Rationale, Scenarios, and Profiles for the Application of the Internet Protocol Suite (IPS) in Space Operations

Draft v0.1

1 INTRODUCTION

1.1 PURPOSE AND SCOPE

This greenbook captures some of the current, planned and possible future uses of the Internet Protocol (IP) as part of Space Operations. It attempts to describe how the Internet Protocol is used in specific scenarios. Of primary focus is low-earth-orbit space operations, which is referred to here as the design reference mission (DRM). This is because most of the program experience drawn upon derives from this type of mission. Application profiles are provided. This includes parameter settings programs have proposed for sending IP datagrams over CCSDS links, the minimal subsets and features of the IP protocol suite and applications expected for interoperability between projects, and the configuration, operations and maintenance of these IP functions. Of special interest is capturing the lessons learned from the Constellation Program in this area, since that program included a fairly ambitious use of the Internet Protocol.

2 OVERVIEW

2.1 BACKGROUND

The following excerpt from the Green Book 734.0-G-0: "Rationale, Scenarios and Requirements for DTN in Space" captures the general need to extend internetworking to the space environment.

"The primary goal of CCSDS is to increase the level of interoperability between space organizations. Today, mission communication architectures are essentially point-to-point between the mission control center and the spacecraft. Standardization of a suite of cross-support services on the ground has extended and is continuing to extend this model so that agencies can share resources such as ground stations for cross support. This sharing is implemented by providing a standardized space link service interface at the ground station that accepts frames (and in the future, packets) for uplink and demultiplexes downlinked frames and delivers them to control centers using IP-based protocols.

"This communication model has worked fine for a long period of time; however, as the number of space assets grows, and missions become more demanding, the communications architecture will become even more complex. In some instances it will be desirable to provide extra network 'hops' both in space and on the ground instead of using only a single data link between the mission control center and the spacecraft. Relays, whether they are spacecraft or ground stations, need to buffer data that cannot be transferred end-to-end because of visibility constraints, provide points for signal regeneration, switch Data Link layers to match the environment, and serve as decision points for data forwarding (routing). Today's communications architecture will be hard-pressed to support these needs. It would become labor intensive, driving up the cost of operations. It imposes the risk of human error, which requires mitigation strategies that add cost. It is program limiting since cost and risk grow as the number of links and cross-links increase."

The SISG report to the IOAG – *Recommendations on a Strategy for Space Internetworking* recommended DTN as the focus for future applications of space internetworking. DTN development by its nature has been tied to discontinuous network environments. However, the needs, goals, and objectives for human space flight are different from the more numerous and generally less complex unmanned projects, and for near term HSF projects a higher level of continuity in the network connectivity is expected. The Internet Protocol Suite (IPS) can provide internetwork layer communication in the HSF niche, including ground networking, pressurized cabin environment applications, and spacecraft external communications and networking, fulfilling specific shorter term needs by means of commercial market place matured products for which DTN is not currently being developed.

Specifically, the IP suite includes protocols which support real-time communication, a large supply of COTS software, and interoperability with networks outside the space environment. In addition, IP offers the potential for a high degree of automation which is key for HSF projects reaching for mission independence from Earth-based control. Lastly, and perhaps most importantly, the potential large scale of HSF networks spur a constant search for mechanisms to reduce cost, and the use of IPS, the

most widely used networking protocols, has the potential to provide significant savings over any other solution.

3 SCENARIOS

Again from the SISG report to the IOAG – *Recommendations on a Strategy for Space Internetworking*: 'IP in Space is conceived as an extension of the available terrestrial IP functionalities to "in space" (up to Lunar distance) or "planetary IP island" networks… it has been concluded that IP in space can be cross supported today by CCSDS compliant infrastructure provided that CCSDS encapsulation services are used'

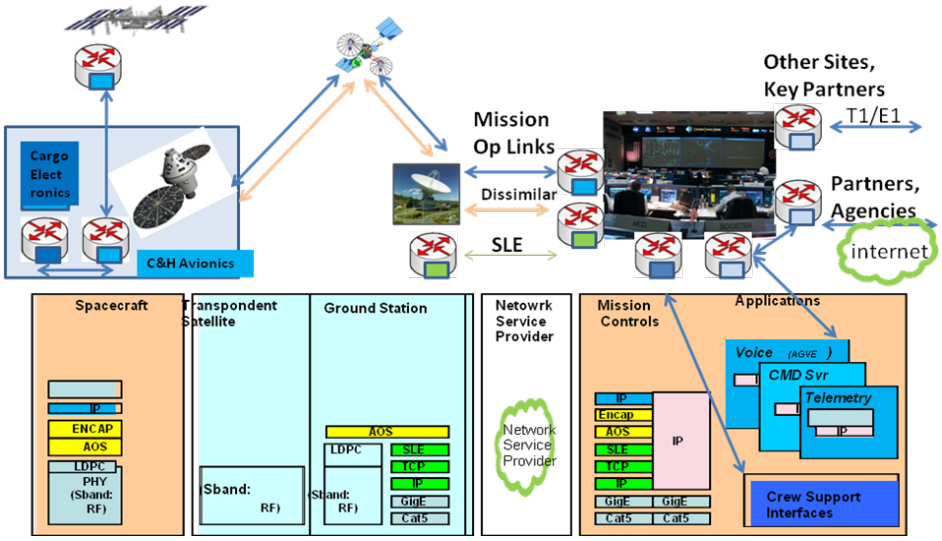


Figure 1 The LEO design reference mission (DRM) highlighting Mission Controls, Spacecraft Cabin and Space-link applications of the Internet Protocol

Figure 1is focused on the first design reference mission. Space Operations are conducted for low-earth orbit. It depicts the context for the first three scenarios discussed.

1. Use of (a) IP within a control center (b) between a control center and ground stations, and (c) between the control center and non-collocated stakeholders or information sources. Sites included in (c) are ground controls for launch, support at other space agency sites and international partners, agencies providing weather, space debris tracking, university and remote experiment participants, and public relations.
   Routers marked in light green and light blue/gray.
2. Use of IP for crew support. This involves communications and computing not essential for mission operations, but complimentary to it. It may involve technologies that did not have to be build into the spacecraft, and could be deployed cheaper and efficiently as cargo. Examples include laptops and video

cameras. No profile exists for these technologies and they are evolved and matured by the commercial market place. These capabilities can also be supported over AOS virtual channels and transmitted over less reliable non-mission critical links, e.g. Ku on Space Station. Some special considerations may apply.
Routers supporting this capability are represented in dark blue

3. Use of IP on the mission operations link. This provides a common multiplexing technology and networking capabilities. The approach was a simple closed network with an IP header in addition to the already standardized space protocol headers. The focus is on the network layer, with important applications included in the spacecraft avionics. Here significant size, weight, and power (SWaP) constraints apply.
Routers supporting this capability are represented in sky blue.
4. The final scenario represents the use of IP in future design reference missions, including as part of lunar or planetary surface systems.

