configuration is power resource limited. Thus, this pass-through configuration is only used for experiments and only run when the satellite is in sunlight and over a ground station to ensure that sufficient power is available.

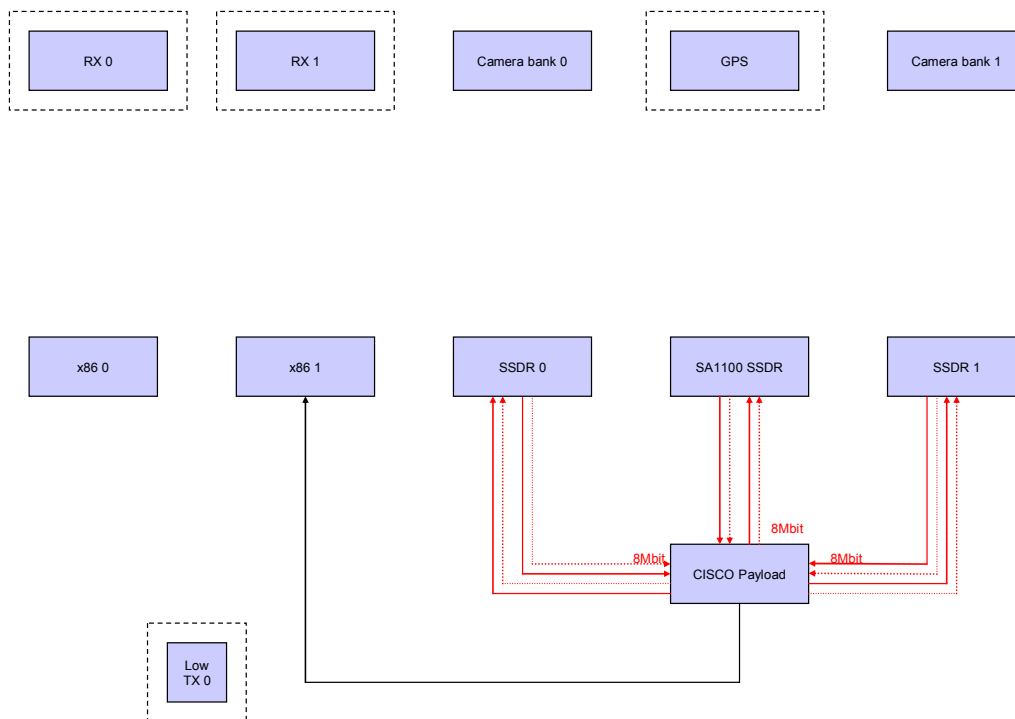


Figure 7.—UK–DMC Cisco router payload connections.

3.5.2 Spacecraft control.—The spacecraft is controlled via an onboard computer (OBC), traditionally referred to as the onboard processor (OBP) from the days when there was only one computer onboard an SSTL satellite. Tasks can be sent to the onboard computer and run as chronological jobs. The onboard computer interfaces to a CAN bus for power management and payload control. The CAN bus operates at 38.4 kbps. All devices on the spacecraft are connected to the CAN bus. The devices that were used in the CLEO–VMOC demonstration were the onboard computer, the imager, the solid state data recorders, and the Cisco router. All telemetry is also sent over the CAN bus. When downloading imagery and using the high-rate 8-Mbps S-band downlink, all imagery is sent in-band on that link. Note, this is contrary to traditional satellite operations where telemetry and data are transmitted on independent links.

3.6 Firmware and Software

3.6.1 Pass-through firmware.—The Cisco router was integrated into the UK–DMC satellite in such a manner as to ensure that this experimental system could be isolated from the rest of the satellite bus if necessary. As shown in figure 7, the router connects to the rest of the satellite through SSDR0 or SSDR1. Currently, whichever SSDR is used for pass-through is unavailable for storage of new images. The remaining two SSDRs are available for storage. Pass-through software was an addition to the SSDR software, and was written and uploaded after launch. Performing software development after launch is an SSTL tradition to spread workload around the launch.

3.6.2 SSDR flight software description.—The SSDRs on the DMC spacecraft are responsible for capturing data from the cameras and making it available for downlink at a later time. The DMC imagers are push-broom-type imagers. There is no local storage on the cameras so each line of data must be stored in real time by the SSDRs. Additionally, the relatively high resolution and wide swath width mean that the data storage requirements are high. A 300- by 600-km image in three spectral bands at 32 m ground sample distance (GSD) requires almost 1 GB of storage.

An open-source operating system called RTEMS (Real-Time Operating System for Multiprocessor Systems) was used for the SSDRs. The main reasons for the selection of RTEMS were that it has a file system and Transmission Control Protocol/Internet Protocol (TCP/IP) stack and is supported across a wide range of processor types. As the secondary data recorder is based on the Intel StrongARM SA1100 Microprocessor, SA111 Companion Chip (Intel Corporation, Santa Clara, CA), cross-platform support was essential for code reuse between the two types of data recorder. RTEMS has been modified because it did not support the exact PowerPC (IBM Corporation, Armonk, NY) processor type used on the primary SSDRs. Therefore, an additional library was written for the MPC8260 PowerQUICC II (Motorola, Inc., Schaumburg, IL) central processing unit. Additionally, the SSDR hardware is custom, so a board support package was also needed.

The applications are a set of cooperating tasks that utilize resources and services from the operating system. Some tasks interact directly with the hardware. This is possible because all RTEMS tasks run in supervisor mode. These tasks are

- configuration
- initialization
- synchronization
- image
- capture
- wash
- system log
- Consultative Committee for Space Data Systems (CCSDS) File Delivery Protocol
- root file system

3.6.3 Image transfer application.—Implementations of two file transfer protocols for image download were developed by SSTL: the CCSDS File Delivery Protocol (CFDP) and a later in-house

transfer protocol design named Saratoga (ref. 10). Both of these applications are reliable rate-based file delivery protocols that use UDP. Saratoga was written to efficiently fill the 8-Mbps downlink with only a 9600-bps uplink, with minimal acknowledgment back-traffic and minimal processing between output packets to fill the downlink pipe. The basic idea is that data is streamed down at 8 Mbps to a local storage device. Holes in the data received from missing packets are noted and requests for retransmission of only the missing data is made via the 9600 link. This protocol was developed to efficiently utilize both the uplink and downlink where downlink capability far exceeds uplink capability. Congestion control is not a concern for the satellite link since the link is not shared with other users or extended across the Internet, and imagery download is the satellite's primary purpose. Saratoga and a stripped-down IP stack replaced the CFDP implementation on the RTEMS TCP/IP stack for increased performance and to decrease memory footprint.

These software applications run on the SSTRs (ref. 11). The processing capabilities of the SSTRs are listed below:

- (1) 0.5/1 GB (4/8 Gb) synchronous dynamic RAM (SDRAM) data storage with 72:64 error-correcting code (ECC) hardware error correction and Reed-Solomon software coding
- (2) Motorola MPC8260 PowerPC processor with on-chip floating point arithmetic unit
- (3) 1-MB EDAC protected program static RAM (SRAM), triple modular redundancy (TMR)
- (4) 2-MB firmware storage flash RAM
- (5) RTEMS operating system (POSIX⁴ application program interface (API), BSD sockets)

SSTL initially used an implementation of the CCSDS CFDP UDP-based transfer protocol in their SSTR operating system. This protocol implementation relied on the supplied RTEMS TCP/IP network stack. The maximum data rate that was obtained for this implementation was approximately 7.5 Mbps. This throughput limitation was an implementation performance issue. To save flash and memory footprint, and to increase download performance by allowing the relatively slow (compared to the router) PowerPC SSTRs to saturate the 8.1-Mbps downlink with packets, SSTL removed both the RTEMS-sourced stack and the CFDP implementation from the SSTR operating system, replacing them with an SSTL-written lightweight "stack" implementing a minimum of IP and UDP features. This stack is used by a rate-based UDP file transfer protocol designed by SSTL and named Saratoga (after a U.S. battleship sunk at Bikini Atoll). Saratoga uses minimal acknowledgments, making it very suitable for the asymmetric links (9.6 kbps up for acks, 8.1 Mbps down for data.). The combination of the rate-based protocol and fast lightweight stack implementation allowed each primary SSTR to fill the 8.1-Mbps downlinks with packets, without pauses due to processing between packets. This enabled SSTL to empty a 1-GB SSTR of images during a 10-min pass over a ground station, and then power that SSTR off until its next scheduled imaging opportunity, saving power and getting the most out of the 10-W downlink power. In addition, SSTL had a requirement to eventually transfer data to the ground at higher rates—40 Mbps for the China-DMC satellite, and the increased performance of Saratoga's design was intended to also benefit that scenario.

Note: Even with Saratoga, the slower SA1100 SSTR can only achieve 3 Mbps on the downlink—hence the desire to move stored GPS reflectometry data through the router to a primary PowerPC-based SSTR before downloading it as quickly as possible during a pass.

SSTL has ceased use of CFDP for internal performance reasons and is not using other CCSDS-based protocols. The use of IP and ease of interconnection with other ground networks for moving satellite telemetry around networks that IP enables meets the overall aims of the CCSDS Space Link Extension (SLE), without using the CCSDS SLE protocols. See section 10.0, "Space Link Extensions—Functional Requirements," for further discussion.

⁴ Institute of Electrical and Electronics Engineers, Inc., New York, NY.

4.0 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. 8): a processor card, the Cisco 3251 Mobile Access Router (MAR), based on Motorola’s MPC8250 PowerQUIC II microprocessor, and a serial communications card, a four-port serial mobile interface card (SMIC) based on Infinion’s PEB/F20534 communications device (ref. 12). 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 coincidentally 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.

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, and so forth) 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) (ref. 13). To date, the Cisco 3251 has operated as expected on orbit (voltage and current readings are nominal). All data flow tests have been successful.



Figure 8.—Cisco router mounted in SSDL experiment tray.

Note: The MAR does not contain nonvolatile RAM (NVRAM) to hold configuration information and commands. Rather, NVRAM is mapped to flash, where the current configuration is stored alongside a filesystem containing the boot Cisco Internetworking Operating System (IOS) firmware image and saved configurations. This increases the reliance of the router on flash memory. Multiple copies of the router software (a commercially available IOS 12.2(11) YQ IOS image) were made once in orbit due to concerns about flash file system corruption from radiation upsets. To date, the flash has functioned normally.

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 SSSDR 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 SSSDR must be configured for "pass-through" mode so that frames are copied between the SSSDR'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.

Potentially there may be instances where one may wish to move data between SSSDRs, which would not require the high-rate transmitter to be active. One example would be to move GPS reflectometry data. The third onboard SSSDR that controls the GPS reflectometry experiment is of an older, less powerful StrongARM-based design and has a top transmission speed of 3 Mbps, even when using the Saratoga IP stack for speed. Although it is useful for storage, it cannot take full advantage of the 8.1Mbps downlink capacity when sending. One may wish to move captured data from the third SSSDR to one of the newer, faster, PowerPC-based SSSDRs through the router interconnecting the two SSSDRs, to later transmit data down at 8.1 Mbps, along with images also stored on the PowerPC-based SSSDR, and to enable shutting down the emptied StrongARM-based SSSDR as soon as possible to reduce power consumption.

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.

5.0 Engineering Model Hardware

Cisco financed the construction of an engineering model containing a mobile router (MR) along with an SSSL SSSDR in order for Cisco and NASA GRC to become familiar with SSSDR 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 GRC.

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 one is able to use a networked laptop from any location at any time.) The USN Alaska ground station at North Pole, AK, was later configured to duplicate SSTL’s ground station links. Coincidentally, this allowed for router passes over Alaska to be conducted at the more comfortable times of 17:00 and 18:00 UTC.

The engineering module and equipment provide a complete setup, replicating the Cisco mobile router payload and an SSTL SSSDR, and a number of limited interconnections onboard the UK–DMC spacecraft (ref. 14). Essentially the module consists of several independent submodules in the same case:

- (1) Cisco router assembly and motherboard: this engineering model was electrically identical to the flight model (FM), bar DC–DC converter and number of temperature sensors on the SSTL-designed motherboard.
- (2) PowerPC-based SSSDR: an SSTL-designed module that captures images from the payload and downlinks them to the ground at a later date (store and forward)
- (3) “Camera emulator” hardware: equivalent to the FM imagers onboard the spacecraft but providing IRGB offset greyscale test images.
- (4) RS–422–LVDS converters: not onboard UK–DMC, which uses low-voltage differential signaling (LVDS) for onboard serial communication, but these patchbay converters convert SSTL’s clock and data to connect to a Cisco router via an EIA–530 connector
- (5) CAN bus control: via a PCI card running installed in the controller PC

Access to all three serial ports was possible via the RS–422 interfaces on the engineering model (fig. 9). This enabled the emulated space-to-ground link to be directly connected to any of three serial ports on the router. An additional serial device could be connected to the engineering model. This structure allows the user to test the pass-through software by connecting an external router to LVDS1 and communicating to the router via the SSSDR running pass-through software. When performing CLEO mobile networking configuration tests with the SSSDR in pass-through mode, an additional router was connected to the third serial port with the space-to-ground emulated link connected to the serial port used by the SSSDR.

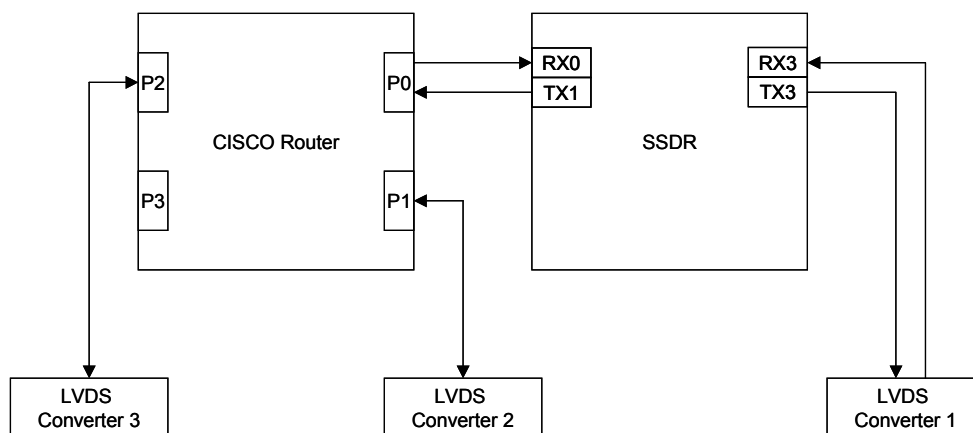


Figure 9.—Engineering model serial interface connections.

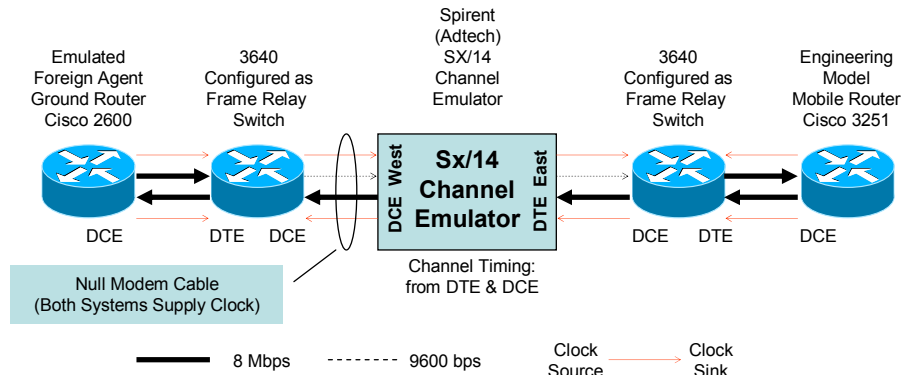


Figure 10.—Engineering model space-to-ground link emulation.

Once the pass-through software was verified, the SSDR in the testbed could be used for its intended purpose, as a mass-storage endhost attached to the router. The router connection was brought out directly via LVDS2 or LVDS3 emulating pass-through, without requiring a second SSDR to be present, as only one SSDR was included in the engineering model.

Because of the requirement to have to physically change cabling and connections to test pass-through and file transfer operations and different addressing on different networks, the engineering model configuration did not correspond directly to the space-based router configuration. So, great care was taken when transporting developed and tested engineering model configurations to CLEO.

The engineering model is implemented in a manner that results in an 8 MHz transmit and receive clock being supplied out of the serial interfaces (because of level translation circuitry). The engineering model would not accept the receive clock. In addition, the serial interfaces on the router are configured as frame-relay links. In order to have the capability of emulating a noisy link, a Spirent SX/14 channel emulator (Spirent Communications, Calabasas, CA) was placed between the emulated terrestrial foreign agent router and the MR in the testbed. Also, in order to emulate the 9600 bps uplink it was necessary to terminate the 8-MHz uplink clock originating from the engineering model’s MR and replace it with a 9600-Hz clock. These two requirements were met by incorporating two additional Cisco 3600 routers into the uplink chain with the channel emulator sandwiched between their serial interfaces (fig. 10). These two additional routers were configured as frame-relay switches. As such, they acted as bridges and all layer-3 communications were unaffected thereby enabling foreign agent advertisements and/or MR solicitations to reach the MR and foreign agent, respectively. In order for the two 3600 routers to both generate clocks—one at 8 MHz and the other at 9600 Hz—a special null-modem cable was made that connected transmit clock (TxC) timing signals on each serial interface to the receive clock (RxC) on the corresponding serial interface. This is described in the cable specifications in appendix D.

6.0 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. We will first describe SSTL’s normal mode of operation and the associated network both with and without the router. This will be followed by a detailed description of the mobile network design.

6.1 SSTL Normal Mode of Operation

An illustration of the effective network topology for SSTL’s normal mode of operation is shown in figure 11. SSTL’s current operational network architecture is set up as a flat network: all space-based IP networked instruments and all ground control and data collection workstations appear, for all effective purposes, to be on the same private subnetwork, SSTL.Private.0/24. This is the case for the DMC as well as other SSTL satellites. In addition, in the past SSTL had used the same addressing scheme for all satellites (i.e., the OBC address is **SSTL.Private.UK–DMC.OBC** for all satellites). This works well for a small number of satellites, as identical firmware where addresses are hard-configured is easily ported to multiple satellites. However, since addresses are not unique, management of a large number of satellites becomes problematic, as satellites must be identified with reference to the pass schedule rather than with an address or other unique identifier. Thus, SSTL has a desire to move to a more scalable network design for the DMC as well as for future systems.

Data is transferred between the spacecraft and ground workstations via static routing, more like layer-3 switching. The OBC is a PowerPC-based computer running a TCP/IP or AX.25 stack. Communication between the workstations and the OBC uses TCP/IP; AX.25 was used in earlier satellites, reflecting SSTL’s amateur radio ham heritage and expertise. The SSDRs also have a limited TCP/IP stack. Some TCP/IP features have been removed when implementing SSTL’s own stack with its Saratoga protocol in order to save memory.

Because of the flat network design, SSTL is able to use broadcast messages from the spacecraft in an elegant manner. Telemetry is sent as broadcast messages to SSTL.Private.255. Once those broadcast messages are received by the ground router, it expands them to a 255.255.255.255 broadcast on the SSTL.Private.0 subnetwork. All machines on that network may listen to this broadcast. Since telemetry is broadcast only on the SSTL.Private.0 subnetwork, the machine that runs the telemetry redirection application⁵ must also reside on that subnetwork.

Telemetry is sent continuously while in contact. As such, as soon as telemetry is being received at the workstations, it is apparent that the link has been closed and applications such as file transfers may begin. Thus, changing from a flat network to a super-subnetted network will require modifications to this

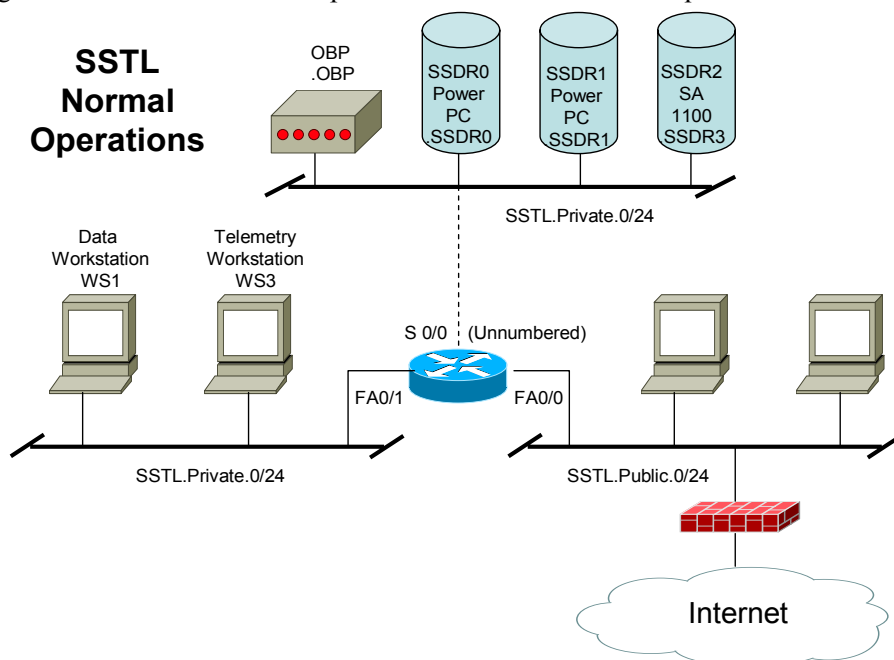


Figure 11.—SSTL satellite and ground network.

⁵ The telemetry redirection application listens for telemetry packets and retransmits those packets as unicast packets to up to 20 host addresses.

broadcast technique—perhaps with the use of multicast rather than broadcast messages. This will also be the case for IPv6, which does not have broadcast messages.

The SSTL satellites and corresponding controllers are on private address space corresponding to University of Surrey address space. Thus, in order to reach any of these assets they have to be mapped to local public addresses around each ground station using NAT techniques. The NAT mapping is apparent in the corresponding configurations located in appendix E of this report.

Note: The configuration shown in figure 11 is the configuration used for low-pass contacts where only telemetry is desired and the router is not active. When one wishes to test connectivity to the OBC, one may ping the OBC private address directly from a machine on the private subnetwork. However, from the open Internet, one must ping a public address that is mapped to the OBC private address via NAT.

6.2 CLEO Using Normal Operations

An illustration of the SSTL’s ground and satellite network topology for normal mode of operation with CLEO connected and SSSDR1 in pass-through mode is shown in figure 12. Operation in this configuration is nearly identical to normal operation. The main differences are that SSSDR1 is not usable for data transmission and that SSSDR0 and SSSDR2 are accessed via the router rather than directly. All SSSDR interfaces are given private addresses and appear to be on the same subnetwork as the ground station workstations. A loopback address, loopback 0, was added to the router configuration in order to access the router using SSTL’s normal access methods. Router statements were added to CLEO to identify which serial ports the SSSDRs were attached to. No true routing protocols are used here. Everything is statically routed (switched).

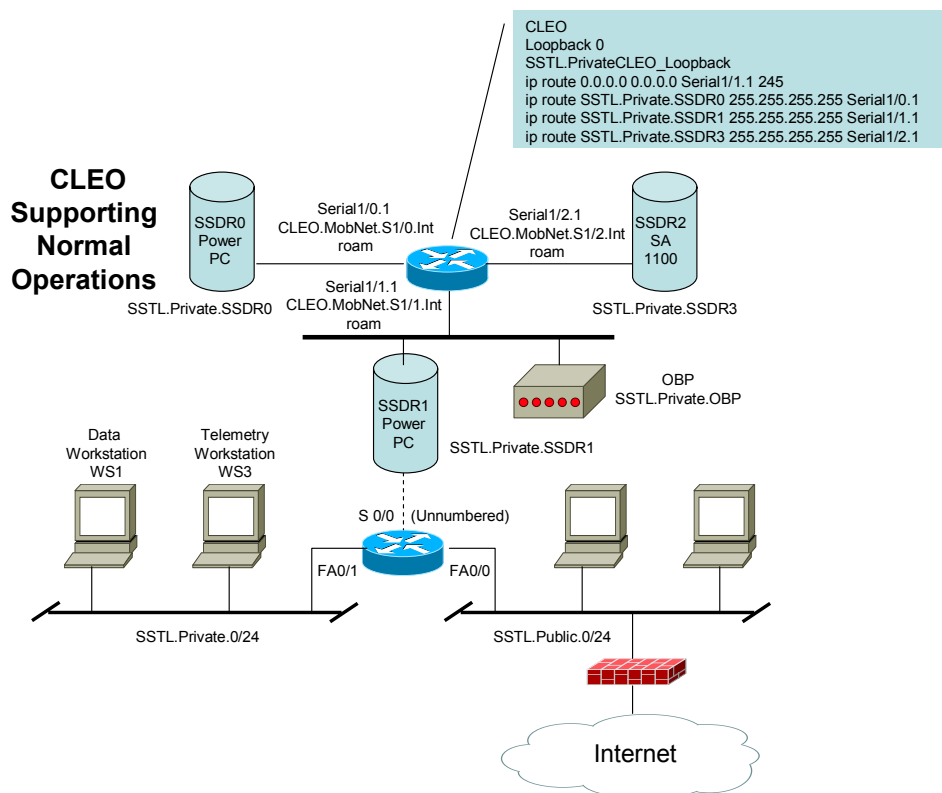


Figure 12.—SSTL satellite and ground network with CLEO supporting normal operations.

