NASA/TM—2008-215203

IPv6 and IPsec Tests of a Space-Based Asset, the Cisco Router in Low Earth Orbit (CLEO)

William Ivancic
Glenn Research Center, Cleveland, Ohio

David Stewart
Verizon Federal Network Systems, Cleveland, Ohio

Lloyd Wood
Cisco Systems Global Government Solutions, Bedfont Lakes, London

Chris Jackson, James Northam, and James Wilhelm
Surrey Satellite Technology Limited, Guildford,United Kingdom

May 2008

NASA STI Program . . . 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 plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and 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 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 also include creating custom thesauri, building customized databases, organizing and publishing research results.

For more information about the NASA STI program, 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 STI Help Desk at 301–621–0134

- Telephone the NASA STI Help Desk at 301–621–0390

- Write to:
  NASA Center for AeroSpace Information (CASI)
  7115 Standard Drive
  Hanover, MD 21076–1320

NASA/TM—2008-215203

IPv6 and IPsec Tests of a Space-Based Asset, the Cisco Router in Low Earth Orbit (CLEO)

William Ivancic
Glenn Research Center, Cleveland, Ohio

David Stewart
Verizon Federal Network Systems, Cleveland, Ohio

Lloyd Wood
Cisco Systems Global Government Solutions, Bedfont Lakes, London

Chris Jackson, James Northam, and James Wilhelm
Surrey Satellite Technology Limited, Guildford,United Kingdom

National Aeronautics and
Space Administration

Glenn Research Center
Cleveland, Ohio 44135

May 2008

Acknowledgments

The primary authors would like to thank all those who contributed to this project's success 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.

Level of Review: This material has been technically reviewed by technical management.

Available from

NASA Center for Aerospace Information
7115 Standard Drive
Hanover, MD 21076–1320

National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161

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

IPv6 and IPsec Tests of a Space-Based Asset, the Cisco router in Low Earth Orbit (CLEO)

Abstract

This report documents the design of network infrastructure to support testing and demonstrating network-centric operations and command and control of space-based assets, using IPv6 and IPsec. These tests were performed using the Cisco router in Low Earth Orbit (CLEO), an experimental payload onboard the United Kingdom – Disaster Monitoring Constellation (UK-DMC) satellite built and operated by Surrey Satellite Technology Ltd (SSTL). On Thursday, 29 March 2007, NASA Glenn Research Center, Cisco Systems and SSTL performed the first configuration and demonstration of IPsec and IPv6 onboard a satellite in low Earth orbit. IPv6 is the next generation of the Internet Protocol (IP), designed to improve on the popular IPv4 that built the Internet, while IPsec is the protocol used to secure communication across IP networks.

This demonstration was made possible in part by NASA's Earth Science Technology Office (ESTO) and shows that new commercial technologies such as mobile networking, IPv6 and IPsec can be used for commercial, military and government space applications. This has direct application to NASA's Vision for Space Exploration. The success of CLEO has paved the way for new space-based Internet technologies, such as the planned Internet Routing In Space (IRIS) payload at geostationary orbit, which will be a U.S. Department of Defense Joint Capability Technology Demonstration.

This is a sanitized report for public distribution. All real addressing has been change to psueco addressing.

Table of Contents

Executive Summary

This report documents the design of network infrastructure to support testing and demonstrating network-centric operations and command and control of space-based assets using IPv6 and IPsec. The tests were performed using the Cisco router in Low Earth Orbit (CLEO), which is an experimental payload onboard the United Kingdom – Disaster Monitoring Constellation (UK-DMC) satellite built and operated by Surrey Satellite Technology Ltd (SSTL). The UK-DMC satellite is a member of the Disaster Monitoring Constellation (DMC), used for observing the Earth for major disasters and for commercial land monitoring.

On Thursday, 29 March 2007, NASA Glenn Research Center, Cisco Systems and SSTL performed the first configuration and demonstration of IPsec and IPv6 on a satellite in low Earth orbit. IPv6 is the next generation of the Internet Protocol (IP), designed to improve on the popular IPv4 that built the Internet, while IPsec is the protocol used to secure communication across IP networks.

NASA Glenn was able to reach across the Internet to the UK-DMC Disaster Monitoring Constellation satellite from Cleveland, Ohio via SSTL's Guildford, England, Mission Control Centre.

The Cisco Systems 3251 mobile access router has been flying onboard the UK-DMC satellite since September 2003. This Cisco router in low Earth orbit (CLEO) was launched with an IPv6-capable Internetworking Operating System (IOS), making it the first to fly IPv6 in space. Prior to 29 March 2007, only IPv4 configurations had been demonstrated and used in experiments with CLEO, while awaiting a window to upgrade the ground networking infrastructure. The Cisco Systems router and firewall used in SSTL's Mission Control Network were given simple software upgrades to add IPv6 capabilities to allow this end-to-end IPv6 testing to take place. The existing DMC constellation uses IPv4 to deliver its remote-sensing imagery.

The router in orbit was configured and tested during twelve-minute periods while the UK-DMC satellite passed over SSTL’s ground station. Static IPv6 and IPv4 routing and IPv4 mobile routing were operated simultaneously. IPsec for IPv4, secure shell using IPv6, Telnet for IPv6 over and IPv4 IPsec tunnel and Web browsing to the router using IPv6 over an IPv4 IPsec tunnel were all demonstrated. These tests have previously been summarised in a published paper [Wood07b]. Additional tests and demonstrations are ongoing that include utilizing ground stations from Universal Space Networks, and working towards testing with the US Army’s Multi-Use Ground Station (MUGS) and with a ground station in Japan.

This demonstration was made possible in part by NASA’s Earth Science Technology Office (ESTO). This demonstration shows that new commercial technologies, such as mobile networking, IPv6 and IPsec, can be used for commercial, military and government space applications. This has direct application to NASA’s Vision for Space Exploration. The success of CLEO has paved the way for new space-based Internet technologies, such as the planned Internet Routing In Space (IRIS) payload at geostationary orbit, which will be a U.S. Department of Defense Joint Capability Technology Demonstration (JCTD).

1 Background

The satellite used for the IPv6 and IPsec Space-Based Network Centric demonstration was the United Kingdom Disaster Monitoring Satellite (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 Disaster Monitoring Constellation[1] (DMC), accelerating the formation of a full international consortium.

Other members of the consortium (and their satellites) include Algeria (AlSAT-1), Nigeria (NigeriaSAT-1, with NigeriaSAT-2 planned for 2009), Turkey (BilSAT-1), China (Beijing-1), and Deimos in Spain – the Deimos DMC satellite is planned to be launched in 2008 alongside the UK-DMC2 satellite [SSTL07].

Each of the first five DMC satellites has similar physical characteristics:

- 686km altitude, 98 degree inclination, sun-synchronous orbit
- ~100kg satellite (BilSAT-1 and Beijing-1 massed more)
- Five-year target design life
  - Note : Alsat-1 passed this on the 28th of Nov 2007.
- Multi-spectral imager (similar to LandSat 2, 3, & 4 Thematic Mapper Bands)
  - 0.52 - 0.62 (Green)
  - 0.63 - 0.69 (Red)
  - 0.76 - 0.9 (NIR)
  - 32m ground resolution
  - 600km push-broom swath width
  - additional 12m panchromatic on BilSat-1; 4m panchromatic on Beijing-1
- 8Mbps S-band downlink (20/40Mbps X-band downlink on Beijing-1)
- 9600 bps S-band uplink

Later satellites to be added to the constellation (UK-DMC2, Deimos-1, NigeriaSat-2) are expected to carry enhanced versions of the standard DMC wide area imaging system. This new system will image 600km wide swaths of the Earth in three spectral bands at a better ground resolution of 22 meters, rather than using the existing 32m DMC imager.

A Cisco Systems 3251 mobile access router has been flying onboard the UK-DMC satellite since September 2003 as an experimental payload called CLEO, the Cisco router in Low Earth Orbit. CLEO was tested and demonstrated in June 2004 as part of a larger internetworking exercise run from Vandenberg Air Force Base, showing that a commercial Internet router could function in orbit and be tasked by remote users 'in the field.' This successful testing was conducted using the widespread version 4 of IP, along with mobile routing for IPv4 [CLEO05, Wood05, Wood07a]. This testing was carried out alongside the UK-DMC's operational use of IP both for image delivery, and for command and control of the satellite.

[1] The Disaster Monitoring Constellation (DMC) is the first Earth observation constellation of multiple low cost small satellites providing daily images for applications including global disaster monitoring.
-- http://zenit.sstl.co.uk/index.php?loc=120

CLEO was launched with an IPv6-capable Internetworking Operating System (IOS), making it the first to fly IPv6 onboard a satellite in space. Prior to the first configuration and demonstration of IPsec and IPv6 on a satellite in low Earth orbit on 29 March 2007 [DMCII07], only IPv4 configurations had been demonstrated and used by the Disaster Monitoring Constellation while awaiting funding support for the NASA contingent as well as a window to upgrade SSTL's ground networking infrastructure. The Cisco Systems router and firewall used in SSTL's Mission Control Network were given simple software upgrades to add IPv6 capabilities to allow this end-to-end IPv6 testing to take place.

The normal mode of operations for the UK-DMC satellite is to uplink to the UK-DMC satellite at 9600 bps and downlink at 8 Mbps with CLEO not active. The 8 Mbps downlink is the operational default as it enables an entire image to be transmitted to the ground during a single satellite pass. This is accomplished using an optimized rate-based file transfer protocol, Saratoga[2], originally developed by SSTL and currently being documented and refined publicly in the Internet Engineering Task Force (IETF) [Wood07c, Wood07d].

For demonstrating IPsec and IPv6 with the MUGS antenna [Miller06], satellite firmware has been modified to provide a powerful 38.4kbps downlink by optionally slowing the 8 Mbps downlink while providing connectivity to CLEO. This is expected to permit successful testing with MUGS.

A detailed explanation of the operations of CLEO and the UK-DMC is provided in a previous NASA technical report [CLEO05].

2 Why test IPv6 and IPsec in space?

IPv6 is intended to eventually replace IPv4 terrestrially, as the larger address space and simpler routing tables of IPv6 ameliorate the most pressing problems with the scalability of IPv4:

a. Exhaustion of availability of unused address space, requiring workarounds such as Network Address Translation (NAT) that become unneeded in IPv6,
b. The desire to return to a true end-to-end architecture with globally routable addressing everywhere rather than deploying NATs, and
c. The size of backbone routing tables needed to keep the Internet fully interconnected.

Modern operating systems all include IPv6 as well as IPv4 functionality in their network stacks. A detailed discussion of the advantages of IPv6 is given elsewhere [Eddy06].

IPsec is the common, popular, way to secure network assets terrestrially, so it makes sense to reuse this technology for the space environment. IPsec is the current baseline for providing network security for NASA's Constellation Program.

[2] Saratoga is a simple, lightweight UDP-based transport protocol intended for use in moving files between immediately neighboring peers which have sporadic, intermittent connectivity using dedicated IP links. Saratoga focuses on high link utilization for fast file transfers. Loss recovery is implemented via a simple ARQ mechanism.

Demonstrations of IPsec in space show how the very similar HAIPE (High Assurance IP Encryptor) protocols, mandated for US DoD and NATO use, could be used in these environments.

3 Satellite and Ground Network

This section describes the overall space/ground network including critical configurations within the ground systems and CLEO for IPsec and IPv6.

The configuration that originally existed in CLEO for the Virtual Mission Operations Center (VMOC)-oriented IPv4 net-centric operation testing in June of 2004 was expanded upon to demonstrate IPv6 and IPsec communication directly to the space-based asset. A brief description of the CLEO configurations that have been running between June 2004 and March 2007 is given in the following section – the technical details of which are given in the CLEO/VMOC report [CLEO05]. The modifications and additions to the original network configuration required to enable various combinations of IPv6 and IPsec testing will also be addressed.

3.1 CLEO/VMOC Network

From June of 2004 through February of 2007, the CLEO/VMOC network for netcentric operations remained relatively unchanged, with the exception of a few inactive nodes being removed from the network. This network is shown in Figure 1 and a detailed scription has been previously published [CLEO05].

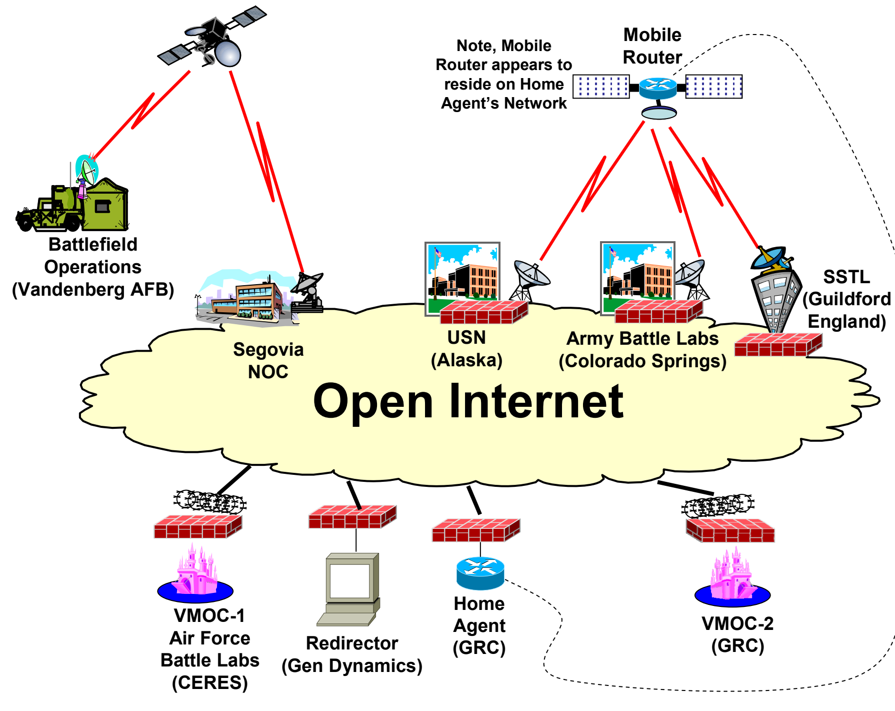

Note, Mobile Router appears to reside on Home Agent's Network
Mobile Router
Battlefield Operations (Vandenberg AFB)
Segovia NOC
USN (Alaska)
Army Battle Labs (Colorado Springs)
SSTL (Guildford England)
Open Internet
VMOC-1 Air Force Battle Labs (CERES)
Redirector (Gen Dynamics)
Home Agent (GRC)
VMOC-2 (GRC)

Figure 1 CLEO/VMOC Netcentric Demonstration June 2004

This network was configured exclusively for IPv4 networking. IPv4 static routing and IPv4 mobile networking capability were configured in the network infrastructure. No IPsec for IPv4 or IPv6 capabilities were turned on, even though those capabilities were already present onboard CLEO in its copy of Cisco's Internetworking Operating System (IOS), as the ground infrastructure being tested for VMOC and the SSTL ground networks did not support IPv6 at that time.

In this network, the ground station routers at the Universal Space Networks' (USN) site in Alaska and the SSTL site in Guildford, England had the ground routers configured as Mobile-IP foreign agents. The Army Space and Missile Defense Battle Lab's ground station in Colorado Springs, Colorado was a receive-only ground station. It could only receive telemetry for the UK-DMC and retransmit that telemetry via the terrestrial Internet.

Once the initial demonstration was over, the UK-DMC communication capability was mothballed at the USN site due to lack of funding, and the VMOC at the Air Force Center for Research Support (CERES) was removed from the open Internet connection and used elsewhere.

The network in Figure 2 depicts what NASA is currently working to implement. Note the addition of four fully-operational, bidirectional UK-DMC-compatible ground stations for a total of six (where there were once two). Work is proceeding to have USN sites in Alaska, Hawaii and Australia operational, as well as a full bidirectional site in Colorado Springs (via the MUGS antenna) and a testing site in Japan. All sites are expected to be fully functional with IPv4 capability and IPv4 foreign agent capability. In addition, each site will be IPv6-compliant.

Note: one caveat regarding this network is that the Japanese site and the Army Space and Missile Defense Battle Lab site are never to be connected to the network simultaneously because

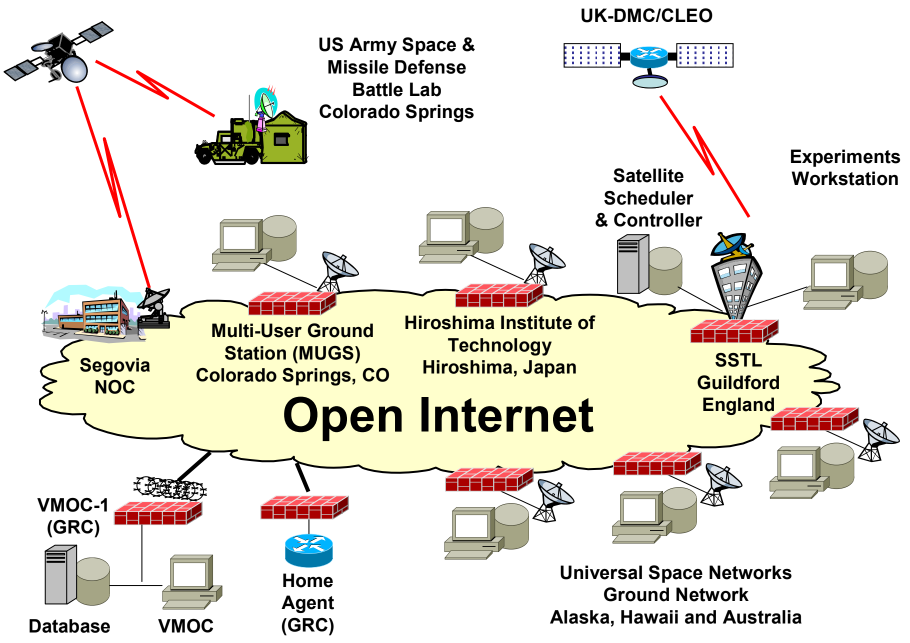


Figure 2 CLEO/VMOC Network (Work in Progress)

the National Institute of Information and Communication (NICT) of Japan are not permitted to be associated with any military activities – research or otherwise.

The network [Figure 2] interconnects a variety of parties, including the United States Government Civilian and Military agencies, Japanese Educational, United Kingdom private industry and United States private industry. This network presents some interesting security issues that must be overcome [Figure 3].

