SSC18-X-09

A Novel IP-Centric Approach to LEO Communications

Brian Chandler
Viasat, Inc.
1725 Breckinridge Pl. Duluth, GA 30096, USA; +1-678-924-2509
brian.chandler@viasat.com

ABSTRACT

A new, fully IP-centric approach for connecting mission operations to spacecraft is presented in this paper. This topology provides for standard IP interfaces to be used for payload and flight components. This allows quick integration and easy reusability of satellite components, specifically lending itself to small satellites and accelerated mission deployments. From a mission operations point of view, satellite payload components and mission operations elements become IP end-points in a network. Ground stations become analogous to IP traffic forwarding, routing, and switching elements. The architecture provides an abstraction to the physical communication channels, routing communication packets over the internet, through ground stations, and onward to spacecraft. Security is supported via IP encryption and decryption devices located in the mission operations center. All command messages, including mission operations commands, as well as payload retransmit requests messages, are encrypted away from the site, eliminating the need for key exchange protocols and security concerns at remote sites. A real-world demonstration of this architecture is performed using an existing network of ground stations and on-orbit spacecraft. From a single mission operations center, these spacecraft have been controlled/flown using a fully network centric approach.

INTRODUCTION

Many traditional LEO satellite communication systems utilize distinct and customized protocols to provide the connection amongst satellites, ground stations, and mission operations centers. These protocols and communications networks are often inflexible and do not lend themselves to scalable and reusable architectures. In recent years, some satellite manufactures have moved to a more open approach whereby the satellites becoming flying IP endpoints. This creates a model whereby more widespread networking techniques may be employed to communicate with these spacecraft.

SPACECRAFT

The spacecraft currently operated (and to be operated in the future), are constructed using network-enabled components connected via industrial-grade switching. This technique has been proven to be capable of LEO operations with many of these spacecraft flying for years, demonstrating the applicability of such technology. The spacecraft themselves can have a variable number of these IP-enabled components onboard, including an on-board computer (OBC) or a high data-rate recorder (HDR). Several examples of spacecraft such as these are built by Surrey Satellite (SSTL). These include the TripleSat constellation, Faraday test satellites, and Carbonite series of spacecraft. Some of which are shown in Figure 1.

Figure 1: Examples of IP-based Spacecraft

It should be noted that the onboard devices are connected to the spacecraft bus via IP, not proprietary hardware connections. In this way, the IP traffic is not tightly coupled with a physical layer, as in many spacecraft. For example, it is possible to send telemetry traffic from the OBC computer over either S-band or X-band downlinks to the ground. This dissociation between the traditional physical and higher layers provides a level of flexibility and redundancy for many functions of the spacecraft.

CURRENT GROUND ARCHITECTURE

The current architecture employed by the existing satellite operators consists of two main elements:

- Ground Station (Antenna)
- Mission Operation Center (MOC).

Currently, the ground station antenna and the MOC are almost always collocated, usually due to technological limitations. This creates a one-to-one relationship between a MOC, which flies the spacecraft and the ground station. This architecture is depicted below in Figure 2.

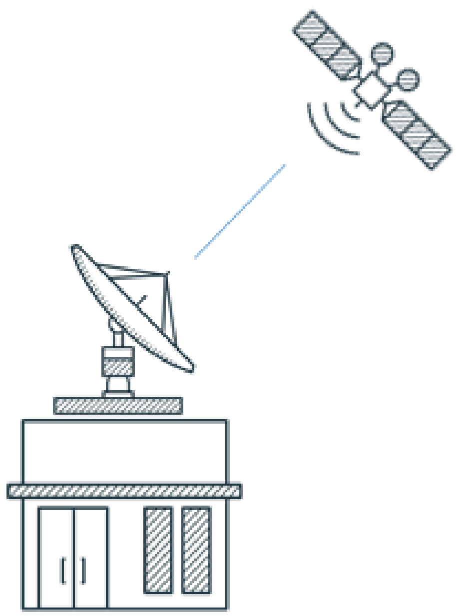

Figure 2: Single Satellite, Single Ground Station

The MOC contains the command/telemetry computers, encryption devices, and other typical Operation Center components.