Note: Due to the hardware implementation of the UK–DMC, the OBC and router serial interface S1/1.1 are physically on the same wired bus. However the OBC address is **SSTL.Private.UK–DMC.OBC**, whereas no such address resides anywhere on CLEO. If both the OBC and CLEO are active in this mode, the router will see all messages destined for **SSTL.Private.UK–DMC.OBC**. The default route for CLEO is to send everything down to the ground. Likewise, the ground router has a static route statement indicating that everything for **SSTL.Private.UK–DMC.OBC** should be sent up the RF link. Thus, a routing loop is created due to hardware implementation. This was corrected by placing an access list in CLEO to silently discard any packets destined for **SSTL.Private.UK–DMC.OBC**, the OBC. Failure to do this results in the 9600 bps uplink quickly becoming overrun with circulating packets even though the OBC had acted upon them.

6.3 CLEO Using Mobile Networking

An illustration of the SSTL’s ground and satellite network topology for mobile networking operation with CLEO connected and SSSDR1 in pass-through mode is shown in figure 13. Operation using mobile networking is completely different from normal static routes (ref. 15). However, the normal operation parameters are also in CLEO and the SSTL ground router, so both modes of operation may occur simultaneously in parallel—this is a very nice feature when troubleshooting operations.

Since CLEO is being used in this configuration for parallel mobile networking and static networking use, either SSSDR0 or SSSDR1 is not usable for data transmission (whichever SSSDR is in pass-through mode). Figure 13 shows SSSDR1 being dedicated to pass-through mode and therefore unusable.

CLEO has each of its serial ports configured as “roaming.” This is done to allow any serial port to be used for the space-ground link (i.e., either SSSDR0 or SSSDR1 can be placed in pass-through mode) without requiring router reconfiguration. This is possible because roaming ports still operate normally, with the exception that a roaming port will respond to mobile IP advertisements as well as send mobile IP solicitation requests (if so configured).

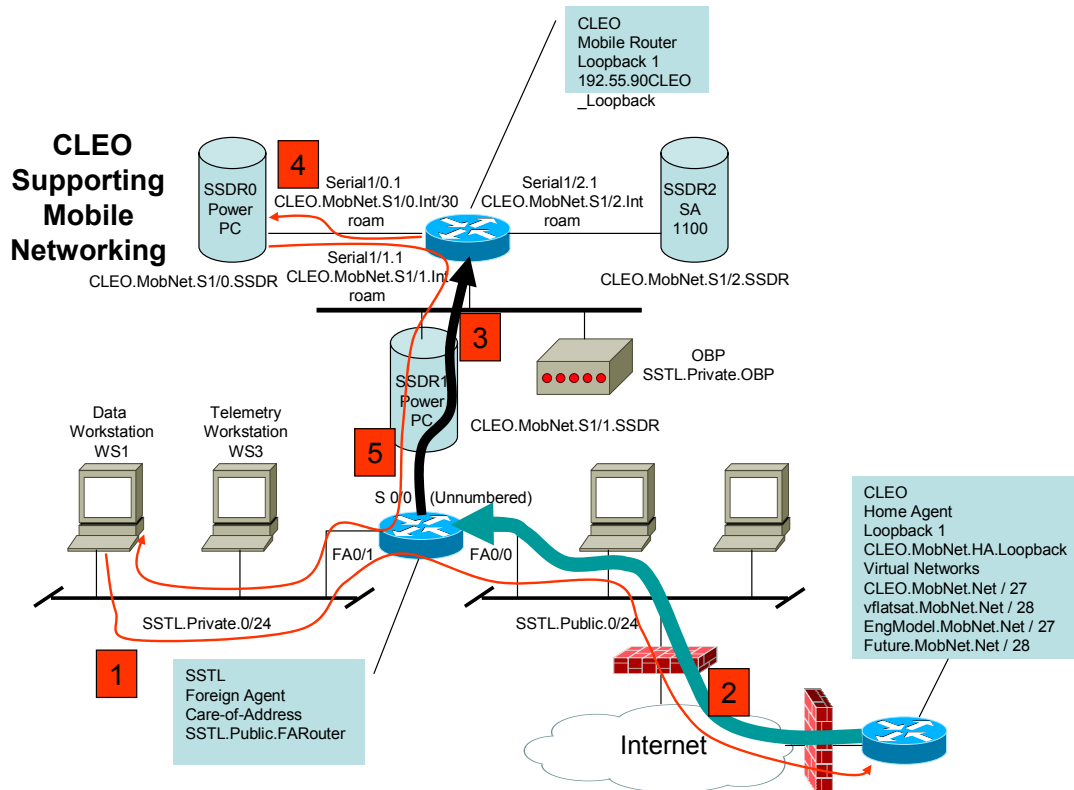


Figure 13.—SSTL satellite and ground network for mobile networking with data flow example.

The advantage that mobile IP provides is that one can share network infrastructure and use any available ground station offering foreign agent service. Thus, the home agent can be anywhere on the reachable Internet and at any ground site, as was the case with the VMOC demonstrations. Similarly, the corresponding node that is communicating via the home agent can be located anywhere on the Internet (fig. 14).

CLEO (or the mobile router) is not configured for reverse tunneling (ref. 16); rather it uses normal mobile routing for Internet Protocol 4 (IPv4), which results in triangular routing. This was initially done simply because some changes in the mobile-IP specification (ref. 17) regarding reverse tunneling and mobile-IP signaling occurred at approximately the time of launch, and it was initially unknown whether those changes were supported in the CLEO's onboard firmware. It turns out they were. Regardless, once we implemented triangular routing we realized that this is the appropriate mode of operation for a space environment. Reverse tunneling forces all mobile communication back through the home agent. Therefore, a reverse-tunneled architecture would require Internet connectivity between the ground station and the home agent to have at least as much bandwidth as the space-to-ground link: 8 Mbps for the UK-DMC and 40 Mbps for the China-DMC. Triangular routing enables the downlink to be fully used for local communication and downloads because the downlink data is not forced back to the home agent.

Figure 13 shows the data flow of a communication session between SSSDR0 and a local workstation using mobile IP:

- (1) The requesting host (corresponding node) initiates a request to SSSDR0. The request is set to the home agent because SSSDR0's address resides on a mobile network being advertised by the home agent located somewhere on the Internet.

- (2) The home agent double-encapsulates the message from the corresponding node and relays the double-encapsulated message to the foreign agent's care-of-address.

- (3) The foreign agent removes one level of encapsulation and forwards the single-encapsulated message to the MR.

- (4) The CLEO removes the encapsulation and performs normal routing, forwarding the message to SSSDR0.

- (5) SSSDR0 sends its reply to the source address of the corresponding node via the MR, the CLEO. Once the foreign agent receives this message from the CLEO, it forwards the message using normal routing.

Note: The corresponding node does not have to reside at the ground station. However, if the corresponding node does not reside at the ground station, then either the path of Internet connectivity between the ground station and the corresponding node must have at least as much capacity as the space-to-ground link, with guaranteed reliability, or some special application must be written that allows an intermediary to temporarily store data at the ground station and retransmit to the corresponding node at a lower rate (ref. 18). Such an application must be written in such a manner as to work with intelligent firewalls in place.

7.0 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. 14). 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

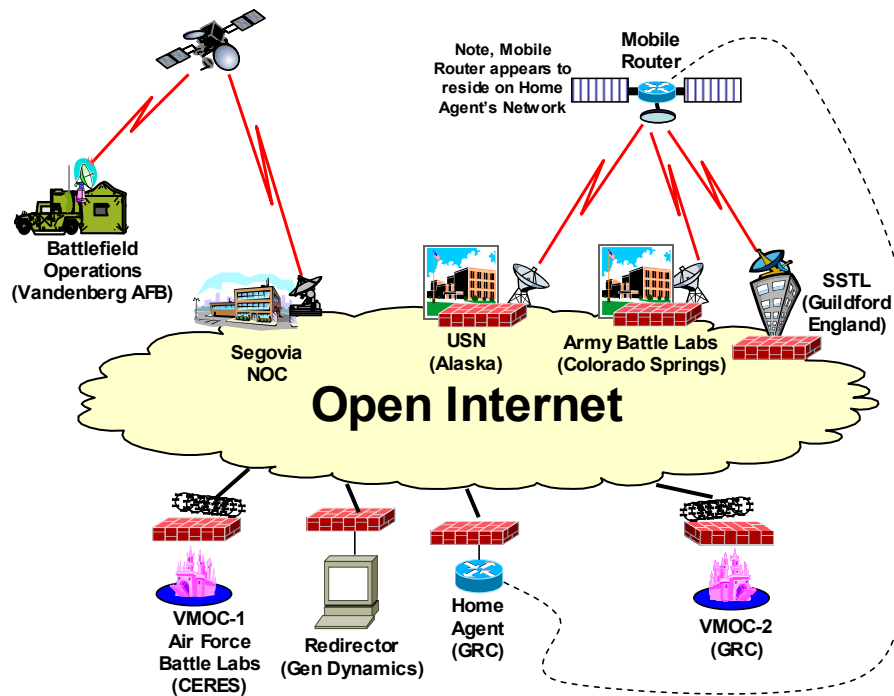


Figure 14.—Secure space-based network-centric operations network.

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 appendix F.

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

- Home agent router: NASA Glenn Research Center in Cleveland, OH
- Primary VMOC: Air Force Space Battlelab Center for Research Support (CERES) in Colorado Springs, CO
- Secondary VMOC: NASA Glenn Research Center in Cleveland, OH
- Redirector: General Dynamics in Los Angeles, CA
- SSTL ground station: Guildford, England
- USN ground station: North Pole, AK
- Army Battle Labs ground station: Colorado Springs, CO (low-rate telemetry, receive only)
- Remote battlefield operations: Vandenberg Air Force Base, CA, connected through the Segovia, Inc. (Hemdon, VA), IP satellite-based network⁶
- 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.

Network security was performed using a number of techniques and technologies to fulfill the overall needs and requirements of the various users (fig. 15). Virtual private networks (VPNs) using IP security (IPsec) tunnels were implemented between the General Dynamics' redirector and the two VMOCs. IPsec

⁶ Segovia's network operations center is in Ashburn, VA with teleports in Laurel, MD; Napa, CA; and Amsterdam, Netherlands. http://www.segoviaip.com/global_network/index.htm.

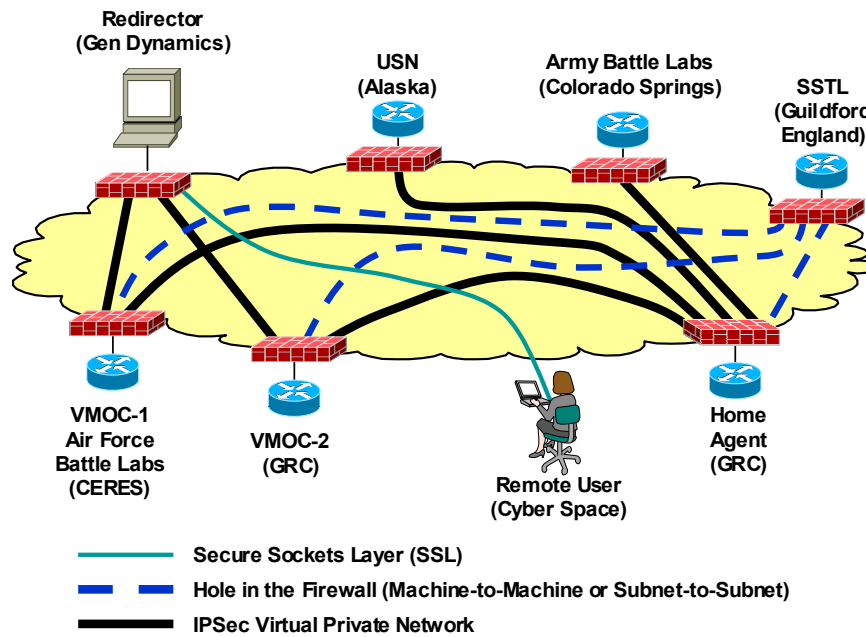


Figure 15.—CLEO-VMOC network security implementation.

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.

7.1 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.

7.2 Ground Stations

Five ground station networks were implemented consisting of three physical ground stations, the flat satellite (flatsat⁷) 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. Figure 16 shows the detailed design of the CLEO ground station network. The system labeled “VMOC LA testbed” is the redirector system that also has a test General Dynamics VMOC co-located there. The test VMOC is used to test and validate new features or enhancements to the General Dynamics VMOC prior to transporting those features to the operational VMOCs at CERES and NASA GRC. Although not shown in this diagram, all General Dynamics VMOCs are protected with VPN gateway firewalls, as is the home agent router.

7.2.1 SSTL ground network.—SSTL’s ground network has been described in detail in section 6.0, “CLEO–SSTL Network Architecture.”

7.2.2 Engineering model flatsat network.—The second ground station network that was implemented was the engineering model network. This ground network and associated CLEO engineering model hardware were used to test all ground and CLEO configurations prior to implementation in the actual operational network. The basic difference between the engineering model ground network and the actual SSTL ground network is that instead of having holes in the firewall to communicate between the home agent and the ground station foreign agent router, IPsec VPN tunnels were implemented at the firewall.

The engineering model flatsat network’s detailed design is shown in figure 17. Note that this network is nearly identical to that of SSTL’s ground and space network. In fact, during initial testing, all addressing was identical to the point where either the flatsat or the SSTL network had to physically be disconnected from the network in order to ensure that both the engineering model and CLEO did not try to register with the home agent router. Physically removing cabling is not a desirable practice. Thus, as soon as the CLEO was configured for mobile networking, the engineering model’s network addressing was changed to allow the engineering model network, SSTL’s ground network, and CLEO to all be connected simultaneously.

Just as in the SSTL ground network, there is an uplink serial connection and a private network that uses the **SSTL.Private.0/24** address block. Thus all machines in this private address space must be mapped to the outside network. In this case, that address space is still private address space in the **EngModel.FA_Inside_Network/24** network. This is reachable by the home agent network via static routes set up in the home agent’s Intel VPN Gateway firewall.

Using an intelligent firewall and mobile-IP triangular routing (rather than reverse tunneling) required special configuration in the foreign agent and home agent routers to resolve the following problem. Requests originating outside the firewall to CLEO came into the firewall via an IPsec tunnel. However, when triangular routing was implemented, the responses would not have a corresponding configuration stored in the firewall because of IP-in-IP encapsulation coming into the firewall and no IP-in-IP encapsulation leaving the firewall. Therefore, the firewall would drop the mobile routing responses as it is designed to do, as the mobile routing responses do not appear to originate in the network the firewall knows, and spoofing is considered undesirable. In order to get around this, a policy-based route had to be set up in the foreign agent ground router that would encapsulate the response in a tunnel back to the home

⁷ Hardware emulation of relevant components of a satellite.

Subnet Masks	Bits	Mask	Hosts
	/24	255.255.255.0	254
	/25	255.255.255.128	126
	/26	255.255.255.192	62
	/27	255.255.255.224	30
	/28	255.255.255.240	14
	/29	255.255.255.248	6
	/30	255.255.255.252	2

CLEO Mobile-Router Topology - 07/14/04
Surrey_GSN_network_071404.skf

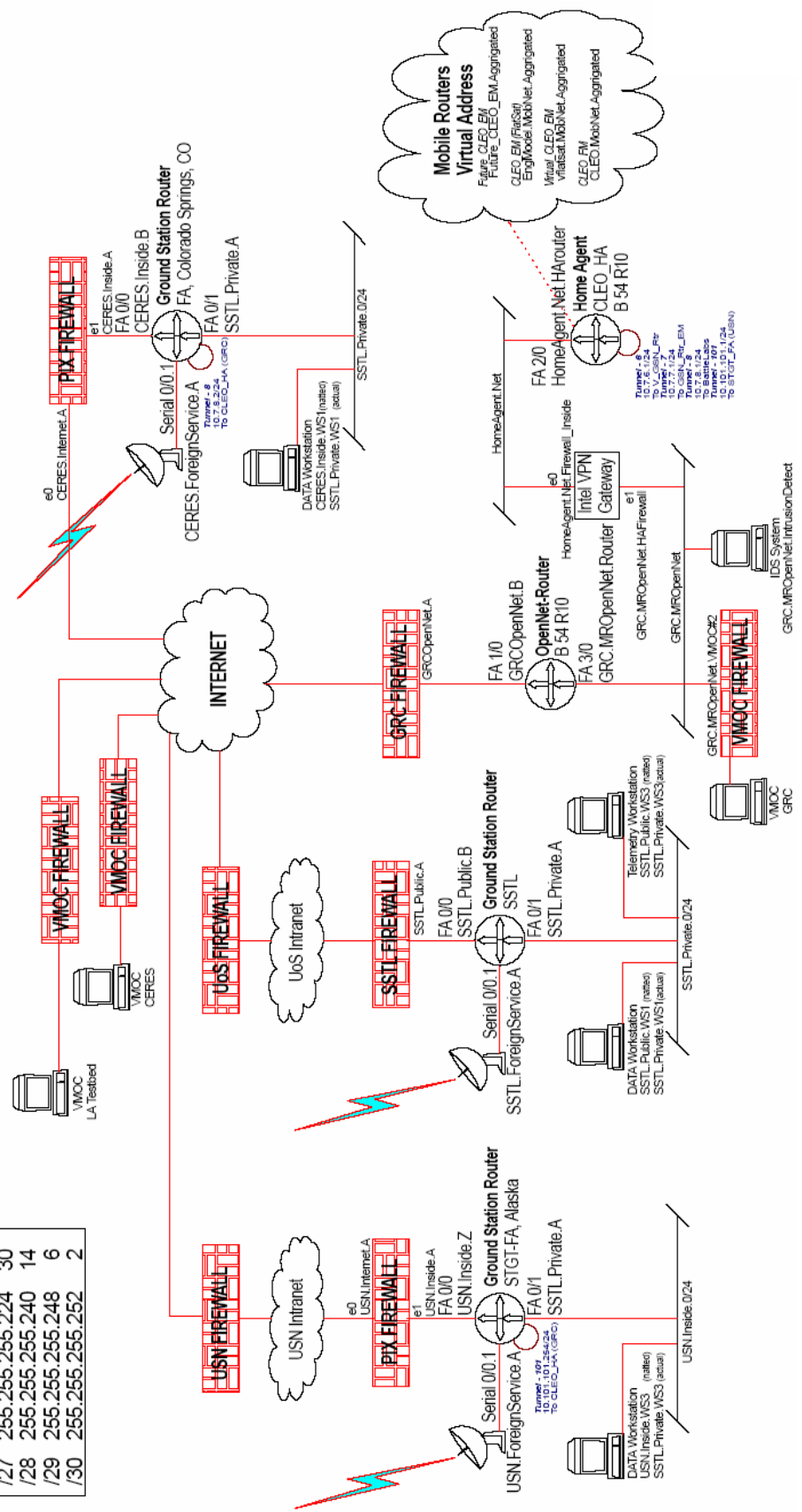


Figure 16.—CLEO–VMOC ground network detailed design.

CLEO Emulator Topology - 07/02/04 Surrey_Flatsat_link-Simulator_network_092204.skf

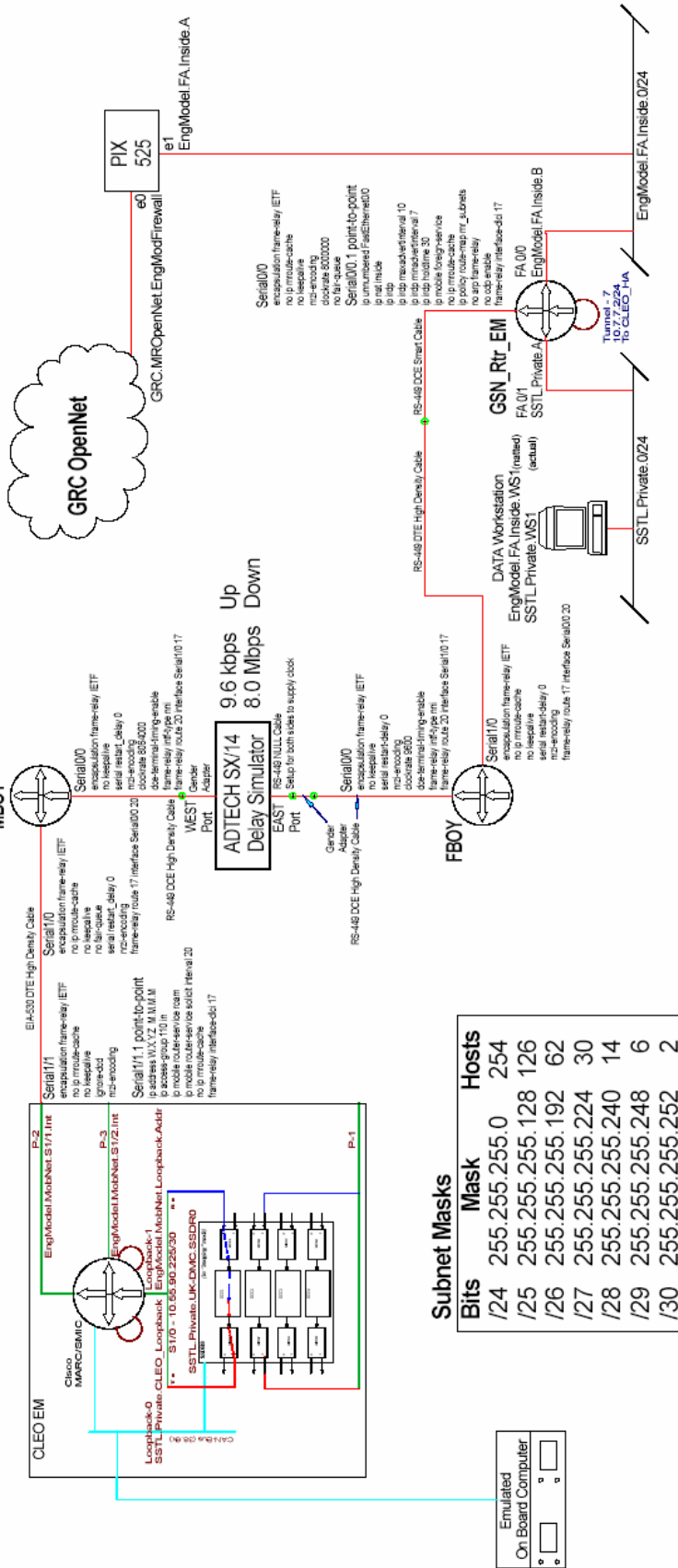


Figure 17.—CLEO engineering model flatsat network with link simulator.

agent. Thus, a pseudo-reverse tunnel was created. The router commands to perform this are highlighted in yellow and shown below. The tunnel interface command sets up a tunnel between the foreign agent and home agent routers. The home agent router has a corresponding tunnel. The policy-based routing is performed on packets coming to the ground router from the space link using a source address. The source addresses used will be the addresses from the actual CLEO mobile network (used when performing one-to-one mapping of configurations to the flight CLEO), **CLEO.MobNet.Aggregate/27** or a test mobile network, **EngModel.MobNet.Aggregate/27**. The access lists allow information from either of these two networks to be routed inside the IP-in-IP tunnel.

```
interface Tunnel7
ip address 10.7.7.2 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination HomeAgent.Net.HARouter
tunnel mode ipip
interface Serial0/0.1 point-to-point
ip unnumbered FastEthernet0/0
ip nat inside
ip irdp
ip irdp maxadvertinterval 10
ip irdp minadvertinterval 7
ip irdp holdtime 30
ip mobile foreign-service
no ip mroute-cache
ip policy route-map mr_subnets
no arp frame-relay
no cdp enable
frame-relay interface-dlci 17
access-list 7 permit CLEO.MobNet.Aggregate 0.0.0.31
access-list 7 permit EngModel.MobNet.Aggregate 0.0.0.31
route-map mr_subnets permit 10
match ip address 7
set ip default next-hop 10.7.7.1
```

7.2.3 Virtual flatsat network.—During the integration and testing of the secure space-based network-centric operations demonstration there was extremely high demand for use of the engineering model flatsat. Cisco Systems and NASA required access to the system in order to test configurations prior to uploading configurations into the CLEO onboard the UK–DMC satellite. General Dynamics required access to test their VMOC command and control. In order to accommodate General Dynamics’ needs and provide a satellite network that could always be accessed, the virtual flatsat network was developed. The virtual flatsat is identical to the engineering model network in operation and includes a ground router, MR, and firewall (fig. 18). Generally, only the virtual flatsat’s MR loopback address is accessed. No other MR interfaces are connected except for serial 1, which is the roaming interface with an address of **vflatsat.ForeignService.A/30**. This virtual flatsat MR is the router that is accessed from General Dynamics’ VMOC Web interface under “virtual flatsat” (see fig. 28 in appendix E).