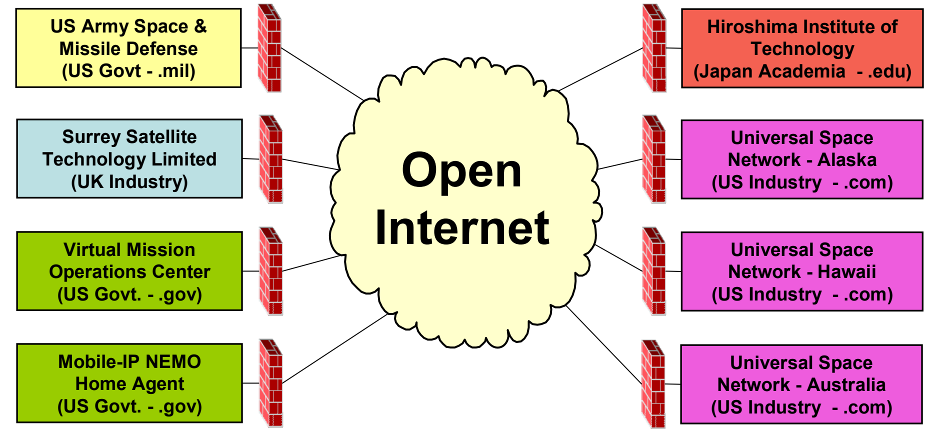

US Army Space & Missile Defense (US Govt - .mil)
Surrey Satellite Technology Limited (UK Industry)
Virtual Mission Operations Center (US Govt. - .gov)
Mobile-IP NEMO Home Agent (US Govt. - .gov)
Open Internet
Hiroshima Institute of Technology (Japan Academia - .edu)
Universal Space Network - Alaska (US Industry - .com)
Universal Space Network - Hawaii (US Industry - .com)
Universal Space Network - Australia (US Industry - .com)

Figure 3 NCO Security Considerations

Glenn Research Center's (GRC's) network is a localized research network directly connected to the open public Internet and isolated from the GRC operational network. Likewise, the US Army Space and Missile Defense network is an experimental network isolated from any operational networks.

USN's networks are currently connected to GRC over the open Internet. Security is handled at the USN firewall. From there, multi-protocol label switching (MPLS) is used to extend virtual local area networks (VLANs) to the various ground station sites, thereby isolating any activity on the VLANs from that of other USN networks. The NICT (Hiroshima) network may or may not be isolated as an experimental network. The SSTL network is a fully operational network connected to GRC via Virtual Private Network (VPN) IPsec tunneling. The overall connectivity is a basic hub/spoke architecture, with the GRC's home-agent (or anchor router for IPv6) network being the hub and all other networks connected to the anchor router via IPv4, IPsec tunnels [Figure 4] originate at the GRC firewall.

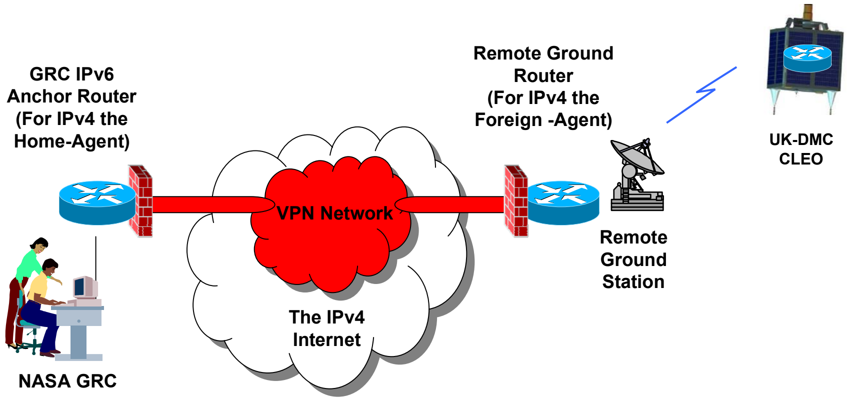


Figure 4 IPsec Virtual Private Network

3.2 Routing and Security Configurations

The CLEO/VMOC network is configured to simultaneously operate with four basic routing configurations: IPv4 Static, IPv4 Mobile Networking, IPv6 Static, and IPv6 Static over IPv4 Mobile. In addition, the network is configured to allow IPsec network-layer security over the space/ground links using IPv4. Each of these configurations is explained in the following sections. A network diagram is available in Appendix A.1, CLEO Mobile Router Topology. The configurations for these can be found in Appendix D, Router Configurations and Route Tables.

3.2.1 IPv4 Static Configuration

IPv4 static routing was initially performed during the June 2004 VMOC tests. Static routing between CLEO and the ground is performed because the LEO satellite passes only last between 8 and 12 minutes. Waiting for RIP (routing information protocol) or OSPF (open shortest path first) or any other dynamic routing protocol can require 30 to 90 seconds or more for routing information to propagate if default timers are not adjusted[3]. Thus, routing may deny access to the spacecraft even though the physical link is up, because routing updates have not yet propagated. Likewise, one may think they have access to the spacecraft even though the physical link is down. For a single downlink, where the entire Internet is at the other end of the link, static routing suffices.

IPv4 Static routing was performed across the IPsec Tunnel VPN firewalls. The GRC home-agent firewall has the static routes to each ground station firewall, and *vice versa*. The GRC home-agent (anchor) router is directly connected to the GRC firewall. Likewise, the ground routers are directly connected, in their network-layer topology, to their private network/public network

[3] Note, Adjusting timers lower to improve router convergence time results in additional router protocol overhead (e.g. hello packets, route updates, etc...). On low-rate radio links, e.g. at 9600 bps for the uplink to the UK-DMC satellite,, this can be significant.

firewalls[4]. In the anchor router and the ground station routers, the default next-hop route is to their firewall which has the static routing information.

Note: SSTL configures their Disaster Monitoring Satellites such that each satellite payload appears to be on the same private sub-network with a different private address; the satellite payloads are effectively bridged onto the private ground station LAN. In order to statically route to the UK-DMC, one must know which ground station that UK-DMC will be at and then communicate with the UK-DMC paylod via the public (or private) address associated with that particular ground station. The public (or private) address is one-for-one NATed between the satellite private network address space and the ground station public (or private) address space using network address translation techniques [CLEO05]. Basically, this is a manual form of "predictive static routing."

3.2.2 IPv4 Mobile Configuration

CLEO has been configured with IPv4 mobile networking since June of 2004 [Appendix D.1]. Mobile networking is extremely useful for IP connectivity with LEO satellites due to its extremely fast convergence time and "set and forget" configuration.[5] To perform mobile networking the spacecraft can be configured to solicit foreign-agent service from the ground router or the ground router can be configured to advertise foreign-agent service to mobile units or both. This is simply a design decision resulting in a small amount of bandwidth overhead. Solicitation and advertisement timers can be easily manipulated. The solicitation timer is set at each "roaming" interface on CLEO. The advertisement timer is set at each radio interface at each ground terminal. No other timers need to be set anywhere else in the network. In these configurations, advertisement is from the foreign agents. The mobile router is not configured to solicit for foreign agent services.

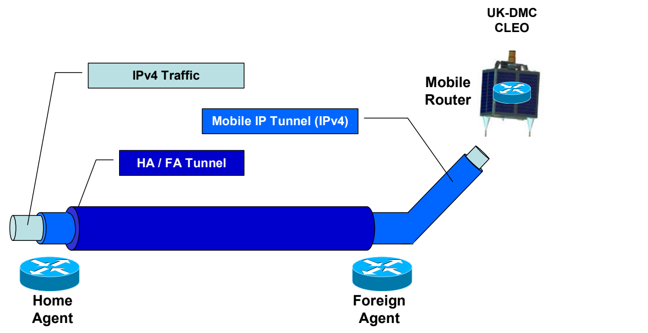


Figure 5 NEMO IPv4 Forward-Bound Mobile Tunnels

For IPv4 mobile networking, the home-agent router is located at GRC. The CLEO mobile network has GRC address space and appears to reside at GRC. Thus, any information destined for the CLEO mobile network (forward bound) gets sent to the GRC home agent where it is encapsulated twice: once to the tunnel between the Home Agent (HA) and the Mobile router; and a second encapsulation to tunnel between the HA and the ground station foreign agent [Fig. 5]. Note: triangular routing is implemented onboard the mobile router. Thus, there is no Mobile-IP

[4] USN has implemented Multi-Protocol Layer Switching between their control centers and their ground stations, effectively extending their local area networks while being able to manage much of the network security at a single location.

[5] "Set and Forget" refers to the ability to configure a system once and then never have to go back and reconfigure. With mobile-ip, once the system is configure, all registrations, tunnel management and mobility management occur automatically.

reverse tunnel from the foreign agents to the home agent. Figure 5 only illustrates forward bound traffic tunnels.

CLEO is not connected directly to the UK-DMC transmitters and receivers, but indirectly via serial ports on two of the onboard SSTL-designed computers: the PowerPC-based Solid State Data Recorders (SSDRs). Here, the SSDR that is used to connect the router to the transmitters and receivers is configured to be in 'bridging' pass-through mode to connect CLEO to the outside world, and is not usable as an SSDR for recording imagery at that time. Since for IPv4 testing of CLEO either of these two SSDRs could be put in pass-through mode. Therefore, each serial port, both serial port S1/0 and serial port S1/1, was configured to be in router "roam" mode so that Mobile-IP signaling was recognized on both ports. Thus, whichever port is in pass-through mode and communicating with the ground will establish a forward-bound Mobile-IP tunnel between CLEO and the Home Agent (HomeAgent.Net.HArouter). This selected interface then becomes the default route out of CLEO once the mobile router has registered and bound with the home agent. This feature is later used for IPv6 communication – see section 3.2.7.

Note, whenCLEO was configured for native IPv6 routing, specifying which SSDR was used for pass-through was imperative as there is no IPv6 mobile routing tunnel that is automatically established – see IPv6 Static Configuration and IPv6 over IPv4 IPsec Configuration.

Since there is no IPv4 Mobile-IP reverse tunnel, in order to defeat egress filtering and policy rules at the firewalls, and pass the IPv4 traffic back through the firewalls, a policy-based route had to be setup in the foreign agent ground router that would encapsulate the response in a tunnel back to the home agent. Thus, a pseudo reverse-tunnel was created. The details of this are in reference CLEO05, section SSTL Ground Network. This pseudo reverse-tunnel is also used for IPv6 traffic (See section 3.2.7).

3.2.3 IPv6 Static Configuration

The UK-DMC disaster monitoring constellation imaging satellite was launched into space in September 2003. The Cisco router's (CLEO's) Internetwork Operating System (IOS) was loaded prior to launch with IPv6 and IPsec (for IPv4 only) capable code[6]. That code was not exercised in space until March of 2007 due to funding and manpower limitations as well as a need to upgrade SSTL's ground infrastructure to accommodate such testing.

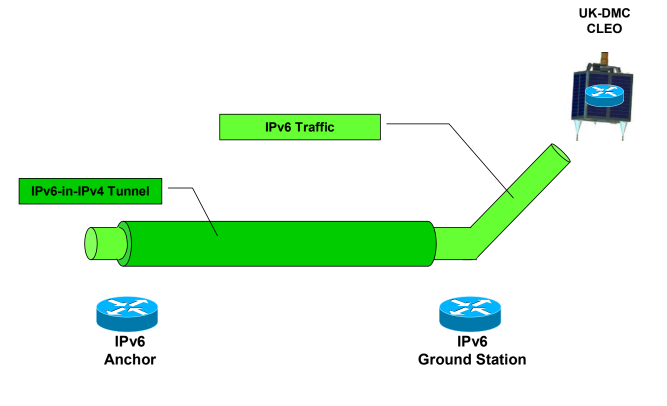


Figure 6 IPv6-in IPv4

[6] Cisco Internetwork Operating System Software IOS (tm) 3200 Software (C3200-I11K9-M), Version 12.2(11)YQ, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)

Since the CLEO/VMOC IPv6 network is never going to propagate out to the open Internet, IPv6 private address space, Unique Local IPv6 Unicast Addresses [RFC4193] is used.

Note, Unique Local IPv6 Unicast addressing has replaced Site Local addressing for IPv6 private address space. Use of this technique improves security as this becomes a closed network and is not reachable by entities on the open Internet as this address space is not routable in the open Internet.

In order to run IPv6 testing over the open Internet, we had to encapsulate the IPv6 traffic in IPv4 using IPv6-in-IPv4 manual tunneling [Fig. 6].

The IPv6-in-IPv4 tunnels' end points were at the IPv6 anchor router (the IPv4 HA) and each ground station router. IPv6 static routing, similar to IPv4 static routing, consisted of routing via a hub-spoke architecture where the IPv4 home agent route becomes the IPv6 anchor point – similar to a rendezvous point for multicast. Each ground station router has four different IPv6 prefixes [Fig. 7], one on a physical interface and three IPv6-in-IPv4 tunnel interfaces. The prefix on the physical interface and on one of the tunnels provides native IPv6 and IPv6 over IPsec-v4 connectivity to CLEO, respectively. The two remaining tunnel prefixes provide IPv6 connectivity back to the anchor router. CLEO was configured with multiple IPv6-in-IPv4 tunnels and multiple IPv6 addresses assigned to the egress interface (serial 1/1.1), one for each ground station.[7] Between the ground stations and CLEO, the IPv6-in-IPv4 tunnels are routed via an IPsec-v4 tunnel to demonstrate secure IPv6 communication to space, while IPv6 on the physical interface demonstrates native IPv6 connectivity to space without IPv4 support. Having two IPv6 paths from the GSN to CLEO necessitated that there were two tunnels between the GSN and anchor routers.

Since both sets of the CLEO network's routing tables (IPv6 & IPv4) are static and not dynamic. CLEO is unaware as to which ground system network (GSN) it is connected. Hence when CLEO receives an IPv6 packet there is no indication which IPv6 prefix delivered it, only a source address of the originator. Therefore two IPv6-in-IPv4 tunnels were used between the anchor router and GSN router. IPv6 packets originating *"directly from the anchor router"* will have a unique source address enabling CLEO to properly route reply packets. This happens because the source address selected for a packet **originating** from the anchor router is the address of the interface from which that the packet is routed. For example, when we want to ping, from the anchor router, CLEO's native IPv6 address via the SSTL's ground site the "echo reply" packet will be routed from CLEO out tunnel 6550[Fig. 7] according to the static route command in CLEO,
"ipv6 route 2001:DB8:XXXX:6540::/64 2001:DB8:XXXX:6550::1".

For traffic that does not originate from a network known to CLEO, the return path is via a preconfigured default path which is also the IPv4 Mobile Network pseudo-reverse-tunnel (see section 3.2.7).

[7] Since UK-DMC only connects to one GSN at a time, only one of the IPv6-in-IPv4 tunnels to the GSN router is "usable" at a time even though all are "active". Thus, one needs to know which static route to use at a given time if communication originates from CLEO.

No network address translation (NAT) was required.

Note, NATing should never be done in IPv6 and NATing should never be required.

Note, predictive static routing is one technique NASA's Constellation Program is looking into for IP in space. This works well forthe testing here as there are only a few ground stations and one space craft. ***Predictive static routing DOES NOT SCALE and is NOT a recommended technique for a complex operational system. Since the goal of the IPv6 and IPsec tests was to demonstrate the viability of IPv6 in space applications and IPsec for securing the RF links, predictive static routing was fine for the subject purposes, yet still proved very difficult to manage.*** *Predictive static routing is NOT a recommended practice. This DOES NOT SCALE AND IS NOT EASILY MAINTAINABLE. The CLEO IPv6 Topology Diagram in Appendix A.2 shows a simple topology with nine ground station end points. Managing nine static routes quickly becomes extremely complex as each ground station tunnel and the anchor point router tunnels must match exactly.*

3.2.4 Native IPv6 Static Routing Originating from the Anchor Router

The first goal was to show IPv6 capability onboard CLEO. Thus, some form of IPv6 routing had to be established. This section describes the data flow for native IPv6 static routing when traffic originates from the anchor router [Figure 7]. In order to most easily illustrate the data flow, the following decription is for a ping command originating from the anchor router.

The example is for the following command entered on anchor router:
"ping 2001:DB8:XXXX:6550::2".

Step 1: An IPv6 ping request originating from the anchor router (src – 2001:DB8:XXXX:6540::1) to (dst – 2001:DB8:XXXX:6550::2), the native IPv6 address assigned to the active serial interface onboard CLEO, is encapsulated in an IPv6-in-IPv4 tunnel. Encapsulating in this manner enables IPv6 traffic to traverse the IPv4 backbone. The anchor router consults its route table and finds a static route (see below) directing all traffic bound for the 2001:DB8:XXXX:6550::/64 prefix to be routed via Tunnel 6540. The IPv6-in-IPv4 tunnel pair is shown below (N*ote, tunnels are unidirectional)*. After setting the IPv6 source address of the packet (ping request) with the IPv6 address of the interface that the packet egresses (Tunnel 6540), the IPv6 packet is then encapsulated in an IPv4 header. The tunnel is between the IPv4 HA router, HomeAgent.Net.HArouter, and SSTL's ground terminal router, SSTL.WAN.FA0/0. Once the IPv6 traffic is encapsulated in IPv4, the traffic can be routed to CLEO using IPv4 static routing or IPv4 mobile routing.