3.1 APPLICATION OF IP IN THE TERRESTRIAL INFRASTRUCTURE OF SPACEFLIGHT OPERATIONS

3.1.1 INTERNAL CONTROL CENTER COMMUNICATION

Communication between flight controller workstations and data distribution servers will logically follow the most cost effective network designs for high-reliability local area networks (LANs). The capabilities of modern IP over Ethernet networks exceed the needs of control center LANs for latency, reliability, and throughput. Various architectures may be based on message bus, IP multicast, or client-server relationships, but the network layer communications for any newly designed control center will almost certainly be the Internet Protocol Suite. IP is the only widely available, vendor independent, internetwork protocol considered in most LAN development today. In fact, the only serious debate tends to center on the use of IPv4 vs. IPv6.

Routing for control center communications will tend to be simple, with end devices pointing to a single router IP address, and protocols such as Virtual Router Redundancy Protocol (VRRP) providing transparent failover. Inter-LAN routing will rely on popular interior gateway protocols, such as Open Shortest Path First (OSPF). The control center LAN will be designed to converge quickly to minimize downtime when a change occurs.

Network management will likewise follow industry standards. One would expect a mixture of SNMP, ICMP, in house customization, and proprietary vendor tools, with out-of-band connections to key network devices.

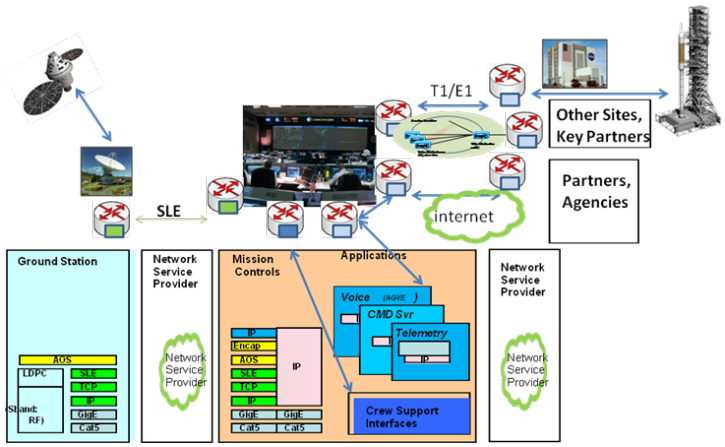


Figure 2 Use of IP for Control Center external communications

(look for mission control vs control center)

3.1.2 CONTROL CENTER TO GROUND SITE COMMUNICATION (AND OTHER WIDE-AREA GROUND COMM.)

Just as control center internal communications will follow contemporary industry trends for LAN design, so will the links from control centers to the ground stations follow industry standard WAN communication. Regardless of the underlying data link and physical layer technologies, the interface to the WAN on each end will be IP at the internetwork layer.

In the case for ground station interfaces p~~P~~rotocols such as CCSDS Space Link Extension (SLE) (~~Figure 2~~3) will deliver uplink and downlink AOS frames inside an outer IP wrapper. Some such protocol as SLE is mandatory when IP is not used on the spacelink. In the case where IP is used over the spacelink, the option exists to route data based on the spacelink IP header. (See section 3.3.2.2). Unlike unmanned probes that have very different uplink (command) and downlink (telemetry) needs, the DRM for human spaceflight uses continuous and more symmetric uplinks and downlinks. Use of space link extensions on the forward link to support AOS frames has resulted in protocol changes that allow the ground station to insert idle frames when no frame has been delivered to transmit. This maintains the synchronous uplink stream while allowing the data stream to be asynchronous, or at least less synchronous, as is the case with networked data. As most unmanned spacecraft do not require a synchronous uplink, other CCSDS link layer protocols (such as TC) may be used.

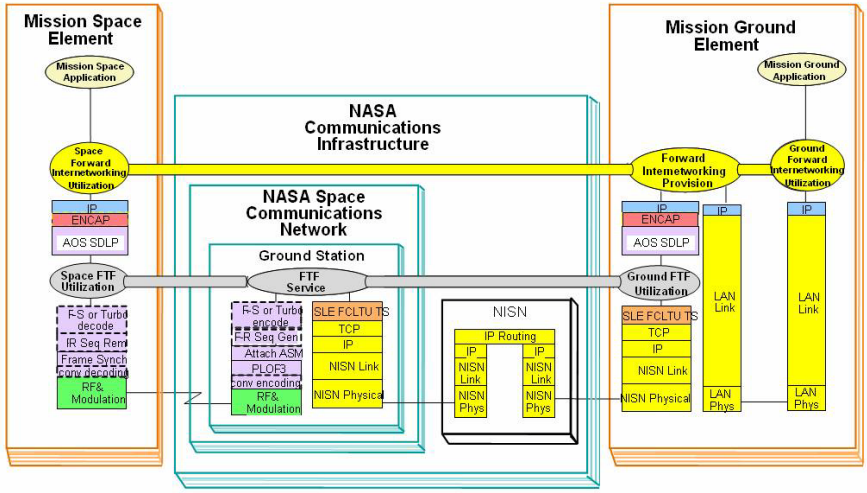


Figure 3 Control Center to Ground Station data exchange using SLE over and IP network

As shown in Figure 2, major control centers must maintain communication with a wide variety of customer, support, and regulatory entities including range safety, ground stations, engineering support, orbital tracking facilities, payload customers, and weather information services, among many others (. Past implementations of point-to-point physical connections will be maintained only for the most critical connections. The ability to provision IP services with sufficient reliability over long distances from commercial and government providers (who in turn rely on commercial providers) promises to make point-to-point connections obsolete. A single, redundant (or a few in the cases where traffic separation is advantageous) IP connection to a contracted service provider will allow the control center to focus on mission control and leave WAN connectivity to the appropriate specialists.

While a variety of options for IP route control can be implemented over a procured long distance link, the configuration most consistent with the separation of control center and WAN responsibilities would be to interface with the WAN using the Border Gateway Protocol (BGP) or another method that maintains routing domain independence between the control center and the WAN provider.

Network management over the WAN is an area of great importance and frequent neglect in analysis of end-to-end communication between spacecraft and control center. Network management data, which we identify here as router and physical device performance statistics, should be made readily available to communications partners on both sides of a shared border. Clear boundaries of control should be maintained but data should be shared continuously and automatically on out-of-band networks specifically built for that purpose. The control center needs at least minimal insight into all communications domains from their own subsystems to the spacecraft in order to quickly isolate anomalies. This is especially true in the case of human spaceflight. Providers tend to have the greater

expertise and can help control center personnel troubleshoot problems more quickly in the case of network and data link layer anomalies. Suppression of the sharing of network data across organizational boundaries leads to finger pointing and lengthens unplanned outages.