Due to space limitations, this virtual flatsat network is not shown in the ground network design in figure 16, the Ground Network Detailed Design. The Cisco PIX 501 firewall is attached to the open network router of figure 16 on the **GRC.MROpenNet/29** subnet. This network is identical in operation and configuration to the engineering model network, with the exception that the LAN network addressing

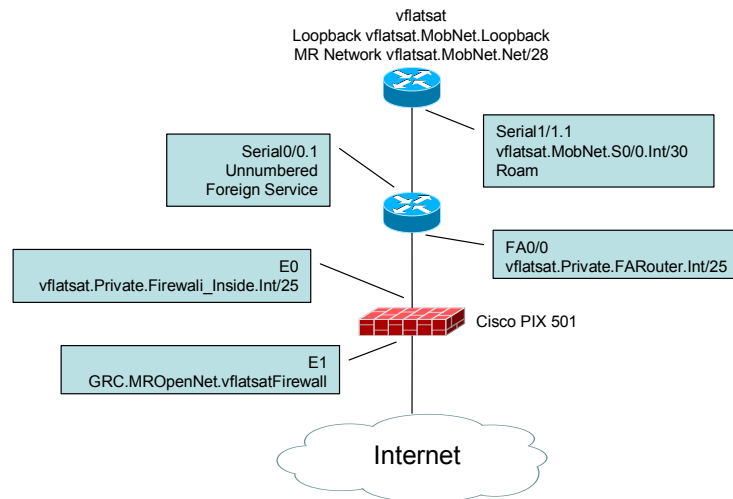


Figure 18.—Virtual flatsat network.

between the foreign agent router and firewall is different. Also, no workstations are connected to the foreign agent router. The pseudo-reverse tunneling configuration is used to enable communication from the MR to the home agent through the firewall.

7.2.4 USN ground station network.—The USN ground station network design is shown in figure 16. It is identical in operation and configuration to SSTL’s ground station network with the following exceptions:

- (1) Connection to the home agent is through the firewall using an IPsec VPN.
- (2) Private address space is used throughout the network.
- (3) The pseudo reverse tunneling configuration is used to enable communication from the MR to the home agent through the firewall.

The workstation located on the **SSTL.Private.0/24** subnet is currently used to run the telemetry redirection application and to locally ping the CLEO to test bidirectional connectivity. This workstation could be used to operate the CFDP or Saratoga file transfer application to receive images from the 8.1-Mbps downlink, thus enabling image retrieval during UK–DMC passes over USN’s Alaska ground station.

The USN ground station has full bidirectional capability, with 9600-bps uplink and 38.4-kbps low-rate and 8.1-Mbps high-rate downlinks. Note, simple real-time telemetry passes are executed using the low-rate downlink transmitter in order to conserve onboard power. Router access from the ground station requires use of the high-rate transmitter onboard the satellite.

7.2.5 Army Battle Labs ground station network.—The Army Battle Labs ground station network design is also shown in figure 16. It is identical to the USN configuration, except that this site is a receive-only site. A workstation was placed on the **SSTL.Private.0/24** subnet for telemetry retransmission.

The Army Battle Labs also implemented a VMOC at this site for comparative analysis with the General Dynamics’ Nautilus Horizon product. The VMOC developed under the comparative analysis task consisted of three main elements. The first was the transportable antenna used for the RF connection to the satellite used in the experiment. This was based upon a commercial antenna system, developed and sold by Integral Systems. The second element was the integrated suite of hardware and software used for satellite state of health operations and payload data analysis. This suite is called the Satellite Mission Suite and was based on COTS and nondevelopmental items (NDI) products from Integral Systems and Integrity Applications Incorporated (Chantilly, VA). The third element was the remote user

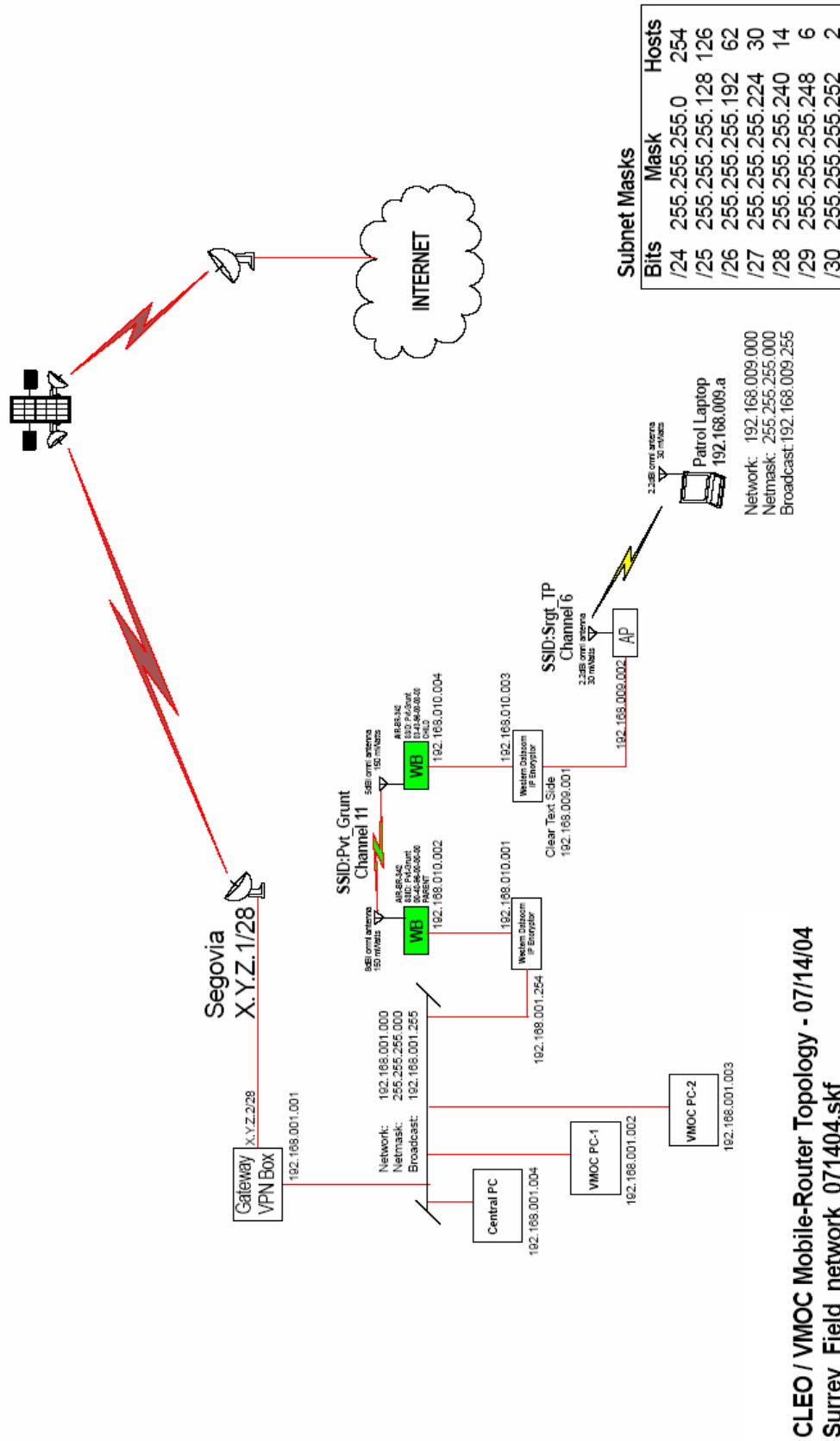


Figure 19.—Vandenberg remote command center field deployment.

element, which is connected to the Internet for accessing system data or performing system operations.

7.2.6 Remote user network.—Figure 19 depicts the network design to support a remote command center and an additional remote user connected via a secure wireless link using a Western DataCom IPE–2M Internet Protocol encryptor, which closely corresponds to a High Assurance IP Encryptor (HAIPE).⁸

Remote connectivity was provided by an Army Space Support Element Toolset (SSET), designed to provide Army and Joint Space Warfighters with a rapid and easily deployable global capability to support Army and Joint operations. The system provides global “reach back” broadband communications that support forward-deployed space soldiers who provide space services (e.g., analysis, estimate, intelligence preparation of the battlefield (IPB), etc.) and products (such as commercial imagery) to supported tactical commanders. The architecture provides connectivity between the U.S. Army Space Command (USARSPACE) Space and Missile Command Operation Center and remote sites with a triply redundant space-based communications suite using Inmarsat, Iridium, and Ku-band satellite services. For the demonstration, only the Ku-band Internet Protocol satellite (IPSAT) services were used. The IPSAT system is the backbone of the broadband communications. The IPSAT capability is provided by the iDirect NetModem II (USA iDirect Technologies, Herndon, VA) and Segovia service providers. The IPSAT operates in the Ku commercial frequency band and provides up to a 2-Mbps downlink to the remote Earth terminal and up to 256-kbps uplink capability back to the hub. These throughput rates can be increased up to 9 Mbps, depending upon geographical location, antenna size, and additional funding to pay for the increased bandwidth.

For this demonstration, the Type-1 encryption units were not used. Rather, the SSET was simply providing access to the open Internet. Security between the open Internet and the remote users was accomplished using a firewall. All communication between the VMOC and the remote command center was performed using VPN tunnels between the remote workstations and the VMOC. Use of SSL has since replaced the VPN tunnels.

The wireless link between the remote mobile user in a high-mobility multipurpose wheeled vehicle, identified as the patrol laptop, and the remote command center was performed using 802.11-b wireless links secured with a pair of Western DataCom IPE–2M High Assurance IP Encryptors.

Intrusion detection was performed at the remote command center.

8.0 USN Ground Station Network

Universal Space Network, Inc. (USN), is an innovative company that has built a ground network of tracking stations to provide cost-effective space operations and telemetry, tracking, and control (TT&C) services to support space assets. USN’s shared infrastructure approach reduces the capital costs of a satellite program and minimizes program risk through access to a larger network. USN provides:

- Global TT&C
- Spacecraft management services
- Ground network design, implementation, and operations
- Satellite services, engineering support

USN provides TT&C and data downlink services for satellites, launch systems, and launch and also provides early orbit-phase operations for spacecraft. USN provides payload data reception and level-zero processing of data in S-, X-, Ku-, and L-band. USN’s current services include a variety of antenna sizes from 3 to 13 m. Data rates up to 160 Mbps are currently supported with future support of up to 600 Mbps.

⁸ The IPE–2M PC/40 Plus High Assurance IP Encryptor is built to meet current High Assurance Internet Protocol Interoperability Specification (HAIPIS) draft standard and has been cleared for limited use in theater.

8.1 Network

USN and the Swedish Space Corporation joined forces to create a worldwide network of satellite ground stations. These ground stations have been combined with those of other collaborative partners to provide a seamless network of tracking stations. All ground sites are networked together, providing customers access to their space assets through a variety of communication means (frame relay, VPN, and integrated services digital network (ISDN)) including standard telecommunications services using TCP/IP. USN's services provide increased reliability and additional spacecraft contact times because of the global network of ground stations and command centers, built-in redundancies, and backup. Remote ground stations are located in

North Pole, AK
South Point, HI
Kiruna, Sweden
Sturup, Sweden
Applied Physics Laboratory of Johns Hopkins University (Laurel, MD)
Western Australia
Pretoria, South Africa
Santiago, Chile
Fucino, Italy
Overberg, South Africa
Perth, Australia
Luxembourg

The USN ground network is a commercially developed, owned, and operated multiuser satellite commercial ground network, with ground station access points to satellites that are interconnected and commanded across a wide area network (WAN). The implementation permits numerous satellite users to share a TT&C network to provide reliable, cost-effective communications. This network enables users to directly communicate from their facilities through the network to their space-based assets.

USN maintains strategically located remote ground stations around the Earth and a permanent communications headquarters operating 24 hours each day of the week. Network customers "rent" communication time and full technical support services from USN. By providing time-shared telecommunications services to both commercial and government customers, USN offers satellite TT&C services to users at a fraction of the cost of purchasing and operating a dedicated ground station.

8.2 Operations

8.2.1 Resource management.—The USN Network Management Center (NMC) is a robust, fault tolerant, distributed facility with mirrored locations in Newport Beach, CA; Horsham, PA; and Kiruna, Sweden. The NMC is actually a VMOC-like center customized for operating a vast network of ground station resources. Scheduling and operation of the network is provided through the NMC. The NMC provides a single point of interface to the USN global network of ground stations. The NMC serves as the primary interface for customer satellite communications and features:

- High-capacity communications for rapid data transfer to customers
- Firewalls for secure telecommanding
- A simplified user interface for customer access
- Other direct connections, based on individual customer mission requirements
- Customer service and support available 24 hours per day, 7 days per week

The NMC functions as a communication clearinghouse (and technical support service) in order to schedule individual user communications. Customers can access the NMC using standard communication technology and security features. For example, users may, from their own desktop computers, access USN's worldwide network of satellite tracking stations for spacecraft communications, spacecraft contact status, collected data quality statistics, and general user account information over the Internet or through a secure, dedicated communication link.

The NMC provides USN customers with scheduling, archival, and operations planning in an automated fashion; users can view pass operations, obtain data, and send commands in real time or not over the USN system.

8.2.2 Scheduling.—All activities utilizing the USN operational network must be scheduled through the USN scheduling process. USN Operations maintains overall responsibility for generation, maintenance, and publication of USN schedules. In addition, Operations is responsible for disseminating USN schedules to users of the network. USN uses a system of first-come-first-served scheduling. USN also employs a system of prioritization based upon mission phase or spacecraft status. Prioritization is based on operational support classifications defined below:

- (1) Launch and early orbit phase: includes launch, initial acquisition, and any maneuvers required for the spacecraft to reach its operational orbit
- (2) Spacecraft emergency: defined as any condition endangering the life or safety of the spacecraft requiring immediate and unrestricted access to USN resources
- (3) Critical mission support: includes spacecraft maneuvers, critical science data recovery, investigation of an anomalous spacecraft condition, and critical command uploads
- (4) Nominal support: considered routine, on-orbit, TT&C activity

Each user of the USN operational network can perform support planning and review network loading up to 6 weeks in advance. It is each user's responsibility to review USN's Contact Schedule and provide conflict-free scheduling requests. Support setup and breakdown times must be considered as a part of the duration of any support request. Average setup times are 25 min., and average breakdown times are 5 min.

Schedule requests are submitted via e-mail to a specific USN email address. The requests are submitted as a comma-delimited text-formatted e-mail or a comma-delimited text attachment in the ASCII format as described in the example below:

```
TIMED,USAK01,Add,04/25/03,115,15:17:12,04/25/03,115,15:27:58,00:10:46,Primary – 4.59 MB,  
Field 1 - Project  
Field 2 - Remote Ground Station  
Field 3 - Action -- *Add or Delete (Upon acceptance this field will reflect "Scheduled")  
Field 4 - Start Date (mm/dd/yy)  
Field 5 - Start DOY (ddd)  
Field 6 - Start Time (hh:mm:ss)  
Field 7 - Stop Date (mm/dd/yy)  
Field 8 - Stop DOY (ddd)  
Field 9 - Stop Time (hh:mm:ss)  
Field 10 - Support Duration (hh:mm:ss)  
Field 11 - Comments or Configurations
```

Note: Modifications to existing scheduled items are accomplished by "Delete" followed by "Add" requests.

All scheduling requests are reviewed and processed upon receipt. USN will ensure supports being requested do not conflict with existing scheduled supports and allow sufficient pre-pass and post-pass

time. The pre- and postpass times are not explicitly shown in the USN Contact Schedule, but are reflected in the spacing of one support from another. All requests fitting into the schedule are entered into the USN Contact Schedule. Requests that could not be entered into the schedule are replied to with a brief explanation.

Once a request is received, processed, and accepted into the USN Contact Schedule, a confirmation message is sent to all project schedulers. This serves as notification that the request has been received. Schedule requests not added to the Contact Schedule are identified in the text portion of the e-mail and the reason noted.

All e-mails contain specific verbiage with regards to the subject heading and text portion. The verbiage will be used “as is” with little or no deviation. This is required in order to maintain standardization of all schedule-related e-mail traffic coming out of the USN Operations Department. This standardization could be used for machine-to-machine autonomous operations.

9.0 General Dynamics Nautilus Horizon

The General Dynamics Nautilus Horizon product provided a framework for the mission partners to define, test, and field an IP-based command and control system capable of supporting secure distributed mission operations of any IP-based platform or sensor. This VMOC provided a path for the rapid development and demonstration of new technologies within the relevant environment.

The VMOC tied remote space operators directly to an orbiting spacecraft via the open Internet through a Web environment. The VMOC was implemented as a geographically distributed, dual, hot-standby operations center. The primary VMOC was located in CERES on Schriever Air Force Base, CO, with the backup VMOC located at NASA GRC in Cleveland, OH. With the satellite ground stations tied to the Internet, the VMOCs are the control elements that orchestrate the tie between the user and the spacecraft. This VMOC will continue spiral development to enhance system interoperability and responsiveness, enhance situational awareness, facilitate “system of systems” solutions, and support automated machine-to-machine interactions.

This master VMOC used Internet Protocols to acquire satellite data, dynamically task satellite payload, and perform TT&C of on-orbit satellite assets. The VMOC performs a number of functions:

- (1) Enables system operators and data users to be remote from ground stations
- (2) Verifies individual users and their authorizations
- (3) Establishes a secure user session with the platform
- (4) Performs user and command prioritization and contention control
- (5) Applies mission rules and performs command appropriateness tests
- (6) Relays data directly to the remote user without human intervention
- (7) Provides a knowledge database and is designed to allow interaction with other, similar systems
- (8) Provides an encrypted gateway for “unsophisticated” user access (remote users of science data)

9.1 Security Manager

The security management concept is illustrated in figure 20. Access to the VMOC was controlled and monitored for intrusion with a “defense-in-depth” strategy. Autonomous network intrusion detection and countermeasures were conducted using the Automated Security Incident Measurement (ASIM) intrusion detection system and the Common Intrusion Detection Director (CIDD). Both ASIM and CIDD were developed by General Dynamics for the Air Force Information Warfare Center, and they are used routinely by most Department of Defense (DOD) bases to mitigate the network risks associated with hackers (external to the monitored connections) and saboteurs (internal to the monitored connections).

For the June 2004 demonstration, the remote user was authenticated via user name and password. Additional VMOC authentication is planned using technologies such as biometrics and smartcards. Each

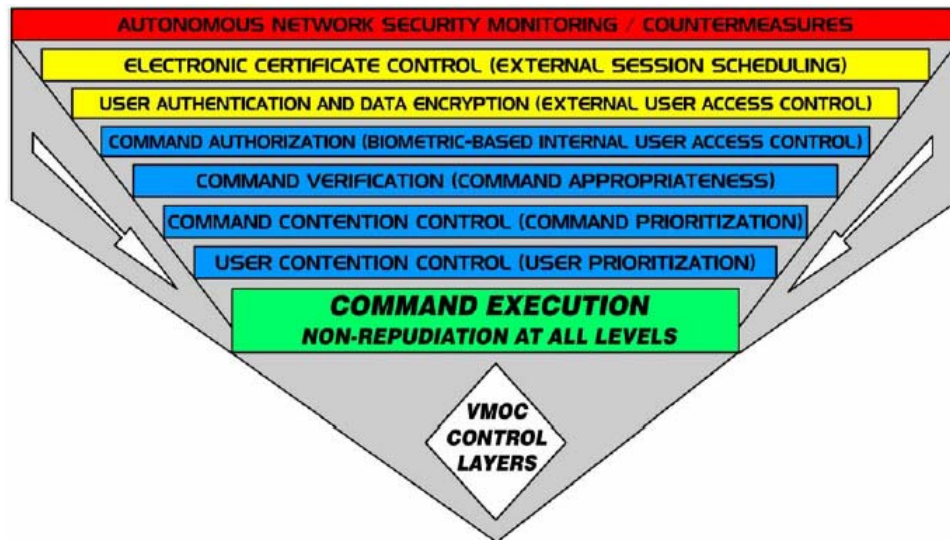


Figure 20.—VMOC security management concept.

user was assigned a priority and ordered by priority in the VMOC’s database. Priorities were demonstrated for command and control. A high-priority user’s request preempts a lower priority user request. In addition, the database included information to determine what authorizations specific users had. For example, one user may be able to request a stored image whereas another may actually be authorized to command the system to take an image.

9.2 Redundancy and Survivability

The VMOC is designed for survivability by utilizing multiple mirrored, geographically separated VMOCs. The demonstration used two VMOCs, with the primary VMOC located at CERES in Colorado Springs, and the secondary VMOC located at NASA GRC in Cleveland, OH. Both VMOCs held mirror images of all hardware and databases. When the primary VMOC was deliberately made to fail, a switch to the secondary at GRC was nearly instantaneous. Furthermore, when the CERES VMOC came back online, the switch back was also indiscernible by the user. Currently, this switch was performed by the redirector, which is a single point of failure. Other techniques are being investigated to perform this dual hot-standby function.

9.3 Systems Integrator

The General Dynamics master VMOC is actually an integrator of systems. That is, the master VMOC coordinates the external user requests with space and ground assets available from SSTL—here, the UK–DMC and images requested via SSTL’s mission planning system—and ground assets from USN. Thus, the master VMOC acts both as a resource coordinator and as an interface to various systems that are available.

9.4 Scheduler

The scheduler takes user requests, prioritizes these requests and then looks at the available resources to determine if and when a request can be granted. Data that is used by the scheduler includes available space-based assets, available ground system support, orbital dynamics, and user priority. For this particular demonstration, the General Dynamics VMOC did not have to determine availability of onboard

assets. That was done by the SSTL mission planning system, as the UK–DMC is under SSTL control and the SSTL mission planning system understands the details of the UK–DMC power management and resource availability better than the external VMOC can. However, future implementations may require the master VMOC to also perform resource management and monitor such resources as available power and battery levels.

Scheduling is an iterative process. The VMOC receives a request, then determines what assets may be available to service that request. The VMOC then queries those assets as to their availability. If all assets are available, the VMOC schedules those assets and schedules the request. If the assets are not available, the VMOC will determine if there is another time the request can be scheduled. If so, the VMOC again queries all necessary assets for availability. This process is repeated until a time can be found when all required assets are available or until the VMOC determines that the request cannot be granted. As additional assets are added to the system, the complexity of the scheduling process grows.

9.5 Data Mining

The General Dynamics VMOC was implemented to perform data mining. When the VMOC receives a request for an image, the VMOC will first examine its database and other image databases to determine if an existing image will fulfill the user’s needs. If so, the stored image will be sent to the user. If an existing image is not available, a new image request will be made. Once the new image is received, it will be sent to the user and stored locally in an image database and will likely also be stored remotely.

10.0 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 (refs. 19 to 21). 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.

10.1 CCSDS Specification Summary⁹

The primary goal of CCSDS is to increase the level of interoperability among space agencies. The SLE Services recommendation furthers that goal by establishing the basis for a set of SLE services to be used in the area where most cross-support activity occurs: between the tracking stations or ground data handling systems of various agencies and the mission-specific components of a mission ground system.

The need for SLE Services arises from the desire of spacecraft operations organizations to standardize the interfaces for the transport and management of space data on the ground so that the technical, management, and operational costs of providing cross-support between the organizations can be greatly reduced.

SLE Services enable the ground segment assets of space agencies, ground station operators, and space data users to interoperate without the need for ad hoc and complicated gateways specifically designed for each new mission. By standardizing on the SLE Services, different organizations will be able to link discrete elements of their ground segments to suit a given mission’s needs without having to re-create the interfaces for each new mission. Since the SLE protocols run over existing communications infrastructure, they help integrate Space Data Systems into the global communications network.

⁹ Note, the following CCSDS SLE summary is excerpted from references 19 to 21.

The advantages of SLE services are

- (1) Space organizations will be able to provide cross support to one another more efficiently.
- (2) Ground station owners will be able to provide standard services to operators of CCSDS-compliant spacecraft.
- (3) Users of spacecraft data will be able to command their payloads and access their data through a familiar interface, using widely available underlying telecommunications technology such as the Internet or ISDN lines.
- (4) The standardization of ground station, control centers, and end-user interfaces will permit re-use of systems for successive missions and eliminate the costs and risks associated with mission-specific implementations.
- (5) A truly global market for standard TT&C COTS products will be created, driving down the cost of these systems.
- (6) SLE services are scalable so that only the actual services required by a service user or a service provider need to be implemented.

CCSDS Space Link Recommendations (Advanced Orbiting System, Packet Telemetry, and Telecommand) define formats and protocols for *the transfer of data from/to data sources/sinks on board a space vehicle to/from data sinks/sources on the ground*. These Space Link protocols are designed to work efficiently in the noisy, high-delay environment of space/ground radio links; thus they do not carry information needed to configure and operate the ground systems that link numerous ground stations with the ground sinks and sources of data.

The SLE Recommendations complement the CCSDS Space Link Recommendations with a range of services that are required to configure, operate, and supervise the ground data systems.

SLE services comprise

- (1) SLE transfer services: concerned with the ground part of the data transfer. This transfer is either within the ground data system or between the ground data system and the ground data sources/sinks.
- (2) SLE management services: control the scheduling and provision of SLE transfer services by ground systems.
- (3) Cross-support services: a generic term that encompasses all services that can be provided by one agency to support another agency in operating a spacecraft. On the ground, cross-support services are of three kinds:
 - (a) SLE Services: extend CCSDS Space Link services as defined in CCSDS Space Link Recommendations
 - (b) Ground communications services: provide ground communications support; for example, to relay operational data
 - (c) Ground domain services: cover all services which handle data related to spacecraft operations but not directly mappable to Space Link data structures defined in CCSDS Space Link Recommendations. Examples of ground domain services are tracking a spacecraft, exchanging spacecraft databases, and mission planning.