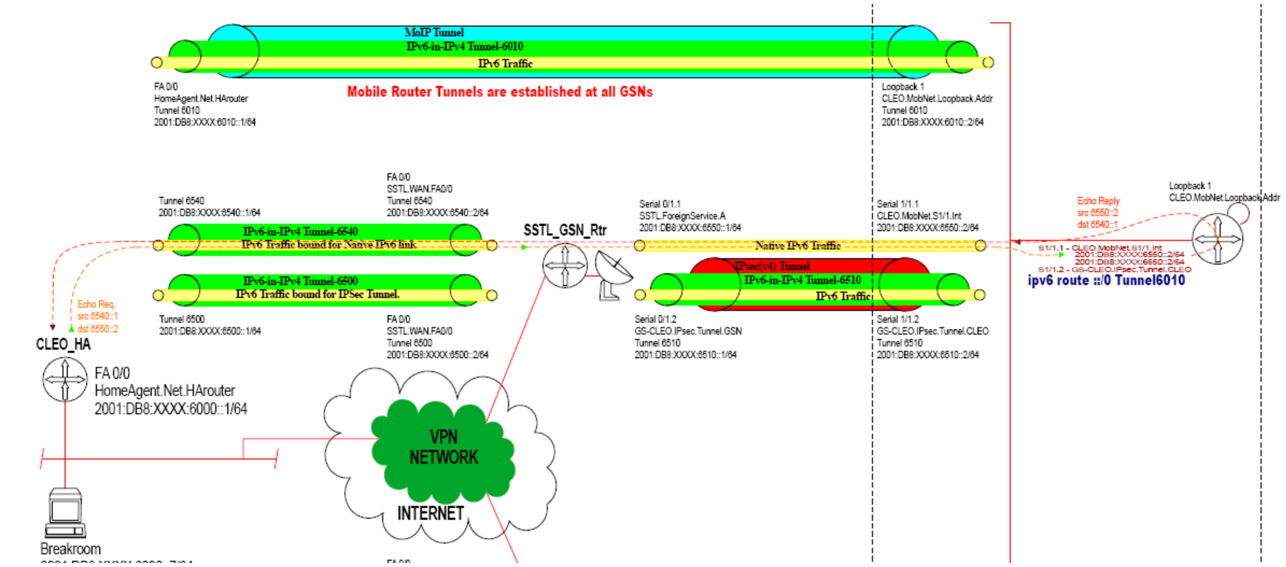


Figure 7 - Data Flow Native IPv6 Originating from IPv6 Anchor Router

Step 1:

IPv6 Anchor Router (IPv4 HA)

```
ipv6 route 2001:DB8:XXXX:6510::/64 Tunnel6500
ipv6 route 2001:DB8:XXXX:6550::/64 Tunnel6540

interface Tunnel6540
 description "IPv6-in-v4 Tunnel to SSTL GSN Router for native IPv6"
 no ip address
 ipv6 address 2001:DB8:XXXX:6540::1/64
 ipv6 enable
 tunnel source HomeAgent.Net.HArouter
 tunnel destination SSTL.WAN.FA0/0
 tunnel mode ipv6ip
```

IPv6 Ground Router (SSTL IPv4 FA)

```
interface Tunnel6540
 description IPv6-in-v4 tunnel for IPv6 traffic to/from CLEO_HA for Native IPv6.
 no ip address
 ipv6 address 2001:DB8:XXXX:6540::2/64
 ipv6 enable
 tunnel source FastEthernet0/0
 tunnel destination HomeAgent.Net.HArouter
 tunnel mode ipv6ip

interface FastEthernet0/0
 description connected to Groundstation Subnet0
 ip address SSTL.WAN.FA0/0 255.255.255.0
```

Step 2 : The IPv4 packet is forwarded to the GRC firewall where it is encapsulated in an IPv4 IPsec tunnel and routed to the SSTL firewall. The SSTL firewall decrypts the packet and forwards the IPv6-in-IPv4 packet to the SSTL ground router.

Step 3: Upon receiving this packet, the SSTL ground router removes the IPv6-in-IPv4 encapsulation, and processes the IPv6 ping request's header. With the exception of the IPv6 default route entry (shown below) pointing default IPv6 traffic back to the anchor router via Tunnel 6500, there are no IPv6 static route entries on the ground routers. Static route entries are not needed at this router because via the IPv6-inIPv4 tunnels and the serial 0/1.1 interface this router appears to have direct connections to both the anchor router and CLEO. As a result the ground router forwards the packet out the serial 0/1.1 interface, since the destination address (dst – 2001:DB8:XXXX:6550::2) belongs to the prefix that is assigned to this interface. In this case, the IPv6 destination address is native to a physical interface, thus there is no encryption or encapsulation of the packet.

.

SSTL Ground Station
Step 3:

```
ipv6 route ::/64 Tunnel6500

ipv6 route 2001:DB8:XXXX:6500::/64 Tunnel6510 /* encrypted link */
ipv6 route 2001:DB8:XXXX:6540::/64 2001:DB8:XXXX:6550::1 /* unencrypted link */
ipv6 route ::/0 Tunnel6010 /* default route – pseudo reverse-tunnel */

interface Serial0/1.1 point-to-point
 ip unnumbered FastEthernet0/0
 ip nat inside
 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
 ipv6 address 2001:DB8:XXXX:6550::1/64
 ipv6 enable
 no arp frame-relay
 no cdp enable
 frame-relay interface-dlci 17
```

Step 4: After receiving the IPv6 ping request, CLEO will echo with the corresponding reply. CLEO uses the source address of the ping request (2001:DB8:XXXX:6540::1)[8] as the reply packet's destination and the source address of the new packet (ping reply) will be the address assigned to the egress interface (2001:DB8:XXXX:6550::2). The egress interface (serial 1/1.1) is determined by a static route in CLEO's routing table pointing traffic destined for prefix 2001:DB8:XXXX:6540::/64 to address 2001:DB8:XXXX:6550::1.

Note the two IPv6 interface addresses. The ":**66**50::" is for testing with the MUGS terminal mentioned earlier, while the ":**65**50::" is for SSTL. If one were to have 9 different ground stations, there would be 9 different IPv6 interface addresses. Only SSTL and MUGS were in the

[8] It is important that the IPv6 ping packet originates from the anchor router, otherwise CLEO will not know which path that the packet was received from. Therefore all traffic back would be routed via the default gateway bypassing desired tunnels and/or encryption and defeating the purpose of each test scenario.

CLEO configurations during these tests. As already noted, this quickly becomes very difficult to manage – see A.2 Predictive Static Routing (Nine Ground Station Destinations)

CLEO
Step 4:

```
ipv6 route 2001:DB8:XXXX:6500::/64 Tunnel6510
ipv6 route 2001:DB8:XXXX:6540::/64 2001:DB8:XXXX:6550::1
ipv6 route 2001:DB8:XXXX:6600::/64 Tunnel6610
ipv6 route 2001:DB8:XXXX:6640::/64 2001:DB8:XXXX:6650::1
ipv6 route ::/0 Tunnel6010
!
interface Serial1/1.1 point-to-point
 ip address CLEO.MobNet.S1/1.Int 255.255.255.248
 ip access-group 110 in
 ip mobile router-service roam
 no ip mroute-cache
 ipv6 address 2001:DB8:XXXX:6550::2/64
 ipv6 address 2001:DB8:XXXX:6650::2/64
 ipv6 enable
 frame-relay interface-dlci 17
```

Step 5: Once the reply packet with source 2001:DB8:XXXX:6550::2 and destination address 2001:DB8:XXXX:6550::1 reaches the SSTL ground network it is placed in a IPv6-in-IPv4 tunnel, forwarded to the SSTL firewall, encrypted, routed via IPv4 across the Internet to the GRC firewall, decrypted and forwarded to the GRC anchor router. The IPv6-in-IPv4 encapsulation is removed and the packet read by the router, its intended destination.

SSTL Ground Router
Step 5:
SSTL Route table

```
C 2001:DB8:XXXX:6540::/64 [0/0]          via ::, Tunnel6540
```

Configuration

```
interface Tunnel6540
 description IPv6-in-v4 tunnel for IPv6 traffic to/from CLEO_HA for Native IPv6.
 no ip address
 ipv6 address 2001:DB8:XXXX:6540::2/64
 ipv6 enable
 tunnel source FastEthernet0/0
 tunnel destination HomeAgent.Net.HArouter
 tunnel mode ipv6ip

interface FastEthernet0/0
 description connected to Groundstation Subnet0
 ip address SSTL.WAN.FA0/0 255.255.255.0
```

3.2.5 IPv6 via IPv4 Mobile Tunnel Configuration

To date, NASA GRC has found that the IPv4 mobile network capability has been the most useful configuration for accessing CLEO, as there are no IPv4 static tunnels to manage, and CLEO automatically registers its location with the HA router once powered on over a ground station. In order to exploit IPv4 mobile networking, and because the CLEO IOS does not have the later IPv6 mobile networking capability due to its early vintage, a separate IPv6 network, which is dedicated to access via IPv4 mobile networking was created onboard CLEO. Any traffic destined to this IPv6 network is placed in a IPv6-in-IPv4 tunnel with the source being the IPv4 HA address and the destination being CLEO. Thus, IPv6 traffic destined to 2001:DB8:XXXX:6010::/64 was sent to CLEO via the mobile router forward-bound tunnels. Since IPv4 mobile networking was configured with no reverse tunneling, IPv6 traffic returning from CLEO's 2001:DB8:XXXX:6010::/64 network was sent back via the mobile network IPv4 pseudo-reverse-tunnel.

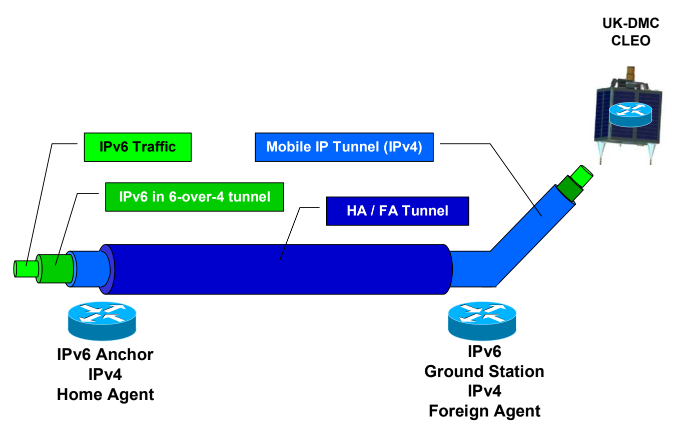


Figure 8 IPv6 over IPv4 Mobile Network

The router configurations required to do this are shown below along with a description of how an IPv6 ping traverses the network. The tunnels used for IPv6 traffic destined to CLEO are shown in Figure 8, and detailed in Appendix B. The return path is described in the example below.

This example is for the following command entered on anchor router "ping 2001:DB8:XXXX:6010::2".

Step 1: The IPv6 ping request originates from the anchor router (dst - 2001:DB8:XXXX:6010::1, src - 2001:DB8:XXXX:6010::2). Notice the source and destination addresses are in the same prefix (2001:DB8:XXXX:6010::/64). From the anchor router and CLEO's point of view this IPv6 prefix is directly connected to both routers via tunnel 6010. Therefore the ping request packet will be encapsulated in a IPv6-in-IPv4 tunnel until received at CLEO. Once encapsulated in an IPv4 packet with a source address of the HA (HomeAgent.Net.HArouter), and a destination address of CLEO (CLEO.MobNet.Loopback.Addr), the packet is sent over the mobile network forward-bound tunnels. Since the destination is CLEO mobile router (MR) address space, Mobile-IP is used to send it on to CLEO.[9]

[9] See reference [CLEO05] for a description of the Mobile-IP operation.

IPv6 Anchor / IPv4 Home Agent
Step 1:

```
interface Tunnel6010
 description "IPv6 Tunnel to CLEO via MR tunnels"
 no ip address
 ipv6 address 2001:DB8:XXXX:6010::1/64
 ipv6 enable
 tunnel source HomeAgent.Net.HArouter
 tunnel destination CLEO.MobNet.Loopback.Addr
 tunnel mode ipv6ip

ip mobile home-agent
ip mobile host CLEO.MobNet.Loopback.Addr virtual-network CLEO.MobNet.S1/0.Net 255.255.255.224
```

Step 2: After the ping request packet is decapsulated and delivered, CLEO responds with the reply back to the anchor router. The IPv6 ping reply is encapsulated in the IPv6-in-IPv4 tunnel 6010 and the encapsulated packet traverses the IPv4 network back to the HA (anchor router). Note: This implementation of Mobile IPv4 is using triangular routing (not reverse tunneling), so the return path to the home agent is different. At this point the ping reply is only encapsulated once with the IPv6-in-IPv4 headers, and is forwarded down CLEO (MR) active interface (Mobile IPv4 default route) to the ground station router.

CLEO / Mobile Router
Step 2 :

```
interface Tunnel6010
 description "IPv6 Tunnel to CLEO_HA via MR protocol"
 no ip address
 ipv6 address 2001:DB8:XXXX:6010::2/64
 ipv6 enable
 tunnel source Loopback1
 tunnel destination HomeAgent.Net.HArouter
 tunnel mode ipv6ip

interface Loopback1
 ip address CLEO.MobNet.Loopback.Addr 255.255.255.255
```

Step 3: When this packet is received on the ground router's serial interface, a policy route statement is invoked based on the packets source address (see highlighted route map command below). This command causes the ground router to place the packet in the IP-in-IP tunnel 7 (the pseudo reverse-routing tunnel), sending it back to the IPv6 anchor router, the HA router, via an IPsec VPN tunnel. The VPN tunnel is between the ground station firewall and the GRC mobile network firewall. *Note, the pseudo-reverse-routing tunnel is always "up".*

Ground Station Router / Foreign Agent Router
Step 3:

```
interface Serial0/1.1 point-to-point
 ip unnumbered FastEthernet0/0
 ip nat inside
 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
 ipv6 address 2001:DB8:XXXX:6550::1/64
 ipv6 enable
 no arp frame-relay
 no cdp enable
 frame-relay interface-dlci 17
!
route-map mr_subnets permit 10
 match ip address 7
 set ip default next-hop HA-SSTL.ipip.psuedo-rev-tunnel.HA
!
access-list 7 permit CLEO.MobNet.S1/0.Net 0.0.0.31
!
interface Tunnel7
 ip address HA-SSTL.ipip.psuedo-rev-tunnel.SSTL 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination HomeAgent.Net.HArouter
 tunnel mode ipip
```

3.2.6 IPv6 over IPv4 IPsec Configuration

The second major goal of this demonstration was to show that one could use IPsec network-layer security to secure the RF link. SSTL operates the UK-DMC in the clear for its primary imaging mission. Since the CLEO IOS was 2003 vintage, it was only capable of IPv4 IPsec. Thus, the IPv6 traffic had to be encapsulated in an IPv4 tunnel prior to encapsulation into an IPv4 Encapsulating Security Payload (ESP) tunnel [Fig. 9].

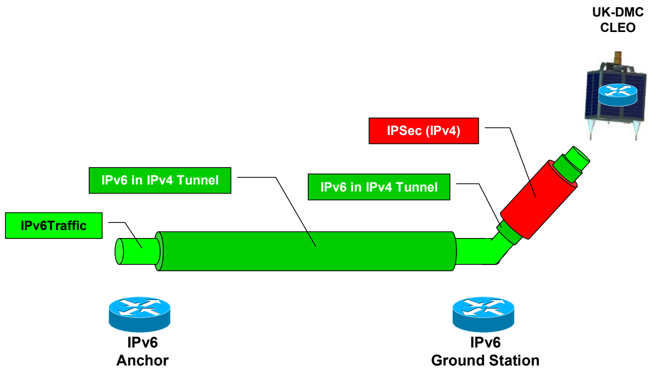


Figure 9 IPv6 over IPv4 IPsec

The details of the traffic flow are for traffic *originating at the anchor router* (not passing through the anchor router – see section 3.2.7 for an explanation) and destined for CLEO via the SSTL ground station. These details are shown in Figure 10.

The example is for the following command entered on anchor router “ping 2001:DB8:XXXX:6510::2”.

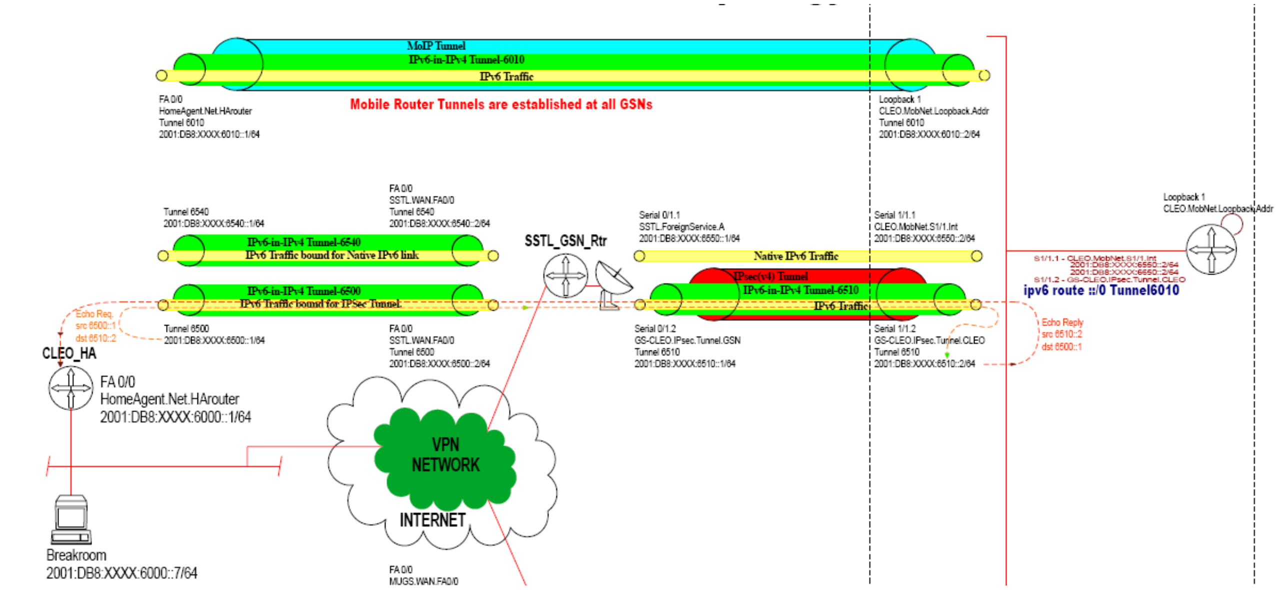


Figure 10 Data Flow IPv6 over IPv4 IPsec

Step 1: The ping request destined for CLEO's interface tunnel 6510 address (2001:DB8:XXXX:6510::2), is routed via Tunnel6500 (see highlighted route statement below). Since the packet egresses out this interface, the source address will be the address of the Tunnel 6500 interface (2001:DB8:XXXX:6500::1 as highlight). The ping request packet is then encapsulated in an IPv6-in-IPv4 tunnel with an IPv4 source address of the anchor router (HomeAgent.Net.HArouter), and an IPv4 destination of the SSTL ground router wide area network (WAN) Interface (SSTL.WAN.FA0/0).

IPv6 Anchor Router
Step 1:

```
ipv6 route 2001:DB8:XXXX:6510::/64 Tunnel6500

interface Tunnel6500
 description "IPv6-in-v4 Tunnel to SSTL GSN Router"
 no ip address
 ipv6 address 2001:DB8:XXXX:6500::1/64
 ipv6 enable
 tunnel source HomeAgent.Net.HArouter
 tunnel destination SSTL.WAN.FA0/0
 tunnel mode ipv6ip
```

Step 2: The IPv4 packet is forwarded to the GRC firewall where it is encapsulated in an IPv4 IPsec tunnel and routed to the SSTL firewall. The SSTL firewall decrypts the packet and forwards the IPv6-in-IPv4 packet to the SSTL ground router.

Step 3: The IPv6-in-IPv4 tunnel encapsulation is removed at the ground station router. The ping request packet's destination address (2001:DB8:XXXX:6510::2) is directly connected via Tunnel 6510, so the packet is encapsulated again with a source address of GS-CLEO.IPsec.Tunnel.GSN and a destination address of GS-CLEO.IPsec.Tunnel.CLEO [Figure 10].