3.2 APPLICATION OF IP WITHIN THE CABIN/HABITAT ENVIRONMENT

In order to make use of an internetworking protocol from the internal vehicle network, there must be the supposition of multiple internal end devices for which multi-hop communication is required. For most spacecraft all critical functions tend to go through a central command processor. A separate implementation may exist for downlink, but manipulation of the downlink will still generally be handled through the one command processor. With HSF requirements continue to arise for multiple end devices for crew support, payload operations, and video operations, among other functions. For these functions IP end devices onboard have been shown to be useful.

Providing an information environment for the crew that leverages appropriate commercial advancements provides many beneficial features. This includes ease of interaction and interoperability, ability to adapt and do things that may not have been anticipated in detail, especially during longer duration missions/

Interoperability is achieved by adapting common technologies to space use rather than having to custom develop them. This is easier within the pressurized compartment than at the space vehicle external interfaces. For example, a common solution is to provide laptops. This enables the crew to work and interact in a similar environment to on earth and allows upgradability and flexibility to provide a limited range of capabilities that could not be accommodated as part of the avionics system during development. This also allows, with exceptions, the use of commercial market place standardized protocols to be used for information exchange.

3.3 APPLICATION OF IP BETWEENSPACECRAFT AND OTHER SYSTEMS

Formatted: Normal

This section discusses the application profile for applying IP to the spacecraft operational links. This concept involves IP as the common traffic muxing/demuxing point for operational communications between the control center, spacecraft, decent/ascent vehicles, launch systems and launch vehicle. In this setting, the CCSDS links carry predominantly one virtual channel for command, telemetry, voice and file transfer. The system supports robustness through dissimilar technologies through alternate virtual channels and hardware paths.

3.3.1 POTENTIAL ADVANTAGES FOR USE OF IP IN SPACE

The extension of IP functionalities into space does not necessarily imply the extension of existing terrestrial networks nor existing best practices for IP networks into space. Spacecraft almost always take a minimalist approach to software design, which will lead to exclusion of portions of the Internet Protocol

Suite (IPS) by one space systems or another. Knowledgeable network engineers from a multi-system program must work together to develop an end-to-end network capable of accomplishing program goals.

The reasons for using IP in space or any communications protocols must ultimately come back to the arguments of cost savings and cost avoidance in comparison to alternatives, because any agency or multination program could develop from scratch a communication profile suitable for the needs of their missions. IPS is a COTS available protocol
stack providing addressing, name resolution, traffic prioritization, multiplexing at multiple layers, standard interfaces to data link layers, static and dynamic routing, mobility, management protocols, multicast, support for real-time applications and security implementable between any two nodes and routers on the network. In addition, a large number COTS applications have been developed, which can either obviate the need for development or simplify the development of applications for space.

IP offers the potential for cost savings for several significant connectivity space networking scenarios:

During ground operations or after docking of two spacecraft restrictions that apply to connectivity over spacelinks are absent. Over such hardline links, IP implementations can mirror those over similar links on Earth with virtually all IP services available for use.

Over space links with consistent connectivity and data rate, IP implementations can take advantage of addressing, traffic prioritization, multiplexing, and security services, among others.

For human space flight (HSF), support for real-time applications (e.g. voice) is key. There is an ongoing focus of terrestrial real-time IP application development, which can be leveraged to reduce development time for real-time space apps.

For crew support and other non-critical applications, use of IP could allow for unmodified use of COTS applications in many situations. IP traffic prioritization can ensure that non-critical traffic does not interfere with operations.

Remote payload operations can be simplified by the end-to-end use of a single network layer and associated security protocols. Security gateways will still be needed for protection from the wider Internet. However, by using the world's most common network protocols end-to-end, functionality can still be significantly greater for remote operators when compared to networking alternatives.

3.3.2 PROGRAMATIC CONSTRAINTS OF LEVERAGING IP

This approach is distinct from the discussions in 3.1 and 3.2 which relate to applying Internet community best current practices in mostly unconstrainted environments. In this setting, a subset of IP capabilities are specifically identified as requirements and negotiated with the contractors building the systems. In this process, current state of the art technology, such as space hardened FPGAs and DSPs, cost and Size Weight and Power provided significant constraints. Since discussions were reduced to an applicable subset of IP protocol features, system engineering and project engineering needed to find what could be supported and verify that it would work. This involved the projects largely not being willing to support IP features unless operational ConOps could be shown to need them, and system engineering wanting the projects to support capabilities unless they could show that the technology and budget really would not

support them. Networking, and IP, bring obvious security concerns, and the focus was mostly on the use of a closed network with a clear security profile. The additional dimension was the concern about breaking well proven ways of doing things by using IP on operational links and introducing new, possibly not articulated risks. To some, the whole concept was considered senseless. Risks were introduced into formal risk tracking, prototyping with anticipated flight like environments was performed, and the risk of using IP for operational purposes was formally accepted by the program. As is the case for many trades, some folks will still consider this approach to introduce unnecessary risk despite the program disposition.

3.3.2.1 Custom Space Router

The growth of IP within HSF has brought about a new class of forwarding device onboard spacecraft, identified here as a custom space router. In addition to handling the normal IP router functions of traffic segregation, data link layer conversion, traffic prioritization, routing table lookup, and security policy enforcer, the custom space router has application gateway responsibilities in conversion between onboard non-IP functions and the IP downlink. Possibly dealing with DTN, space packet, or other CCSDS traffic adds to the complexity of the device. Such complexity and specialization may unfortunately prevent commercial standardization of the space router in the near term, which would aid the growth of IP onboard. Development of internal spacecraft LAN standards for C2 and for formatting of data in the downlink could allow standardization of the application gateway functions. However, those areas are outside the scope of this paper.

3.3.2.2 Ground Station Communications Options

Figure 4 uses Space Link Extensions (SLE) to move all higher mission specific protocols to the Mission Controls. This exploits the parallelism in design of forwarding non-IP data from the same or other spacecraft. The role of the ground station in the communication process may however vary depending on the network and data link implementation on the spacecraft in question. The flexibility of communication with a spacecraft which uses IP over the RF link can be significantly enhanced through the presence of an IP router at the ground site. Ideally such a router would be run by the administrators of the ground station. However, the special circumstances of implementing IP over a space link, generally lie outside the expertise of the ground station personnel. Unfortunately, the same can be said for most WAN providers and control center network experts. Consequently, agreements tend to default back to the forwarding of link layer data through mechanisms such as SLE. In the case of a single ground station forwarding to a single control center, the use of SLE does not constitute a significant loss of capability. The wasted processing of adding an additional SLE/TCP/IP wrapper to an IP/ENCAP/AOS packet-in-frame is not significant in a terrestrial network. .

Figures 4 and 5 show the difference between an ground station forwarding data link layer frames and one with an “in-line” IP router forwarding IP data to and from the spacecraft. In case of a project using multiple ground stations, multiple simultaneous links (to one or more vehicle), or multiple control

centers there are advantages to having router(s) at ground station(s). Mobile IP could make ground station handovers nearly transparent to control centers. Ground station routers can use IP QoS to enforce traffic prioritization of data from multiple control centers. Critical data can be automatically routed over a back-up link. No custom applications need to be developed to send different vehicle data to different primary consumers on the ground.