In presenting the SLE cross support concept, the following assumptions are made in the context of a single space mission:

- (1) Within this space mission a single spacecraft is considered.
- (2) This spacecraft's telecommand and telemetry is compliant with CCSDS Telecommand Recommendations and either Packet Telemetry or Advanced Orbiting Systems.
- (3) All end users (i.e., sources or sinks of space data on the ground) are affiliated to a single mission manager.

10.2 Shared Networks and Infrastructure

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.

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 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).

10.3 SSTL Constellation Mission Planning System (MPS)

The DMC Mission Planning concept (fig. 21) is based on the cooperation of distributed MPSs, one system being located at each ground control center. An MPS is solely responsible for the full planning and scheduling of the operations of a single satellite, and each satellite has a dedicated MPS. An MPS can nevertheless forward a request submitted by one of its users to another MPS of the DMC ground segment.

Each MPS has the following main objectives:

- (1) Plan one satellite payload instrument and ground segment operations according to the image requests of the users and operators
- (2) Plan the onboard recorders, downlink, slew, and acquisition activities required to enable the observations of one satellite
- (3) Plan the satellite maintenance activities
- (4) Preprocess and forward image requests to other MPSs of the DMC ground segment
- (5) Schedule the onboard operations for a single satellite and the ground segment operations for the whole DMC ground segment required to upload schedule and acquire data for this satellite
- (6) Provide status on the progress of the implementation of the image requests submitted by the users

The full DMC MPS distributed system is composed of a community of these MPSs, each of them configured and tailored for a specific satellite of the DMC. Since, the MPS is based on cooperative planning and draws on distributed system principles, each MPS has to act as an entry point to the DMC for submission and planning of imaging requests. The method for linking the DMC partners' MPS is using Simple Object Access Protocol (SOAP) messages via Web Services remote procedure calls (RPC). The following functions are available via the Web Services RPC:

- Requesting the status of an MPS site
- Submission of imaging requests (raw observation requests, ROR) by a remote user or MPS
- Submission of planned images (preprocessed observation requests, POR) by a remote user or MPS
- Descoping of planned images by a remote user or MPS
- Publishing of availability plan of local MPS to DMC partners
- Calculation of imaging opportunities for a remote MPS-routed ROR or POR request
- Status on the progress of a remotely submitted image request

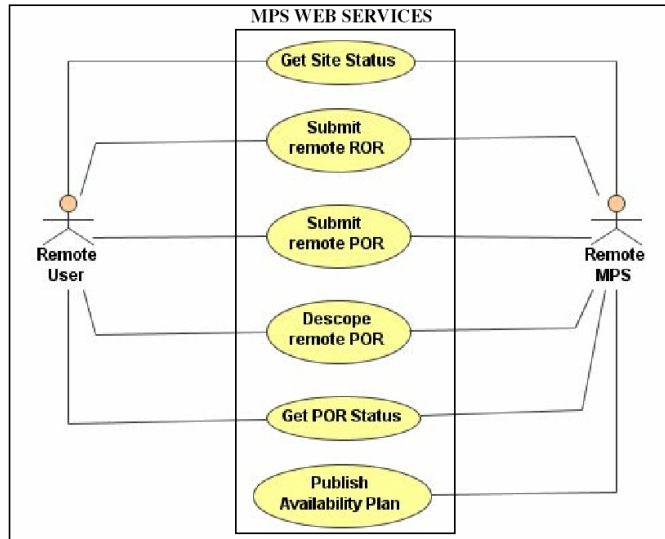


Figure 21.—SSSL Mission Planning System (MPS).

10.4 VMOC–SSSL Interfaces

The following is a brief overview of how the General Dynamics VMOC is using the SSSL mission planning service. The SSSL mission planning service interface provides the following system call functions:

getSiteStatus: The `getSiteStatus` function call returns a string indicating the status of the system.

submitRemoteROR: The `submitRemoteROR` function call creates an order on the SSSL MPS, which contains an array of possible times when an image of an area of interest, passed as an argument to the function, can be captured.

submitRemotePOR: The `submitRemotePOR` creates a request for an image to be taken at a particular time.

getOrderStatus: The `getOrderStatus` function call returns the status of requests created by the `submitRemotePOR` call associated with an order from the `submitRemoteROR` call. Orders can have multiple requests associated with them.

getOrderLineItemStatus: The `getOrderLineItemStatus` function call returns the status of a request made through the `submitRemotePOR` call. For example, the status might be “InPlan,” “Scheduled,” “Captured,” “Downloaded,” or “Descoped,” among others.

descscopeRemotePOR: The `descscopeRemotePOR` function call is used to cancel a request made with the `submitRemotePOR` call.

The VMOC uses these calls in the following sequence:

- (1) A user creates image requests through the VMOC Web interface.
- (2) A daemon process running on the VMOC checks for new requests every 5 min, and for each request calls `submitRemoteROR` to obtain a set of possible times for the imaging task.
- (3) If the previous step returns any valid times, the daemon creates a resource and task in STK/Scheduler (Analytical Graphics, Inc., Exton, PA), using the times obtained in step (2) as the possible times for the task. The priority of the task in STK/Scheduler is set according to the priority in the request.

(4) After processing all new requests, the daemon runs the STK/Scheduler schedule deconfliction routine and updates the status of the tasks in the VMOC database.

(5) Each morning (note: all time references here are to Pacific standard time, as used during the operational demonstration at Vandenberg Air Force Base), a scheduled task on the VMOC processes those tasks that are assigned in the next 24 hour scheduling period by STK Scheduler and submits the task(s) to the SSSL MPS using the submitRemotePOR call. For example, at 4 a.m. October 1, the process would try to submit requests to SSSL for any task assigned in between 9 a.m. October 2 and 9 a.m. October 3. (The gap between the time the process is run and the start time of the period for assigned tasks is because tasks for the time period are uploaded to the satellite the evening of the October 1. Tasks are submitted in the morning to allow time for handling errors and other unexpected events, as well as to hopefully obtain a better shot at getting on the schedule before resources on the satellite are allocated for other tasks.

(6) If the task submission is successful, the request id is recorded in the VMOC database, and the task is marked as “Exported” in the VMOC system.

(7) Another scheduled task periodically processes all exported tasks and performs the following routines:

- (a) Checks the status of the SSSL request using the getOrderLineItemStatus call
- (b) Looks for the image on the SSSL File Transfer Protocol (FTP) server if the status of the request is “Downloaded”
- (c) Is downloaded and the GeoTIFF-formatted image is processed if the image is present. Geo information is extracted and stored as metadata for the task, and the TIFF image is converted to JPEG format for use on the VMOC Web site.

For the OSD-sponsored June 2004 Vandenberg demonstrations (refs. 22 to 24), a very conservative approach was taken implementing this interface. The functionality of the VMOC, as existed for and tested in the June demonstration, was based on interfacing to a single SSSL mission planning system commanding the UK–DMC satellite, and not the fully distributed SSSL MPS, which was deployed after the demonstration was completed. The VMOC was later updated to work with the distributed MPS, with the VMOC handing off more opportunity calculation to the MPS rather than second-guessing the MPS with an approximate model of the UK–DMC schedule that neglected a number of platform power and availability constraints from other UK–DMC users. Images for the VMOC are currently arbitrarily limited to one image per day because that is what SSSL provided for the June demonstration. For testing purposes, one image per day is sufficient.

The process for getting the image to the FTP server for the VMOC to retrieve is currently a manual one. SSSL personnel copy each VMOC image retrieved to the SSSL FTP server. This process can be easily automated in the future.

There are several ongoing improvements to the way the VMOC interoperates with the SSSL MPS. The submitRemoteROR is currently called once for each VMOC request. However, there is no guarantee the times returned by this call will still be valid or available if and when a submitRemotePOR is made to create the request in the SSSL system. Ideally, submitRemoteROR would be called periodically to update the times and the corresponding task in STK/Scheduler to match the SSSL MPS schedule. However, it is unclear as to how this would impact the SSSL system. If there are many users creating requests, there could be a significant amount of calls being made to the SSSL MPS service. This capability will likely be added by the second quarter of 2005. In addition, the SSSL MPS service provides a call to “descope” or cancel a request once it is made. Thus, a request could be cancelled and another image request executed every time the schedule for the VMOC tasks in STK/Scheduler are recomputed. Prior to implementing this algorithm, SSSL will be consulted to ensure this does not cause problems for SSSL by abusing or overtaxing the MPS interface. Also, there is no guarantee that another image can be successfully requested from SSSL once a task has been descope.

10.5 VMOC–USN Interfaces

Currently there is no automated interface between the USN ground network and the VMOC for requesting access to the ground system. Scheduling of the USN ground station is currently performed manually using e-mail. However this process could be readily automated as previously noted in the USN Ground Network “Scheduling” section, 8.2.2.

10.6 SSTL–USN Interfaces

Currently there is no automated interface between the USN ground network and SSTL for requesting access to the USN ground system. However, it is certainly feasible for SSTL to use USN infrastructure for additional command and control as well as image retrieval. The additional equipment required at each USN site is a router, uplink modem and downlink modem; network infrastructure is already present. Total equipment cost would be approximately \$10,000.

11.0 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.

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 onboard computer 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 SSSDR 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 SSSDR 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 SSSDR through the router was tested successfully.

Secure shell (ssh) was added, as was HyperText Transfer Protocol (HTTP) command access and multilayer 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 IOS command line functionality
- Earth image file transfer from an SSDR to ground through CLEO using static routing

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) Network Time Protocol (NTP). This test is for completeness. However, the CLEO 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.
- (4) Distributed file transfer across multiple ground stations. This would require new file transfer application in both SSDR and in terrestrial systems (ref. 18).
- (5) 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.

11.1 First Remote Access and Commanding of the CLEO

The following screen captures show early remote across-the-Internet access and commanding to the CLEO, a COTS router, a Cisco 3250 Mobile Access Router, from a remote site. This event took place at 10:29 UTC on May 21, 2004. The UK-DMC satellite built by SSTL was in contact with the Guildford, England, ground station at the time of these measurements. The remote commanding occurred from NASA GRC in Cleveland, OH, via the SSTL ground station in Guildford, England. Access was accomplished by both telnetting and Web browsing into the CLEO.

The screen capture in figure 22 shows the round-trip time pings from NASA GRC to the onboard router via SSTL's ground station. Note, the first pings were lost as the satellite was not yet visible to the ground station, and the uplink had not yet been established.

The screen capture in figure 23 shows the tail end of a "show running configuration" command and the round-trip time pings from the space-based asset, CLEO, to a workstation at SSTL's ground station.

Note: Access at this time was via a telnet session from NASA GRC to CLEO, and the ping commands were sent from CLEO to the ground.

```
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\ivancic>ping Bad Address

Pinging Bad Address with 32 bytes of data:

Request timed out.
Request timed out.

Ping statistics for Bad Address :
    Packets: Sent = 2, received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Documents and Settings\ivancic>ping SSTL.Public_Inside.WS1

Pinging SSTL.Public_Inside.WS1 [32 bytes of data]:

Reply from SSTL.Public_Inside.WS1 :=32 time=194ms TTL=103
Reply from SSTL.Public_Inside.WS1 :=32 time=187ms TTL=103
Reply from SSTL.Public_Inside.WS1 :=32 time=188ms TTL=103

Ping statistics for SSTL.Public_Inside.WS1 :
    Packets: Sent = 3, received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 187ms, Maximum = 194ms, Average = 189ms
Control-C
^C
C:\Documents and Settings\ivancic>ping SSTL.Public_Inside.WS1

Pinging SSTL.Public_Inside.WS1 [32 bytes of data]:

Reply from SSTL.Public_Inside.WS1 :=32 time=221ms TTL=103
Reply from SSTL.Public_Inside.WS1 :=32 time=186ms TTL=103
Reply from SSTL.Public_Inside.WS1 :=32 time=186ms TTL=103
Reply from SSTL.Public_Inside.WS1 :=32 time=186ms TTL=103

Ping statistics for SSTL.Public_Inside.WS1 :
    Packets: Sent = 4, received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 186ms, Maximum = 221ms, Average = 194ms

C:\Documents and Settings\ivancic>
```

Figure 22.—Pings from NASA Glenn to CLEO via Guildford.

```

C:\ Command Prompt
ip route SSSL.Private.AISat.SSDR0 255.255.255 Serial1/0.1
ip route SSSL.Private.AISat.SSDR1 255.255.255 Serial1/1.1
ip route SSSL.Private.AISat.SSDR1 255.255.255 Serial1/2.1
ip route SSSL.Private.UK-DMC.SSDR0 255.255.255 Serial1/0.1
ip route SSSL.Private.UK-DMC.SSDR1 255.255.255 Serial1/1.1
?
?
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
?
radius-server retransmit 3
radius-server authorization permit missing Service-Type
?
line con 0
  exec-timeout 0 0
  stopbits 1
line aux 0
line vty 0 4
  password cisco
?
end
CLEO-MR# ping Bad Address

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to Bad Address , timeout is 2 seconds:
*****
Success rate is 0 percent (0/5)
CLEO-MR#ping SSSL.Private.WS1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to SSSL.Private.WS1 , timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 128/144/168 ms
CLEO-MR#ping SSSL.Private.WS1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to SSSL.Private.WS1 , timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/126/172 ms
CLEO-MR#exit

Connection to host lost.

C:\Documents and Settings\ivancic>

```

Figure 23.—Pings from CLEO to SSSL workstation.

11.2 Mobile Routing Results

On Friday, May 28, the home agent was placed on the GRC open network, and MR networking was verified. A host machine was using address **HomeAgent.Net.User1** with the home agent at **HomeAgent.Net.HARouter**. The host machine set the home agent as the default gateway. The router was accessed via **CLEO.MobNet.Loopback.Addr**, the MR loopback address (figs. 24 and 25).

A second host machine was NATted as **EngModel.Internet.Firewall** with a default gateway of **GRC.MROpenNet.Router**, the NASA open network router. This second host machine was accessing CLEO via normal routing; the machine **HomeAgent.Net.User1** was accessing CLEO using mobile routing.

On Wednesday, June 2, the home agent was placed behind NASA GRC's Intel VPN firewall with appropriate holes configured to allow the NASA GRC home agent to access the SSSL ground station foreign agent. A TFTP session was performed between machine **HomeAgent.Net.User1** and CLEO

using mobile networking. The transfer was successful, as the pseudo-reverse tunneling allowed us to transition the firewall.

Mobile routing was confirmed by monitoring the home agent MR using “debug ip mobile” and “debug ip mobile route.” The monitored results are shown in figure 26 as a screen capture of a portion of an Ethereal capture packet sniffing capture.

Note: the Internet Control Message Protocol (ICMP) actually used the mobile tunnel. The home agent address is **HomeAgent.Net.HARouter**, and the MR’s care-of-address is **SSTL.Public_Inside.FARouter**. These are two useful addresses to filter on. The MR loopback address is **CLEO.MobNet.Loopback.Addr**. A capture of the mobile networking debug monitoring is shown in appendix G.

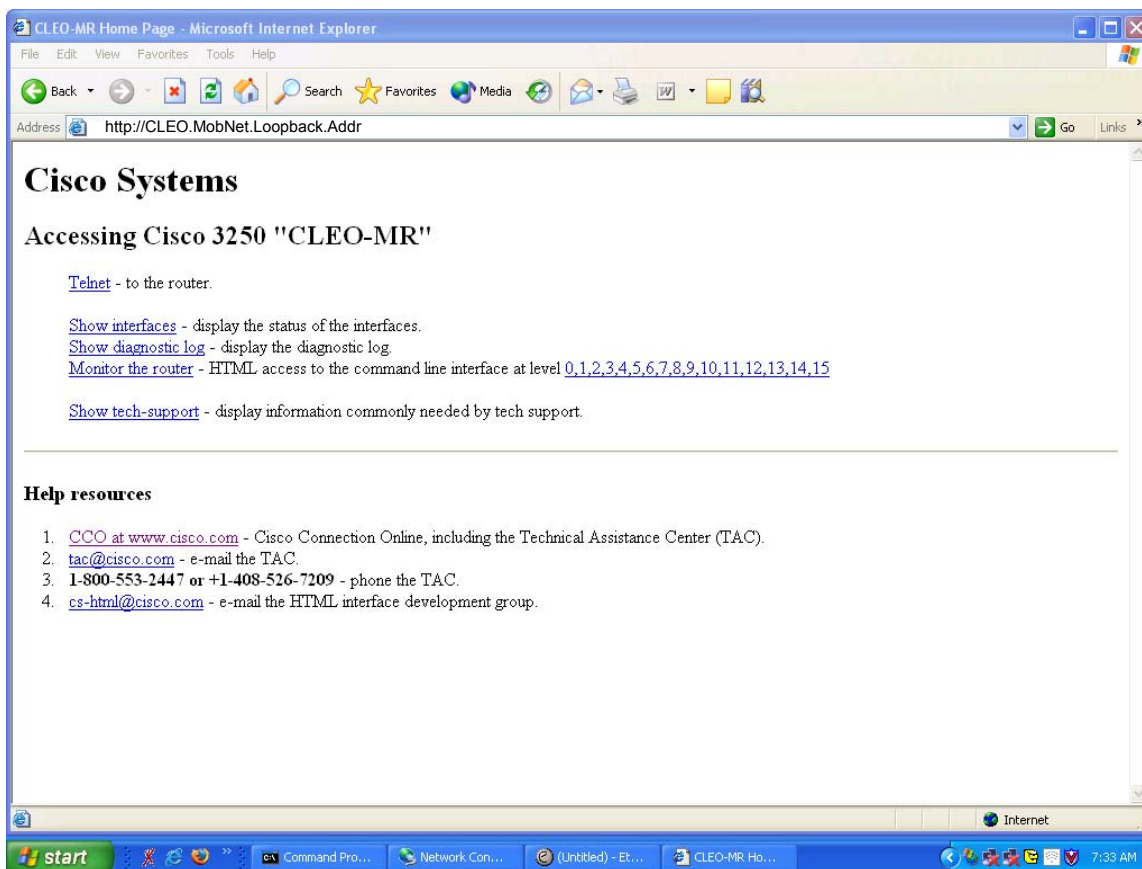


Figure 24.—HTTP access to CLEO via mobile routing.

CLEO-MR

[Home](#) [Exec](#) [Configure](#)

Command	<input type="text"/>
---------	----------------------

Output

Command base-URL was: /level/15/exec/-
Complete URL was: /level/15/exec/-/sho/int/s1\0/CR
Command was: sho int s1/0

```
Serial1/0 is up, line protocol is up
Hardware is DSCC4 Serial
MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 65/255
Encapsulation FRAME-RELAY IETF, loopback not set
Keepalive not set
Broadcast queue 0/64, broadcasts sent/dropped 7/0, interface broadcasts 0
Last input 00:00:00, output 00:00:58, output hang never
Last clearing of "show interface" counters 00:06:59
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 1536 kilobits/sec
5 minute input rate 527000 bits/sec, 47 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    18224 packets input, 24974126 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 1 giants, 0 throttles
    3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    26 packets output, 5524 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
```

command completed.

Figure 25.—“Show interface” commanding of CLEO using HTTP.

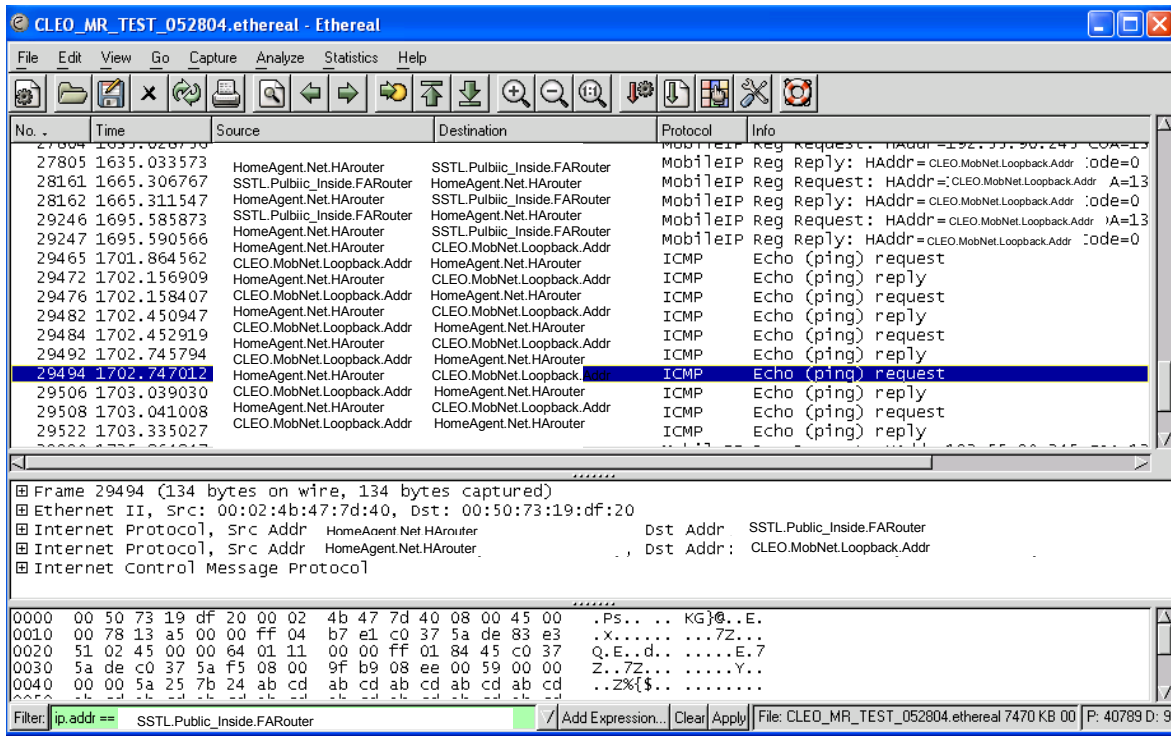


Figure 26.—Ethereal capture of mobile networking at home agent router.

12.0 VMOC Test and Demonstration

The VMOC concept demonstration showed the utility of the TCP/IP 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 SSSL 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 failover 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 databases, 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?

The following scenarios were successfully demonstrated by the VMOC using the SSTL, Army Battlelab and USN ground networks and the UK–DMC and CLEO as the ground infrastructure and space-based asset:

(1) Multiple field users commanded and controlled sensors on a known space-based asset. Several field users of various priorities and clearances were authorized direct access to the UK–DMC. The users were quickly trained to understand how to use and task the platform.

Concept of Operations (ConOp): In this ConOp the users were trained on the operation of the platform rather than simply requesting data. VMOC operators preconfigured the VMOCs to request images from the UK–DMC satellite. The varying accesses and priorities of the field users dictate who can directly task the platform or schedule access time. The VMOC coordinated priorities and conflicting requests and resolved them with the users.

(2) Field users requested information from a single platform or sensor. Several field users of various priorities and clearances were authorized access to real-time or archived sensor data. The users did not know how to use or task the platform, and did not need to in order to acquire useful data.

ConOp: In addition to direct access to platform sensors, the VMOCs were also tied to existing Knowledge Management systems that contain archived data that is of interest to the users. In addition to the VMOC database, NASA’s Earth Observing System (EOS) Data Distribution System (raw data and archived telemetry from EOS mission spacecraft) was used during the demonstration. VMOC operators preconfigured the platform, accesses, and priorities of the field users, who could then schedule access to real-time data from the platform sensors or archived data. Any data requested from the platform was delivered to the user and added to the Knowledge Management system for later retrieval by other users. The VMOC determined priorities and conflicting requests and resolved them with the users. In this ConOp, some of the users had not been trained on the operation of the platform. A Web page interface allowed the user to define what information they needed, and the system determined how to best get them that information.

(3) Machine-to-machine tasking was demonstrated via the VMOC accessing the SSTL MPS. The VMOC was used to determine a target of interest. The VMOC then tasked the UK–DMC via the SSTL MPS for an image. The MPS determined if the UK–DMC (or, potentially, another DMC space asset) could meet the request and, if so, obtained the requested information. This data (image) was then made available to the VMOC, which stored it locally in its database and pushed the requested information to a command post and designated users.

13.0 Future Work

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

13.1 Onboard Routing Between Devices

The UK–DMC satellite also has a GPS reflectometry experiment onboard. A third onboard SSSDR controls the GPS reflectometry experiment and stores the data from that experiment. To download the data, that SSSDR 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 SSSDR 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 SSSDR controlling that experiment

to ground requires dedicating passes to that SSSDR. Data can be moved through the router to be stored on a primary imaging SSSDR 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 SSSDRs, each on a different subnet.

Transferring the data offline to the faster PowerPC-based SSSDR1 or SSSDR2 (controlling the imagers) means less pass time is wasted during transfers, that the SSSDR3 does not have to be powered up storing data until a pass or at the same time as the high-speed downlink, and that SSSDR1 or SSSDR2 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.

13.2 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 end user.

One could conceivably use USN's and SSTL's ground stations to perform this multi-ground station file transfer, with 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.