MULTI-SITE & MULTI-SATELLITE SYSTEM

Moving away from an architecture whereby a single MOC is connected to a single ground station and operates with a single satellite is obviously useful. The major uses of such a system are to:

- Provide greater flexibility and availability in the execution of existing missions by enabling a wider range of ground station assets to be utilized.
- Enable large constellation missions with multiple satellites which require many minutes over many ground stations, all operated by a single MOC.

These requirements drive a separation of the various components as can be seen in Figure 3. A single MOC is able to reach several satellites via a network of ground stations, presumably located throughout the world.

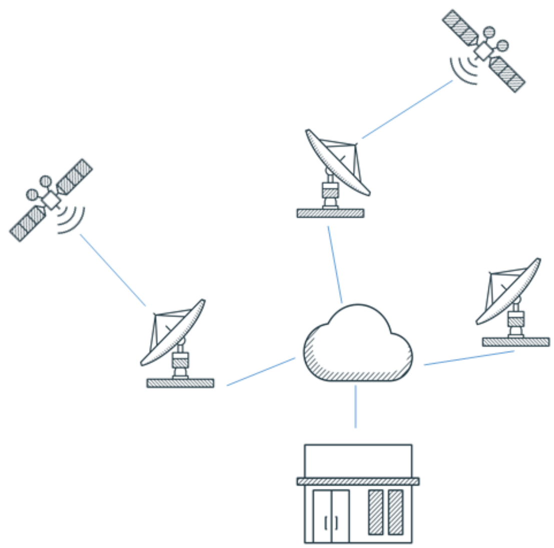

Figure 3: Multi Satellite, Multi-Ground Station

Per the diagram, this architecture incorporates a new element, the Internet, into the design. This enabling element also creates challenges which are explored in the later sections.

SECURITY CONSIDERATIONS

Security is always an important topic when considering the design of a satellite communications network. Satellites typically provide encryption for the over-the-air portion, in order to provide an authentication mechanism for commanding as well as provide protection of the downlinked information. In the existing architecture, a single MOC would contain the security appliance to provide this encryption. The colocation of the encryption appliance inside the MOC provides the physical security that one would desire.

In order to enable a large and distributed ground station network, it is still desirable to maintain the physical colocation of the security appliance in the MOC. Placing the encryption device at a potentially untrustworthy ground station location creates undesirable security vulnerabilities. In addition, it creates the need for a key exchange mechanism with several remote sites. Therefore, a major system design requirement is for the encryption device to remain at the centralized MOC. This provides the same level of protection for the terrestrial portion as the over-the-air portion. In addition, the IP-based design of the spacecraft was fully exploited by utilizing standard IPSEC tunneling as the encryption mechanism.

COMMUNICATION STACK

The communication stack for the existing design with a collocated MOC and Ground Station is seen below in Figure 4.

Moving through the stack, the Operations Computer generates commands and processes telemetry. These messages are not encrypted and sent to/from the router. The router provides both IPSEC encryption/decryption as well as link-layer (OSI layer 2) processing. The router is then connected, via a proprietary physical connection to the modem for physical layer processing. From the modem, the signal is provided to/from the antenna for communication with the satellite.