For past projects some agencies have built networks within networks to allow control centers insight into and control of resources at ground stations. Such an approach confuses boundaries of responsibility and would make interagency standardization more difficult in terms or both routing schemes and network management. Keeping all connectivity at the ground station with the space network provider appears to provide the best boundaries, while WAN providers, who would have a point of presences at the ground site, could continue to focus on providing a service similar to that for all other customers, albeit with some potentially different service level agreements.

Since, as mentioned above, ground station personnel are not generally internetworking layer experts, and because some unique challenges arise in the use of IPS over space links, approaches to handling certain aspects of IP in space should be addressed and standardized. These generally involve an adaptation or tailoring of certain protocols and industry standard methods which have evolved over many years on reliable terrestrial links which are assumed to be have two-way functionality when working.

The number of configurable SLE connections when multiple ground stations and spacecraft are involved can become large. The requirement for redundancy during critical operations, the number of spacecraft, the number of links (e.g. S-band and Ka) and the number of ground stations all multiply to give the number of SLE connections that have to be configured.. A subset would be needed at any time. Since an SLE server typically supports a significant number of SLE connections, and the design reference mission starts with manageable number of ground stations and spacecraft, the large volume of SLE connections to be managed was not seen as a negative by control center engineers already accustomed to relying on SLE. In addition, if link layer security is used, rather than IPsec, the use of SLEs allows the security association to be maintained end-to-end between the spacecraft and mission controls.

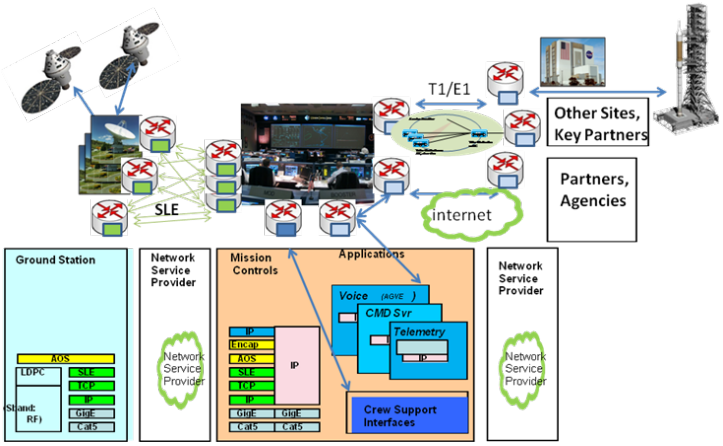


Figure 4 Control Center with multiple ground stations and spacecraft, use of SLE

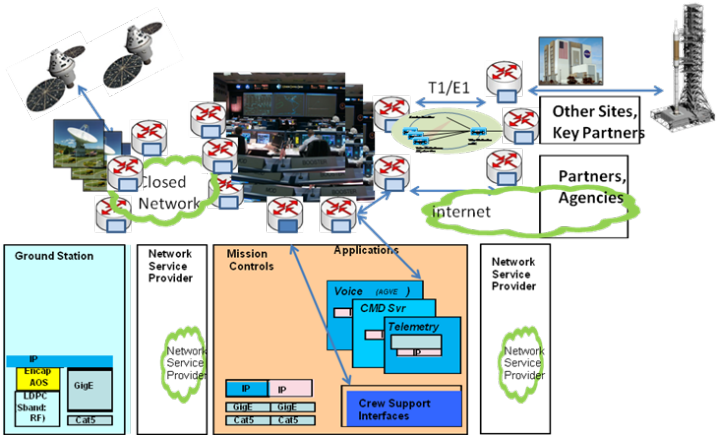


Figure 5 Control Center with multiple ground stations and spacecraft via IP network

3.3.3 LIMITATIONS OF IPS IN SPACE ENVIRONMENTS

The Internet Protocol Suite is very mature for mainstream terrestrial communications, and has a wide range of proposed solutions to fringe environments. However, redundancy requirements, mobility, intermittency, parallel network paths (e.g. S-band and Ku-band) and the possibility of one-way links require very special consideration and have to be closely examined in the reference mission phases. This has included risk identification and retirement including such activities as prototyping.

The terrestrial Internet has evolved around high availability bi-directional links in the core network, with possible failover and dial-up links that are mostly at the exterior. While a network path is good, it normally provides a significant period of connectivity. During this period packets may be lost, for example during congestive events along the network path, and the protocols have been designed to deal with congestion responses and robustness to packet loss. This may be at the transport (non-critical bulk data transport, such as files) or an application layer appropriate response. For this configuration, the Internet community offers best current practices, which utilize subsets of protocols and configurations for which Internet Engineering Task Force (IETF) Requests For Comments (RFCs) have been published. These best current practices are believed to be robust and dependable and have substantial fielding. Unfortunately solutions to truly intermittent (or non-continous) or mobile ad hoc networks, although aptly proposed and captured in RFCs, do not fall in the mainstream of accepted robust solutions which would apply for general space like operational environments.

The approach has been to test the application of IP based on a Design Reference Mission (DRM) basis. This points to areas where the use of IP may be overextended.

3.3.3.1 Intermittency

For Human Space Flight (HSF) focused on operations in low earth orbit (LEO), the following intermittency situations exist. Again it should be noted that this specific section is scoped to the mission critical operations links of the spacecraft rather than the non-mission critical high rate links (e.g. Ku on Space Station). Please see section 3.2 for that discussion.

- On pad operations and launch count-down, there may be periods where the network is altered for the purposes of checking out alternate communication paths
- During ascent, there will be radio link dropouts. There nominally are two network communications paths, one is through terrestrial tracking stations, and the other is over TDRSS. For the purpose of this discussion, it is assumed that the TDRSS path is established while still on the pad. The outages depending on the communications network path chosen and the antenna suite employed on the launch vehicle or spacecraft. They include look angles with bad antenna gain during launch vehicle roll/pitch maneuvers, tracking station handover – such as when the vehicle pitches and the launch head tracking station is looking into the plume, and outages when the human-rating-mandated launch escape system (nominally escape rocket tower fastened to spacecraft top) separates.
- On-Orbit, handovers between TDRSS, possible outages for periods collecting radio metrics for orbit determination, reconfiguration of the link parameters (e.g. data rate), or change in (or periodic deallocation of) the frequency allocation for a given communications path. Common for operations with a high gain antenna (see 3.2), outages due to spacecraft orbital

attitude are probably less of a consideration given the anticipated (cumulative across apertures) antenna gain patterns for the operational link.

- During Rendezvous, Proximity, Docking and Undocking operations networking solutions become more complex, due to the Human Rating requirement to have direct (verbal) communications between space vehicles during this phase. This might include a period of (including outage due to) link and network routing reconfiguration.

- While docked a hardline link is available. During quiescent dock periods, the spacecraft is normally powered down, but powered up periodically for checkout purposes.