13.3 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. As noted in the USN description, this could be performed via machine-to-machine e-mail transactions.

13.4 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.

A system-of-systems VMOC approach was demonstrated in October 2005. The demonstration was called Theater Space Apportionment for Effect (TSAFE). The TSAFE VMOC provides the 14th Air Force the new tools and test environment needed to redefine the Space Task Order Process and automate the tie between the Space Air Operations Center (AOC) and the Director of Space Forces (DIRSPACEFOR) in the Combined Air Operations Centers (CAOCs) of independent theaters.

13.5 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, IPv6. This would be highly beneficial as the US DOD has mandated IPv6 for all Global Information Grid—Broadband Extension (GIG—BE) elements.

14.0 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 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 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.

(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 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: $r = \frac{1}{2} k = 7$, 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.

15.0 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 IPs.

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 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 responsiveness 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.

16.0 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 use networks and infrastructure owned and/or controlled by various parties.

References

1. da Silva Curiel, A.; Underwood, C.I.; and Ward, J.W.: Space at Surrey: Recent Successes and Future Missions. SSTL1, 22nd International Symposium on Space Technology and Science, Morioka, Japan, 2000.

2. Oldfield, M., et al.: 60 Satellite Years of Experience in Using Commercial Components in Space. SSTL2, Proceedings of Components for Space Seminar, Royal Military College of Science, Shrivenham, 1998, pp. 94–101.
3. Boroffice, R., et al.: Small Satellites and the Nigerian Space Programme. SSTL3, 34th COSPAR Scientific Assembly, The Second World Space Congress, Houston, TX, 2002.
4. Bradford, A., et al.: BILSAT–1: A Low-Cost, Agile, Earth Observation Microsatellite for Turkey. *Acta Astronaut.*, vol. 53, nos. 4–10, 2003, pp. 761–769.
5. da Silva, Curiel, et al.: Second Generation Disaster-Monitoring Microsatellite Platform. *Acta Astronaut.*, vol. 51, nos. 1–9, 2002, pp. 191–197.
6. Wilhelm, James: SSTL UK–DMC Groundstation RF Interface Control Document, Reference XHPG–64188–01, 2004.
7. Miller, James: 9600 Baud Packet Radio Modem Design. Paper presented at the ARRL 7th Computer Networking Conference, 1988, pp. 135–140.
8. Comtech EF Data.™, ciM–25/600, IP-Enabled M&C Installation and Operation Manual, Part Number CD/CIM25600.IOM, rev. 3, 2004.
9. Cooke, D.; Lancaster, R.; and Buckley, J.: Cisco Router 3200 UK–DMC Payload Interface Control Document. SSTL Internal Technical Document, 2003.
10. Jackson, C.: Saratoga File Transfer Protocol. SSTL Internal Technical Document DMNG–61536, 2004.
11. MPC8260 Solid State Data Recorder. Issue–9034–1, 14–08–2002.
<http://www.sstl.co.uk/documents/MPC8260%20Solid%20State%20Data%20Recorder.pdf> Accessed Feb. 11, 2005.
12. Cisco 3200 Series Mobile Access Router Software Configuration Guide. Cisco Text Part Number: OL–1926–06, 2004.
13. van der Zel, V.: Nigeria and UK–DMC Thermal Vacuum Test Procedure. SSTL Internal Technical Document, 2003.
14. Cisco GSE Installation Guide and User Manual. SSTL Internal Document SPFC–60082–01, 2004.
15. Leung, Kent, et al.: Application of Mobile-ip to Space and Aeronautical Networks. NASA/TM—2001-210590, 2001.
16. Ivancic, William D., et al.: Securing Mobile Networks in an Operational Setting. NASA/TM—2004-213894, 2004.
17. Perkins, C.: IP Mobility Support for IPv4. RFC 3344, 2002.
18. Ivancic, W.: Cisco Router in Low Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC) Data Flow, 2004.
http://roland.grc.nasa.gov/~ivancic/papers_presentations/VMOC_dataflow.ppt Accessed Feb. 11, 2005.
19. Space Link Extension Services—Executive Summary. Yellow Book, CCSDS 910.0–Y–1, 2002.
20. Cross Support Concept—Part 1. Space Link Extension Services, Green Book, CCSDS 910.3–G–2, 2002.
21. Cross Support Reference Model—Part 1. Space Link Extension Services, Blue Book, CCSDS 910.4–B–1, 1996.
22. 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.
23. Schmitt, C.: VMOC Metrics Collection Data Report. Prepared for Contract DASG6201D0003, 2004.
24. 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.

Appendix A Acronyms

AISAT-1	Algerian DMC satellite
AOC	Air Operations Center
API	application program interface
ASIM	Automated Security Incident Measurement
BILSAT-1	Turkish DMC satellite
BNSC	British National Space Centre
CAN	Controller Area Network
CAOC	Combined Air Operations Center
CCSDS	Consultative Committee for Space Data Systems
CERES	U.S. Air Force Center for Research Support
CFDP	CCSDS File Delivery Protocol
CIDD	Common Intrusion Detection Director
CLEO	Cisco router in low Earth orbit
ConOp	Concept of Operations
COTS	commercial-off-the-shelf
CPFSK	continuous phase frequency shift keying
DIRSPACEFOR	Director of Space Forces
DMC	Disaster Monitoring Constellation
DOD	Department of Defense
DTE	data terminal equipment
ECC	error-correcting code
EM	engineering model
EOS	Earth Observation System
FA	foreign agent
flatsat	flat satellite
FM	flight model
FTP	File Transfer Protocol
GIG-BE	Global Information Grid—Broadband Extention
GPS	Global Positioning System
GRC	Glenn Research Center
GSD	ground sample distance
HA	home agent
HAIPE	High Assurance Internet Protocol Encryptor
HAIPIIS	High Assurance Internet Protocol Interoperability Specification
HDLC	high-level data-link control
HTTP	hypertext transfer protocol
ICMP	Internet Control Message Protocol
IESS	Intelsat Earth Station Standards
IETF	Internet Engineering Task Force
IOS	Cisco Systems' Internetworking Operating System
IP	Internet Protocol
IPB	intelligence preparation of the battlefield
IPSAT	Internet Protocol satellite
IPsec	IP security
IPv4	Internet Protocol 4
IPv6	Internet Protocol 6
ISDN	Integrated Services Digital Network

ITU	International Telecommunication Union
LAN	local area network
LHCP	left-hand circular polarized
LLA	Latitude, Longitude, Altitude
LVDS	low-voltage differential signaling
MAR	Cisco Systems Mobile Access Router
MARC	mobile access router card
MOSAIC	Microsatellite Applications in Collaboration
MoST	China Ministry of Science and Technology
MPS	Mission Planning System
MR	mobile router
NASA	National Aeronautics and Space Administration
NAT	network address translation
NDI	nondevelopmental items
NigeriaSAT-1	Nigerian DMC satellite
NIMA	National Imagery and Mapping Agency
NMC	Network Management Center
NNSA	National Nuclear Security Administration
NRO	National Reconnaissance Organization
NTP	Network Time Protocol
NVRAM	nonvolatile RAM
OBC	onboard computer
OBP	onboard processor
OSD	Office of the Secretary of Defense
POR	preprocessed observation requests
QPSK	quadrature phase shift keying
RAI-NC	Rapid Acquisition Initiative—Network Centric
RAM	random-access memory
RF	radiofrequency
RHCP	right-hand circular polarized
ROR	raw observation requests
RPC	remote procedure calls
RTEMS	Real-Time Operating System for Multiprocessor Systems
RxC	receive clock
SDRAM	synchronous dynamic RAM
SLE	Space Link Extension
SMIC	serial mobile interface card
SOAP	Simple Object Access Protocol
SRAM	static RAM
SSDR	solid-state data recorder
SSET	Space Support Element Toolset
ssh	secure shell
SSL	Secure Sockets Layer
SSTL	Surrey Satellite Technology Limited
TCA	Transformational Communication Architecture
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TMR	triple modular redundancy
TSAFE	Theater Space Apportionment for Effect
TT&C	telemetry, tracking, and control
TxC	transmit clock

UDP	User Datagram Protocol
UK-DMC	BNSC UK DMC satellite
UK-MoD	United Kingdom Ministry of Defence
USARSPACE	U.S. Army Space Command
USN	Universal Space Network
VMOC	virtual mission operations center
VPN	virtual private network
WAN	wide area network
XML	extensible markup language

Appendix B Participating Organizations

Below is a listing of the organizations who participated in this demonstration:

Civil organizations involved in this demonstration:

NASA Glenn Research Center—mobile networking expertise (has Space Act agreement with Cisco and Western Datacom).

Commercial organizations involved in this demonstration:

Cisco Systems—CLEO, funded integration work with SSTL
Surrey Satellite Technology Limited (SSTL)—DMC satellites, imaging support
General Dynamics Advanced Information Systems—developed VMOC
Integral Systems—transportable antenna; ran pared-down VMOC in parallel
Universal Space Network (USN)—Alaska ground station providing telemetry
Western DataCom—HAIPE encryption, expertise

U.S. Military organizations involved in this demonstration:

Air Force Space Battlelab—VMOC program manager for U.S. DOD
Air Force Research Lab—will experiment with VMOC with TacSat-2
Army Space and Missile Defense Battle Lab—set up equipment at Vandenberg and provided Colorado Springs telemetry receiving ground station
Space and Missile Systems Center, CERES—alternate VMOC site and satellite operations center
Naval Research Lab—will experiment with VMOC with TacSat-1
Air Force Information Warfare Center—network security
14 Air Force—at Vandenberg. Maj. Gen. Hamel was primary DOD sponsor of VMOC
30 Space Wing—at Vandenberg. Provided sundry support
United States Strategic Command CL18—helped define utility of VMOC
DOD Chief Information Officer—sponsor of VMOC
Rapid Acquisition Incentive—Net Centricity (RAI-NC)—funded VMOC demonstration

Appendix C Points of Contact

Ivancic, Will	NASA GRC Principal Investigator for IP in Space	wivancic@grc.nasa.gov	+1-216-433-3494
Paulsen, Phil	NASA GRC Project Manager	Phillip.E.Paulsen@nasa.gov	+1-216-433-6507
Stewart, David	Verizon Network design, integration, and test	dstewart@grc.nasa.gov	+1-216-433-9644
Shell, Dan	Cisco Systems Mobility/Wireless/Satellite	dshell@cisco.com	+1-440-331-5663
Wood, Lloyd	Cisco Systems CLEO-VMOC project coordination	lwood@cisco.com	+44-20-8824-4236
Heberle, Jay	USN System Applications Engineer	jheberle@uspacenet.com	+1-410-586-9508
Lynch, Scott	USN System Integration	lynch@uspacenet.com	+1-215-328-9130
Boyd, Matt	USN Operations	mboyd@uspacenet.com	+1-215-328-9130
Miller, Eric	General Dynamics VMOC Program Manager	Eric.miller@gd-ais.com	+1-805-606-8609
Walke, Jon	General Dynamics VMOC System Engineer	Jon.walke@gd-ais.com	+1-805-606-8609
John Snider	General Dynamics Advanced Info Systems Security Engineer	John.snider@gd-ais.com	+1-281-642-7150
Graves, Mark	General Dynamics Advanced Info Systems Senior Software Engineer	mark.graves@gd-ais.com	+1-310-348-6344
Kurisasi, Lance	General Dynamics Advanced Info Systems Senior Software Engineer	lance.kurisasi@gd-ais.com	+1-310-338-3562
Jackson, Chris	SSTL Senior System Engineer	C.Jackson@SSTL.co.uk	+44-1483-689-141
Bean, Neville	SSTL Operations	N.Bean@SSTL.co.uk	+44-1483-689-141
Northam, James	SSTL Operations	J.Northam@SSTL.co.uk	+44-1483-689-141
Conner, CAPT Brett	AF Space Battlelab Chief, Scientific & Technical Evaluations	brett.conner@schriever.af.mil	+1-719-567-9937
Groves, Steven	Space and Missile Defense Command Battle Lab	Steven.Groves@SMDC-CS.ARMY.MIL	+1-719-554-4166

Appendix D Cabling

Critical cabling documentation and diagrams are provided in this appendix.

D.1 Engineering Model Null Modem Serial Cable (Both Systems Supply Clocking)

This cable is used in the engineering model between the ground router and the space router for the serial links (fig. 27). The cable connects between one of the frame-relay routers and the Adtech SX/14 Data Link Simulator (Spirent Communications, Rockport, MD) RS442/449 interfaces (figs. 10 and 17).

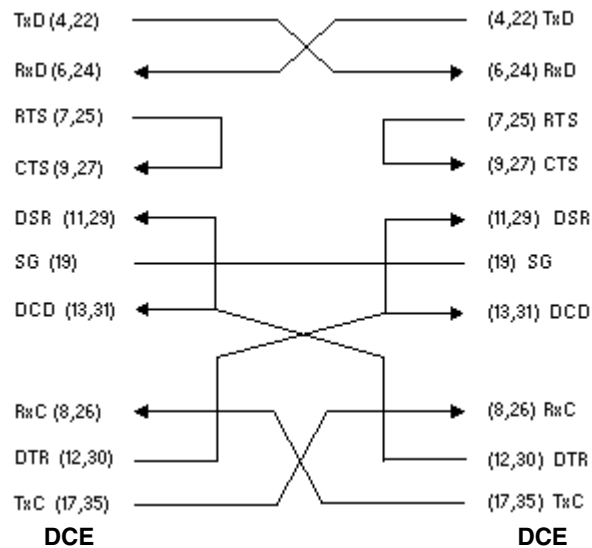


Figure 27.—Engineering model null modem serial cable.

D.2 Ground Station Router-to-Modems Cable

This cable is used in the Universal Space Network and Integral Systems ground stations (Integral Systems downlink only) between the ground router and the uplink modulator and downlink demodulator (fig. 28). Note that the uplink modulator provides the transmit clock to the router and the downlink demodulator provides receive clock to the same serial interface of the router. Thus, the router serial interface is a data terminal equipment (DTE) interface and the transmit clock and receive clock are at different rates.

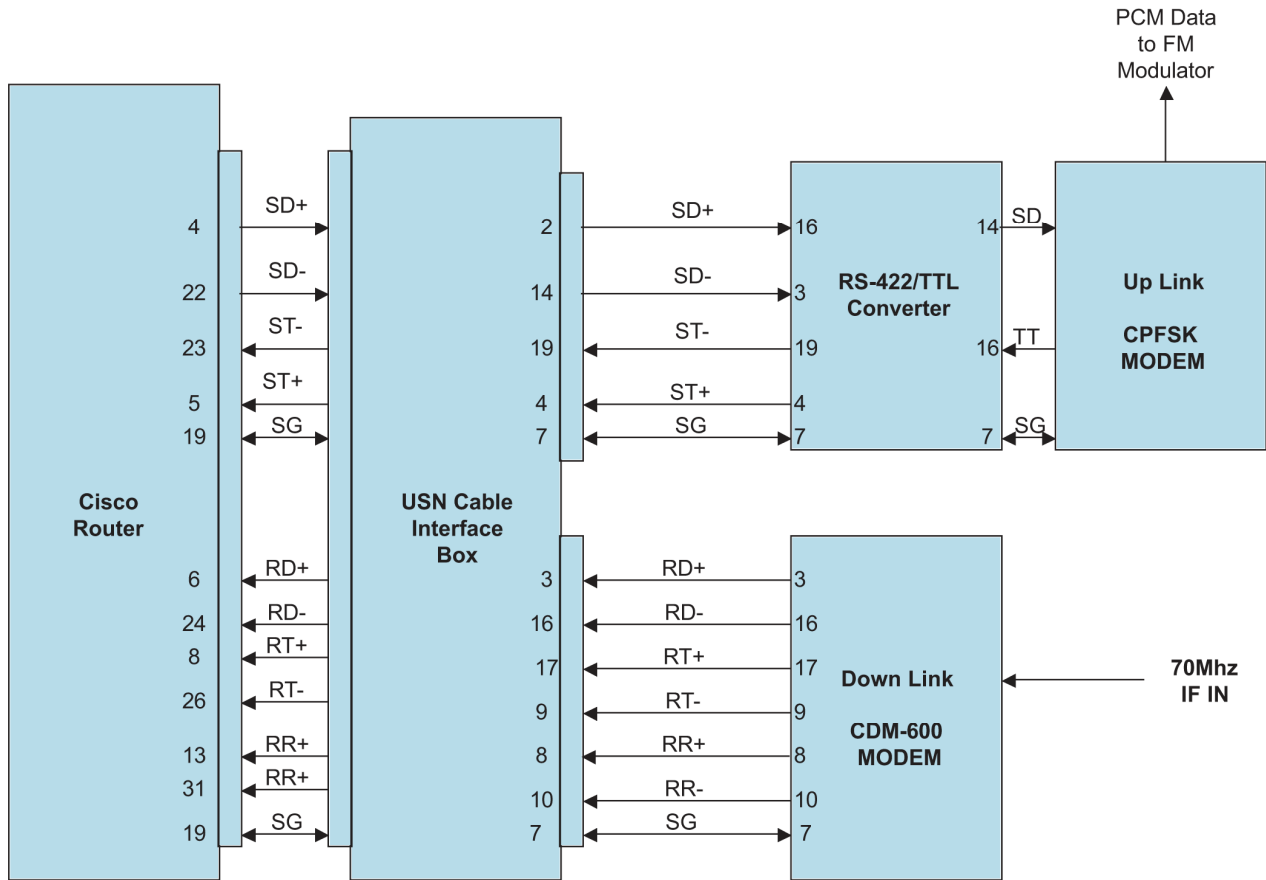


Figure 28.—Ground station router-to-modems cable.

Appendix E VMOC Screen Shots

E.1 Log Screen

The log screen shows all recent activities and associated priorities (fig. 29).

AFSBL Demo (CERES)
DAI-33924885840398
Logged in as: will.ivancic
Roles: Operator | Public | User | Admin

Home Data Library Documents Feedback Logout
Tasks Schedule Tools Log TT&C Operations Administration

Mission Log

Priority: All Messages per Page: 10 Show Messages

Legend: High Medium Low

Date	Logged By	Message
2004-07-16 15:49:23.910	jon.walke	Failover capability has been temporarily disabled in order to work the redirection architecture. Operations will remain on the CERES VMOC until further notice.
2004-07-16 15:47:50.073	jon.walke	Added Paul Zetocha, Ross Wainwright, Beth Stargardt, and Brian Buckley with the TACSAT-2 program.
2004-07-08 13:25:11.130	john.snider	Lance enabled SSL on all Servers, can now externally get in via: https://www.vmoc.net for mobile demo purposes.
2004-06-30 17:04:02.760	john.snider	Added Dan Ogar, BAH employee as operator, for RIMPAC demo
2004-06-24 21:05:37.000	jon.walke	The AFSBL Demo VMOC's (CERES & GRC) remain online and operational, but the schedule and access tools do not go beyond 21 Jun 04 and not tasking, telemetry or commanding is operational with the SSTL ground station.
2004-06-15 20:53:29.333	jon.walke	Data replication is restored with the CERES VMOC. Operations are back to normal with normal system backup capability. Primary operations will remain on the GRC system with the CERES system acting as backup.

Figure 29.—VMOC log screen.

E.2 TT&C Screen

The telemetry, tracking, and control (TT&C) screen shows the ground station of interest (selectable) and the server's time and date (figs. 30 and 31). The Telemetry and Commanding areas show their respective contact start and stop times as well as a countdown timer. Viewing of real-time and simulated telemetry and commanding is issued from this window.

The real-time telemetry window for the UK-DMC satellite is shown in figure 31. This data is pulled from the UK-DMC telemetry stream that is redistributed to the VMOCs from the various ground stations. The telemetry arrives at the VMOCs as UDP packets with a data format that is consistent for all SSTL satellites. The information shown in the Simulated UK-DMC System Status window is only a small portion of the information available from the telemetry packets.

Note: The real-time telemetry window proved useful in debugging the USN uplink as the VMOC could be used by USN to monitor power levels received onboard the UK-DMC.

The screenshot displays the 'Satellite TT&C' interface. At the top, there is a navigation bar with buttons for Home, Data Library, Documents, Feedback, Logout, Tasks, Schedule, Tools, Log, TT&C (highlighted), Operations, and Administration. The user is logged in as 'will.ivancic' with roles 'Operator | Public | User | Admin'. The interface is divided into three main sections: Ground station selection, Telemetry, and Commanding.

Ground station: USN_Alaska (dropdown menu)

Server time: Fri, 15 Oct 2004 14:16:39Z

Telemetry

Next contact starts:	Fri, 15 Oct 2004 15:22:27Z
Next contact ends:	Fri, 15 Oct 2004 15:33:27Z
Count down:	Starts: -01:05:48

- [View real-time telemetry](#)
- [View simulated telemetry](#)

Commanding

Next contact starts:	Fri, 15 Oct 2004 15:22:27Z
Next contact ends:	Fri, 15 Oct 2004 15:33:27Z
Count down:	Starts: -01:05:48

- [show version](#) [virtual flatsat]

Figure 30.—VMOC telemetry, tracking, and control (TT&C) screen.

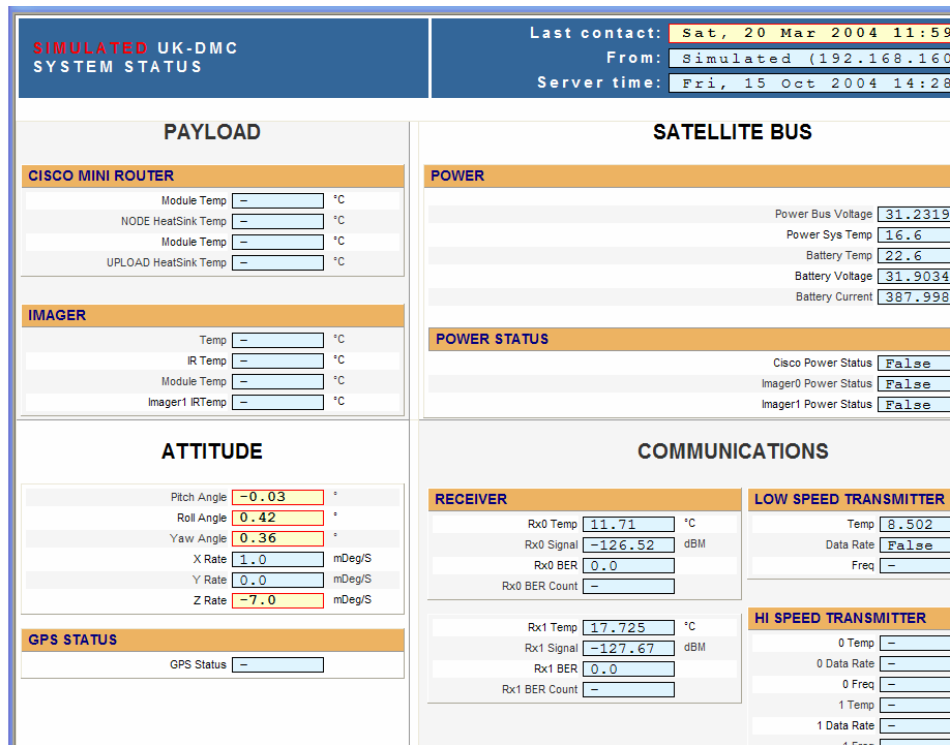


Figure 31.—Real-time telemetry.

E.3 Tools Screen

The tools screen provides information regarding access to various assets.

The Sensor/Target Access Report form will generate a list of time periods when the selected latitude/longitude will be in the field of view of the selected sensor.

The Ground Station/Platform Access Report provides two reports: (1) the Azimuth/Elevation/Range report, which lists the azimuth, elevation, and range between the platform and the selected ground station and (2) the Access report, which generates a list of time periods when the selected ground station will be in line of sight of the selected platform.

The Satellite LLA (Latitude, Longitude, Altitude) Position Report gives the latitude, longitude, and altitude of a given satellite in 5-min intervals over a specified range of time.

The J-Track screen (fig. 32) is useful for visually determining when a specific spacecraft will be in visual contact with known locations. The screen shot shows the location of the UK-DMC satellite on October 15, 2004, at 14:47:05 GMT. The J-Track screen uses the Java-based J-Track program available from NASA at <http://science.nasa.gov/Realtime/>.

NASA JTrack

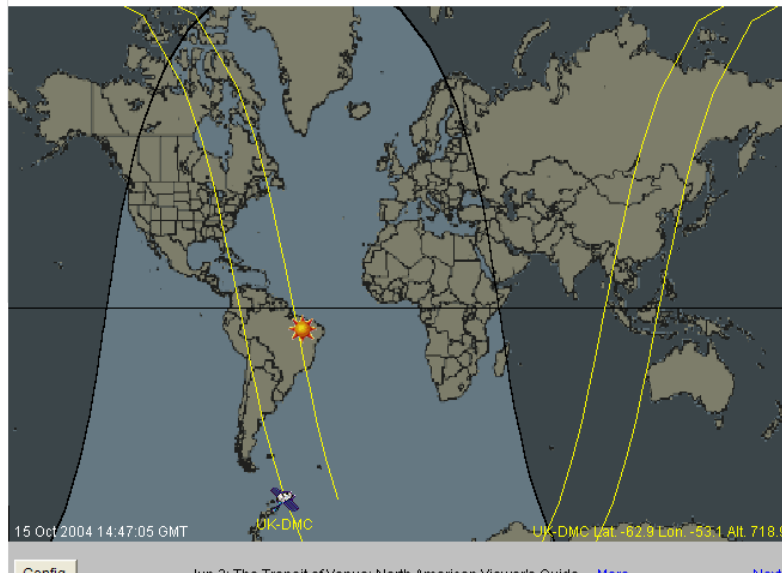


Figure 32.—NASA J-Track screen.