A virtual channel (sub-interface S 0/1.2) assigned the subnet GS-CLEO.IPsec.Tunnel.Net, was created on the serial link between the ground router and CLEO for encrypted traffic[10]. This virtual channel used a DLCI of 18 and has a crypto map specified. This interface will be repeated in every Ground station network router using the same IPv4 address and cryptographic information, so from CLEO's point of view the same IPsec-v4 tunnel will be established every time CLEO connects to a ground router. This can be done since the IPv4 subnet (GS-CLEO.IPsec.Tunnel.Net) is not advertised outside of the ground router and is only utilized by the IPv6-in-IPv4 tunnel designated to traverse this IPsec-v4 connection. Thus, CLEO only has one sub-interface and one set of configurations dedicated to an IPsec connection to be used by all ground routers, but there will be a unique IPv6-in-IPv4 tunnel (endpoints: GS-CLEO.IPsec.Tunnel.GSN, GS-CLEO.IPsec.Tunnel.CLEO) for each ground router. Since UK-DMC can only connect to one ground station at a time only the tunnel with the same IPv6 prefix as the active ground station will be usable, so the operator will have to know what ground station is being utilized and which IPv6 prefix is assigned.

If the IPv6 traffic entering the ground station router is destined to transit the IPsec link, the IPv6 packet is re-encapsulated in a IPv6-in-IPv4 tunnel and then further encapsulated in an Encapsulating Security Payload (ESP) packet. The IPsec ESP security associations are established over this virtual channel using the Internet Key Exchange (IKE) protocol. The details of this are shown in the specific router configuration sections below.

Note that in the ground and CLEO routers only virtual channels with Frame Relay DLCI 18 have a crypto map specified. Unsecured traffic is passed between the ground and CLEO via native IPv6 (sub-interface Serial0/1.1). Secure traffic is encapsulated in a IPv6-in-IPv4 tunnel (interface Tunnel6510) and then further encapsulated in an IPv4 ESP packet (sub-interface Serial0/1.2 and crypto map CLEO_auth).

SSTL Ground Station Router
Step 3:

```
interface Tunnel6510
 description IPv6-in-v4 tunnel for IPv6 traffic to/from CLEO_MR. Tunnel terminates at CLEO_MR via   IPsec-v4 tunnel.
 no ip address
 ipv6 address 2001:DB8:XXXX:6510::1/64
 ipv6 enable
 tunnel source GS-CLEO.IPsec.Tunnel.GSN
 tunnel destination GS-CLEO.IPsec.Tunnel.CLEO
 tunnel mode ipv6ip
!
interface Serial0/1.1 point-to-point
 ip unnumbered FastEthernet0/0
 ip nat inside
 ip irdp
```

[10] A separate Frame Relay sub-interface (DLCI 18) was used for 2 reasons. First, the GSN router is in a production environment, so the main DLCI was minimally modified to avoid risk of negatively impacting SSTL's network. Second, the packets for the IKE handshake for the IPsec tunnel needs to have source and destination addresses that match those specified in the Security Association. Due to the way the router assigns source addresses a separate sub-interface was needed.

```
 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
 ipv6 address 2001:DB8:XXXX:6550::1/64
 ipv6 enable
 no arp frame-relay
 no cdp enable
 frame-relay interface-dlci 17
!
interface Serial0/1.2 point-to-point
```

This interface will be repeated in every GSN router so that an IPsec-v4 tunnel will be established everytime CLEO connects.

```
 ip address GS-CLEO.IPsec.Tunnel.GSN 255.255.255.0
 no ip mroute-cache
 no arp frame-relay
 no cdp enable
 frame-relay interface-dlci 18
 crypto map CLEO_auth
```

Cryptographic Information – Ground Router

```
crypto isakmp key CLEO_ IPSEC address GS-CLEO.IPsec.Tunnel.CLEO
!
crypto  IPsec transform-set CLEO_set esp-des esp-md5-hmac
!
crypto map CLEO_auth 1  IPsec-isakmp
 set peer GS-CLEO.IPsec.Tunnel.CLEO
 set transform-set CLEO_set
 match address 115

access-list 115 permit ip GS-CLEO.IPsec.Tunnel.Net 0.0.0.255 GS-CLEO.IPsec.Tunnel.Net 0.0.0.255
```

Onboard CLEO, the ESP packet is deciphered and then the IPv6-in-IPv4 encapsulation is removed. If CLEO has the return path in its route tables, then the return data will take the reverse path back as follows: At CLEO, if the destination address is associated with the encrypted path, the return packet will be IPv6-in-IPv4 encapsulated, then encapsulated in an IPv4 ESP packet. The ground router will decrypt the ESP packet, decapsulate the IPv6-in-IPv4 packet, and re-encapsulate in a IPv6-in-IPv4 packet destined for the anchor router. At the ground station firewall, the IPv6-in-IPv4 packet is placed in an IPv4 IPsec virtual private network (VPN) tunnel and forwarded to the GRC CLEO/VMOC mobile network firewall where the VPN tunnel is decapsulated. The packet then is then fowarded to the anchor router, which removes the IPv6-in-IPv4 encapsulation and passes the IPv6 packet to its destination.

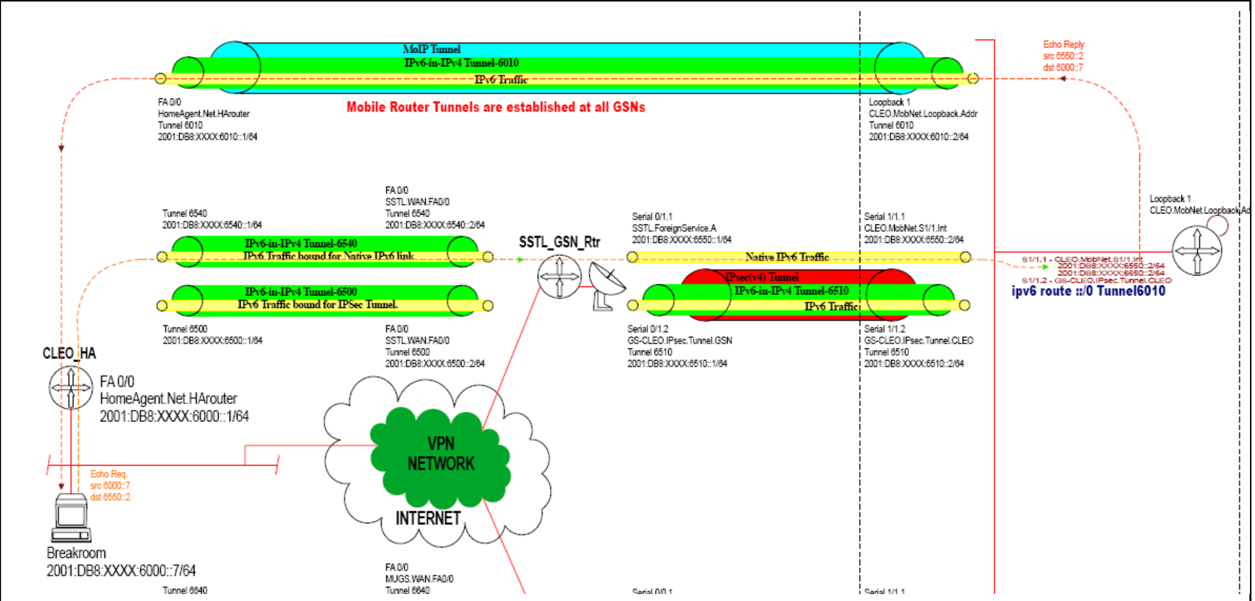


Figure 11 IPv6 Static Route Return Path

3.2.7 IPv6 Static Route Host-Originated Forward Path

Figure 11 shows the path of IPv6 packets that originate from remote hosts (rather than from the IPv6 anchor router). The data source address is the host's, Breakroom's, address, 2001:DB8:XXXX:6000::7/128. The data flow is not intuitive. Flows (communication) originating from the host, Breakroom, and destined for the IPv6 network on CLEO, 2001:DB8:XXXX:6540::/64, are shown by the dashed line. The IPv6 network, 2001:DB8:XXXX:6540::/64, corresponds to the IPv6 network on CLEO that is reachable via native IPv6. This network is reached by the SSTL ground station serial interface associated with the Frame Relay virtual channel DLCI 17.

The data takes the following forward path.

Step 1: Data enters the IPv6 anchor router and is mapped into a IPv6-in-IPv4 tunnel, which terminates at SSTL's ground router and corresponds to the IPv6 network onboard CLEO.

Step 1:

```
interface Tunnel6540
 description "IPv6-in-v4 Tunnel to SSTL GSN Router for native IPv6"
 no ip address
 ipv6 address 2001:DB8:XXXX:6540::1/64
 ipv6 enable
 tunnel source HomeAgent.Net.HArouter
 tunnel destination SSTL.WAN.FA0/0
 tunnel mode ipv6ip
```

Step 2: The IPv6-in-IPv4 encapsulated packets are sent to the GRC firewall (not shown in Figure 11) where they are encapsulated in an IPv4 IPsec tunnel, a VPN tunnel. The IPv4 IPsec encapsulation is removed at SSTL's firewall and the IPv6-in-IPv4 encapsulated packet is forwarded to the SSTL ground router [Figure 4].

Step3: The SSTL ground router removes the IPv6-in-IPv4 encapsulation and forwards the data through the serial link sub-interface corresponding to the IPv6 network onboard CLEO.

Step 3:
SSTL Ground Router

```
interface Serial0/1.1 point-to-point
description interface for native IPv6 network 2001:DB8:XXXX:6550::1/64
 ip nat inside
 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
 ipv6 address 2001:DB8:XXXX:6550::1/64
 ipv6 enable
 no arp frame-relay
 no cdp enable
 frame-relay interface-dlci 17
```

Step 4: The data is received at CLEO.

Step 4:
CLEO

```
interface Serial1/1.1 point-to-point
 ip address CLEO.MobNet.S1/1.Int 255.255.255.248
 ip access-group 110 in
 ip mobile router-service roam
 no ip mroute-cache
 ipv6 address 2001:DB8:XXXX:6550::2/64
 ipv6 address 2001:DB8:XXXX:6650::2/64
 ipv6 enable
 frame-relay interface-dlci 17
```

3.2.8 IPv6 Static Route “Default” Return Path

The corresponding return path is extremely non-intuitive. The source address is an IPv6 address corresponding to an interface or tunnel end-point on CLEO (the previous destination address).

Step 1: If the destination address is an IPv6 address that does not reside in CLEO’s route tables, then the IPv6 traffic takes the default IPv6 route, Tunnel6010.

CLEO / Mobile Router
Step 1:

```
ipv6 route ::/0 Tunnel6010
```

Step 2: The IPv6 traffic is encapsulated in a IPv6-in-IPv4 tunnel with a source address of the loopback1 interface, CLEO.MobNet.Loopback.Addr, and a destination address of the IPv4 HA, HomeAgent.Net.HArouter.

CLEO / Mobile Router
Step 2:

```
interface Tunnel6010
 description "IPv6 Tunnel to CLEO_HA via MR protocol"
 no ip address
 ipv6 address 2001:DB8:XXXX:6010::2/64
 ipv6 enable
 tunnel source Loopback1
 tunnel destination HomeAgent.Net.HArouter
 tunnel mode ipv6ip
```

Reference for Step 2 :

```
interface Loopback1
 ip address CLEO.MobNet.Loopback.Addr 255.255.255.255
```

Step 3: If the IPv4 mobile router has registered with the HA, the default path is the active Mobile IP interface. If the IPv4 mobile router **is not** registered with the home agent, then the default route is taken. In the configuration here, this is the Serial 1/1.1 interface. The static route is weighted with a low priority of “245”. If Mobile IP registrations are active, the Mobile IP route weight is “100”, the Cisco default weight for Mobile IP. Therefore, Mobile IP routes have higher precedence than the specified static default route, which has a weight of “254”. Thus, traffic will use the active Mobile IP interface if Mobile IP registrations are active – no matter which interface that is, or which SSDR is in bridging ‘pass-through’ mode to support that interface.

CLEO / Mobile Router
Step 3:

```
ip route 0.0.0.0 0.0.0.0 Serial1/1.1 245
```

Step 4: Any data on Interface Serial 0/0.1 with a source address of CLEO.MobNet.S1/0.Net through CLEO.MobNet.Aggrigated.end is sent to HA-SSTL.ipip.psuedo-rev-tunnel.HA, which is Tunnel7. The key commands are highlighted below.

SSTL Ground Router
Step 3:

```
interface Serial0/1.1 point-to-point
 ip unnumbered FastEthernet0/0
 ip nat inside
 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
 ipv6 address 2001:DB8:XXXX:6550::1/64
 ipv6 enable
 no arp frame-relay
 no cdp enable
 frame-relay interface-dlci 17
```

Reference for Step 4:

```
route-map mr_subnets permit 10
 match ip address 7
 set ip default next-hop HA-SSTL.ipip.psuedo-rev-tunnel.HA
```

Sub- Reference for Step 4:

```
access-list 7 permit CLEO.MobNet.S1/0.Net 0.0.0.31
```

Step 5: A tunnel has to be established between the ground station routers (Foreign Agent routers for IPv4) and the anchor router (Home Agent router for IPv4) in order to defeat both egress filtering and policy rules at the firewalls. In this configuration, that tunnel is Tunnel 7. This tunnel can also be thought of as a pseudo-reverse-tunnel for Mobile IP. Note,one of the reasons to deploy reverse tunneling is firewall traversal. Tunneling results in the packet being encapsulated with a source address of SSTL.WAN.FA0/0, the SSTL ground router WAN Ethernet interface, and the destination address of HomeAgent.Net.HArouter, the HA router.

Step 5:

```
interface Tunnel7
 ip addressHA-SSTL.ipip.psuedo-rev-tunnel.SSTL 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination HomeAgent.Net.HArouter
 tunnel mode ipip
```

Reference for Step 5:

```
interface FastEthernet0/0
 description connected to Groundstation Subnet0
 ip address SSTL.WAN.FA0/0 255.255.255.0
```

Step 6: The Tunnel 7 packet is sent to the SSTL firewall, where it is encrypted and passed over an IPsec tunnel to the GRC CLEO/VMOC firewall. The IPsec packet is decrypted. The firewall knows to forward packets with a destination address of HomeAgent.Net.HArouter to the HA router, the IPv6 anchor router. The first encapsulation is removed. Now the packet is in an IPv6-in-IPv4 tunnel, tunnel 6010, whose source is CLEO.MobNet.Loopback.Addr (CLEO Loopback 1, MR IPv6 address), destination HomeAgent.Net.HArouter. The packet is de-encapsulated again and the IPv6 addresses exposed. At this point, normal IPv6 routing now takes over.

Note: Packets are forwarded through the network via multiple layers of static routing. This works for what we were trying to demonstrate. This is, however, NOT recommended practice for operational systems, which should be architected more cleanly.

4 Tests and Demonstrations

The two questions that were addressed in the tests and demonstrations were:

1) Is it viable to run IPv6 on a space-based asset?

2) Can one secure the RF link using network-layer security (IPv4 IPsec)?

Network services that have been demonstrated with CLEO to date for common network technologies are shown in the following table:

Demonstration	**IPv4**	**IPv6**	**IPv4/ IPsec**
Console port access via the CAN bus	X		
Telnet	X	X	X
Static Routing	X	X	X
Mobile-IP NEMO	X	Q	DNC
HTTP	X	X	X
SHTTP	X	X	X
Secure Shell	X	X	
TFTP	X		
FTP	X		
Cisco IOS command line functionality	X	X	
Earth image file transfer from an SSDR to ground through CLEO using static routing	X		

Q ≡ Qualified as follows: IPv6 was encapsulated in IPv4 and IPv4 NEMO was used. The current IPv6 NEMO was not yet developed when the CLEO IOS was loadind in 2003.

DNC ≡ Did Not Configure. With some thought, we may be able to demonstrate this, but the value was not considered worth the effort and IPv4 IPsec has already been demonstrated in other configurations.

The router in orbit, CLEO, was configured and tested during periods of up to twelve minutes while the UK-DMC satellite passed over SSTL's ground station. Static IPv6 and IPv4 routing and IPv4 mobile routing were operated simultaneously. IPsec for IPv4, secure shell using IPv6, Telnet for IPv6 over and IPv4 IPsec tunnel, and Web browsing to the router using IPv6 over an IPv4 IPsec tunnel were demonstrated, as were:

- Console port access via the Controller Area Network (CAN) bus
- Telnet
- Static Routing
- Mobile-IP mobile networks
- Router access via Hypertext Transfer Protocol (HTTP)
- Secure Shell (ssh) access
- Secure Web access
- Trivial File Transfer Protocol (TFTP) copying of configuration files to ground
- File Transfer Protocol (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

See Appendix C for detailed test logs.

5 Use of other Ground Stations

Use of other ground stations with CLEO and the UK-DMC satellite for IPv6 capability testing is underway. Universal Space Network (USN) was involved in previous testing of CLEO with IPv4, and is examining similar testing for IPv6, as is the Japanese National Institute of Information and Communications Technology (NICT). In configuring unique IPv6 addresses with these ground stations, the existing SSTL network model used by DMC ground stations which uses a private IPv4 local area network (LAN) and uses NAT to connect to the public Internet. The SSTL model was designed for a single ground station, and has simply been duplicated as the number of ground stations has been increased.

The Multi-Use Ground Station (MUGS) project has also examined IPv6 access to CLEO [Miller06]. However, the phased-array antenna in use with MUGS has been unsuccessful at closing the downlink at the high-rate of 8.1 Mbps, thereby making access to CLEO during a pass problematic. CLEO is currently only reached using this high-rate downlink.

The MUGS antenna can successfully close a low-rate 38.4kbps downlink from the UK-DMC satellite. Access to CLEO via the low-rate downlink will be possible after a firmware modification that allows downlink connectivity to CLEO via changing the powerful 8 Mbps transmitter to send at 38.4 kbps, increasing the chances of successful reception by the MUGS antenna. Such firmware has recently been developed and successful testing was performed on the 15th of October, 2007.

6 Other possible tests

Now that IPv4, IPv6 and IPsec have been shown to work onboard the UK-DMC satellite with the CLEO router, the major testing of this Cisco router in space is complete, and the router has been shown to be as functional as its terrestrial counterparts.

Another test envisioned involves network management. This would demonstrate that a space payload could be managed from ground systems using the Simple Network Management Protocol (SNMP) and commercially-available network management software, just as terrestrial networked devices are managed.

7 Header compression

One complaint about IPv6 is that its larger address space leads to larger IP headers, which decreases link utilization. While this becomes an important concern for small packets, such as Voice over IP (VoIP) where the payload size is roughly similar to the header size, the impact on larger packets, especially at maximum link transmission unit (MTU) sizes, is minimal.

One way to decrease header overhead still further is to use header compression across serial links. However, header compression is always the last part of a networking standard to be agreed and then implemented; in this case header compression over standard Frame Relay links was only agreed in 2001 [FRF20]. The IOS firmware flown onboard CLEO does not implement header compression over Frame Relay or of IPv6 headers, so this could not be used.