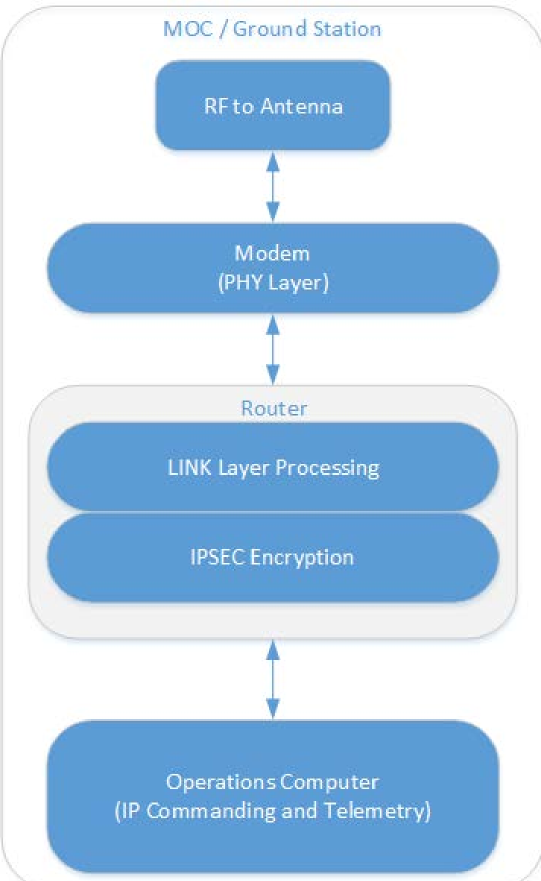

Figure 4: Original Communication Stack

There are several issues to overcome in this design if it is to be decentralized and distributed. The IPSEC security appliance needs to remain at the MOC. At the same time, the non-Ethernet based connection between the router and modem presents a problem with moving the modem. Therefore, it was decided to incorporate link-layer functionality into the modem and have the router only perform IPSEC encryption. The redesigned communication stack can be seen in Figure 5.

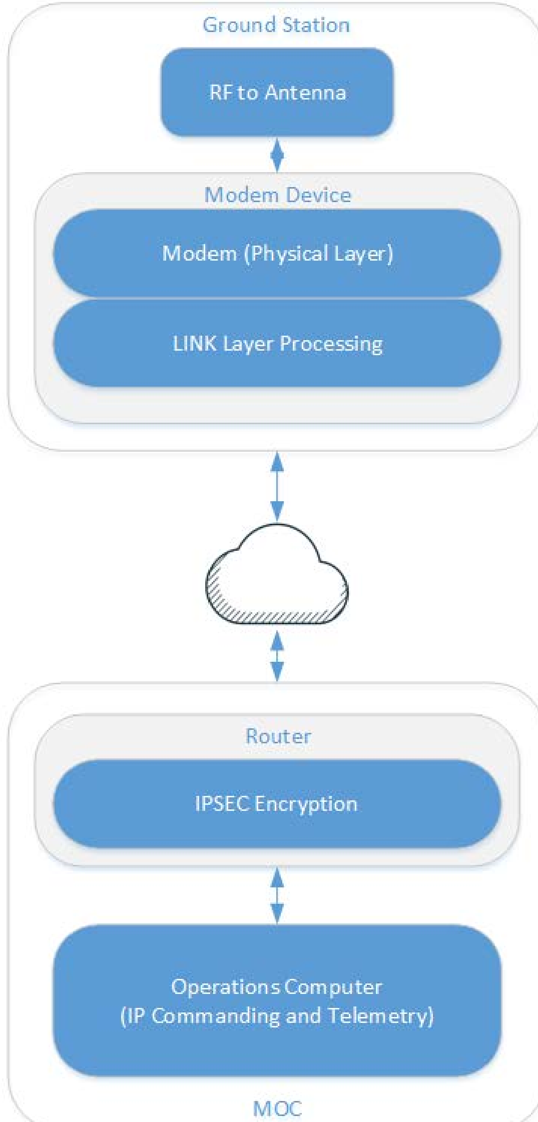

Figure 5: New Communication Stack

The interface type on the boundaries between the MOC and Ground Station is now at the IP layer, which is a necessity in order to make use of the Internet.

The incorporation of the link-layer processing into the modem was accomplished fairly straightforwardly using modern software-defined radios (SDRs). This was able to be fully implemented and tested.

NETWORKING

Network Connectivity

One requirement of the design of the system was to be able to communicate with existing spacecraft without on-orbit reconfiguration. This would allow them to continue operating with existing, traditional ground segments, as well as operated with the new networked/centralized model.