Virtual Mission Operations Center
AFSBL DEMO (CERES)

33924885840398
Logged in as: will.ivancic
Roles: Operator | Public | User | Admin

Home Data Library Documents Feedback Logout
Tasks Schedule Tools Log TT&C Operations Administration

UK-DMC
Schedule
List Schedule
Full Schedule

Tasks in the VMOC database

Select tasks to display
 All Exported Assigned Unassigned Requested Executed Error Cancelled
 Reset Show Tasks

Username	Task Name	Tag	Latitude	Longitude	State	Priority	Scheduled Start Time	Scheduled Stop Time
mark.graves	Mt. St. Helens	AAFO	46.2000	-122.2000	Error	3		
mark.graves	Palmdale	AAGC	34.5980	-118.1300	Error	7		
joe.user	Indianapolis	AABC	39.7520	-86.1610	Executed	3	2004-05-22 15:26:12	2004-05-22 15:26:13
joe.user	Philadelphia	AABH	40.0000	-75.0000	Executed	7	2004-05-26 14:40:03	2004-05-26 14:40:06
joe.ops	Savannah, GA	AABK	32.0000	-81.1500	Executed	3	2004-05-27 15:15:44	2004-05-27 15:15:47
joe.ops	New Orleans	AABM	30.0000	-90.0000	Error	3	2004-05-28 15:52:44	2004-05-28 15:52:47
joe.user	Between St. Petersburg and Orlando FL	AABP	28.1600	-82.0700	Executed	7	2004-06-04 15:21:04	2004-06-04 15:21:07
joe.user	Cape Cod	AACE	41.3800	-70.6300	Executed	7	2004-06-05 14:23:59	2004-06-05 14:24:02
larry.dikeman	My home	AABG	40.7700	-90.0200	Error	3	2004-06-07 04:36:14	2004-06-07 04:36:17
joe.user	Houston	AACI	29.7700	-95.3900	Executed	7	2004-06-08 16:13:56	2004-06-08 16:13:59
jon.walke	Albuquerque	AACJ	35.1000	-106.6000	Executed	3	2004-06-10 06:53:09	2004-06-10 06:53:09
joe.ops	Augusta, ME	AADE	44.3100	-69.7900	Error	7	2004-06-10 14:16:18	2004-06-10 14:16:21
joe.ops	southern california	AADG	33.4900	-115.5000	Error	7	2004-06-10 17:30:19	2004-06-10 17:30:22
joe.ops	Washington	AADF	47.1000	-119.8000	Error	7	2004-06-10 17:34:06	2004-06-10 17:34:09
joe.user	Suwannee	AAEC	29.5852	-83.7057	Executed	7	2004-06-12 15:27:51	2004-06-12 15:27:52

Figure 33.—VMOC schedule screen.

E.4 Schedule Screen

The schedule screen provides information regarding scheduled request. Information can be sorted using the following criteria: Exported, Assigned, Unassigned, Requested, Executed, and Cancelled commands as well as request with Errors (fig. 33).

Figure 34.—VMOC task screen.


E.5 Task Screen

The task screen is where one enters tasks (fig. 34). For the UK–DMC, the only task available is to request an image. The image request is entered as longitude and latitude. Priorities can also be assigned by the user. These prioritize the user’s request.

E.6 Data Library Screen

One searches for existing images from the Data Library screen (fig. 35). This is the entry point for data mining. Currently the image database can be searched with filters for scheduled tasks, collected data, and image markup data that have been appended by users.

An associated VMOC tool is the Java-based image viewer map tool. It allows the user to search the globe visually and select the area of interest. The core of the VMOC map tool is the National Imagery and Mapping Agency (NIMA) global map, shown in figure 36. Areas can be selected (fig. 36) and zoomed in on as illustrated in figure 37, which highlights Colorado Springs, CO. Once the location is selected and highlighted, VMOC automatically populates the Data Library search tool for the user. The VMOC will search the appropriate archives and highlight the areas on the map coinciding with the images currently available that are in any way included in the user-defined area of interest. These are the tinted green areas shown in figure 37. If the archived data does not meet the user’s needs, the location request (red dashed box) can be forwarded to the scheduling portion of the VMOC for direct sensor tasking. The VMOC database images can be combined with the NIMA mapping images to enhance the usefulness of the NIMA information—particularly by providing time-sensitive imaging.


 33924885840398
 Logged in as: will.ivancic
 Roles:

[Home](#) [Data Library](#) [Documents](#) [Feedback](#) [Logout](#)

Data Library Search

Sources Scheduled Tasks Collected Data Image Markup

Keywords

Task Start Date After and/or Before
Enter dates in the format YYYY-MM-DD HH:MM:SS

Area of Interest

Top

Left Right

Bottom

[Launch Viewer Tool](#)

Or

Latitude/Longitude

Latitude: Longitude:

(enter latitudes and longitudes in degrees, with North/East positive and South/West negative)

Figure 35.—VMOC data library screen.

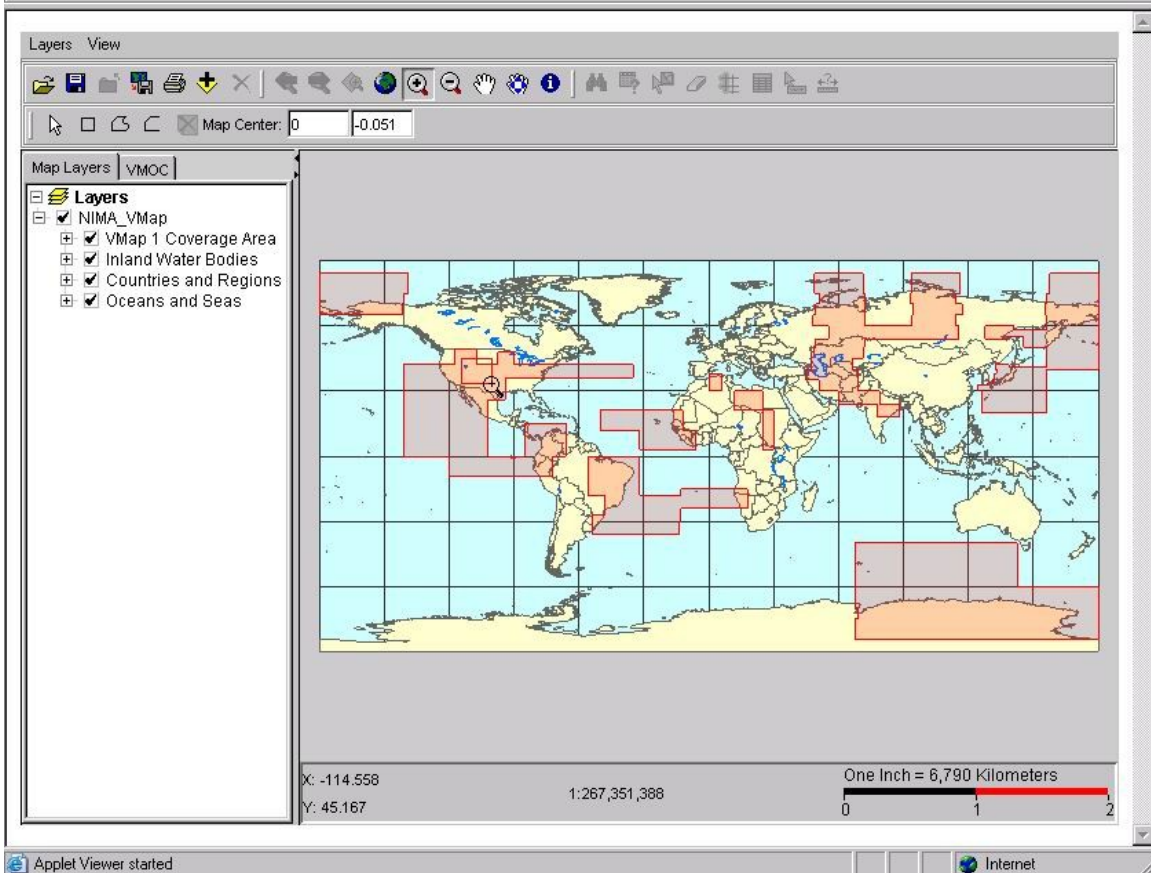


Figure 36.—NIMA global map.

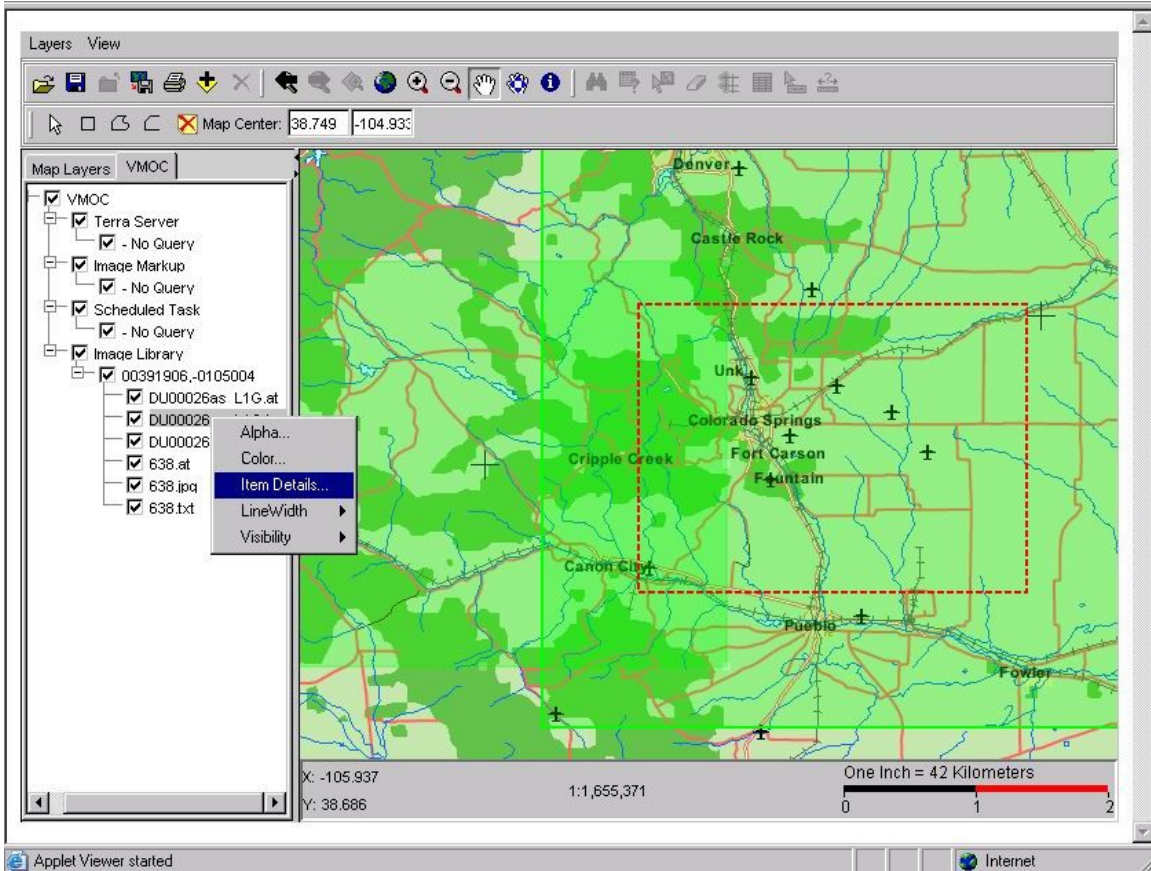


Figure 37.—NIMA map of Colorado Springs area.

Appendix F

Router Configurations

Listings of all router configurations are provided in this appendix to aid in recreation of all or portions of this network.

F.1 CLEO—Home Agent

This configuration is for the CLEO home agent router. This is the home agent router for CLEO, the CLEO engineering model, and the virtual flatsat. Address space has also been allocated for a future mobile network, Future_CLEO_EM.Aggregated.

```
CLEO_HA#
Current configuration : 4103 bytes
!
! Last configuration change at 19:41:39 UTC Thu Jun 10 2004
! NVRAM config last updated at 19:42:01 UTC Thu Jun 10 2004
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CLEO_HA
!
enable password xxxx
!
ip subnet-zero
!
!
ip ftp username xxxx
ip ftp password xxxx
!
!
!
mta receive maximum-recipients 0
!
!
!
interface Tunnel6
description "MR subnets reach-back for triangular routing from V_CLEO_EM's
(Virtual_FlatSat) foreign agent (FA)."
```

```
ip address 10.7.6.1 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination vflatsat.FA_Inside_Network.Router
tunnel mode ipip
!
interface Tunnel7
description "MR subnets reach-back for triangular routing from CLEO_EM's (FlatSat) FA."
ip address 10.7.7.1 255.255.255.0
```

```
tunnel source FastEthernet0/0
tunnel destination EngModel.FA_Inside_Network.FArouter
tunnel mode ipip
```

```
!
```

```
interface Tunnel8
description "MR subnets reach-back for triangular routing from Colorado Springs' (Army
            Battle Labs) FA. Ground station was disassembled after June 2004, VMOC
            Demo"
```

```
ip address 10.7.8.1 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination CERES.FA_Inside_Network.FArouter
tunnel mode ipip
```

```
!
```

```
interface Tunnel101
description "MR subnets reach-back for triangular routing from STGT-FA (USN's Ground
            Station FA)."
```

```
ip address 10.101.101.1 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination USN.FA_Inside_Network.Router
tunnel mode ipip
```

```
! Purpose of Tunnels 6, 7, 8 & 101:
```

```
!*** It was decided upon initial configuration to have the mobile router (MR) in the spacecraft to use
triangular routing as opposed to reverse tunneling. This allowed direct downloads from the spacecraft to
the Data Workstation that is directly connected to the current foreign agent.
```

```
This also created a problem that reverse tunneling alleviates, egress filtering. When utilizing triangular
routing, a packet sourced from a node on or behind the MR will have a source address that is from the
home agent's domain or is private address space. Thus when the MR is attached to a foreign network,
packets originating from the MR's networks destined for an address outside of the foreign network will be
discarded by the foreign firewall's egress filters (i.e., firewall rules to guard against spoofing an address).
The following four tunnels were created to solve this problem, but still use the triangular routing. There is
a tunnel from each foreign agent back to the home agent (this router). The foreign agent has a policy route
defined that will take any packet with a source address from a MR subnet and forward it to the home
agent via the tunnel. Thus the packet appears to originate from the home agent (a.k.a. its home domain).
```

```
***!
```

```
!
```

```
!
```

```
!
```

```
interface FastEthernet0/0
ip address HomeAgent.Net.HArouter 255.255.255.248
duplex auto
speed auto
```

```
!
```

```
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
```

```
!
```

```
interface Serial2/0
no ip address
shutdown
```



```

serial restart_delay 0
no fair-queue
!
interface Serial2/1
no ip address
shutdown
serial restart_delay 0
!
interface Serial2/2
no ip address
shutdown
serial restart_delay 0
!
interface Serial2/3
no ip address
shutdown
serial restart_delay 0
!
router mobile
! Enables Mobile IP
!
ip classless
!
!
ip route 0.0.0.0 0.0.0.0 HomeAgent.Net.Firewall_Inside
ip route SSTL.Private.0 255.255.255.0 HomeAgent.Net.Firewall_Inside
ip route 192.168.140.0 255.255.255.0 HomeAgent.Net.Firewall_Inside
ip route 192.168.150.0 255.255.255.0 HomeAgent.Net.Firewall_Inside
ip route 192.168.160.0 255.255.255.0 HomeAgent.Net.Firewall_Inside
! Static Routes
!
ip http server
! Enable Router's HTTP Server
!
!
ip mobile home-agent
! Enables Mobile IP Home Agent function
!
ip mobile virtual-network CLEO.MobNet.Aggregate 255.255.255.224
ip mobile virtual-network vflatsat.MobNet.Aggregate 255.255.255.240
ip mobile virtual-network EngModel.MobNet.Aggregate 255.255.255.224
ip mobile virtual-network Future_CLEO_EM.Aggregated 255.255.255.240
! Define virtual networks for address space used by the Mobile Routers
!
ip mobile host Future_CLEO_EM.Loopback0 virtual-network Future_CLEO_EM.Aggregated
255.255.255.240
ip mobile host EngModel.MobNet.Loopback.Addr virtual-network EngModel.MobNet.Aggregate
255.255.255.224
ip mobile host vflatsat.MobNet.Loopback0 virtual-network vflatsat.MobNet.Aggregate 255.255.255.240
ip mobile host CLEO.MobNet.Loopback.Addr virtual-network CLEO.MobNet.Aggregate
255.255.255.224

```

```

! Assign virtual networks to individual MR
!
ip mobile mobile-networks Future_CLEO_EM.Loopback0
description "MR subnets for Future_CLEO_EM router"
network Future_CLEO_EM.Loopback0 255.255.255.255
network Future_CLEO_EM.Net1 255.255.255.252
network Future_CLEO_EM.Net2 255.255.255.248
! Emulated satellite system setup for future deployment at Surrey Satellite Technology LTD
!
ip mobile mobile-networks EngModel.MobNet.Loopback.Addr
description "MR Subnets for CLEO_EM (Flatsat) router"
network EngModel.MobNet.Aggregate 255.255.255.252
network EngModel.Mobnet.S1/2.Net 255.255.255.252
network EngModel.Mobnet.S1/3.Net 255.255.255.252
network EngModel.Mobnet.S1/1.Net 255.255.255.248
network EngModel.Mobnet.S1/0.Net 255.255.255.248
! Emulated Satellite System Setup at NASA GRC, for testing router configurations before uploading to
onboard router
!
ip mobile mobile-networks vflatsat.MobNet.Loopback0
description "MR subnets for V_CLEO_EM (Virtual Flatsat) router"
network vflatsat.MobNet.Net1 255.255.255.248
network vflatsat.MobNet.Net2 255.255.255.252
network vflatsat.MobNet.Loopback0 255.255.255.255
! Emulated satellite system setup for VMOC testing, when CLEO_FM (satellite) was not available
!
ip mobile mobile-networks CLEO.MobNet.Loopback.Addr
description "MR Subnets for CLEO_FM (Satellite Onboard) router"
network CLEO.MobNet.S1/4.Net 255.255.255.248
network CLEO.MobNet.S1/3.Net 255.255.255.252
network CLEO.MobNet.S1/1.Net 255.255.255.248
network CLEO.MobNet.S1/2.Net 255.255.255.252
network CLEO.MobNet.Aggregate 255.255.255.252
! Satellite Onboard Router Mobile IP subnet definitions
!
ip mobile secure host Future_CLEO_EM.Loopback0 spi 777 key ascii Phone-Home algorithm md5 mode
prefix-suffix
ip mobile secure host EngModel.MobNet.Loopback.Addr spi 666 key ascii Phone-Home algorithm md5
mode prefix-suffix
ip mobile secure host vflatsat.MobNet.Loopback0 spi 777 key ascii Phone-Home algorithm md5 mode
prefix-suffix
ip mobile secure host CLEO.MobNet.Loopback.Addr spi 666 key ascii Phone-Home algorithm md5
mode prefix-suffix
! Mobile Router information for authentication
!
!
!
call rsvp-sync
!
!
mgcp profile default

```

```

!
!
!
dial-peer cor custom
!
!
!
line con 0
  exec-timeout 10000 0
line aux 0
line vty 0 4
  password cisco
  login
!
ntp clock-period 17179961
ntp server 128.118.25.3
!
end

```

CLEO_HA#

F.2 Cisco Router in Low Earth Orbit—CLEO

Using 2367 out of 131072 bytes

```

!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
ip domain-name CLEO-MR.sstl.com
!
aaa new-model
For HTTP Access Authentication
!
!
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
enable secret 5 $1$24l$XO42qKW.681XToTMHZCSe1
enable password xxxxxxxxx
HTTP access for exec user
!
username VMOC password 0 VMOC
username XXXX privilege 15 password 0 XXXX
HTTP access for non privileged user

```

```
ip subnet-zero
!  
ip ssh time-out 60  
ip ss auth 2
```

For secure shell access

```
!  
!  
interface Loopback0  
ip address SSTL.Private.CLEO_Loopback 255.255.255.255  
Non-Mobile IP access from Surrey Ground station router or public Intranet via Natted address.  
!  
int Loopback 1  
ip address CLEO.MobNet.Loopback.Addr 255.255.255.255  
Mobile Router's address  
!  
!  
interface Serial1/0  
no ip address  
encapsulation frame-relay IETF  
no ip mroute-cache  
no keepalive  
ignore-dcd  
nrzi-encoding  
!  
interface Serial1/0.1 point-to-point  
ip address EngModel.MobNet.S1/0.Net 255.255.255.252  
ip mobile router-service roam  
! Mobile Router command configures this as a roaming interface  
!  
no ip mroute-cache  
frame-relay interface-dlci 17  
SSDR0 interface and Mobile networking Roaming  
!  
interface Serial1/1  
no ip address  
encapsulation frame-relay IETF  
no ip mroute-cache  
no keepalive  
ignore-dcd  
nrzi-encoding  
!  
interface Serial1/1.1 point-to-point  
ip address EngModel.MobNet.S1/1.Net 255.255.255.248  
ip mobile router-service roam  
! Mobile Router command configures this as a roaming interface  
!  
no ip mroute-cache  
frame-relay interface-dlci 17  
SSDR1 interface and Mobile Networking Roaming
```

NOTE: Currently this link has the OBC active.

```
!  
interface Serial1/2  
no ip address  
encapsulation frame-relay IETF  
no ip mroute-cache  
no keepalive  
ignore-dcd  
nrzi-encoding  
!  
interface Serial1/2.1 point-to-point  
ip address EngModel.MobNet.S1/2.Net 255.255.255.252  
ip mobile router-service roam  
! Mobile Router command configures this as a roaming interface  
!  
no ip mroute-cache  
frame-relay interface-dlci 17  
SSDR2 and Mobile networking Roaming  
!  
interface Serial1/3  
mtu 512  
no ip address  
encapsulation frame-relay IETF  
no ip mroute-cache  
no keepalive  
ignore-dcd  
nrzi-encoding  
!  
interface Serial1/3.1 point-to-point  
ip address EngModel.MobNet.S1/3.Net 255.255.255.248  
no ip mroute-cache  
frame-relay interface-dlci 17  
Not Active  
!  
router mobile  
Turns Mobile IP on  
!  
ip mobile secure home-agent HomeAgent.Net.HArouter spi 666 key ascii Phone-Home  
! Mobile Router information for HA authentication  
!  
ip mobile router  
address CLEO.MobNet.Loopback.Addr 255.255.255.224  
home-agent HomeAgent.Net.HArouter priority 105  
register lifetime 60  
Mobile networking commands  
!  
ip http server  
ip http authentication local  
ip classless  
ip route 0.0.0.0 0.0.0.0 serial1/1.1 245
```

Static default route for non-Mobile Router mode, so that Surrey always has local access. Set the admin distance high so Mobile Router's inserted default route takes precedence in the routing table.

```
!  
ip route SSTL.Private.SSDR0 255.255.255.255 Serial1/0.1  
ip route SSTL.Private.SSDR1 255.255.255.255 Serial1/1.1  
ip route SSTL.Private.SSDR2 255.255.255.255 Serial1/2.1  
ip route SSTL.Private.UK-DMC.SSDR0 255.255.255.255 Serial1/0.1  
ip route SSTL.Private.UK-DMC.SSDR1 255.255.255.255 Serial1/1.1  
Static routes for SSDRS  
!  
! radius-server retransmit 3  
radius-server authorization permit missing Service-Type  
!  
line con 0  
  exec-timeout 0 0  
  stopbits 1  
line aux 0  
line vty 0 4  
  password cisco  
!  
end
```

F.3 Surrey Satellite Technology Limited (SSTL) Ground Router

```
interface FastEthernet0/0  
  description connected to Groundstation Subnet0  
  ip address SSTL.Public_Inside.FARouter 255.255.255.128  
  Work station Lan Public network  
  ip directed-broadcast  
  ip nat outside  
  duplex auto  
  speed auto  
!  
interface Serial0/0  
  no ip address  
  encapsulation frame-relay IETF  
  no ip mroute-cache  
  no keepalive  
  no fair-queue  
  nrzi-encoding  
!  
interface Serial0/0.1 point-to-point  
  ip unnumbered FastEthernet0/0  
  no ip mroute-cache  
  no arp frame-relay  
  no cdp enable  
  frame-relay interface-dlci 17  
  Uplink to UK -DMC primary  
!  
interface FastEthernet0/1
```

```

description connected to Antenna0 LAN
NATTED Private LAN for workstations
ip address SSTL.Private.LAN.Int 255.255.255.0
ip directed-broadcast
directs telemetry broadcast from OBC out this interface
!
ip nat inside
duplex auto
speed auto
!
interface Serial0/1
mtu 512
no ip address
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
no fair-queue
ignore-dcd
nrzi-encoding
!
interface Serial0/1.1 point-to-point
ip unnumbered FastEthernet0/0
no ip mroute-cache
no arp frame-relay
no cdp enable
frame-relay interface-dlci 17
UK-DMC uplink secondary
!
router rip
passive-interface Serial0/0
network SSTL.Public_Inside.Network
!
ip default-gateway SSTL.Public_Inside.Firewall.Inside
ip nat inside source static SSTL.Private.WS1 SSTL.Public_Inside.WS1
ip nat inside source static SSTL.Private.WS2 SSTL.Public_Inside.WS2
ip nat inside source static SSTL.Private.WS3 SSTL.Public_Inside.WS3
MAPS inside workstation to public addresses
!
ip nat inside source static SSTL.Private.CLEO_Loopback SSTL.Public_Inside.CLEO_Loopback0
SSTL.Private.CLEO_Loopback is direct access loopback on CLEO_FM for direct connection (telnet/ssh)
without Mobile IP
!
no ip classless
ip route 0.0.0.0 0.0.0.0 SSTL.Public_Inside.Firewall.Inside
!
ip route SSTL.Public_Inside.WS1 255.255.255.255 FastEthernet0/1
ip route SSTL.Public_Inside.WS2 255.255.255.255 FastEthernet0/1
ip route SSTL.Public_Inside.WS3 255.255.255.255 FastEthernet0/1
Points natted public addresses to the natted private LAN Work Station.
!
ip route SSTL.Public_Inside.CLEO_Loopback0 255.255.255.255 Serial0/0.1

```

```

Natted address for CLEO_FM direct connect loopback
!
ip route SSTL.Private.BILSAT.OBC 255.255.255.255 Serial0/0.1
ip route SSTL.Private.UK-DMC.OBC 255.255.255.255 Serial0/0.1
ip route SSTL.Private.NigeriaSat.OBC 255.255.255.255 Serial0/0.1
ip route SSTL.Private.AISat.OBC 255.255.255.255 Serial0/0.1
ip route SSTL.Private.CLEO_Loopback 255.255.255.255 Serial0/0.1
Static routes for SSDRS & CLEO_FM
!
ip http server

```

F.4 Universal Space Network (USN) Ground Router

```

!
! No configuration change since last restart
!
version 12.2
no parser cache
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname STGT-FA
!
logging buffered 10000 debugging
logging rate-limit 50
no logging console
aaa new-model
aaa authentication login default line enable local-case
enable secret 5 $1$857P$q0VJZBwWJgaRwuMv.0cwV0
enable password 7 06131C2F014F02
!
ip subnet-zero
no ip source-route
!
!
no ip domain-lookup
ip domain-name nascom.nasa.gov
ip host NM2 150.144.1.38
ip host NM 150.144.1.37
ip host Mac 150.144.1.50
ip host LPT 150.144.1.42
ip host ASPC 150.144.1.33
!
no ip bootp server
ip audit notify log
ip audit po max-events 100
!
no call rsvp-sync
!