8 Summary and Conclusions

So long as one has an IP compliant system in space and utilizes the *proper IP protocols*, IP in space is relatively simple and one can run any delay or disruption tolerant application once connectivity is established, particulary in regarding LEO systems. Proper IP protocols and applications requires awareness of the round trip time (RTT) delays, asymmetry of the links, and other link characteristics when chosing which protocols and applications to use.

The UK-DMC has low error-rates low round-trip times, and high link-asymmetry (i.e. 9600 bps up and 8.14 Mbps down). The UK-DMC can be thought of as an example of a Delay/Disruption Tolerant Network (DTN). Delay is not an issue for this LEO system, but connectivity is intermittent, though predictable (scheduled). Passes last on average 8 to 12 minutes. Hence DTN techniques are applicable. SSTL's current image transfer techniques utilize DTN technology, albeit non-standard. The are working to standardize some of their protocols within the Internet Engineering Task Force (IETF) and Internet Research Task Force (IRTF).

Static routing was useful here for testing it provided deterministic paths that would force traffic over specific links such as an IPsec space/ground link or a native IPv6 space/ground link for testing purposes. **Do not use static routes this in an operational system.** *A major requirement of an operational system should be that the operational system be capable of operation without deterministic paths.* That is, for an operational system dynamic routing, Mobile-IP or something other than static routes should be used. *Predictive static routing is NOT a recommended practice, since this DOES NOT SCALE AND IS NOT EASILY MAINTAINABLE.*

9 Organizations and Contacts

9.1 Participating Organizations

NASA Glenn Research Center (NASA GRC) – secure mobile networking expertise.
Cisco Systems – CLEO router, funded integration work with SSTL.
Surrey Satellite Technology Ltd (SSTL) – DMC satellites, imaging and infrastructure support.
General Dynamics Advanced Information Systems (GD-AIS) – Army and Air Force Support.
Universal Space Network – Ground Stations
Air Force Research Lab (AFRL) – Provided Internet Protocol Commanding and Management of Satellites (IPCMS) system via USN contract.
Missile Defence Battle Lab (SMDBL) – Multi-User Ground Station (MUGS)

9.2 Points of Contact

Ivancic, Will	NASA GRC	Principal Investigator for IP in Space	wivancic@grc.nasa.gov	+1-216-433-3494
Stewart, David	Verizon	Network design, integration and test	dstewart@grc.nasa.gov	+1-216-433-9644
Wood, Lloyd	Cisco Systems	CLEO/VMOC project co-ordination	lwood@cisco.com	+44-20-8824-4236
Northam, James	SSTL	Operations	j.northam@sst;.co.uk	+44 (0)1483 803803
Jackson, Chris	SSTL	Operations	c.jackson@sstl.co.uk	+44 (0)1483 803803

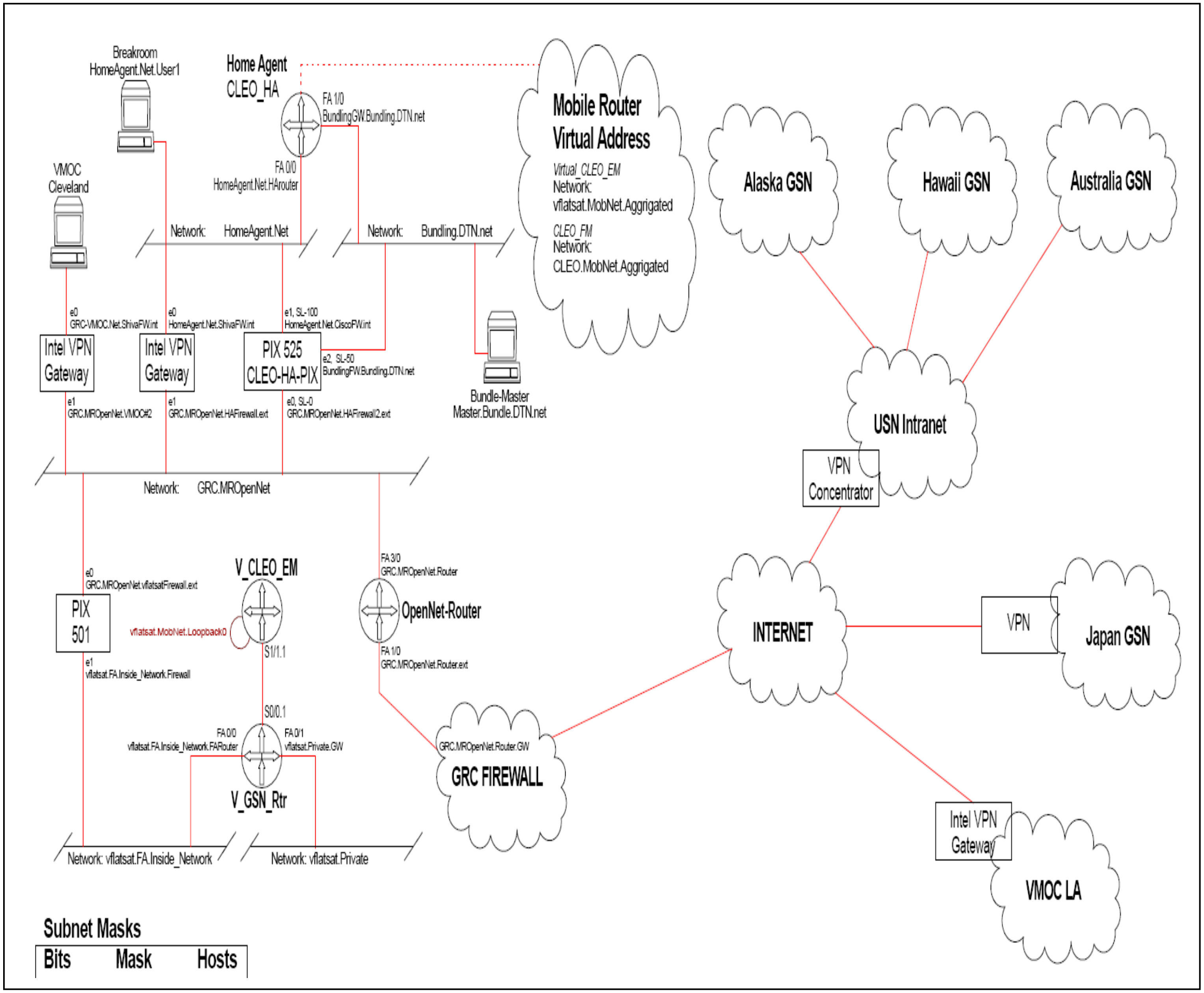
References

CLEO05	W. Ivancic, D. Stewart, D. Shell, L. Wood, P. Paulsen, C. Jackson, D. Hodgson, J. Northam, N. Bean, E. Miller, M. Graves and L. Kurisaki: “Secure, Network-Centric Operations of a Space-Based Asset: Cisco Router in Low-Earth Orbit (CLEO) and Virtual Mission Operations Center (VMOC),” NASA/TM-2005-213556, May 2005.
DMCII07	Cisco router on UK-DMC first to use IPv6 onboard a satellite in orbit, news item from DMC International Imaging, 29 March 2007.
Eddy06	W. Eddy, W. Ivancic and J. Ishac, “Analysis of IPv6 features and usability,” North American IPv6 Task Force Technology Report, September 2006.
FRF20	Frame Relay IP Header Compression Implementation Agreement, FRF.20, Frame Relay Forum Technical Committee, June 2001.
Miller06	E. Miller, A. Kirkham, W. Ivancic, et al., “Small satellite multi-mission command and control for maximum effect,” US Air Force Space Command's High Frontier, vol. 3 no. 1, pp. 58-64, November 2006.
RFC4193	R. Hinden, B. Haberman, “Unique Local IPv6 Unicast Addresses,” RFC 4193, October 2005.
SSTL07	SSTL satellites sign up for 2008 launch, SSTL press release, 8 October 2007.
Wood05	L. Wood, D. Shell, W. Ivancic, B. Conner, E. Miller, D. Stewart and D. Hodgson, |”CLEO and VMOC: enabling warfighters to task space payloads,” IEEE Milcom 2005, Atlantic City, New Jersey, 17-20 October 2005.
Wood07a	L. Wood, W. Ivancic, D. Hodgson, E. Miller, B. Conner, S. Lynch, C. Jackson, A. da Silva Curiel, D. Shell, J. Walke and D. Stewart, “Using Internet nodes and routers onboard satellites,” Special issue on Space Networks, International Journal of Satellite Communications and Networking, vol. 25 issue 2, pp. 195-216, March/April 2007.
Wood07b	L. Wood, W. Ivancic, D. Stewart, J. Northam, C. Jackson and A. da Silva Curiel, “IPv6 and IPsec on a satellite in space,” paper IAC-07-B2.6.06, 58th International Astronautical Congress, Hyderabad, India, September 2007.
Wood07c	L. Wood, W. M. Eddy, W. Ivancic, J. McKim and C. Jackson, “Saratoga: a Delay-Tolerant Networking convergence layer with efficient link utilization,” International Workshop on Space and Satellite Communications (IWSSC '07), Salzburg, September 2007.
Wood07d	L. Wood, W. M. Eddy, W. Ivancic, J. McKim and C. Jackson, “Saratoga: A Scalable File Transfer Protocol,” work in progress as an internet-draft, version -00 submitted to the IETF TSVWG working group, October 2007.

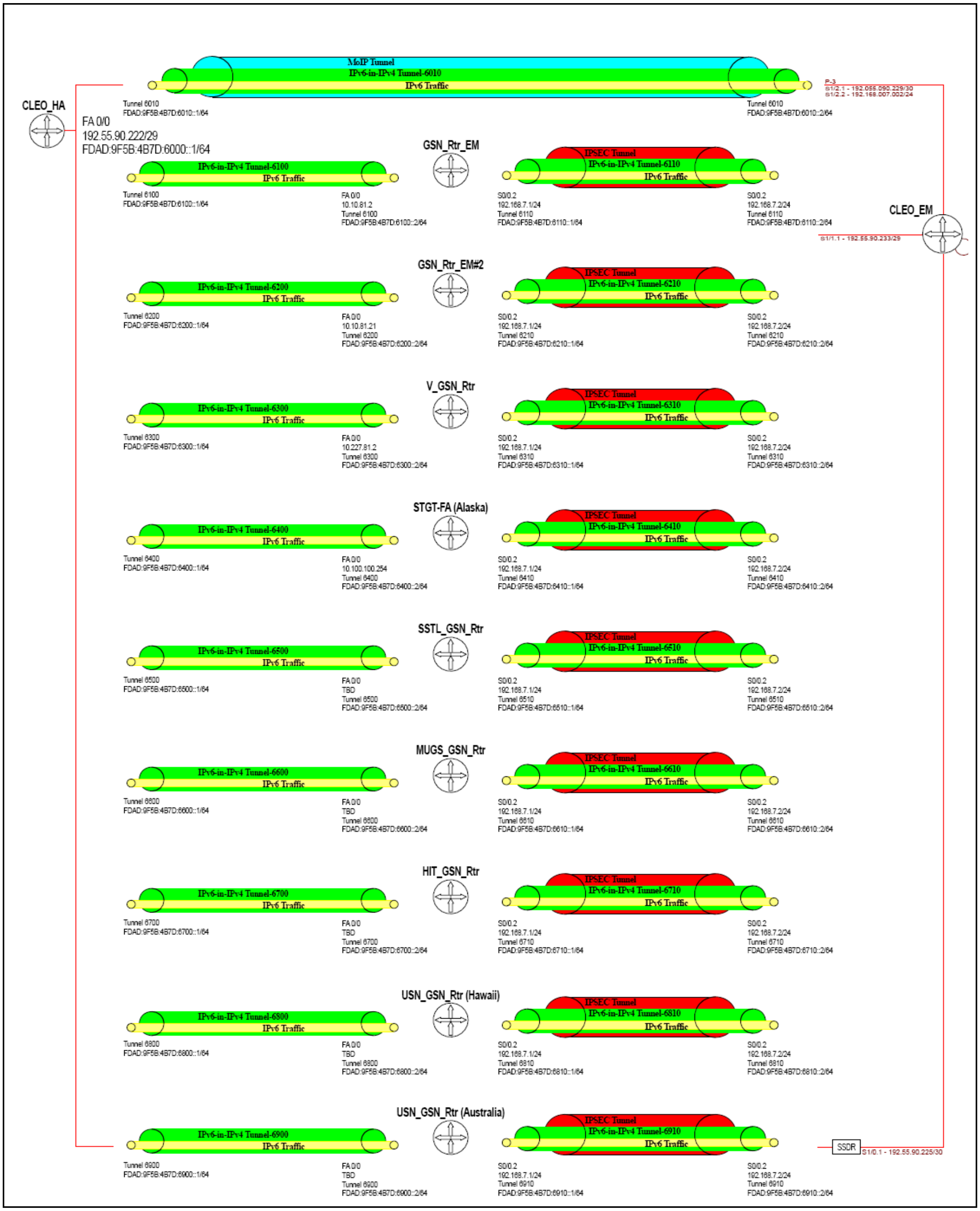
Appendices

A. IPv6 Network Topologies

A.1. CLEO Mobile Router Topology

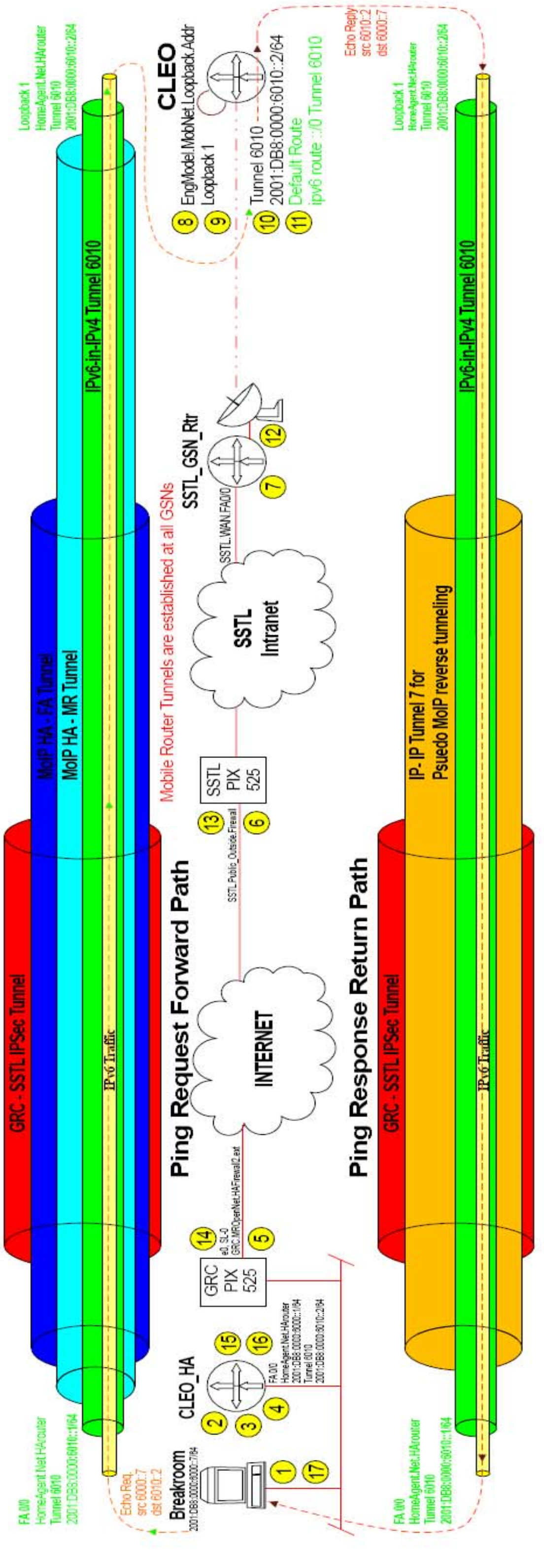


A.2. Predictive Static Routing (Nine Ground Station Destinations)



B. IPv6 Ping over IPv4 Mobile Network

B.1. Data Flow



Ⓝ Corresponds to the step in the ping Sequence. (see Excel spreadsheet)

🟧 IP- IP Tunnel 7

🟥 VPN IPSec Tunnel

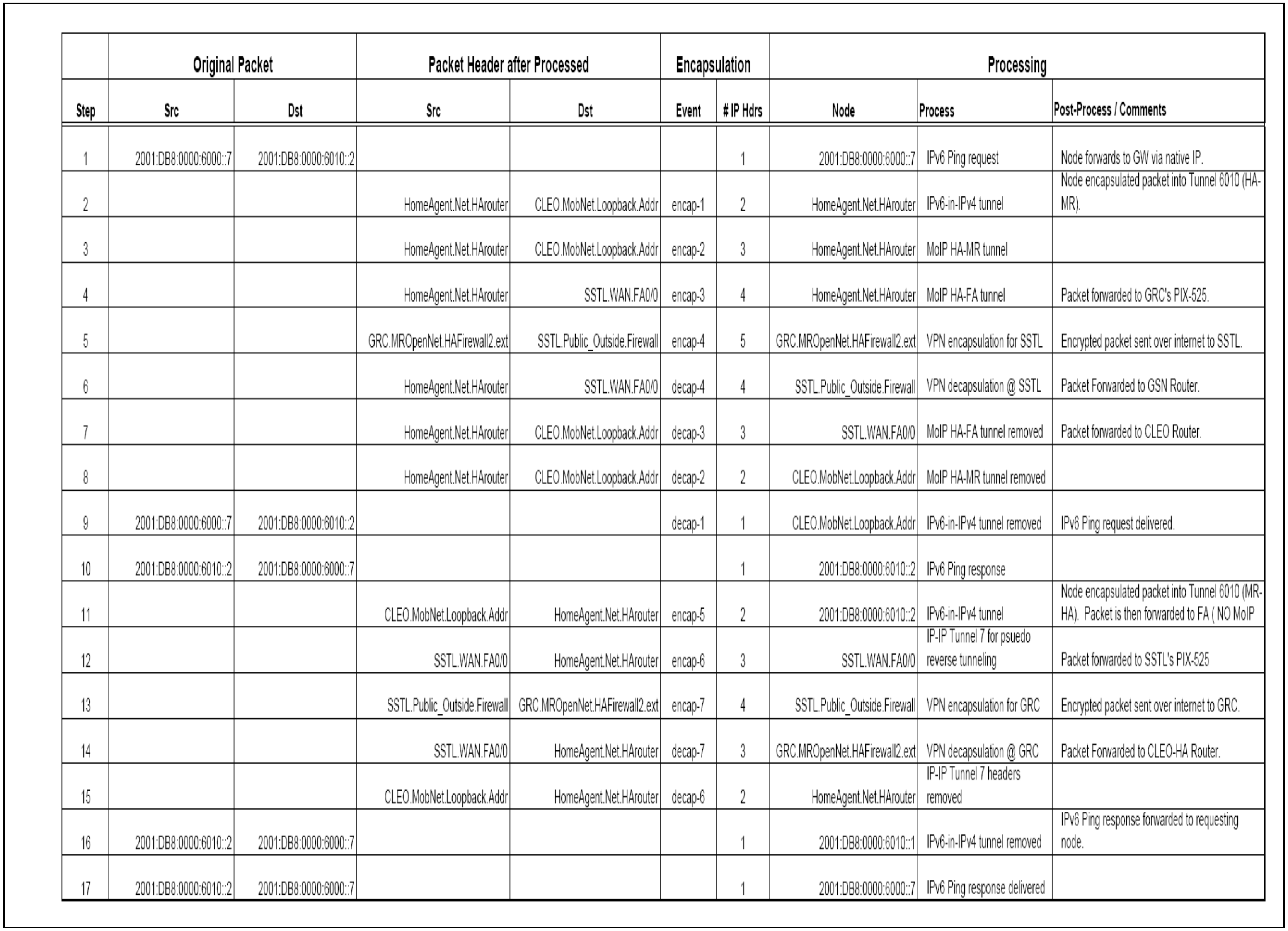
🟦 MoIPv4 HA-MR Tunnel

🟦 MoIPv4 HA-FA Tunnel

🟩 IPv6-in-IPv4 Tunnel 6010

🟨 IPv6 Traffic (no Tunnel)