One of the main network configuration limitations is that the spacecraft devices all have IP addresses in the 192.168.1.0/23 subnet. The addresses in this subnet are meant for use on local networks only and are not Internet-addressable. Now that the traffic is required to transit the Internet to communicate with the MOC, it is necessary to somehow encapsulate this traffic and join multiple locally addressed networks together.

To solve this problem, the multi-point generic routing encapsulation (mGRE) protocol was employed. This created a tunnel between the various ground stations and the MOC whereby 192.168.x.x traffic could freely flow and be routed between network elements. The mGRE tunnel is shown below in Figure 6.

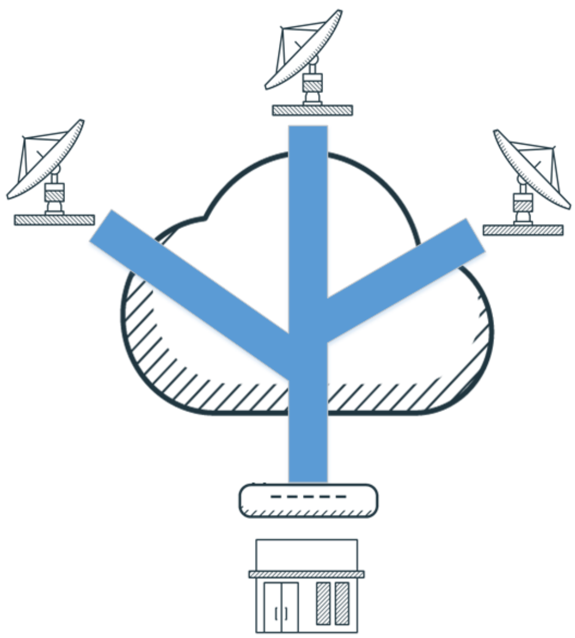

Figure 6: Multi-point Tunneling

The mGRE tunnel was fairly simple to setup as well as adaptable to future ground stations. A new ground station can be added as a new endpoints of the tunnel.

Multi-Satellite Routing

In addition to just network connectivity from MOC to ground stations, the traffic must also be routed to the correct spacecraft. With multiple LEO spacecraft and multiple sites, the command data generated at the MOC must be sent to the ground station only during the duration of the LEO pass. This creates a temporally dynamic nature to the problem. Considering the spacecraft are not actually connected via a true IP/Ethernet network, the ground stations must provide some "spoofing" to the same effect.

In order to accomplish this, before the pass the ground station advertises the routes for the upcoming spacecraft endpoints using open shortest path first (OSPF) routing protocol. At the end of the pass, the routes are removed. This allows the spacecraft to "appear" at different ground stations at different times and get command packets routed to them. The OSPF routing protocol traverses the mGRE tunnel back to the MOC to provide the required routes. This also had the positive effect that no changes to the mission operations software were required.

SUMMARY AND TESTING

The described network was implemented using several worldwide Viasat ground stations as well as a MOC at the SSTL headquarters in Guildford, UK. Several spacecraft were successfully communicated with, both in S-band and X-band, including the Carbonite-1, shown below in Figure 7.

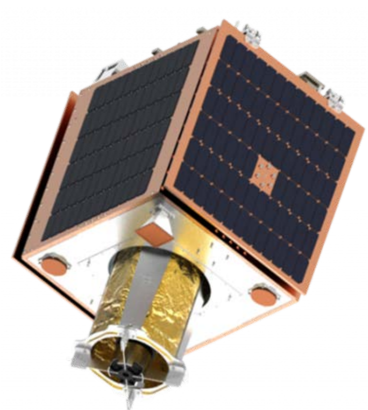

Figure 7: Carbonite-1 Spacecraft

Overall, the project was a technical success and has created new operational capabilities for the participants involved. To date, hundreds of passes have been taken using this technology.

Acknowledgments

Viasat would like thank the team at Surrey Satellite (SSTL) for their dedication and assistance in making this architecture a reality.