```



```

!
!
!
!
!
!
interface Tunnel101
ip address 10.101.101.254 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination HomeAgent.Net.HArouter
tunnel mode ipip
!
interface FastEthernet0/0
ip address USN.FA_Inside_Network.Router 255.255.255.0
ip directed-broadcast
ip accounting output-packets
ip nat outside
no ip mroute-cache
duplex auto
speed auto
no cdp enable
!
interface Serial0/0
no ip address
encapsulation frame-relay IETF
no keepalive
ignore-dcd
nrzi-encoding
!
interface Serial0/0.1 point-to-point
ip unnumbered FastEthernet0/0
ip accounting output-packets
ip nat inside
ip irdp
ip irdp maxadvertinterval 15
ip irdp minadvertinterval 10
ip irdp holdtime 45
ip mobile foreign-service
no ip mroute-cache
ip policy route-map mr_subnets
no arp frame-relay
no cdp enable
frame-relay interface-dlci 17
!
interface FastEthernet0/1
ip address SSTL.Private.LAN.Int 255.255.255.0
ip directed-broadcast
ip nat inside
duplex auto
speed auto

```

```

no cdp enable
router mobile
!
ip default-gateway USN.FA_Inside_Network.Firewall
ip nat inside source static SSSL.Private.WS1 USN.FA_Inside_Network.WS1
ip nat inside source static SSSL.Private.WS2 USN.FA_Inside_Network.WS2
ip nat inside source static SSSL.Private.WS3 USN.FA_Inside_Network.WS3
ip nat inside source static SSSL.Private.CLEO_Loopback USN.FA_Inside_Network.CLEO_Loopback0
ip nat inside source static SSSL.Private.UK-DMC.OBC USN.FA_Inside_Network.UK-DMC.OBC
ip classless
ip route 0.0.0.0 0.0.0.0 USN.FA_Inside_Network.Firewall
ip route USN.FA_Inside_Network.WS1 255.255.255.255 FastEthernet0/1
ip route USN.FA_Inside_Network.WS2 255.255.255.255 FastEthernet0/1
ip route USN.FA_Inside_Network.WS3 255.255.255.255 FastEthernet0/1
ip route USN.FA_Inside_Network.CLEO_Loopback0 255.255.255.255 Serial0/0.1
ip route SSSL.Private.UK-DMC.OBC 255.255.255.255 Serial0/0.1
ip route SSSL.Private.CLEO_Loopback 255.255.255.255 Serial0/0.1
no ip http server
no ip pim bidir-enable
ip mobile foreign-agent care-of FastEthernet0/0
!
logging trap debugging
access-list 7 permit CLEO.MobNet.Aggregate 0.0.0.31
access-list 10 permit USN.FA_Inside_Network 0.0.0.255
no cdp run
route-map mr_subnets permit 10
  match ip address 7
!
snmp-server engineID local 00000009020000053276D220
snmp-server community omni-lpt RO 3
snmp-server location LPT STGT-FA ()
snmp-server contact ASPC 286-3574 OMNI 286-3203
snmp-server chassis-id 2134229
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server enable traps dlsw

```

```

snmp-server enable traps dial
snmp-server enable traps dsp card-status
snmp-server enable traps voice poor-qov
snmp-server enable traps xgcp
snmp-server host 150.155.40.67 nolan
!
dial-peer cor custom
!
banner motd □C

```

```

*****
* *
* WARNING! This is a U.S. Federal Government computer. This system *
* is for the use of the OMNI project only. By accessing and using *
* the computer system you are consenting to system monitoring, *
* including the monitoring of keystrokes, with no expectation of *
* privacy. Unauthorized use of, or access to, this computer system *
* may subject you to disciplinary action and criminal prosecution. *
* *
*****

```

```

!
line con 0
session-timeout 99
exec-timeout 99 0
line aux 0
line vty 0 4
session-timeout 99
exec-timeout 99 0
password 7 03174F0C12420E616020
transport input telnet ssh
!
ntp peer 150.144.40.38
ntp peer 150.144.41.38 prefer
end

```

F.5 Virtual Flatsat Foreign Agent Ground Router

```

!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname V_GSN_RTR
!
boot system flash:c2600-ik9o3s-mz.122-23a
enable password vflatsat
!
username vmoc
username all

```

```

ip subnet-zero
!
!
no ip domain-lookup
!
ip audit notify log
ip audit po max-events 100
!
call rsvp-sync
!
!
interface Tunnel6
ip address 10.7.6.2 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination HomeAgent.Net.HArouter
tunnel mode ipip
!
interface FastEthernet0/0
description Ground Station Subnet-0
ip address vflatsat.FA_Inside_Network.Router 255.255.255.128
ip directed-broadcast
ip nat outside
no ip mroute-cache
duplex auto
speed auto
no cdp enable
!
interface Serial0/0
no ip address
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
no fair-queue
nrzi-encoding
!
interface Serial0/0.1 point-to-point
ip unnumbered FastEthernet0/0
ip irdp
ip irdp maxadvertinterval 45
ip irdp minadvertinterval 30
ip irdp holdtime 135
ip mobile foreign-service
no ip mroute-cache
ip policy route-map mr_subnets
no arp frame-relay
no cdp enable
frame-relay interface-dlci 17
!
interface FastEthernet0/1
description Antenna-0 LAN
ip address SSTL.Private.LAN.Int 255.255.255.128

```

```

ip directed-broadcast
ip nat inside
ip irdp
ip irdp maxadvertinterval 45
ip irdp minadvertinterval 30
ip irdp holdtime 135
ip mobile foreign-service
ip policy route-map mr_subnets
duplex auto
speed auto
!
interface Serial0/1
mtu 512
no ip address
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
no fair-queue
ignore-dcd
nrzi-encoding
!
interface Serial0/1.1 point-to-point
ip unnumbered FastEthernet0/0
no ip mroute-cache
no arp frame-relay
no cdp enable
frame-relay interface-dlci 17
!
router mobile
!
ip default-gateway vflatsat.FA_Inside_Network.Firewall
ip classless
ip route 0.0.0.0 0.0.0.0 vflatsat.FA_Inside_Network.Firewall
ip route 10.168.1.128 255.255.255.128 Serial0/0.1
ip route SSTL.Private.UK-DMC.OBC 255.255.255.248 Serial0/0.1
ip http server
ip mobile foreign-agent care-of FastEthernet0/0
!
access-list 7 permit vflatsat.MobNet.Aggregate 0.0.0.15
route-map mr_subnets permit 10
match ip address 7
set ip default next-hop 10.7.6.1
!
!
!
!
!
!
dial-peer cor custom
!
!
!
!
!
!
line con 0

```

```
exec-timeout 10000 0
line aux 0
line vty 0 4
exec-timeout 15 0
password vflatsat
login
!
end
```

F.6 Virtual Flatsat Mobile Router

```
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Virtual_Flatsat_at_NASA-GRC_in_Cleveland_Ohio
!
boot system flash:c3200-i11k9-mz.122-11.YQ
aaa new-model
!
!
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
enable password vflatsat
!
username vmoc password 0 VMOC
username sstl privilege 15 password 0 sstl55
ip subnet-zero
!
!
no ip domain lookup
!
ip audit notify log
ip audit po max-events 100
no crypto isakmp enable
!
!
!
!
interface Loopback0
ip address vflatsat.MobNet.Loopback0 255.255.255.255
!
interface FastEthernet0/0
ip address vflatsat.Mobnet.Net1.Int 255.255.255.248
duplex auto
speed auto
!
```

```

interface Serial1/0
no ip address
no ip proxy-arp
ip nat inside
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
ignore-dcd
nrzi-encoding
clockrate 2000000
!
interface Serial1/0.1 point-to-point
ip address vflatsat.ForeignService.Firewall255.255.255.252
ip mobile router-service roam
no ip mroute-cache
no cdp enable
frame-relay interface-dlci 17
!
    interface Serial1/1
no ip address
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
ignore-dcd
nrzi-encoding
clockrate 2000000
!
interface Serial1/1.1 point-to-point
ip address vflatsat.ForeignService.Firewall255.255.255.252
ip mobile router-service roam
frame-relay interface-dlci 17
!
interface Serial1/2
no ip address
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
ignore-dcd
nrzi-encoding
clockrate 2000000
!
interface Serial1/2.1 point-to-point
ip address 10.1.1.1 255.255.255.0
ip access-group 10 in
ip nat inside
frame-relay interface-dlci 17
!
interface Serial1/2.2 point-to-point
ip nat outside
no cdp enable
!

```

```

interface Serial1/3
mtu 512
no ip address
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
ignore-dcd
nrzi-encoding
clockrate 2000000
!
interface Serial1/3.1 point-to-point
frame-relay interface-dlci 17
!
router mobile
!
ip http server
ip http authentication local
ip classless
ip mobile secure home-agent HomeAgent.Net.HArouter spi 777 key ascii Phone-Home algorithm md5
mode prefix-suffix
ip mobile router
address vflatsat.MobNet.Loopback0 255.255.255.240
home-agent HomeAgent.Net.HArouter priority 105
register lifetime 60
!
!
!
radius-server retransmit 3
radius-server authorization permit missing Service-Type
!
line con 0
exec-timeout 10000 0
stopbits 1
line aux 0
line vty 0 4
password sst110
!
end

```

F.7 Engineering Model (EM) Flatsat Foreign Agent Ground Router

```

GSN_Rtr_EM#sh run
Building configuration...

```

```

Current configuration : 2938 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption

```



```

!
hostname GSN_Rtr_EM
! This is an emulation of the Surrey Ground Station Router (GSN_Rtr) that connects to the Satellite. This
configuration mirrors the configuration of said GSN_Rtr as closely as possible.
!
enable password xxxx
!
ip subnet-zero
!
no ip domain lookup
!
mta receive maximum-recipients 0
!
interface Tunnel7
description "MR subnets reach-back for triangular routing from CLEO_EM's (FlatSat) FA."
ip address 10.7.7.2 255.255.255.0
tunnel source FastEthernet0/0
tunnel destination HomeAgent.Net.HArouter
tunnel mode ipip
! Tunnel provides path back to Home Agent for packets with source address from Mobile Router's
subnets.
!
interface FastEthernet0/0
description connected to Groundstation Subnet 0
ip address EngModel.FA_Inside_Network.FArouter 255.255.255.128
ip nat outside
duplex auto
speed auto
! Interface provides Internet connectivity via firewall, This is also the outside interface for the Router's
Network Address Translation.
!
interface Serial0/0
no ip address
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
nrzi-encoding
clockrate 8000000
no fair-queue
! Interface provides connection to CLEO_EM (Flatsat) via Adtech Delay Simulator.
!
interface Serial0/0.1 point-to-point
ip unnumbered FastEthernet0/0
! This is a frame-relay sub-interface, it does not have an IP or MAC address.
ip nat inside
! Network Address Translation (NAT) inside interface to NAT CLEO_EM loopback0 interface
(SSTL.Private.CLEO_Loopback). This allows direct access to CLEO_EM even if Mobile Router
capabilities are not functioning.
ip irdp
ip irdp maxadvertinterval 10
ip irdp minadvertinterval 7

```

```

ip irdp holdtime 30
! Internet Router Discovery Protocol (IRDP) this is the mechanism used for the foreign agent (FA) to
send out advertisements for Mobile IP. Present config, advertisement will be sent out at least every 10
seconds, but not more than every 7 seconds, and the advertisement is good for 30 seconds.
ip mobile foreign-service
! Turns foreign agent advertising on this interface.
no ip mroute-cache
ip policy route-map mr_subnets
! Applies policy route "mr_subnets" to packets received on this interface.
no arp frame-relay
no cdp enable
frame-relay interface-dlci 17
!
interface FastEthernet0/1
description connected to Antenna0 LAN
ip address SSTL.Private.LAN.Int 255.255.255.0
ip directed-broadcast
ip nat inside
duplex auto
speed auto
! The operations workstations (Data & telemetry) are located in private address space on this interface,
and NATed to the public address space of interface Fa0/0.
!
interface Serial0/1
mtu 512
no ip address
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
ignore-dcd
nrzi-encoding
no fair-queue
!
interface Serial0/1.1 point-to-point
ip unnumbered FastEthernet0/0
no ip mroute-cache
no arp frame-relay
no cdp enable
frame-relay interface-dlci 17
! Unused interface.
!
router mobile
! Enable Mobile IP.
!
router rip
redistribute mobile
passive-interface Serial0/0
network SSTL.Public_Inside.Network
!
ip default-gateway EngModel.FA.Inside_Network.Firewall
! Default Gateway for packets originating from this router (i.e. Telnet from console port).

```

```

ip nat inside source static SSTL.Private.WS1 EngModel.FA.Inside_Network.WS1
ip nat inside source static SSTL.Private.WS2 EngModel.FA.Inside_Network.WS2
ip nat inside source static SSTL.Private.WS3 EngModel.FA.Inside_Network.WS3
! NAT statements for hosts residing on interface Fa 0/1.
!
ip nat inside source static SSTL.Private.CLEO_Loopback
EngModel.FA.Inside_Network.CLEO_Loopback0
! NAT statement for CLEO_EM direct access Loopback0 interface.
!
ip classless
ip route 0.0.0.0 0.0.0.0 EngModel.FA.Inside_Network.Firewall
! Default route for router's Routing Table (i.e. Where the router sends a received packet when none of the
other routing entries apply.).
!
ip route EngModel.FA.Inside_Network.WS1 255.255.255.255 FastEthernet0/1
ip route EngModel.FA.Inside_Network.WS2 255.255.255.255 FastEthernet0/1
ip route EngModel.FA.Inside_Network.WS3 255.255.255.255 FastEthernet0/1
ip route EngModel.FA.Inside_Network.CLEO_Loopback0 255.255.255.255 Serial0/0.1
! Static routes for NATed addresses.
!
ip route SSTL.Private.UK-DMC.OBC 255.255.255.255 Serial0/0.1
ip route SSTL.Private.UK-DMC.SSDR0 255.255.255.255 Serial0/0.1
ip route SSTL.Private.UK-DMC.SSDR1 255.255.255.255 Serial0/0.1
ip route SSTL.Private.UK-DMC.SSDR2 255.255.255.255 Serial0/0.1
ip route SSTL.Private.UK-DMC.OBC 255.255.255.255 Serial0/0.1
ip route SSTL.Private.CLEO_Loopback 255.255.255.255 Serial0/0.1
! Static routes for direct access of SSDRs, OBC and onboard router.
!
ip http server
! Enable Router's Web Server.
!
ip mobile foreign-agent care-of FastEthernet0/0
! Enable foreign agent Services and use IP address of Fa0/0 as the care-of-address (COA).
!
access-list 7 permit CLEO.MobNet.Aggregate 0.0.0.31
access-list 7 permit EngModel.MobNet.Aggregate 0.0.0.31
! Access list for Policy Route "mr_subnets"
!
route-map mr_subnets permit 10
  match ip address 7
  set ip default next-hop 10.7.7.1
! Policy Route definition that takes packets originating from CLEO_EM (access list 7) on interface
Serial0/0 and forward them to the Home Agent (HA) via Tunnel7 (10.7.7.1).
!
call rsvp-sync
!
mgcp profile default

!
dial-peer cor custom
!

```

```
line con 0
  exec-timeout 30 0
line aux 0
line vty 0 4
  exec-timeout 30 0
  password xxxx
  login
!
!
end
```

F.8 Engineering Model Flatsat Mobile Router (CLEO_EM)

```
CLEO_EM#sh run
Current configuration : 2845 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CLEO_EM
!
aaa new-model
!
aaa authorization exec default local
aaa session-id common
enable secret 5 $1$MSTIS$UimCca/SF.DWMimW0OVtH0
enable password sstl1
!
username VMOC password 0 VMOC
username sstl privilege 15 password 0 sstl55
clock timezone EDT -5
ip subnet-zero
!
no ip domain lookup
ip domain name CLEO-EM.sstl.com
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 60
ip ssh authentication-retries 2
!
interface Loopback0
ip address SSTL.Private.CLEO_Loopback 255.255.255.255
!
interface Loopback1
ip address EngModel.MobNet.Loopback.Addr 255.255.255.255
!
interface FastEthernet0/0
```

```

no ip address
shutdown
duplex auto
speed auto
!
interface Serial1/0
no ip address
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
ignore-dcd
nrzi-encoding
!
interface Serial1/0.1 point-to-point
ip address EngModel.MobNet.S1/0.Int 255.255.255.252
ip mobile router-service roam
no ip mroute-cache
frame-relay interface-dlci 17
!
interface Serial1/1
no ip address
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
ignore-dcd
nrzi-encoding
!
interface Serial1/1.1 point-to-point
ip address EngModel.MobNet.S1/1.Int 255.255.255.248
ip access-group 110 in
ip mobile router-service roam
ip mobile router-service solicit interval 20
no ip mroute-cache
frame-relay interface-dlci 17
!
interface Serial1/2
mtu 512
no ip address
encapsulation frame-relay IETF
no ip route-cache
no ip mroute-cache
no keepalive
ignore-dcd
nrzi-encoding
!
interface Serial1/2.1 point-to-point
ip address EngModel.MobNet.S1/2.Int 255.255.255.252
ip mobile router-service roam
no ip route-cache
no ip mroute-cache
frame-relay interface-dlci 17

```

```

!
interface Serial1/3
ip address EngModel.MobNet.S1/3.Int 255.255.255.248
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
ignore-dcd
nrzi-encoding
!
interface Serial1/3.1 point-to-point
no ip mroute-cache
frame-relay interface-dlci 17
!
router mobile
!
ip http server
ip http authentication local
ip classless
ip route 0.0.0.0 0.0.0.0 Serial1/1.1 245
ip route SSTL.Private.UK-DMC.SSDR0 255.255.255.255 Serial1/0.1
ip route SSTL.Private.UK-DMC.SSDR2 255.255.255.255 Serial1/2.1
ip mobile secure home-agent HomeAgent.Net.HArouter spi 666 key ascii Phone-Home algorithm md5
mode prefix-suffix
ip mobile router
address EngModel.MobNet.Loopback.Addr 255.255.255.224
home-agent HomeAgent.Net.HArouter priority 105
register lifetime 60
!
!
access-list 10 deny SSTL.Private.UK-DMC.OBC
access-list 10 permit any
access-list 110 deny ip any host SSTL.Private.UK-DMC.OBC log
access-list 110 permit ip any any
radius-server retransmit 3
radius-server authorization permit missing Service-Type
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
line vty 0 4
exec-timeout 45 0
password sstl10

```

F.9 Engineering Model Flatsat Router—MR_Frame_Relay_Router

```

Mboy#sh run
Building configuration...

```

```

Current configuration : 1607 bytes

```

```

!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Mboy
!
boot system slot0:c3640-is-mz_CoCOA_sm
!
ip subnet-zero
!
!
!
frame-relay switching
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
bridge irb
!
!
!
interface Serial0/0
no ip address
encapsulation frame-relay IETF
no keepalive
serial restart_delay 0
nrzi-encoding
clockrate 8064000
dce-terminal-timing-enable
frame-relay intf-type nni
frame-relay route 20 interface Serial1/0 17
!
interface Serial0/1
no ip address
shutdown
serial restart_delay 0
no cdp enable
!
interface Serial0/2
no ip address
shutdown
serial restart_delay 0
no cdp enable
!
interface Serial0/3

```

```

no ip address
shutdown
serial restart_delay 0
no cdp enable
!
interface Serial1/0
no ip address
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
no fair-queue
serial restart_delay 0
nrzi-encoding
frame-relay route 17 interface Serial0/0 20
!
interface Serial1/1
no ip address
shutdown
serial restart_delay 0
no cdp enable
!
interface Serial1/2
no ip address
shutdown
serial restart_delay 0
no cdp enable
!
interface Serial1/3
no ip address
shutdown
serial restart_delay 0
no cdp enable
!
ip classless
no ip http server
ip pim bidir-enable
!
!
no cdp run
!
call rsvp-sync
!
voice-port 2/0/0
!
voice-port 2/0/1
!
voice-port 2/1/0
!
voice-port 2/1/1
!
!