Tunnel Composition by Sequence



	Original Packet		Packet Header after Processed		Encapsulation		Processing		
Step	Src	Dst	Src	Dst	Event	# IP Hdrs	Node	Process	Post-Process / Comments
1	2001:DB8:0000:6000::7	2001:DB8:0000:6010::2				1	2001:DB8:0000:6000::7	IPv6 Ping request	Node forwards to GW via native IP.
2			HomeAgent.Net.HArouter	CLEO.MobNet.Loopback.Addr	encap-1	2	HomeAgent.Net.HArouter	IPv6-in-IPv4 tunnel	Node encapsulated packet into Tunnel 6010 (HA-MR).
3			HomeAgent.Net.HArouter	CLEO.MobNet.Loopback.Addr	encap-2	3	HomeAgent.Net.HArouter	MoIP HA-MR tunnel	
4			HomeAgent.Net.HArouter	SSTL.WAN.FA0/0	encap-3	4	HomeAgent.Net.HArouter	MoIP HA-FA tunnel	Packet forwarded to GRC's PIX-525.
5			GRC.MROpenNet.HAFirewall2.ext	SSTL.Public_Outside.Firewall	encap-4	5	GRC.MROpenNet.HAFirewall2.ext	VPN encapsulation for SSTL	Encrypted packet sent over internet to SSTL.
6			HomeAgent.Net.HArouter	SSTL.WAN.FA0/0	decap-4	4	SSTL.Public_Outside.Firewall	VPN decapsulation @ SSTL	Packet Forwarded to GSN Router.
7			HomeAgent.Net.HArouter	CLEO.MobNet.Loopback.Addr	decap-3	3	SSTL.WAN.FA0/0	MoIP HA-FA tunnel removed	Packet forwarded to CLEO Router.
8			HomeAgent.Net.HArouter	CLEO.MobNet.Loopback.Addr	decap-2	2	CLEO.MobNet.Loopback.Addr	MoIP HA-MR tunnel removed	
9	2001:DB8:0000:6000::7	2001:DB8:0000:6010::2			decap-1	1	CLEO.MobNet.Loopback.Addr	IPv6-in-IPv4 tunnel removed	IPv6 Ping request delivered.
10	2001:DB8:0000:6010::2	2001:DB8:0000:6000::7				1	2001:DB8:0000:6010::2	IPv6 Ping response	
11			CLEO.MobNet.Loopback.Addr	HomeAgent.Net.HArouter	encap-5	2	2001:DB8:0000:6010::2	IPv6-in-IPv4 tunnel	Node encapsulated packet into Tunnel 6010 (MR-HA). Packet is then forwarded to FA (NO MoIP
12			SSTL.WAN.FA0/0	HomeAgent.Net.HArouter	encap-6	3	SSTL.WAN.FA0/0	IP-IP Tunnel 7 for psuedo reverse tunneling	Packet forwarded to SSTL's PIX-525
13			SSTL.Public_Outside.Firewall	GRC.MROpenNet.HAFirewall2.ext	encap-7	4	SSTL.Public_Outside.Firewall	VPN encapsulation for GRC	Encrypted packet sent over internet to GRC.
14			SSTL.WAN.FA0/0	HomeAgent.Net.HArouter	decap-7	3	GRC.MROpenNet.HAFirewall2.ext	VPN decapsulation @ GRC	Packet Forwarded to CLEO-HA Router.
15			CLEO.MobNet.Loopback.Addr	HomeAgent.Net.HArouter	decap-6	2	HomeAgent.Net.HArouter	IP-IP Tunnel 7 headers removed	
16	2001:DB8:0000:6010::2	2001:DB8:0000:6000::7				1	2001:DB8:0000:6010::1	IPv6-in-IPv4 tunnel removed	IPv6 Ping response forwarded to requesting node.
17	2001:DB8:0000:6010::2	2001:DB8:0000:6000::7				1	2001:DB8:0000:6000::7	IPv6 Ping response delivered	

C. Test Logs

C.1. IPsec Security Associations

Note: Peers are GS-CLEO.IPsec.Tunnel.CLEO (CLEO Interface) and GS-CLEO.IPsec.Tunnel.GSN (SSTL ground router interface)

Note: Repeated “show crypto ip security associations” commands will show increasing crypto counters.

C.1.1. SSTL Ground Router

PuTTY log 2007.03.29 06:14:42

```
router2# sh cryp ip sa
interface: Serial0/1.2
  Crypto map tag: CLEO_auth, local addr. GS-CLEO.IPsec.Tunnel.GSN

 protected vrf:
 local ident (addr/mask/prot/port): (GS-CLEO.IPsec.Tunnel.Net/255.255.255.0/0/0)
 remote ident (addr/mask/prot/port): (GS-CLEO.IPsec.Tunnel.Net/255.255.255.0/0/0)
 current_peer: GS-CLEO.IPsec.Tunnel.CLEO:500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 9, #pkts encrypt: 9, #pkts digest 9
  #pkts decaps: 9, #pkts decrypt: 9, #pkts verify 9
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 36, #recv errors 0

  local crypto endpt.: GS-CLEO.IPsec.Tunnel.GSN, remote crypto endpt.: GS-CLEO.IPsec.Tunnel.CLEO
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1.2
  current outbound spi: 64D89AF7

  inbound esp sas:
   spi: 0x14B91BCA(347675594)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2000, flow_id: 1, crypto map: CLEO_auth
    sa timing: remaining key lifetime (k/sec): (4463194/3457)
    IV size: 8 bytes
    replay detection support: Y

  inbound ah sas:
  inbound pcp sas:
  outbound esp sas:
   spi: 0x64D89AF7(1691917047)
```

```
router2#sh cryp ip sa

interface: Serial0/1.2
  Crypto map tag: CLEO_auth, local addr. GS-CLEO.IPsec.Tunnel.GSN

 protected vrf:
 local ident (addr/mask/prot/port): (GS-CLEO.IPsec.Tunnel.Net/255.255.255.0/0/0)
 remote ident (addr/mask/prot/port): (GS-CLEO.IPsec.Tunnel.Net/255.255.255.0/0/0)
 current_peer: GS-CLEO.IPsec.Tunnel.CLEO:500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 193, #pkts encrypt: 193, #pkts digest 193
  #pkts decaps: 83, #pkts decrypt: 83, #pkts verify 83
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 36, #recv errors 0

  local crypto endpt.: GS-CLEO.IPsec.Tunnel.GSN, remote crypto endpt.: GS-
CLEO.IPsec.Tunnel.CLEO
  path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1.2
  current outbound spi: 64D89AF7

  inbound esp sas:
   spi: 0x14B91BCA(347675594)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2000, flow_id: 1, crypto map: CLEO_auth
    sa timing: remaining key lifetime (k/sec): (4463181/3036)
    IV size: 8 bytes
    replay detection support: Y

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x64D89AF7(1691917047)
```

C.1.2. CLEO

```
CLEO-MR#sh cry ip sa

interface: Serial1/1.2
  Crypto map tag: CLEO_auth, local addr. GS-CLEO.IPsec.Tunnel.CLEO

 local ident (addr/mask/prot/port): (GS-CLEO.IPsec.Tunnel.Net/255.255.255.0/0/0)
 remote ident (addr/mask/prot/port): (GS-CLEO.IPsec.Tunnel.Net/255.255.255.0/0/0)
 current_peer: GS-CLEO.IPsec.Tunnel.GSN
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 54, #pkts encrypt: 54, #pkts digest 54
  #pkts decaps: 64, #pkts decrypt: 64, #pkts verify 64
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: GS-CLEO.IPsec.Tunnel.CLEO, remote crypto endpt.: GS-CLEO.IPsec.Tunnel.GSN
  path mtu 1500, media mtu 1500
  current outbound spi: 14B91BCA

  inbound esp sas:
   spi: 0x64D89AF7(1691917047)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2000, flow_id: 1, crypto map: CLEO_auth
    sa timing: remaining key lifetime (k/sec): (4607985/3374)
    IV size: 8 bytes
    replay detection support: Y

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x14B91BCA(347675594)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
```

CLEO-MR#sh cry ip sa

```
interface: Serial1/1.2
  Crypto map tag: CLEO_auth, local addr. GS-CLEO.IPsec.Tunnel.CLEO

 local ident (addr/mask/prot/port): (GS-CLEO.IPsec.Tunnel.Net/255.255.255.0/0/0)
 remote ident (addr/mask/prot/port): (GS-CLEO.IPsec.Tunnel.Net/255.255.255.0/0/0)
 current_peer: GS-CLEO.IPsec.Tunnel.GSN
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 62, #pkts encrypt: 62, #pkts digest 62
  #pkts decaps: 70, #pkts decrypt: 70, #pkts verify 70
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: GS-CLEO.IPsec.Tunnel.CLEO, remote crypto endpt.: GS-
CLEO.IPsec.Tunnel.GSN
  path mtu 1500, media mtu 1500
  current outbound spi: 14B91BCA

  inbound esp sas:
   spi: 0x64D89AF7(1691917047)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2000, flow_id: 1, crypto map: CLEO_auth
    sa timing: remaining key lifetime (k/sec): (4607984/3366)
    IV size: 8 bytes
    replay detection support: Y

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x14B91BCA(347675594)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
```

```
CLEO-MR# sh cry ip sa

interface: Serial1/1.2
  Crypto map tag: CLEO_auth, local addr. GS-CLEO.IPsec.Tunnel.CLEO

 local ident (addr/mask/prot/port): (GS-CLEO.IPsec.Tunnel.Net/255.255.255.0/0/0)
 remote ident (addr/mask/prot/port): (GS-CLEO.IPsec.Tunnel.Net/255.255.255.0/0/0)
 current_peer: GS-CLEO.IPsec.Tunnel.GSN
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 70, #pkts encrypt: 70, #pkts digest 70
  #pkts decaps: 76, #pkts decrypt: 76, #pkts verify 76
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

  local crypto endpt.: GS-CLEO.IPsec.Tunnel.CLEO, remote crypto endpt.: GS-CLEO.IPsec.Tunnel.GSN
  path mtu 1500, media mtu 1500
  current outbound spi: 14B91BCA

  inbound esp sas:
   spi: 0x64D89AF7(1691917047)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 2000, flow_id: 1, crypto map: CLEO_auth
    sa timing: remaining key lifetime (k/sec): (4607983/3359)
    IV size: 8 bytes
    replay detection support: Y

  inbound ah sas:

  inbound pcp sas:

  outbound esp sas:
   spi: 0x14B91BCA(347675594)
    transform: esp-des esp-md5-hmac ,
    in use settings ={Tunnel, }
```

C.2. IPv6 Telnet to CLEO from Remote Host, “Breakroom”

```
User Access Verification

Username: sstl
Password:

CLEO-MR#sh run
Building configuration...

Current configuration : 5651 bytes
!
! Last configuration change at 10:13:19 utc Thu Mar 29 2007 by sstl
! NVRAM config last updated at 10:13:21 utc Thu Mar 29 2007 by sstl
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CLEO-MR
```

C.3. IPv6 Telnet IPv6 SSH to CLEO from Remote Host, “Breakroom”

```
login as: sstl
Sent username "sstl"
sstl@2001:DB8:XXXX:6550::2's password:

CLEO-MR#sh run
Building configuration...

Current configuration : 5651 bytes
!
! Last configuration change at 10:13:19 utc Thu Mar 29 2007 by sstl
! NVRAM config last updated at 10:13:21 utc Thu Mar 29 2007 by sstl
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CLEO-MR
!.
```

C.4. tracert cleo-6

```
Tracing route to CLEO-6 [2001:DB8:XXXX:6010::2]
over a maximum of 30 hops:

 1  <1 ms  <1 ms  <1 ms 2001:DB8:XXXX:6000::1
 2 358 ms 358 ms 357 ms CLEO-6 [2001:DB8:XXXX:6010::2]

Trace complete.

C:\Documents and Settings\dstewart>tracert mr-sstl-6

Tracing route to MR-SSTL-6 [2001:DB8:XXXX:6510::2]
over a maximum of 30 hops:

 1  <1 ms  <1 ms  <1 ms 2001:DB8:XXXX:6000::1
 2  *    *    *  Request timed out.
 3 407 ms 407 ms 407 ms MR-SSTL-6 [2001:DB8:XXXX:6510::2]

Trace complete.

C:\Documents and Settings\dstewart>tracert mr-sstl-6n

Tracing route to MR-SSTL-6n [2001:DB8:XXXX:6550::2]
over a maximum of 30 hops:

 1  <1 ms  <1 ms  <1 ms 2001:DB8:XXXX:6000::1
 2  *    *    *  Request timed out.
 3  *    *    *  Request timed out.
 4  *    *    *  Request timed out.
 5  *    *    *  Request timed out.
 6  *  ^C ← Reverse path is via pseudo-reverse tunnel!
```

D. Router Configurations and Route Tables

D.1. CLEO – Home Agent Configuration

(Home Agent router for CLEO, CLEO – EM and Virtual FlatSat)

```
Current configuration : 10862 bytes
!
! No configuration change since last restart
!
ersion 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CLEO_HA
!
enable password cisco
!
ip subnet-zero
!
ip ftp username vmoc
ip ftp password sstl
no ip domain lookup
!
ipv6 unicast-routing
!
mta receive maximum-recipients 0
!
interface Tunnel5
 description "MR subnets reachback for triangular routing from FlatSat."
 ip address HA-Flatsat.ipip.psuedo-rev-tunnel.HA 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination SSTL.WAN.FA0/0
 tunnel mode ipip
!
interface Tunnel6
 description "MR subnets reachback for triangular routing from V_FlatSat."
 ip address HA-vflatsat.ipip.psuedo-rev-tunnel.HA 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination vflatsat.WAN.FA0/0
 tunnel mode ipip
!
interface Tunnel7
 description "MR subnets reachback for triangular routing from SSTL's GSN FA"
 ip address HA-SSTL.ipip.psuedo-rev-tunnel.HA 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination SSTL.WAN.FA0/0
 tunnel mode ipip
!
interface Tunnel13
 description "MR subnets reachback for triangular routing from CLEO_MR's MUGS' GSN FA"
 ip address HA-MUGS.ipip.psuedo-rev-tunnel.HA 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination MUGS.WAN.FA0/01
 tunnel mode ipip
!
interface Tunnel22
 description "MR subnets reachback for triangular routing from CLEO_EM's 2nd GSN FA - GSN_Rtr_EM#2"
 ip address HA-EM2FA.ipip.psuedo-rev-tunnel.HA 255.255.255.0
 tunnel source HomeAgent.Net.HArouter
 tunnel destination SSTL.WAN.FA0/01
 tunnel mode ipip
!
interface Tunnel6010
 description "IPv6 Tunnel to CLEO via MR tunnels"
 no ip address
 ipv6 address 2001:DB8:XXXX:6010::1/64
 ipv6 enable
 tunnel source HomeAgent.Net.HArouter
 tunnel destination CLEO.MobNet.Loopback.Addr
 tunnel mode ipv6ip
!
interface Tunnel6020
 description "IPv6 Tunnel to Virtual CLEO_EM via MR tunnels"
 no ip address
 ipv6 address 2001:DB8:XXXX:6020::1/64
 ipv6 enable
 tunnel source HomeAgent.Net.HArouter
 tunnel destination vflatsat.MobNet.Loobpack0
 tunnel mode ipv6ip
!
interface Tunnel6030
 description "IPv6 Tunnel to CLEO_EM via MR tunnels"
 no ip address
 ipv6 address 2001:DB8:XXXX:6030::1/64
 ipv6 enable
 tunnel source HomeAgent.Net.HArouter
 tunnel destination EngModel.MobNet.Loopback.Addr
 tunnel mode ipv6ip
!
interface Tunnel6100
 description "IPv6-in-v4 Tunnel to 1st Flatsat GSN FA - GSN_Rtr_EM"
 no ip address
 ipv6 address 2001:DB8:XXXX:6100::1/64
 ipv6 enable
 tunnel source FastEthernet0/0
 tunnel destination SSTL.WAN.FA0/0
 tunnel mode ipv6ip
!
interface Tunnel6140
 description "IPv6-in-v4 Tunnel to 2nd Flatsat GSN FA - GSN_Rtr_EM for native IPv6"
 no ip address
 ipv6 address 2001:DB8:XXXX:6140::1/64
 ipv6 enable
 tunnel source HomeAgent.Net.HArouter
 tunnel destination SSTL.WAN.FA0/0
 tunnel mode ipv6ip
!
interface Tunnel6200
 description "IPv6-in-v4 Tunnel to 2nd Flatsat GSN FA - GSN_Rtr_EM#2"
 no ip address
 ipv6 address 2001:DB8:XXXX:6200::1/64
 ipv6 enable
 tunnel source HomeAgent.Net.HArouter
 tunnel destination vflatsat.WAN.FA0/01
 tunnel mode ipv6ip
!
interface Tunnel6240
 description "IPv6-in-v4 Tunnel to 2nd Flatsat GSN FA - GSN_Rtr_EM#2 for native IPv6"
 no ip address
 ipv6 address 2001:DB8:XXXX:6240::1/64
 ipv6 enable
 tunnel source HomeAgent.Net.HArouter
 tunnel destination vflatsat.WAN.FA0/01
 tunnel mode ipv6ip
!
interface Tunnel6300
 description "IPv6-in-v4 Tunnel to Virtual Flatsat GSN FA - V_GSN_Rtr"
 no ip address
 ipv6 address 2001:DB8:XXXX:6300::1/64
 ipv6 enable
 tunnel source FastEthernet0/0
 tunnel destination vflatsat.WAN.FA0/0
 tunnel mode ipv6ip
!
interface Tunnel6340
 description "IPv6-in-v4 Tunnel to Virtual Flatsat GSN FA - V_GSN_Rtr for Native IPv6"
 no ip address
 ipv6 address 2001:DB8:XXXX:6340::1/64
 ipv6 enable
 tunnel source FastEthernet0/0
 tunnel destination vflatsat.WAN.FA0/0
 tunnel mode ipv6ip
!
interface Tunnel6400
 description "IPv6-in-v4 Tunnel to USN's Alaska GSN FA - STGT-FA"
 no ip address
 ipv6 address 2001:DB8:XXXX:6400::1/64
 ipv6 enable
 tunnel source FastEthernet0/0
 tunnel destination USN-AK.WAN.FA0/0
 tunnel mode ipv6ip
!
interface Tunnel6500
 description "IPv6-in-v4 Tunnel to SSTL GSN Router"
 no ip address
 ipv6 address 2001:DB8:XXXX:6500::1/64
 ipv6 enable
 tunnel source HomeAgent.Net.HArouter
 tunnel destination SSTL.WAN.FA0/0
 tunnel mode ipv6ip
!
interface Tunnel6540
 description "IPv6-in-v4 Tunnel to SSTL GSN Router for native IPv6"
 no ip address
 ipv6 address 2001:DB8:XXXX:6540::1/64
 ipv6 enable
 tunnel source HomeAgent.Net.HArouter
 tunnel destination SSTL.WAN.FA0/0
 tunnel mode ipv6ip
!
interface Tunnel6600
 description "IPv6-in-v4 Tunnel to MUGS' GSN Router"
 no ip address
 ipv6 address 2001:DB8:XXXX:6600::1/64
 ipv6 enable
 tunnel source FastEthernet0/0
 tunnel destination MUGS.WAN.FA0/01
 tunnel mode ipv6ip
!
interface Tunnel6640
 description "IPv6-in-v4 Tunnel to MUGS GSN FA - MUGS_GSN_Rtr for Native IPv6"
 no ip address
 ipv6 address 2001:DB8:XXXX:6640::1/64
 ipv6 enable
 tunnel source FastEthernet0/0
 tunnel destination MUGS.WAN.FA0/01
 tunnel mode ipv6ip
!
interface Tunnel6700
 description "IPv6-in-v4 Tunnel to HIT GSN Router"
 no ip address
 ipv6 address 2001:DB8:XXXX:6700::1/64
 ipv6 enable
 tunnel source FastEthernet0/0
 tunnel mode ipv6ip
!
interface FastEthernet0/0
 ip address HomeAgent.Net.HArouter 255.255.255.248
 duplex auto
 speed auto
 ipv6 address 2001:DB8:XXXX:6000::1/64
 ipv6 enable
!
router mobile
!
ip classless
ip route 0.0.0.0 0.0.0.0 HomeAgent.Net.ShivaFW.int
ip route SSTL.WAN.Net 255.255.255.0 HomeAgent.Net.CiscoFW.int
ip route 10.2.205.0 255.255.255.0 HomeAgent.Net.CiscoFW.int
ip route EngModel.Net 255.255.255.0 HomeAgent.Net.CiscoFW.int
ip route Test.Net 255.255.255.0 HomeAgent.Net.CiscoFW.int
ip route SSTL.DMC.Net 255.255.255.0 HomeAgent.Net.ShivaFW.int
ip route SSTL.DMC.CLEO_Loopback 255.255.255.255 SSTL.WAN.FA0/0 200
ip route VMOC.Net.14 255.255.255.0 HomeAgent.Net.ShivaFW.int
ip route VMOC.Net.15 255.255.255.0 HomeAgent.Net.ShivaFW.int
ip route VMOC.Net.16 255.255.255.0 HomeAgent.Net.ShivaFW.int
ip http server
ip mobile home-agent
ip mobile virtual-network CLEO.MobNet.S1/0.Net 255.255.255.224
ip mobile virtual-network vflatsat.MobNet.Aggrigated 255.255.255.240
ip mobile virtual-network EngModel.MobNet.Aggrigated 255.255.255.224
ip mobile virtual-network EngModel.MobNet.Aggrigated 255.255.255.240
ip mobile host vflatsat.MobNet.Loobpack0 virtual-network EngModel.MobNet.Aggrigated 255.255.255.240
ip mobile host EngModel.MobNet.Loopback.Addr virtual-network EngModel.MobNet.Aggrigated 255.255.255.224
ip mobile host vflatsat.MobNet.Loobpack0 virtual-network vflatsat.MobNet.Aggrigated 255.255.255.240
ip mobile host CLEO.MobNet.Loopback.Addr virtual-network CLEO.MobNet.S1/0.Net 255.255.255.224
ip mobile mobile-networks vflatsat.MobNet.Loobpack0
 description "Test MR for verifying IPSEC to FA"
 network vflatsat.MobNet.Net1 255.255.255.248
 network vflatsat.MobNet.Net2 255.255.255.252
 network vflatsat.MobNet.Loobpack0 255.255.255.255
ip mobile mobile-networks EngModel.MobNet.Loopback.Addr
 description "Flatsat - CLEO_EM"
 network 10.55.90.248 255.255.255.248
 network EngModel.MobNet.S1/1.Net 255.255.255.248
 network EngModel.MobNet.S1/3.Net 255.255.255.252
 network EngModel.MobNet.S1/2.Net 255.255.255.252
 network EngModel.MobNet.Aggrigated 255.255.255.252
ip mobile mobile-networks vflatsat.MobNet.Loobpack0
 description " Virtual Flatsat - V_CLEO_EM "
 network vflatsat.MobNet.Loobpack0 255.255.255.255
 network vflatsat.MobNet.Net2 255.255.255.252
 network vflatsat.MobNet.Net1 255.255.255.248
ip mobile mobile-networks CLEO.MobNet.Loopback.Addr
 description " CLEO Space Asset - CLEO_FM "
 network CLEO.MobNet.S1/0.Net 255.255.255.252
 network CLEO.MobNet.S1/2.Net 255.255.255.252
 network CLEO.MobNet.S1/1.Net 255.255.255.248
 network CLEO.MobNet.S1/3.Net 255.255.255.252
 network 192.55.90.248 255.255.255.248
ip mobile secure host vflatsat.MobNet.Loobpack0 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.Loobpack0 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
!
access-list 1 permitHA-SSTL.ipip.psuedo-rev-tunnel.SSTL log
access-list 101 permit ip any host GRC.ntp.server
ipv6 host MR-EM2-6 2001:DB8:XXXX:6210::2
ipv6 host MR-EM1-6 2001:DB8:XXXX:6110::2
ipv6 host FE-EM1-6 2001:DB8:XXXX:6100::2
ipv6 host HA-EM1-6 2001:DB8:XXXX:6100::1
ipv6 host MR-EMV-6 2001:DB8:XXXX:6310::2
ipv6 host MR-SSTL-6 2001:DB8:XXXX:6510::2
ipv6 host CLEO-6 2001:DB8:XXXX:6010::2
ipv6 host MR-SSTL-6n 2001:DB8:XXXX:6550::2
ipv6 host FS-SSTL-6n 2001:DB8:XXXX:6550::1
ipv6 host FS-SSTL-6 2001:DB8:XXXX:6510::1
ipv6 host FE-SSTL-6 2001:DB8:XXXX:6500::2
ipv6 host FE-SSTL-6n 2001:DB8:XXXX:6540::2
ipv6 host HA-SSTL-6n 2001:DB8:XXXX:6540::1
ipv6 host HA-SSTL-6 2001:DB8:XXXX:6500::1
ipv6 host FS-MUGS-6 2001:DB8:XXXX:6610::1
ipv6 host FS-MUGS-6n 2001:DB8:XXXX:6650::1
ipv6 host FE-MUGS-6n 2001:DB8:XXXX:6640::2
ipv6 host FE-MUGS-6 2001:DB8:XXXX:6600::2
```

```
ipv6 host HA-MUGS-6 2001:DB8:XXXX:6600::1
ipv6 host HA-MUGS-6n 2001:DB8:XXXX:6640::1
ipv6 host V_flat-6 2001:DB8:XXXX:6020::2
ipv6 host FE-EMV-6 2001:DB8:XXXX:6300::2
ipv6 host FS-EMV-6 2001:DB8:XXXX:6310::1
ipv6 host FS-EM1-6 2001:DB8:XXXX:6110::1
ipv6 host HA-EM2-6 2001:DB8:XXXX:6200::1
ipv6 host FE-EM2-6 2001:DB8:XXXX:6200::2
ipv6 host FS-EM2-6 2001:DB8:XXXX:6210::1
ipv6 host HA-EMV-6 2001:DB8:XXXX:6300::1
ipv6 host HA-AK-6 2001:DB8:XXXX:6400::1
ipv6 host FE-AK-6 2001:DB8:XXXX:6400::2
ipv6 host FS-AK-6 2001:DB8:XXXX:6410::1
ipv6 host MR-AK-6 2001:DB8:XXXX:6410::2
ipv6 host MR-MUGS-6 2001:DB8:XXXX:6610::2
ipv6 host HA-HIT-6 2001:DB8:XXXX:6700::1
ipv6 host FE-HIT-6 2001:DB8:XXXX:6700::2
ipv6 host FS-HIT-6 2001:DB8:XXXX:6710::1
ipv6 host MR-HIT-6 2001:DB8:XXXX:6710::2
ipv6 host HA-HI-6 2001:DB8:XXXX:6800::1
ipv6 host FE-HI-6 2001:DB8:XXXX:6800::2
ipv6 host FS-HI-6 2001:DB8:XXXX:6810::1
ipv6 host MR-HI-6 2001:DB8:XXXX:6810::2
ipv6 host HA-AUSI-6 2001:DB8:XXXX:6900::1
ipv6 host FE-AUSI-6 2001:DB8:XXXX:6900::2
ipv6 host FS-AUSI-6 2001:DB8:XXXX:6910::1
ipv6 host MR-AUSI-6 2001:DB8:XXXX:6910::2
ipv6 host Flat-6 2001:DB8:XXXX:6030::2
ipv6 host MR-MUGS-6n 2001:DB8:XXXX:6650::2
ipv6 route 2001:DB8:XXXX:6110::/64 Tunnel6100
ipv6 route 2001:DB8:XXXX:6150::/64 Tunnel6140
ipv6 route 2001:DB8:XXXX:6210::/64 Tunnel6200
ipv6 route 2001:DB8:XXXX:6250::/64 Tunnel6240
ipv6 route 2001:DB8:XXXX:6310::/64 Tunnel6300
ipv6 route 2001:DB8:XXXX:6350::/64 Tunnel6340
ipv6 route 2001:DB8:XXXX:6410::/64 Tunnel6400
ipv6 route 2001:DB8:XXXX:6510::/64 Tunnel6500
ipv6 route 2001:DB8:XXXX:6550::/64 Tunnel6540
ipv6 route 2001:DB8:XXXX:6610::/64 Tunnel6600
ipv6 route 2001:DB8:XXXX:6650::/64 Tunnel6640
ipv6 route 2001:DB8:XXXX:6710::/64 Tunnel6700
!
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
line con 0
 exec-timeout 10000 0
 speed 115200
line aux 0
line vty 0 4
 exec-timeout 10000 0
 password cisco
 login
```

```
!
ntp clock-period 17180072
ntp server GRC.ntp.server
```

D.2. CLEO – Home Agent Route Tables

```
IPv6 Routing Table - 43 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
   U - Per-user Static route
   I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

L 2001:DB8:XXXX:6000::1/128 [0/0]   via ::, FastEthernet0/0
C 2001:DB8:XXXX:6000::/64 [0/0]     via ::, FastEthernet0/0
L 2001:DB8:XXXX:6010::1/128 [0/0]   via ::, Tunnel6010
C 2001:DB8:XXXX:6010::/64 [0/0]     via ::, Tunnel6010
L 2001:DB8:XXXX:6020::1/128 [0/0]   via ::, Tunnel6020
C 2001:DB8:XXXX:6020::/64 [0/0]     via ::, Tunnel6020
L 2001:DB8:XXXX:6030::1/128 [0/0]   via ::, Tunnel6030
C 2001:DB8:XXXX:6030::/64 [0/0]     via ::, Tunnel6030
L 2001:DB8:XXXX:6100::1/128 [0/0]   via ::, Tunnel6100
C 2001:DB8:XXXX:6100::/64 [0/0]     via ::, Tunnel6100
S 2001:DB8:XXXX:6110::/64 [1/0]     via ::, Tunnel6100
L 2001:DB8:XXXX:6140::1/128 [0/0]   via ::, Tunnel6140
C 2001:DB8:XXXX:6140::/64 [0/0]     via ::, Tunnel6140
S 2001:DB8:XXXX:6150::/64 [1/0]     via ::, Tunnel6140
L 2001:DB8:XXXX:6200::1/128 [0/0]   via ::, Tunnel6200
C 2001:DB8:XXXX:6200::/64 [0/0]     via ::, Tunnel6200
S 2001:DB8:XXXX:6210::/64 [1/0]     via ::, Tunnel6200
L 2001:DB8:XXXX:6240::1/128 [0/0]   via ::, Tunnel6240
C 2001:DB8:XXXX:6240::/64 [0/0]     via ::, Tunnel6240
S 2001:DB8:XXXX:6250::/64 [1/0]     via ::, Tunnel6240
L 2001:DB8:XXXX:6300::1/128 [0/0]   via ::, Tunnel6300
C 2001:DB8:XXXX:6300::/64 [0/0]     via ::, Tunnel6300
S 2001:DB8:XXXX:6310::/64 [1/0]     via ::, Tunnel6300
L 2001:DB8:XXXX:6340::1/128 [0/0]   via ::, Tunnel6340
C 2001:DB8:XXXX:6340::/64 [0/0]     via ::, Tunnel6340
S 2001:DB8:XXXX:6350::/64 [1/0]     via ::, Tunnel6340
L 2001:DB8:XXXX:6400::1/128 [0/0]   via ::, Tunnel6400
C 2001:DB8:XXXX:6400::/64 [0/0]     via ::, Tunnel6400
S 2001:DB8:XXXX:6410::/64 [1/0]     via ::, Tunnel6400
L 2001:DB8:XXXX:6500::1/128 [0/0]   via ::, Tunnel6500
C 2001:DB8:XXXX:6500::/64 [0/0]     via ::, Tunnel6500
S 2001:DB8:XXXX:6510::/64 [1/0]     via ::, Tunnel6500
L 2001:DB8:XXXX:6540::1/128 [0/0]   via ::, Tunnel6540
C 2001:DB8:XXXX:6540::/64 [0/0]     via ::, Tunnel6540
S 2001:DB8:XXXX:6550::/64 [1/0]     via ::, Tunnel6540
L 2001:DB8:XXXX:6600::1/128 [0/0]   via ::, Tunnel6600
C 2001:DB8:XXXX:6600::/64 [0/0]     via ::, Tunnel6600
S 2001:DB8:XXXX:6610::/64 [1/0]     via ::, Tunnel6600
L 2001:DB8:XXXX:6640::1/128 [0/0]   via ::, Tunnel6640
C 2001:DB8:XXXX:6640::/64 [0/0]     via ::, Tunnel6640
S 2001:DB8:XXXX:6650::/64 [1/0]     via ::, Tunnel6640
L FE80::/10 [0/0]                   via ::, Null0
L FF00::/8 [0/0]                    via ::, Null0
```

```
CLEO_HA#show hosts

Default domain is not set
Name/address lookup uses static mappings

Codes: UN - unknown, EX - expired, OK - OK, ?? - revalidate
       temp - temporary, perm - permanent
       NA - Not Applicable None - Not defined

Host                              Port  Flags      Age Type   Address(es)
MR-EM2-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6210::2
MR-EM1-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6110::2
FE-EM1-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6100::2
HA-EM1-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6100::1
MR-EMV-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6310::2
MR-SSTL-6                  None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6510::2
CLEO-6                     None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6010::2
MR-SSTL-6n                 None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6550::2
FS-SSTL-6n                 None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6550::1
FS-SSTL-6                  None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6510::1
FE-SSTL-6                  None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6500::2
FE-SSTL-6n                 None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6540::2
HA-SSTL-6n                 None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6540::1
HA-SSTL-6                  None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6500::1
FS-MUGS-6                  None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6610::1
FS-MUGS-6n                 None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6650::1
FE-MUGS-6n                 None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6640::2
FE-MUGS-6                  None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6600::2
HA-MUGS-6                  None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6600::1
HA-MUGS-6n                 None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6640::1
V_flat-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6020::2
FE-EMV-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6300::2
FS-EMV-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6310::1
FS-EM1-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6110::1
HA-EM2-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6200::1
FE-EM2-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6200::2
FS-EM2-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6210::1
HA-EMV-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6300::1
HA-AK-6                    None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6400::1
FE-AK-6                    None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6400::2
FS-AK-6                    None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6410::1
MR-AK-6                    None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6410::2
MR-MUGS-6                  None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6610::2
HA-HIT-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6700::1
FE-HIT-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6700::2
FS-HIT-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6710::1
MR-HIT-6                   None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6710::2
HA-HI-6                    None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6800::1
FE-HI-6                    None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6800::2
FS-HI-6                    None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6810::1
MR-HI-6                    None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6810::2
HA-AUSI-6                  None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6900::1
FE-AUSI-6                  None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6900::2
FS-AUSI-6                  None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6910::1
MR-AUSI-6                  None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6910::2
Flat-6                     None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6030::2
MR-MUGS-6n                 None  (perm, OK) 24  IPv6   2001:DB8:XXXX:6650::2
```

D.3. CLEO Configuration

```
Current configuration : 5651 bytes
!
! Last configuration change at 10:13:19 utc Thu Mar 29 2007 by sstl
! NVRAM config last updated at 10:13:21 utc Thu Mar 29 2007 by sstl
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CLEO-MR
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa session-id common
enable secret 5 $1$24lL$XO42qKW.681XToTMHZCSe1
enable password cisco123
!
username VMOC password 0 VMOC
username sstl privilege 15 password 0 sstl55
clock timezone utc 0
ip subnet-zero
!
ip ftp username vmoc
ip ftp password sstl
no ip domain lookup
ip domain name CLEO-MR.sstl.com
!
ip cef
ip audit notify log
ip audit po max-events 100
ip ssh time-out 60
ip ssh authentication-retries 2
ipv6 unicast-routing
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
 lifetime 60
crypto isakmp key CLEO_ IPSEC address GS-CLEO.IPsec.Tunnel.GSN
!
crypto  IPsec transform-set CLEO_set esp-des esp-md5-hmac
!
crypto map CLEO_auth 1  IPsec-isakmp
 set peer GS-CLEO.IPsec.Tunnel.GSN
 set transform-set CLEO_set
 match address 115
!
interface Loopback0
 ip address SSTL.DMC.CLEO_Loopback 255.255.255.255
!
interface Loopback1
```

```
 ip address CLEO.MobNet.Loopback.Addr 255.255.255.255
!
interface Tunnel6010
 description "IPv6 Tunnel to CLEO_HA via MR protocol"
 no ip address
 ipv6 address 2001:DB8:XXXX:6010::2/64
 ipv6 enable
 tunnel source Loopback1
 tunnel destination HomeAgent.Net.HArouter
 tunnel mode ipv6ip
!
interface Tunnel6510
 description IPv6-in-v4 tunnel for IPv6 traffic to/from CLEO_EM. Tunnel terminates at SSTL's GSN_Rtr via IPSEC v4 tunnel.
 no ip address
 ipv6 address 2001:DB8:XXXX:6510::2/64
 ipv6 enable
 tunnel source GS-CLEO.IPsec.Tunnel.CLEO
 tunnel destination GS-CLEO.IPsec.Tunnel.GSN
 tunnel mode ipv6ip
!
interface Tunnel6610
 description IPv6-in-v4 tunnel for IPv6 traffic to/from CLEO_EM. Tunnel terminates at MUGS_GSN_Rtr via IPSEC v4 tunnel.
 no ip address
 ipv6 address 2001:DB8:XXXX:6610::2/64
 ipv6 enable
 tunnel source GS-CLEO.IPsec.Tunnel.CLEO
 tunnel destination GS-CLEO.IPsec.Tunnel.GSN
 tunnel mode ipv6ip
!
interface FastEthernet0/0
 no ip address
 no ip mroute-cache
 shutdown
 duplex auto
 speed auto
 no cdp enable
!
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 CLEO.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
 ip access-group 110 out
 encapsulation frame-relay IETF
 no ip mroute-cache
 no keepalive
 ignore-dcd
 nrzi-encoding
interface Serial1/1.1 point-to-point
 ip address CLEO.MobNet.S1/1.Int 255.255.255.248
 ip access-group 110 in
 ip mobile router-service roam
 no ip mroute-cache
 ipv6 address 2001:DB8:XXXX:6550::2/64
 ipv6 address 2001:DB8:XXXX:6650::2/64
 ipv6 enable
 frame-relay interface-dlci 17
!
interface Serial1/1.2 point-to-point
 ip address GS-CLEO.IPsec.Tunnel.CLEO 255.255.255.0
 ip nat outside
 no ip mroute-cache
 no arp frame-relay
 no cdp enable
 frame-relay interface-dlci 18
 crypto map CLEO_auth
!
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 CLEO.MobNet.S1/2.Int 255.255.255.252
 ip mobile router-service roam
 no ip mroute-cache
 frame-relay interface-dlci 17
!
interface Serial1/3
 ip address CLEO.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.DMC.UK-DMC.OBP1 255.255.255.255 Serial1/0.1
ip route SSTL.DMC.UK-DMC.OBP2 255.255.255.255 Serial1/1.1
ip route SSTL.DMC.UK-DMC.OBP3 255.255.255.255 Serial1/2.1
ip route SSTL.DMC.UK-DMC.SSDR0 255.255.255.255 Serial1/0.1
ip route SSTL.DMC.UK-DMC.SSDR1 255.255.255.255 Serial1/1.1
ip route SSTL.DMC.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 CLEO.MobNet.Loopback.Addr 255.255.255.224
 home-agent HomeAgent.Net.HArouter priority 105
 register lifetime 60
!
access-list 110 deny ip any host SSTL.DMC.UK-DMC.OBP0
access-list 110 permit ip any any
access-list 115 permit ip GS-CLEO.IPsec.Tunnel.Net 0.0.0.255 GS-CLEO.IPsec.Tunnel.Net 0.0.0.255
ipv6 host HA-6 2001:DB8:XXXX:6010::1
ipv6 host CLEO-6 2001:DB8:XXXX:6010::2
ipv6 host FS-SSTL-6n 2001:DB8:XXXX:6550::1
ipv6 host FS-SSTL-6 2001:DB8:XXXX:6510::1
ipv6 host FE-SSTL-6 2001:DB8:XXXX:6500::2
ipv6 host FE-SSTL-6n 2001:DB8:XXXX:6540::2
ipv6 host HA-SSTL-6n 2001:DB8:XXXX:6540::1
ipv6 host HA-SSTL-6 2001:DB8:XXXX:6500::1
ipv6 host MR-SSTL-6 2001:DB8:XXXX:6510::2
ipv6 host MR-SSTL-6n 2001:DB8:XXXX:6550::2
ipv6 host FS-MUGS-6 2001:DB8:XXXX:6610::1
ipv6 host FS-MUGS-6n 2001:DB8:XXXX:6650::1
ipv6 host FE-MUGS-6n 2001:DB8:XXXX:6640::2
ipv6 host FE-MUGS-6 2001:DB8:XXXX:6600::2
ipv6 host HA-MUGS-6 2001:DB8:XXXX:6600::1
ipv6 host HA-MUGS-6n 2001:DB8:XXXX:6640::1
ipv6 host MR-MUGS-6 2001:DB8:XXXX:6610::2
ipv6 host MR-MUGS-6n 2001:DB8:XXXX:6650::2
ipv6 route 2001:DB8:XXXX:6500::/64 Tunnel6510
ipv6 route 2001:DB8:XXXX:6540::/64 2001:DB8:XXXX:6550::1
ipv6 route 2001:DB8:XXXX:6600::/64 Tunnel6610
ipv6 route 2001:DB8:XXXX:6640::/64 2001:DB8:XXXX:6650::1
ipv6 route ::/0 Tunnel6010
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
!
ntp server HomeAgent.Net.HArouter
```

D.4. CLEO Route Tables

```
CLEO-MR# show ipv6 route

IPv6 Routing Table - 17 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
   I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea

L 2001:DB8:XXXX:6010::2/128 [0/0]   via ::, Tunnel6010
C 2001:DB8:XXXX:6010::/64 [0/0]     via ::, Tunnel6010
S 2001:DB8:XXXX:6500::/64 [1/0]     via ::, Tunnel6510
L 2001:DB8:XXXX:6510::2/128 [0/0]   via ::, Tunnel6510
C 2001:DB8:XXXX:6510::/64 [0/0]     via ::, Tunnel6510
S 2001:DB8:XXXX:6540::/64 [1/0]     via 2001:DB8:XXXX:6550::1, Null
L 2001:DB8:XXXX:6550::2/128 [0/0]   via ::, Serial1/1.1
C 2001:DB8:XXXX:6550::/64 [0/0]     via ::, Serial1/1.1
S 2001:DB8:XXXX:6600::/64 [1/0]     via ::, Tunnel6610
L 2001:DB8:XXXX:6610::2/128 [0/0]   via ::, Tunnel6610
C 2001:DB8:XXXX:6610::/64 [0/0]     via ::, Tunnel6610
S 2001:DB8:XXXX:6640::/64 [1/0]     via 2001:DB8:XXXX:6650::1, Null
L 2001:DB8:XXXX:6650::2/128 [0/0]   via ::, Serial1/1.1
C 2001:DB8:XXXX:6650::/64 [0/0]     via ::, Serial1/1.1
L FE80::/10 [0/0]                   via ::, Null0
L FF00::/8 [0/0]                    via ::, Null0
S ::/0 [1/0]                        via ::, Tunnel6010
```

CLEO-MR#

D.5. SSTL Ground Router Configuration

```
Current configuration : 6186 bytes
! Last configuration change at 09:40:13 GMT Thu Mar 29 2007 by dave
! NVRAM config last updated at 19:55:47 GMT Mon Apr 2 2007 by dave
version 12.3
service timestamps debug datetime
service timestamps log datetime
service password-encryption
!
hostname router2
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$f7d1$c0x/3HpXErqN4XNNKnOwF.
enable password 7 0305491F0E1A337345001702
!
clock timezone GMT 0
no aaa new-model
ip subnet-zero
ip cef
ip domain name sstl.co.uk
ip name-server SSTL.WAN.dns1
ip name-server SSTL.WAN.dns2
!
ip audit po max-events 100
ipv6 unicast-routing
ipv6 host HA-SSTL-6 2001:DB8:XXXX:6500::1
ipv6 host FE-SSTL-6 2001:DB8:XXXX:6500::2
ipv6 host FS-SSTL-6 2001:DB8:XXXX:6510::1
ipv6 host MR-SSTL-6 2001:DB8:XXXX:6510::2
ipv6 host HA-SSTL-6n 2001:DB8:XXXX:6540::1
ipv6 host FE-SSTL-6n 2001:DB8:XXXX:6540::2
ipv6 host FS-SSTL-6n 2001:DB8:XXXX:6550::1
ipv6 host MR-SSTL-6n 2001:DB8:XXXX:6550::2
!
username sstl privilege 15 password 7 01121410531E14302A45400E
username dave privilege 15 password 7 104D000A0618
!
ip ssh rsa keypair-name router2.sstl.co.uk
!
crypto isakmp policy 1
 hash md5
 authentication pre-share
 lifetime 60
crypto isakmp key CLEO_IPSEC address GS-CLEO.IPsec.Tunnel.CLEO
!
crypto IPsec transform-set CLEO_set esp-des esp-md5-hmac
!
crypto map CLEO_auth 1 IPsec-isakmp
 set peer GS-CLEO.IPsec.Tunnel.CLEO
 set transform-set CLEO_set
 match address 115
!
interface Tunnel7
```

```
 ip addressHA-SSTL.ipip.psuedo-rev-tunnel.SSTL 255.255.255.0
 tunnel source FastEthernet0/0
 tunnel destination HomeAgent.Net.HArouter
 tunnel mode ipip
interface Tunnel6500
 description IPv6-in-v4 tunnel for IPv6 traffic to/from CLEO_HA.
 no ip address
 ipv6 address 2001:DB8:XXXX:6500::2/64
 ipv6 enable
 tunnel source FastEthernet0/0
 tunnel destination HomeAgent.Net.HArouter
 tunnel mode ipv6ip
!
interface Tunnel6510
 description IPv6-in-v4 tunnel for IPv6 traffic to/from CLEO_MR. Tunnel terminates at CLEO_MR via   IPsecv4 tunnel.
 no ip address
 ipv6 address 2001:DB8:XXXX:6510::1/64
 ipv6 enable
 tunnel source GS-CLEO.IPsec.Tunnel.GSN
 tunnel destination GS-CLEO.IPsec.Tunnel.CLEO
 tunnel mode ipv6ip
!
interface Tunnel6540
 description IPv6-in-v4 tunnel for IPv6 traffic to/from CLEO_HA for Native IPv6.
 no ip address
 ipv6 address 2001:DB8:XXXX:6540::2/64
 ipv6 enable
 tunnel source FastEthernet0/0
 tunnel destination HomeAgent.Net.HArouter
 tunnel mode ipv6ip
!
interface FastEthernet0/0
 description connected to Groundstation Subnet0
 ip address SSTL.WAN.FA0/0 255.255.255.0
 ip helper-address SSTL.DMC.Broadcast
 ip directed-broadcast
 ip nat outside
 duplex auto
 speed auto
interface Serial0/0
 no ip address
 encapsulation frame-relay IETF
 no ip mroute-cache
 shutdown
 no keepalive
 nrzi-encoding
 no fair-queue
!
interface Serial0/0.1 point-to-point
 ip unnumbered FastEthernet0/0
 ip nat inside
 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
!
interface FastEthernet0/1
 description connected to Antenna0 LAN
 ip address SSTL.DMC.FA0/1 255.255.255.0
 ip helper-address SSTL.WAN.FA0/055
 ip directed-broadcast
 ip nat inside
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 encapsulation frame-relay IETF
 no ip mroute-cache
 no keepalive
 nrzi-encoding
 no fair-queue
!
interface Serial0/1.1 point-to-point
 ip unnumbered FastEthernet0/0
 ip nat inside
 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
 ipv6 address 2001:DB8:XXXX:6550::1/64
 ipv6 enable
 no arp frame-relay
 no cdp enable
 frame-relay interface-dlci 17
!
interface Serial0/1.2 point-to-point
 description Private address interface for IPsecv4 tunnel that terminates at CLEO_MR. This interface will be repeated in every GSN router so that an IPsecv4 tunnel will be established everytime CLEO connects.
 ip address GS-CLEO.IPsec.Tunnel.GSN 255.255.255.0
 no ip mroute-cache
 no arp frame-relay
 no cdp enable
 frame-relay interface-dlci 18
 crypto map CLEO_auth
!
router mobile
!
router rip
 passive-interface Serial0/1
 network 10.0.0.0
!
ip default-gateway SSTL.WAN.FW-int
ip nat inside source static SSTL.DMC.WS2 SSTL.WAN.WS2
ip nat inside source static SSTL.DMC.WS1 SSTL.WAN.WS1
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 SSTL.WAN.FW-int
ip route 10.1.0.0 255.255.0.0 SSTL.WAN.FW-int
ip route SSTL.DMC.UK-DMC.OBP0 255.255.255.252 Serial0/1.1
ip route SSTL.DMC.Nigeria.OBP 255.255.255.248 Serial0/1.1
ip route SSTL.DMC.UK-DMC.SSDR0 255.255.255.255 Serial0/1.1
ip route SSTL.DMC.UK-DMC.SSDR1 255.255.255.255 Serial0/1.1
ip route SSTL.DMC.UK-DMC.SSDR2 255.255.255.255 Serial0/1.1
ip routeSSTL.DMC.UK-DMC.OBP 255.255.255.255 Serial0/1.1
ip route SSTL.DMC.CLEO_Loopback 255.255.255.255 Serial0/1.1
ip route SSTL.DMC.Net.249 255.255.255.255 Serial0/1.1
ip route SSTL.DMC.Net.250 255.255.255.255 Serial0/1.1
ip route SSTL.DMC.Net.251 255.255.255.255 Serial0/1.1
ip route SSTL.DMC.Net.252 255.255.255.255 Serial0/1.1
ip route SSTL.DMC.Net.253 255.255.255.255 Serial0/1.1
ip route SSTL.DMC.Net.254 255.255.255.255 Serial0/1.1
!
ip mobile foreign-agent care-of FastEthernet0/0
!
access-list 7 permit CLEO.MobNet.S1/0.Net 0.0.0.31
access-list 10 permit SSTL.DMC.WS1
access-list 115 permit ip GS-CLEO.IPsec.Tunnel.Net 0.0.0.255 GS-CLEO.IPsec.Tunnel.Net 0.0.0.255
ipv6 route ::/64 Tunnel6500
!
route-map mr_subnets permit 10
 match ip address 7
 set ip default next-hop HA-SSTL.ipip.psuedo-rev-tunnel.HA
!
snmp-server engineID local 00000009020000044D4104E0
snmp-server community Groundstation RO
snmp-server location Surrey Mission Operations Centre
snmp-server contact Chris Jackson,+44 1483 689-141,c.jackson@sstl.co.uk
snmp-server enable traps tty
snmp-server host 131.227.81.116 Groundstation
!
dial-peer cor custom
!
line con 0
 exec-timeout 0 0
 password 7 08205E5A010C172819020203
 login
line aux 0
line vty 0 4
 exec-timeout 60 1
 login local
!
ntp clock-period 17179725
ntp source FastEthernet0/0
ntp server SSTL.snmp-server.host
!
end
```

D.6. SSTL Ground Router Route Tables

```
router2#sh ipv6 route

IPv6 Routing Table - 9 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
   U - Per-user Static route
   I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
   O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
   ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

S ::/64 [1/0]                       via ::, Tunnel6500
C 2001:DB8:XXXX:6500::/64 [0/0]     via ::, Tunnel6500
L 2001:DB8:XXXX:6500::2/128 [0/0]   via ::, Tunnel6500
C 2001:DB8:XXXX:6510::/64 [0/0]     via ::, Tunnel6510
L 2001:DB8:XXXX:6510::1/128 [0/0]   via ::, Tunnel6510
C 2001:DB8:XXXX:6540::/64 [0/0]     via ::, Tunnel6540
L 2001:DB8:XXXX:6540::2/128 [0/0]   via ::, Tunnel6540
L FE80::/10 [0/0]                   via ::, Null0
L FF00::/8 [0/0]                    via ::, Null0
```

REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

The 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 Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)* 01-05-2008	**2. REPORT TYPE** Technical Memorandum	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE IPv6 and IPsec Tests of a Space-Based Asset, the Cisco Router in Low Earth Orbit (CLEO)	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Ivancic, William; Stewart, David; Wood, Lloyd; Jackson, Chris; Northan, James; Wilhelm, James	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER WBS 430728.02.04.02.01
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	**8. PERFORMING ORGANIZATION REPORT NUMBER** E-16474
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) National Aeronautics and Space Administration Washington, DC 20546-0001	**10. SPONSORING/MONITORS ACRONYM(S)** NASA
	11. SPONSORING/MONITORING REPORT NUMBER NASA/TM-2008-215203

12. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified-Unlimited
Subject Category: 04
Available electronically at http://gltrs.grc.nasa.gov
This publication is available from the NASA Center for AeroSpace Information, 301-621-0390

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This report documents the design of network infrastructure to support testing and demonstrating network-centric operations and command and control of space-based assets, using IPv6 and IPsec. These tests were performed using the Cisco router in Low Earth Orbit (CLEO), an experimental payload onboard the United Kingdom--Disaster Monitoring Constellation (UK-DMC) satellite built and operated by Surrey Satellite Technology Ltd (SSTL). On Thursday, 29 March 2007, NASA Glenn Research Center, Cisco Systems and SSTL performed the first configuration and demonstration of IPsec and IPv6 onboard a satellite in low Earth orbit. IPv6 is the next generation of the Internet Protocol (IP), designed to improve on the popular IPv4 that built the Internet, while IPsec is the protocol used to secure communication across IP networks. This demonstration was made possible in part by NASA's Earth Science Technology Office (ESTO) and shows that new commercial technologies such as mobile networking, IPv6 and IPsec can be used for commercial, military and government space applications. This has direct application to NASA's Vision for Space Exploration. The success of CLEO has paved the way for new space-based Internet technologies, such as the planned Internet Routing In Space (IRIS) payload at geostationary orbit, which will be a U.S. Department of Defense Joint Capability Technology Demonstration. This is a sanitized report for public distribution. All real addressing has been changed to psueco addressing.

15. SUBJECT TERMS

Communication; Networking security; Internet protocols

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** STI Help Desk (email:help@sti.nasa.gov)
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU	69	**19b. TELEPHONE NUMBER** *(include area code)* 301-621-0390