```



```

mgcp profile default
!
dial-peer cor custom
!
!
!
line con 0
exec-timeout 10000 0
line aux 0
line vty 0 4
login
!
!
end

```

F.10 Engineering Model Flatsat Router—FA_Frame_Relay_Router

```

Fboy#sh run
Current configuration : 1505 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Fboy
!
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
frame-relay switching
!
no voice hpi capture buffer
no voice hpi capture destination
!
bridge irb
!
interface Serial0/0
no ip address
encapsulation frame-relay IETF
no keepalive
serial restart-delay 0
nrzi-encoding
clockrate 9600
dce-terminal-timing-enable

```

```

frame-relay intf-type nni
frame-relay route 20 interface Serial1/0 17
!
interface Serial0/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial0/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial0/3
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/0
no ip address
no ip proxy-arp
encapsulation frame-relay IETF
no ip mroute-cache
no keepalive
serial restart-delay 0
nrzi-encoding
frame-relay route 17 interface Serial0/0 20
!
interface Serial1/1
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
interface FastEthernet2/0
no ip address
shutdown
duplex auto
speed auto
!
interface Hssi3/0
no ip address

```

```
shutdown
serial restart-delay 0
!
no ip http server
ip classless
!
dial-peer cor custom
!
line con 0
exec-timeout 10000 0
line aux 0
line vty 0 4
password cisco
login
!
!
!
end
```


Appendix G

Mobile Router Debug Captures for First Space-Based Mobile Network Session

The following is a capture of mobile networking debug monitoring at the home agent router from section 11.2, “Mobile Routing Results”:

```
MR Tunnell src HomeAgent.Net.HARouter dest CLEO.MobNet.Loopback.Addr reverse-allowed
Routing Options -
Service Options - MN registered using
Mobile Networks: CLEO.MobNet.Aggregate/255.255.255.252 (S)
CLEO.MobNet.S1/2.Net/255.255.255.252 (S)
CLEO.MobNet.S1/1.Net/255.255.255.248 (S)
CLEO.MobNet.S1/3.Net/255.255.255.252 (S)
CLEO.MobNet.S1/4.Net/255.255.255.248 (S)
CLEO_HA#
May 28 11:02:50.173: MobileIP: ParseRegExt type MHAE(32) addr 7C00ECC end 7C00EE2
May 28 11:02:50.173: MobileIP: ParseRegExt skipping 20 to next
May 28 11:02:50.173: MobileIP: HA 112 rcv registration for MN CLEO.MobNet.Loopback.Addr on
FastEthernet0/0 using HomeAddr CLEO.MobNet.Loopback.Addr COA SSTL.Public_Inside.FARouter
HA HomeAgent.Net.HARouter lifetime 60 options sbdmg-t-
May 28 11:02:50.173: MobileIP: Authenticating MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:02:50.173: MobileIP: Authentication algorithm MD5
May 28 11:02:50.173: MobileIP: Authenticated MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:02:50.173: MobileIP: Mobility binding for MN CLEO.MobNet.Loopback.Addr updated
May 28 11:02:50.173: MobileIP: Roam timer started for MN CLEO.MobNet.Loopback.Addr using
CLEO.MobNet.Loopback.Addr, lifetime 60
May 28 11:02:50.173: MobileIP: HA accepts registration from MN CLEO.MobNet.Loopback.Addr
May 28 11:02:50.173: MobileIP: Authentication algorithm MD5
May 28 11:02:50.173: MobileIP: MN CLEO.MobNet.Loopback.Addr MHAE added (SPI 666) to MN
CLEO.MobNet.Loopback.Addr
May 28 11:02:50.177: MobileIP: MN CLEO.MobNet.Loopback.Addr - HA sent reply to
SSTL.Public_Inside.FARouter
May 28 11:03:20.449: MobileIP: ParseRegExt type MHAE(32) addr 7DFFF2C end 7DFFF42
May 28 11:03:20.449: MobileIP: ParseRegExt skipping 20 to next
May 28 11:03:20.449: MobileIP: HA 112 rcv registration for MN CLEO.MobNet.Loopback.Addr on
FastEthernet0/0 using HomeAddr CLEO.MobNet.Loopback.Addr COA SSTL.Public_Inside.FARouter
HA HomeAgent.Net.HARouter lifetime 60 options sbdmg-t-
May 28 11:03:20.449: MobileIP: Authenticating MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:03:20.449: MobileIP: Authentication algorithm MD5
May 28 11:03:20.449: MobileIP: Authenticated MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:03:20.449: MobileIP: Mobility binding for MN CLEO.MobNet.Loopback.Addr updated
May 28 11:03:20.449: MobileIP: Roam timer started for MN CLEO.MobNet.Loopback.Addr using
CLEO.MobNet.Loopback.Addr, lifetime 60
May 28 11:03:20.449: MobileIP: HA accepts registration from MN CLEO.MobNet.Loopback.Addr
May 28 11:03:20.449: MobileIP: Authentication algorithm MD5
May 28 11:03:20.449: MobileIP: MN CLEO.MobNet.Loopback.Addr MHAE added (SPI 666) to MN
CLEO.MobNet.Loopback.Addr
May 28 11:03:20.449: MobileIP: MN CLEO.MobNet.Loopback.Addr - HA sent reply to
SSTL.Public_Inside.FARouter
```

May 28 11:03:50.720: MobileIP: ParseRegExt type MHAЕ(32) addr 7DFFDEC end 7DFFE02
May 28 11:03:50.720: MobileIP: ParseRegExt skipping 20 to next
May 28 11:03:50.724: MobileIP: HA 112 rcv registration for MN CLEO.MobNet.Loopback.Addr on FastEthernet0/0 using HomeAddr CLEO.MobNet.Loopback.Addr COA SSTL.Public_Inside.FARouter HA HomeAgent.Net.HARouter lifetime 60 options sbdmg-t-
May 28 11:03:50.724: MobileIP: Authenticating MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:03:50.724: MobileIP: Authentication algorithm MD5
May 28 11:03:50.724: MobileIP: Authenticated MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:03:50.724: MobileIP: Mobility binding for MN CLEO.MobNet.Loopback.Addr updated
May 28 11:03:50.724: MobileIP: Roam timer started for MN CLEO.MobNet.Loopback.Addr using CLEO.MobNet.Loopback.Addr, lifetime 60
May 28 11:03:50.724: MobileIP: HA accepts registration from MN CLEO.MobNet.Loopback.Addr
May 28 11:03:50.724: MobileIP: Authentication algorithm MD5
May 28 11:03:50.724: MobileIP: MN CLEO.MobNet.Loopback.Addr MHAЕ added (SPI 666) to MN CLEO.MobNet.Loopback.Addr
May 28 11:03:50.724: MobileIP: MN CLEO.MobNet.Loopback.Addr - HA sent reply to SSTL.Public_Inside.FARouter
May 28 11:04:20.996: MobileIP: ParseRegExt type MHAЕ(32) addr 7C00D8C end 7C00DA2
May 28 11:04:20.996: MobileIP: ParseRegExt skipping 20 to next
May 28 11:04:20.996: MobileIP: HA 112 rcv registration for MN CLEO.MobNet.Loopback.Addr on FastEthernet0/0 using HomeAddr CLEO.MobNet.Loopback.Addr COA SSTL.Public_Inside.FARouter HA HomeAgent.Net.HARouter lifetime 60 options sbdmg-t-
May 28 11:04:20.996: MobileIP: Authenticating MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:04:21.000: MobileIP: Authentication algorithm MD5
May 28 11:04:21.000: MobileIP: Authenticated MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:04:21.000: MobileIP: Mobility binding for MN CLEO.MobNet.Loopback.Addr updated
May 28 11:04:21.000: MobileIP: Roam timer started for MN CLEO.MobNet.Loopback.Addr using CLEO.MobNet.Loopback.Addr, lifetime 60
May 28 11:04:21.000: MobileIP: HA accepts registration from MN CLEO.MobNet.Loopback.Addr
May 28 11:04:21.000: MobileIP: Authentication algorithm MD5
May 28 11:04:21.000: MobileIP: MN CLEO.MobNet.Loopback.Addr MHAЕ added (SPI 666) to MN CLEO.MobNet.Loopback.Addr
May 28 11:04:21.000: MobileIP: MN CLEO.MobNet.Loopback.Addr - HA sent reply to SSTL.Public_Inside.FARouter
May 28 11:04:51.271: MobileIP: ParseRegExt type MHAЕ(32) addr 7E001AC end 7E001C2
May 28 11:04:51.271: MobileIP: ParseRegExt skipping 20 to next
May 28 11:04:51.271: MobileIP: HA 112 rcv registration for MN CLEO.MobNet.Loopback.Addr on FastEthernet0/0 using HomeAddr CLEO.MobNet.Loopback.Addr COA SSTL.Public_Inside.FARouter HA HomeAgent.Net.HARouter lifetime 60 options sbdmg-t-
May 28 11:04:51.271: MobileIP: Authenticating MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:04:51.271: MobileIP: Authentication algorithm MD5
May 28 11:04:51.271: MobileIP: Authenticated MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:04:51.271: MobileIP: Mobility binding for MN CLEO.MobNet.Loopback.Addr updated
May 28 11:04:51.275: MobileIP: Roam timer started for MN CLEO.MobNet.Loopback.Addr using CLEO.MobNet.Loopback.Addr, lifetime 60
May 28 11:04:51.275: MobileIP: HA accepts registration from MN CLEO.MobNet.Loopback.Addr
May 28 11:04:51.275: MobileIP: Authentication algorithm MD5
May 28 11:04:51.275: MobileIP: MN CLEO.MobNet.Loopback.Addr MHAЕ added (SPI 666) to MN CLEO.MobNet.Loopback.Addr
May 28 11:04:51.275: MobileIP: MN CLEO.MobNet.Loopback.Addr - HA sent reply to SSTL.Public_Inside.FARouter

May 28 11:05:21.551: MobileIP: ParseRegExt type MHAE(32) addr 7C01A0C end 7C01A22
May 28 11:05:21.551: MobileIP: ParseRegExt skipping 20 to next
May 28 11:05:21.551: MobileIP: HA 112 rcv registration for MN CLEO.MobNet.Loopback.Addr on FastEthernet0/0 using HomeAddr CLEO.MobNet.Loopback.Addr COA SSTL.Public_Inside.FARouter HA HomeAgent.Net.HARouter lifetime 60 options sbdmg-t-
May 28 11:05:21.551: MobileIP: Authenticating MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:05:21.551: MobileIP: Authentication algorithm MD5
May 28 11:05:21.551: MobileIP: Authenticated MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:05:21.551: MobileIP: Mobility binding for MN CLEO.MobNet.Loopback.Addr updated
May 28 11:05:21.551: MobileIP: Roam timer started for MN CLEO.MobNet.Loopback.Addr using CLEO.MobNet.Loopback.Addr, lifetime 60
May 28 11:05:21.555: MobileIP: HA accepts registration from MN CLEO.MobNet.Loopback.Addr
May 28 11:05:21.555: MobileIP: Authentication algorithm MD5
May 28 11:05:21.555: MobileIP: MN CLEO.MobNet.Loopback.Addr MHAE added (SPI 666) to MN CLEO.MobNet.Loopback.Addr
May 28 11:05:21.555: MobileIP: MN CLEO.MobNet.Loopback.Addr - HA sent reply to SSTL.Public_Inside.FARouter
May 28 11:05:51.831: MobileIP: ParseRegExt type MHAE(32) addr 7C009CC end 7C009E2
May 28 11:05:51.831: MobileIP: ParseRegExt skipping 20 to next
May 28 11:05:51.831: MobileIP: HA 112 rev registration for MN CLEO.MobNet.Loopback.Addr on FastEthernet0/0 using HomeAddr CLEO.MobNet.Loopback.Addr COA SSTL.Public_Inside.FARouter HA HomeAgent.Net.HARouter lifetime 60 options sbdmg-t-
May 28 11:05:51.831: MobileIP: Authenticating MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:05:51.831: MobileIP: Authentication algorithm MD5
May 28 11:05:51.831: MobileIP: Authenticated MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:05:51.831: MobileIP: Mobility binding for MN CLEO.MobNet.Loopback.Addr updated
May 28 11:05:51.831: MobileIP: Roam timer started for MN CLEO.MobNet.Loopback.Addr using CLEO.MobNet.Loopback.Addr, lifetime 60
May 28 11:05:51.831: MobileIP: HA accepts registration from MN CLEO.MobNet.Loopback.Addr
May 28 11:05:51.835: MobileIP: Authentication algorithm MD5
May 28 11:05:51.835: MobileIP: MN CLEO.MobNet.Loopback.Addr MHAE added (SPI 666) to MN CLEO.MobNet.Loopback.Addr
May 28 11:05:51.835: MobileIP: MN CLEO.MobNet.Loopback.Addr - HA sent reply to SSTL.Public_Inside.FARouter
May 28 11:06:22.110: MobileIP: ParseRegExt type MHAE(32) addr 7DFF52C end 7DFF542
May 28 11:06:22.110: MobileIP: ParseRegExt skipping 20 to next
May 28 11:06:22.110: MobileIP: HA 112 rcv registration for MN CLEO.MobNet.Loopback.Addr on FastEthernet0/0 using HomeAddr CLEO.MobNet.Loopback.Addr COA SSTL.Public_Inside.FARouter HA HomeAgent.Net.HARouter lifetime 60 options sbdmg-t-
May 28 11:06:22.110: MobileIP: Authenticating MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:06:22.110: MobileIP: Authentication algorithm MD5
May 28 11:06:22.110: MobileIP: Authenticated MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:06:22.110: MobileIP: Mobility binding for MN CLEO.MobNet.Loopback.Addr updated
May 28 11:06:22.110: MobileIP: Roam timer started for MN CLEO.MobNet.Loopback.Addr using CLEO.MobNet.Loopback.Addr, lifetime 60
May 28 11:06:22.110: MobileIP: HA accepts registration from MN CLEO.MobNet.Loopback.Addr
May 28 11:06:22.110: MobileIP: Authentication algorithm MD5
May 28 11:06:22.110: MobileIP: MN CLEO.MobNet.Loopback.Addr MHAE added (SPI 666) to MN CLEO.MobNet.Loopback.Addr
May 28 11:06:22.110: MobileIP: MN CLEO.MobNet.Loopback.Addr - HA sent reply to SSTL.Public_Inside.FARoutersho ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is HomeAgent.Net.Firewall_Inside to network 0.0.0.0

GRC.OpenNet/24 is variably subnetted, 9 subnets, 5 masks
M vflatsat.MobNet.Aggregate/28 is directly connected, Mobile0
M CLEO.MobNet.S1/1.Net/29 [3/1] via 0.0.0.0, 00:07:52, Tunnel1
M CLEO.MobNet.S1/2.Net/30 [3/1] via 0.0.0.0, 00:07:52, Tunnel1
M CLEO.MobNet.Aggregate/30 [3/1] via 0.0.0.0, 00:07:52, Tunnel1
M CLEO.MobNet.Aggregate/27 is directly connected, Mobile0
M CLEO.MobNet.S1/4.Net/29 [3/1] via 0.0.0.0, 00:07:52, Tunnel1
M CLEO.MobNet.Loopback.Addr/32 [3/1] via SSTL.Public_Inside.FARouter, 00:07:52, Tunnel2
M CLEO.MobNet.S1/3.Net/30 [3/1] via 0.0.0.0, 00:07:52, Tunnel1
C HomeAgent.Net/29 is directly connected, FastEthernet0/0
10.0.0.0/24 is subnetted, 4 subnets
C 10.7.8.0 is directly connected, Tunnel8
C 10.7.7.0 is directly connected, Tunnel7
C 10.7.6.0 is directly connected, Tunnel6
C 10.7.76.0 is directly connected, Tunnel76
S SSTL.Private.0/24 [1/0] via HomeAgent.Net.Firewall_Inside
S* 0.0.0.0/0 [1/0] via HomeAgent.Net.Firewall_Inside
CLEO_HA#
CLEO_HA#pin
May 28 11:06:52.386: MobileIP: ParseRegExt type MHAE(32) addr 7DFFF2C end 7DFFF42
May 28 11:06:52.386: MobileIP: ParseRegExt skipping 20 to next
May 28 11:06:52.390: MobileIP: HA 112 rcv registration for MN CLEO.MobNet.Loopback.Addr on
FastEthernet0/0 using HomeAddr CLEO.MobNet.Loopback.Addr COA SSTL.Public_Inside.FARouter
HA HomeAgent.Net.HARouter lifetime 60 options sbdmg-t-
May 28 11:06:52.390: MobileIP: Authenticating MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:06:52.390: MobileIP: Authentication algorithm MD5
May 28 11:06:52.390: MobileIP: Authenticated MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:06:52.390: MobileIP: Mobility binding for MN CLEO.MobNet.Loopback.Addr updatedg 1
May 28 11:06:52.390: MobileIP: Roam timer started for MN CLEO.MobNet.Loopback.Addr using
CLEO.MobNet.Loopback.Addr, lifetime 60
May 28 11:06:52.390: MobileIP: HA accepts registration from MN CLEO.MobNet.Loopback.Addr
May 28 11:06:52.390: MobileIP: Authentication algorithm MD5
May 28 11:06:52.390: MobileIP: Authenticated MN CLEO.MobNet.Loopback.Addr using SPI 666
May 28 11:06:52.390: MobileIP: Mobility binding for MN CLEO.MobNet.Loopback.Addr updatedg 1
May 28 11:06:52.390: MobileIP: Roam timer started for MN CLEO.MobNet.Loopback.Addr using
CLEO.MobNet.Loopback.Addr, lifetime 60
May 28 11:06:52.390: MobileIP: HA accepts registration from MN CLEO.MobNet.Loopback.Addr
May 28 11:06:52.390: MobileIP: Authentication algorithm MD5
May 28 11:06:52.390: MobileIP: MN CLEO.MobNet.Loopback.Addr MHAE added (SPI 666) to MN
CLEO.MobNet.Loopback.Addr

May 28 11:06:52.390: MobileIP: MN CLEO.MobNet.Loopback.Addr - HA sent reply to SSTL.Public_Inside.FARouter92.55.90.245

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to CLEO.MobNet.Loopback.Addr, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 292/293/296 ms

CLEO_HA#

May 28 11:07:22.666: MobileIP: ParseRegExt type MHAЕ(32) addr 7E00E2C end 7E00E42

May 28 11:07:22.666: MobileIP: ParseRegExt skipping 20 to next

May 28 11:07:22.666: MobileIP: HA 112 rev registration for MN CLEO.MobNet.Loopback.Addr on FastEthernet0/0 using HomeAddr CLEO.MobNet.Loopback.Addr COA SSTL.Public_Inside.FARouter HA HomeAgent.Net.HARouter lifetime 60 options sbdmg-t-

May 28 11:07:22.670: MobileIP: Authenticating MN CLEO.MobNet.Loopback.Addr using SPI 666

May 28 11:07:22.670: MobileIP: Authentication algorithm MD5

May 28 11:07:22.670: MobileIP: Authenticated MN CLEO.MobNet.Loopback.Addr using SPI 666

May 28 11:07:22.670: MobileIP: Mobility binding for MN CLEO.MobNet.Loopback.Addr updated

May 28 11:07:22.670: MobileIP: Roam timer started for MN CLEO.MobNet.Loopback.Addr using CLEO.MobNet.Loopback.Addr, lifetime 60

May 28 11:07:22.670: MobileIP: HA accepts registration from MN CLEO.MobNet.Loopback.Addr

May 28 11:07:22.670: MobileIP: Authentication algorithm MD5

May 28 11:07:22.670: MobileIP: MN CLEO.MobNet.Loopback.Addr MHAЕ added (SPI 666) to MN CLEO.MobNet.Loopback.Addr

May 28 11:07:22.670: MobileIP: MN CLEO.MobNet.Loopback.Addr - HA sent reply to SSTL.Public_Inside.FARouter

May 28 11:07:52.950: MobileIP: ParseRegExt type MHAЕ(32) addr 7C004CC end 7C004E2

May 28 11:07:52.950: MobileIP: ParseRegExt skipping 20 to next

May 28 11:07:52.950: MobileIP: HA 112 rev registration for MN CLEO.MobNet.Loopback.Addr on FastEthernet0/0 using HomeAddr CLEO.MobNet.Loopback.Addr COA SSTL.Public_Inside.FARouter HA HomeAgent.Net.HARouter lifetime 60 options sbdmg-t-

May 28 11:07:52.950: MobileIP: Authenticating MN CLEO.MobNet.Loopback.Addr using SPI 666

May 28 11:07:52.950: MobileIP: Authentication algorithm MD5

May 28 11:07:52.950: MobileIP: Authenticated MN CLEO.MobNet.Loopback.Addr using SPI 666

May 28 11:07:52.950: MobileIP: Mobility binding for MN CLEO.MobNet.Loopback.Addr updated

May 28 11:07:52.950: MobileIP: Roam timer started for MN CLEO.MobNet.Loopback.Addr using CLEO.MobNet.Loopback.Addr, lifetime 60

May 28 11:07:52.950: MobileIP: HA accepts registration from MN CLEO.MobNet.Loopback.Addr

May 28 11:07:52.950: MobileIP: Authentication algorithm MD5

May 28 11:07:52.950: MobileIP: MN CLEO.MobNet.Loopback.Addr MHAЕ added (SPI 666) to MN CLEO.MobNet.Loopback.Addr

May 28 11:07:52.954: MobileIP: MN CLEO.MobNet.Loopback.Addr - HA sent reply to SSTL.Public_Inside.FARouter

CLEO_HA#

May 28 11:08:23.230: MobileIP: ParseRegExt type MHAЕ(32) addr 7E002EC end 7E00302

May 28 11:08:23.230: MobileIP: ParseRegExt skipping 20 to next

May 28 11:08:23.230: MobileIP: HA 112 rev registration for MN CLEO.MobNet.Loopback.Addr on FastEthernet0/0 using HomeAddr CLEO.MobNet.Loopback.Addr COA SSTL.Public_Inside.FARouter HA HomeAgent.Net.HARouter lifetime 60 options sbdmg-t-

May 28 11:08:23.230: MobileIP: Authenticating MN CLEO.MobNet.Loopback.Addr using SPI 666

May 28 11:08:23.230: MobileIP: Authentication algorithm MD5

May 28 11:08:23.230: MobileIP: Authenticated MN CLEO.MobNet.Loopback.Addr using SPI 666

May 28 11:08:23.234: MobileIP: Mobility binding for MN CLEO.MobNet.Loopback.Addr updated
May 28 11:08:23.234: MobileIP: Roam timer started for MN CLEO.MobNet.Loopback.Addr using
CLEO.MobNet.Loopback.Addr, lifetime 60
May 28 11:08:23.234: MobileIP: HA accepts registration from MN CLEO.MobNet.Loopback.Addr
May 28 11:08:23.234: MobileIP: Authentication algorithm MD5
May 28 11:08:23.234: MobileIP: MN CLEO.MobNet.Loopback.Addr MHAЕ added (SPI 666) to MN
CLEO.MobNet.Loopback.Addr
May 28 11:08:23.234: MobileIP: MN CLEO.MobNet.Loopback.Addr - HA sent reply to
SSTL.Public_Inside.FARouter
May 28 11:09:23.234: MobileIP: Roam timer expired for MN CLEO.MobNet.Loopback.Addr
May 28 11:09:23.234: MobileIP: MN CLEO.MobNet.Loopback.Addr Delete tunnel route
CLEO.MobNet.Loopback.Addr/255.255.255.255 via gateway SSTL.Public_Inside.FARouter
May 28 11:09:23.234: MobileIP: Deleted Tunnel2 src HomeAgent.Net.HARouter dest
SSTL.Public_Inside.FARouter
May 28 11:09:23.234: MobileIP: MN CLEO.MobNet.Loopback.Addr Delete tunnel route
CLEO.MobNet.Aggregate/255.255.255.252 via gateway 0.0.0.0
May 28 11:09:23.234: MobileIP: MN CLEO.MobNet.Loopback.Addr Delete tunnel route
CLEO.MobNet.S1/2.Net/255.255.255.252 via gateway 0.0.0.0
May 28 11:09:23.234: MobileIP: MN CLEO.MobNet.Loopback.Addr Delete tunnel route
CLEO.MobNet.S1/1.Net/255.255.255.248 via gateway 0.0.0.0
May 28 11:09:23.238: MobileIP: MN CLEO.MobNet.Loopback.Addr Delete tunnel route
CLEO.MobNet.S1/3.Net/255.255.255.252 via gateway 0.0.0.0
May 28 11:09:23.238: MobileIP: MN CLEO.MobNet.Loopback.Addr Delete tunnel route
CLEO.MobNet.S1/4.Net/255.255.255.248 via gateway 0.0.0.0
May 28 11:09:23.238: MobileIP: Deleted Tunnel1 src HomeAgent.Net.HARouter dest
CLEO.MobNet.Loopback.Addr

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (<i>Leave blank</i>)	2. REPORT DATE May 2005	3. REPORT TYPE AND DATES COVERED Technical Memorandum	
4. TITLE AND SUBTITLE Secure, Network-Centric Operations of a Space-Based Asset: Cisco Router in Low Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC)		5. FUNDING NUMBERS WBS-22-258-70-03	
6. AUTHOR(S) William Ivancic, Dave Stewart, Dan Shell, Lloyd Wood, Phil Paulsen, Chris Jackson, Dave Hodgson, James Northam, Neville Bean, Eric Miller, Mark Graves, and Lance Kurisaki		8. PERFORMING ORGANIZATION REPORT NUMBER E-14999	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) National Aeronautics and Space Administration John H. Glenn Research Center at Lewis Field Cleveland, Ohio 44135-3191		10. SPONSORING/MONITORING AGENCY REPORT NUMBER NASA TM-2005-213556	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) National Aeronautics and Space Administration Washington, DC 20546-0001		11. SUPPLEMENTARY NOTES William Ivancic and Phil Paulsen, NASA Glenn Research Center; Dave Stewart, Verizon Federal Network Systems, Cleveland, Ohio 44135; Dan Shell, Cisco Systems, Inc., Richfield, Ohio 44286; Lloyd Wood, Cisco Systems, Inc., Bedford 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; and Mark Graves and Lance Kurisaki, General Dynamics Advanced Information Systems, Los Angeles, California 90045. Responsible person, William Ivancic, organization code RCN, 216-433-3494.	
12a. DISTRIBUTION/AVAILABILITY STATEMENT Unclassified - Unlimited Subject Category: 17 Available electronically at http://gltrs.grc.nasa.gov This publication is available from the NASA Center for AeroSpace Information, 301-621-0390.		12b. DISTRIBUTION CODE	
13. ABSTRACT (<i>Maximum 200 words</i>) This report documents the design of network infrastructure to support operations demonstrating the concept of network-centric operations and command and control of space-based assets. These demonstrations showcase major elements of the Transformal Communication Architecture (TCA), using Internet Protocol (IP) technology. These demonstrations also rely on IP technology to perform the functions outlined in the Consultative Committee for Space Data Systems (CCSDS) Space Link Extension (SLE) document. A key element of these demonstrations was the ability to securely use networks and infrastructure owned and/or controlled by various parties. This is a sanitized technical report for public release. There is a companion report available to a limited audience. The companion report contains detailed networking addresses and other sensitive material and is available directly from William Ivancic at Glenn Research Center.			
14. SUBJECT TERMS Satellite; Information security; Network		15. NUMBER OF PAGES 111	
		16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT