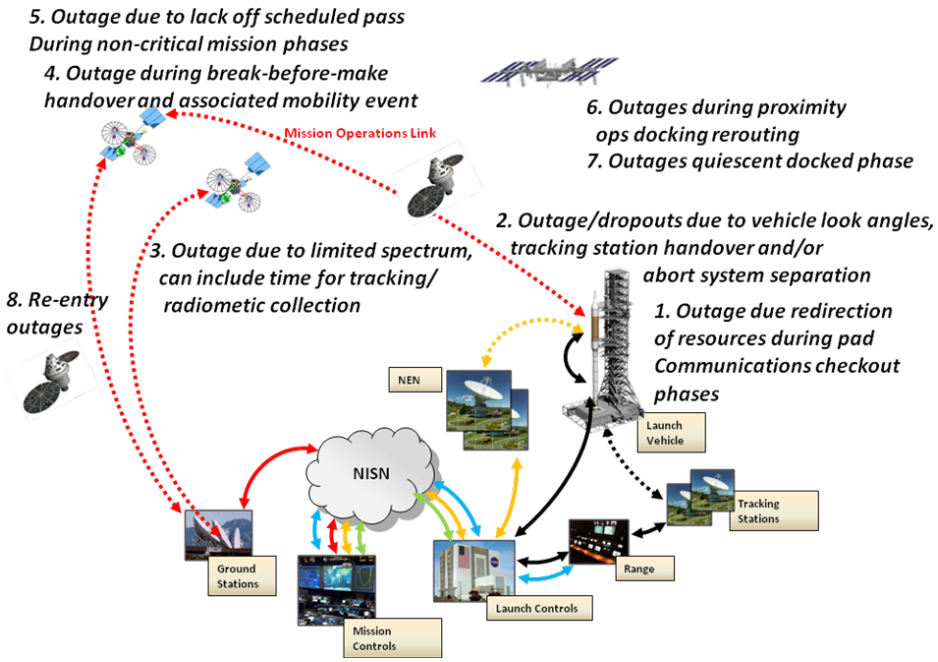


Figure 6 Operational link communications outages during LEO operations

3.3.3.2 Mobility

The DRM assumes a mesh of SLEs is setup to each ground station. As such, a handover can be addressed below the vehicle link IP layer by switching between which SLE to use to forward and receive data over. For the ground station options that use IP forwarding of vehicle data directly at the ground stations, a variety of IP protocols are available . Mobile IP may be used in a simple case (see CCSDS Orange book on the topic). For more complex networks (See section 3.4), OSPF can be used, as well as IP multicast. Routing protocols are not critical for the spacelink given today's approach for support of

critical mission phases, but will be key to automation of future, more complex networks. Tools that help automate handovers that will result in cost reduction, intermittency reduction and operational simplicity, but must meet reliability expectations.

3.3.3.3 One-way Links

Space systems have traditionally defined requirements for protocols to function over one-way connections. CCSDS has generally used this principle as guidance in standards definition. For HSF support for one-way links is seen as a requirement during contingency situations for critical mission phases. This can include “commanding in the blind” and retrieval of telemetry signals following periods of telemetry dropout. Depending on configured rates the signal may be stronger in one direction than the other, so that in a contingency situation one direction may drop while the other continues to function.

For the DRM of interest, during non-contingency situations, one-way links do not exist. For non-critical mission phases workarounds exist for one-way contingencies. During critical mission phases communication configuration will be tightly controlled. In fact, the rarity of the occurrence of one-way links calls into questions the validity of this condition as a major design driver. Nonetheless HSF programs have adopted conservative approaches for IP profiles that can address critical mission contingencies.

The following are some examples of protocols which assume the existence of a two-way link by a communication partner to function normally.

TCP: (Transmission Control Protocol) – This reliable transport protocol requires every transmitted bite to be acknowledged. As such, it tend to be poor choice over high latency or noisy links. Space agencies have generally stayed away from any critical application which relies on TCP.

IKE: This key exchange protocol is an integral part of IPSec, and most commercial implementations tend have been designed for low latency, low loss networks and with a low capability to tune options by customers. However, the parameters in question, such as connectivity timeouts, are not deficiencies in the protocol itself. Testing with open software has supported the idea that IKE generated keys could continue to support connectivity over a one-way link for any predetermined period. Once that period is reached, some alternate method of communication must be engaged.

Routing Protocols: Most routing protocols relay information from the perspective that a link is either functioning in a multi-directional capacity or is completely down. In the case of a one-way link, such protocols would actually inhibit connectivity.

Commercial IP header compression implementations: Both IP header compression and robust header compression require convergent settings at the link layer on both sides of a link over which header compression is implemented. To ensure the convergent settings, link layer protocols that support header compression such as frame relay and PPP employ negotiation between routers on the link. Commercial routers tend to employ header compression only over links which support PPP, frame relay, or proprietary variants of HDLC.

RTCP: Real-time Transport Control Protocol is defined in RFC 3550 (RTP). It is an optional exchange of receiver and sender reports for the purpose of performance monitoring and optimization. The loss or absence of individual RTCP packets does not impact the functioning of applications using RTP. Voice performance monitoring and optimization can be covered through the existing telemetry processing systems without the use of RTCP, for the case of a single control center controlling a single spacecraft as in the DRM.

3.3.3.4 Parallel connections and routing

The DRM may include parallel S-band and Ka-band connections to a Spacecraft. The Ka-band is through a high gain antenna that is deployed later in the mission. Since traditional IP networks do not normally use multiple parallel links for different types of application, some unique consideration is required. Rather than using MPLS style traffic engineering underneath IP, the main discussion focused on having different subnets on the spacecraft for different applications (e.g. a high definition TV device), and using the different host addresses on the different subnets to make routing decisions to send data over one link or the other. It was noted that an opportunity for automated failover exists if the two link layers over the two (S-band and Ka) links can signal to the router if the interface is up or down. This allows the router to select among a list of routes which allow both subnets to be reachable via either interface with different metrics.

3.4 APPLICATION OF IP TO LUNAR AND PLANETARY SURFACE MISSIONS

Material from NASA programs relative to this section do exist and will be provided at a future time. Further, we invite participation in developing this section from all interested parties.

3.4.1 LUNAR AND PLANETARY SURFACE PROFILES (TBD)

Surface (planetary, lunar, asteroid, etc.) System Networks

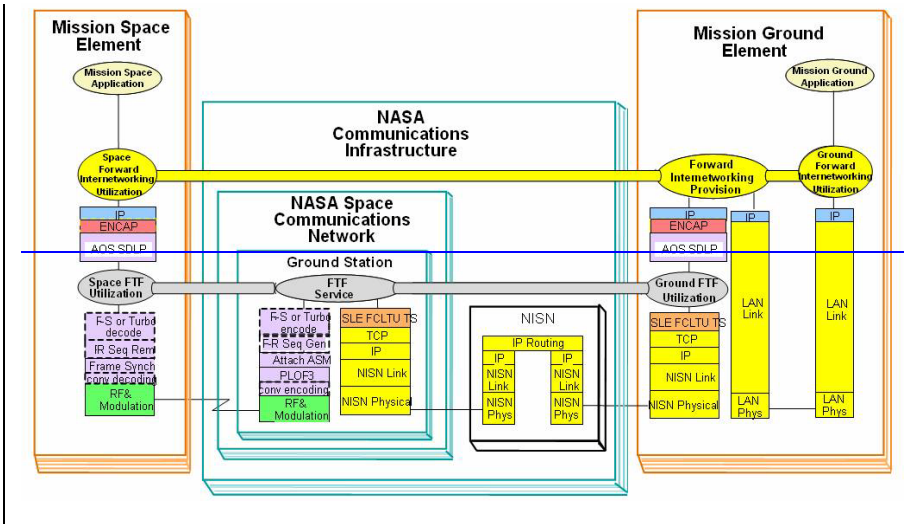
3.4.2 PROFILES FOR CONSTELLATION LUNAR MISSIONS (TBD)

3.5 OPERATION AND MANAGEMENT OF THE NETWORK

This section is still under development.

For the DRM, the number of network parameters and topologies are somewhat manageable. As a result, the can be configured, monitored and controlled through the control center in a manner similar to other link parameters.

Since IP protocols are relatively complex, to reduce management burden and increase interoperability, control protocols are used to verify that both sides of the link are in a common state or to default to an interoperable state. Routing protocols address network changes. These protocols are already implemented in routers that are trusted to forward missions data between the control center and ground stations. As experience with these protocols on the spacelink in non-mission critical settings is gained, they may be used in increasing degree in future Design Reference Missions.



4 PROTOCOL AND IMPLEMENTATION PROFILE

The profile discussed in this section provides IP datagram transport with limited routing and Quality of Service. Details of the resulting per section RFC or blue book tailoring is found in Appendix A.

Quality of Service is leveraged, because, even though Mission Controls is assumed to oversee the data scheduled on the uplink to ensure it isn't oversubscribed, discussions did indicate the need for protocols at the SLE and IP layers to cover shorter term jitter/aggregation.

Unicast and multicast were defined. Multicast addresses traditional settings were a telemetry streams or a voice loop data from a spacecraft can be processed by any recipient, and network layer addressing does not limit who can receive the data. One advantage to this relates to reducing reduplication on resource constrained links when the data is to be received by both launch and mission controls. For the DRM, Mission Controls will process all spacecraft data and disseminate it in post-processed form. Mission Control traditionally ingests telemetry and voice loops, and makes them available in calibrated form available for other parties over IP networks (including using IP multicasting for dissemination of the post-processed telemetry data). Voice is similarly disseminated between terrestrial participants using T1/E1 DS0 channels.

Header compression is defined to address the IP overhead issue on low rate operational links. Header compression capabilities can be costly if they have to be implemented in hardware, so significant work was needed to select an appropriate sub functionality that was robust. For the DRM, the need for actually implementing the IP header compression protocols was balanced against the telemetry volume reduction the IP headers would imply during the critical mission phases such as ascent.

IP addressing and routing is setup statically for the initial design reference mission. These parameters are controlled together with other link settings such as frequencies, link rates, coding choices and space link protocol profiles. Profiles for IP protocols reflect RFC compliant subsets that were selected to work over one-way links and tolerate the anticipated intermittencies. Mobility leveraged the planned infrastructure below the IP layer to provide concurrent redundant AOS frame transport between all necessary ground stations and mission controls. This meant that the mobility problem was being addressed below the IP layer for TDRSS-like satellite handovers in orbit. The recording of the RF links in the design reference mission was used to avoid having the IP network ensure that all signals sent from space would be retrievable, a requirement not natural to IP networks.

To implement the voice loops, bandwidth efficient vocoder data (G.729) is transported over the IP operational network. Several vocoder frames were grouped into an IP packet (e.g. 100 ms "ptime"). Jitter buffers were sized to accommodate higher levels of jitter and playout times were controllable form the ground. Although voice activation is supported (silence suppression was not), it is anticipated that during critical mission phases, mission controls would continue transmitting voice packets even when the person designated to speak on the air ground loop at the control center was not keyed to talk. For the DRM, performance monitoring and optimization was done via the telemetry processing and display system rather than utilizing RTCP.

Most of these limitations can become counterproductive as more complex mission phases are approached. Having statically configured parameters will at some point reduce reliability due to misconfiguration, and the personnel overheads required to oversee them also become large. To allow link controls, mobility and routing to do their job requires a high degree of trust in them to respond correctly in the environments encountered. Extensive experience with these environments, and lab equipment with flight like settings do not exist, but current thoughts are discussed in the fourth scenario. Finally, note than DTN will be picking up some of the needs for the future design reference missions.

4.1 IP PROTOCOL LAYERS – BASIC CONNECTIVTY

This Section describes the appropriate CCSDS standards and IETF RFCs for management and operations of end-to-end IP networking over space links starting at the network layer and proceeding upwards to transport and some specific applications.

4.1.1 NETWORK LAYER CONNECTIVITY

This section defines how data packets will be instructed to traverse a space network. The approach is based on a dynamic/mobile network environment with automatic multihop routing from one endpoint to another endpoint. Data paths are not forced to go through earth-based systems (hub and spoke) if a more direct path exists between end systems.

NOTE: Static routing can be used to facilitate routing convergence, to provide routing information when only simplex links are available, and to minimize packet loss when routing changes occur. Route path changes are especially prevalent within networks that consist of constantly moving systems. Requiring support for managed (often referred to as static) hardware address mappings and routing table entries ensures that it will be possible to support critical operations with little or no interference from conditions such as simplex links or route convergence issues caused by link interruptions.

While the utilization of static routes often requires more administrative resources and manual processes than dynamic routing, it is possible to automate and minimize the administrative impact of static routing given a deterministic routing environment of reasonable scale.

Application Profile (Goal 4): The protocol stacks to support critical applications are described below according to the OSI reference layers, starting at the internetwork layer (layer 3), proceeding to the transport layer (layer 4) and concluding with applications (layer 5-7).

4.1.1.1 Internetwork Layer - IP Version 4 (IPv4)

This section contains requirements for implementing the IPv4 packet format that is the basic unit of interoperability for near term space projects that use IPS. IP packets contain network source and destination information, along with traffic prioritization and transport protocol identification fields. IPv4 hosts can be automatically configured via the Dynamic Host Configuration Protocol (DHCP). It is anticipated that IPv6 will be needed for the future design reference missions. This is based on the commercial IPv6 deployment and the concept of leveraging Commercial Off the Shelf (COTS) technologies. The next design reference mission is also anticipated to feature increased level of spacecraft to spacecraft routing and a reduced dependence on manual configuration and control of the network.

Projects must implement version 4 of the Internet Protocol (IPv4) as specified in STD-0005, RFC 0791, Internet Protocol (IP) Specification, Version 4.

IP provides end-to-end addressing capability and traffic prioritization markings for data. STD-0005 includes the following Request for Comments (RFCs): 791, 792, 919, 922, 950 and, 1122. RFC 791 is updated by RFC 1349, Type of Service in the Internet Protocol Suite, which is obsoleted by RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. RFC 2474 is included as a separate requirement. RFC 792, Internet Control Message Protocol, is updated by RFC 950, Internet Standard Subnetting Procedure, which is specified separately. STD-0005, and hence this requirement, applies only to IPv4.

Projects must use unicast addresses as defined in RFC 1918, Address Allocation for Private Internets.

Using private unicast address space would allow easier administration/allocation of addresses and ensure the availability of enough contiguous address space for the project network. Using publicly routable addresses would allow direct communication between non-project networks and space assets. This requirement simply ensures that the private address spaces, which by convention are not routed across the Internet, are supported by the project. RFC 1918 applies to IPv4 addressing only.

Projects must use multicast addresses as defined in RFC 3171, IANA Guidelines for IPv4 Multicast Address Assignments.

Existing ground infrastructure may already use public multicast addresses (224.0.0.0/8 through 233.0.0.0/8). The 239.0.0.0/8 address block is used for multicast in private networks. RFC 3171 applies to IPv4 addressing only.

Projects must comply with STD-0003, RFC 1122, Requirements for Internet Hosts–Communications Layers.

The aforementioned document reflects a neatly packaged requirements and specifications list outlining fundamental Internet host and routing functions. The document leverages the maturation and experienced gained via 10+ years of

commercial internet deployments. This is the baseline specification document utilized by commercial network equipment providers in providing standards compliant devices using the internet protocols. While STD-0003, RFC 1122 was written for IPv4 hosts before IPv6 was developed, it specifies behaviors that are generic to hosts connecting to any IP network including IPv6 networks.

4.1.2 TRANSPORT LAYER

UDP is the common denominator for all critical applications which make use of the IP suite in the space environment. RTP is an additional transport protocol for real-time applications that typically runs between the application and UDP. TCP may provide reliable transport in a planetary surface environment, including, possibly the transport for DTN.

4.1.2.1 User Datagram Protocol (UDP)

UDP provides an unreliable connectionless datagram transport service. Applications using UDP that need sequencing, duplicate suppression, or reliability will need to implement these features at the application layer. Because UDP does not require any feedback from the receiver, it works over simplex links. UDP does not provide network congestion control mechanisms, so applications with large amounts of data to send may want to limit their transmission rates or investigate standard UDP-based congestion control mechanisms like the Datagram Congestion Control Protocol (DCCP).

Projects must implement STD-0006, RFC 0768, User Datagram Protocol, for communication with all IP-addressable endpoints.

UDP is the standard Internet transport for unreliable datagram transfer, and functions over simplex paths. STD-0006 is also known as RFC 0768.

4.1.2.2 Real-time Transport Protocol (RTP)

RTP is built on top of the UDP, and is functionality suited for carrying real-time content. RTP provides payload-type identification, sequence numbering, time stamping, and delivery monitoring. RTP, in general, will be used by the project in support of voice and video data.

Projects must implement STD-0064, RFC 3550, RTP: A Transport Protocol for Real-Time Applications, Section 5.

RTP is the industry standard transport protocol for handling real-time data like voice. Supporting RTP will facilitate the use of COTS applications like Voice Over Internet Protocol (VoIP) phones.

4.1.2.3 Transmission Control Protocol (TCP) (Optional)

TCP is a reliable connection-oriented data transport protocol that delivers all data in order with no errors in a timely manner. Duplicate data are discarded. A timer at the TCP sender will cause data to be retransmitted if it is not acknowledged within a reasonable time. TCP also provides both flow control and network congestion control. TCP requires feedback from the receiver, therefore requiring a duplex communication path. TCP's congestion control mechanism can cause it to under-utilize bandwidth when the round trip time or the packet loss rate of paths is high. For this reason, TCP will not be suitable for many space-to-ground applications.

Projects should implement STD-0007, RFC 0793, Transmission Control Protocol and RFC 1323, TCP Extensions for High Performance.

TCP is the standard Internet protocol for reliable data delivery over bi directional paths, and is used by many common applications including e-mail Simple Mail Transfer Protocol (SMTP) and web browsing (Hypertext Transfer Protocol [HTTP]). TCP provides a common transport service that frees applications from having to implement congestion control and reliable data delivery, thus freeing them to focus on application-specific issues. TCP should only be used when there are not lengthy communications delays. STD-0007 is also known as RFC 0793. RFC 3168 updates RFC 0793.

RFC 1323 defines extensions that allow tuning of TCP parameters for better performance over paths with high bandwidth*delay products. Without these extensions, TCP performance degrades as the product of the network bandwidth and the end-to-end delay increases.

4.1.3 APPLICATIONS

Some direction on the implementation of voice, video, and file transfer applications are included below. In general, application level specifications are provided by other CCSDS documents.

4.1.3.1 Voice Exchange

This section specifies interoperability requirements for digitally encoded audio stream distribution between space systems.

Projects must transfer voice data over a one-way link.

This is necessary to support some planned operations with one-way links. This capability can also be useful during contingency operations.

Projects must transfer voice in accordance with STD-0064, RFC 3550 and RFC 3551.

Real-Time Transport Protocol (RTP) is the most commonly used transport for Voice Over Internet Protocol (VoIP) applications. It uses UDP with either unicast or multicast addressing and its packets contain information typically needed for internet streaming applications.

Projects should use ITU G.729, Coding of Speech at 8 kbit/s Using Conjugate-Structure Algebraic-Code-Excited Linear Prediction (CS-ACELP). ***(optional)***

ITU G.729 is an audio codec that is commonly used in Voice Over Internet Protocol (VoIP) applications. It provides voice conversation quality audio with relatively low network bandwidth.

4.1.3.2 Motion Imagery Transfer

There are many different formats for the transfer of motion imagery, and it would be difficult or impossible to support them all. C3I has chosen the file format defined in ISO/IEC 15444-3, Information Technology – JPEG 2000 Image Coding System – Part 3: Motion JPEG 2000, that will hopefully support a wide range of applications, from science to outreach.

Projects must transfer motion imagery over a one-way link.

This is necessary to support some planned operations with one-way links. This capability can also be useful during contingency operations.

Projects must transfer motion imagery in accordance with STD-0064, RFC 3550, Section 5.

Real-Time Transport Protocol (RTP) is the most commonly used transport for motion imagery over IP applications. It uses UDP and its packets contain information typically needed for internet streaming applications. RTCP will not be used.

4.1.3.3 File Transfer

This section specifies interoperability requirements for reliable transfers of files between project systems. File transfer may also be used to support file based commanding, software upgrades, and still image transfer.

Projects must assign a delivery priority to each file sent to another system.

Some file transfers may require a greater delivery priority than other data exchanges.

Projects must transfer files in accordance with CCSDS 727.0-B-3, CCSDS File Delivery Protocol (CFDP).

CFDP provides file transfer and remote file system access over connectionless and unreliable network transports including UDP.

4.2 IP DATAGRAM FORWARDING

This section contains requirements specific to IP datagram forwarding by routers.

Projects must perform multihop routing as specified in RFC 1812, Requirements for IP Version 4 Routers, as updated by RFC 2644, Changing the Default for Directed Broadcasts in Routers.

These Projects are generally referred to as routing elements. This and STD-0003 leverage the maturation and experience gained via 10+ years of commercial internet deployments. These are the baseline specification documents utilized by commercial network equipment providers in providing standards compliant devices using the internet protocols. RFC 2644 allows routers to decline to forward directed broadcasts. While RFC 1812 was written for IPv4 routers before IPv6 was developed, it specifies behaviors that are generic to routers operating in any IP network including IPv6 networks.

4.2.1 NETWORK CONFIGURATION

This section contains requirements for configuring various parameters of IP systems. It is desirable for the configuration parameters to be changeable via local and remote (over the network) management interfaces. Simple Network Management Protocol (SNMP), C3I-105, Simple Network Management Protocol, provides a management interface for remote configuration.

Projects must provide a mechanism to manually configure the addresses of all IP-addressable interfaces.

While most IP addresses will remain fixed throughout a mission, it may be desirable to reconfigure some or all addresses on a particular system. The exception for devices that support only IP address autoconfiguration and self-assigned addresses is an attempt to allow COTS network appliances that may not support full manual configuration. Typically this mechanism is implemented in a management interface.

Projects must provide IP network address to data link-layer address mappings for IP addresses external to the system.

The link-layer addresses of the next hop(s) is (are) required to transmit the packet. The population of the mapping information may be via a management interface (local or remote), or via an automated protocol like the Address Resolution Protocol (ARP) on Ethernet. In general, protocols for address resolution are link-layer dependent.

Projects must use managed associations to map IP addresses to data link-layer addresses for IP addresses external to the system.

If there is no address resolution protocol, the only way for one IP node to determine the data link address of a neighboring node (needed in order to communicate with the neighbor) is to use managed entries. This requirement merely says that systems will be able to have and use managed entries; the actual set of entries in use at any particular

time by a particular system may consist of a mix of dynamically populated and managed entries.

Projects must accept modifications to the IP address to data link layer address mapping information via the network for IP addresses external to the system.

Ground controllers may need to manage entries in the IP-to-data link layer mapping tables of the various IP-addressable systems. This requirement ensures that the IP-to-data link mapping information can be managed remotely (via IP).

Projects must use static routing table entries.

Ground controllers need to be able to manually configure the path that packets take through the network. This is especially important early in the Program as the communications network will be managed more manually.

Projects must accept changes to the routing tables via the network.

There needs to be some way for ground controllers to manipulate the routing tables.

Projects must have a default route specified in the routing tables.

There will always be a usable route in the routing table even if the routing process is not functioning (i.e., in an emergency). This default route will be the route of last resort. The next hop in the default route may include redundancy like with the Virtual Router Redundancy Protocol (VRRP).

In general, symbolic names are used to reference Projects when humans are interacting with Projects or there is a visual representation of the network. This visual representation is usually portrayed via a network management station or something similar. Symbolic names are also used to mask potential IP address changes that may take place on Projects, which are not assigned their own block of static IP addresses. This allows the system to refer to one identifying label for each system and would alleviate the need to keep track of IP address changes if they should occur. Given the fact that initially there will be a small finite number of Projects, it is recommended that there be a technology evolution and growth path from using static host tables to Domain Name service for symbolic name to address mappings.

4.2.2 ROUTING FAILOVER AMBIGUITY RESOLUTION

It is anticipated that in the first design reference mission, routes are managed entities, and hence a heavy dependence on static routes exist. As things evolve the network is anticipated to become more complex and experience is gained throughout the first design reference mission phase. For such future design reference missions, dynamic routing becomes the normal mode of operation, but the ability to fallback to or fix routing problems by resorting to managed routes still exists.

If automated routing protocols are used, they may inject routes into forwarding tables that shadow or conflict with entries that are injected by hand via the management

interface. There should be no ambiguity in which entry is used. During the course of normal operation, network data paths will change. Route convergence is required to be completed within a reasonable amount of time.

Projects must fail over to default routes within 20 seconds when there is a loss of all routing information or a loss of communication to all system network neighbors that are participating in the dynamic routing protocol.

In case of a loss of all dynamic routing information, Projects need to fail over to a well-known, operational, default route. Such routes may be sub-optimal in terms of performance, but should be extremely robust. The exact value of the default route will be configured. The 20-second timer begins with the loss of connectivity and ends with the failover to the default route, so that the system needs to detect loss of connectivity and fail over to the default route in no more than 20 seconds from the time data link layer connectivity is lost. Dynamic routing protocols typically include configuration parameters to increase the failover time if that is desired.

4.2.3 ROUTE ADVERTISEMENT RESTRICTIONS

When automated routing protocols are used, participants can choose what information they provide to these protocols. Requirements in this section are to ensure that systems can implement multiple default routes (with different administrative costs) for redundancy without having to advertise and propagate these routes throughout the network. For instance, a system may have a backup default route to be used in an off nominal condition and may not want to advertise that route as a possible network path for other Systems.

4.3 NETWORK LAYER SECURITY

Network layer security can be used to secure a wide range of information exchanges. An IP Security (IPsec) based approach is adopted to provide end-to-end security for systems that will communicate primarily over IP.

Projects must implement SHA-256 based 256-bit Hash Based Messaged Authentication Codes (HMACs) and SHA-256 based truncated 128-bit HMACs in accordance with RFC 4868, Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, Sections 2.1, 2.1.1, 2.2, 2.3, and 2.6 (HMAC-SHA-256-128 only).

SHA-256 based HMACs will provide the high level of integrity protection needed for vehicle commanding and other critical data. The strength of SHA-256 bit HMACs will be needed within the ISS mission timeframe due to advancements in computing power that could obsolete the SHA-1 based HMACs before the start of the lunar phase.

Projects must implement RFC 4301, Security Architecture for the Internet Protocol, at all Internet Protocol (IP) based intersystem data exchange interfaces.

The C3I security architecture uses a combination of network layer security and application layer security to provide a robust and flexible set of security services (i.e., authentication, integrity, confidentiality) that can be used to provide ample security for a variety of mission types. IPsec was chosen for the network layer security portion of the

security architecture because IPsec is a widely recognized and implemented industry standard RFC 4301 defines the overall approach to IPsec, which provides a configurable ability to encrypt and/or authenticate (and verify the integrity of) IP packets in such a way that does not interfere with routing or access to the IP Header.

Projects must implement RFC 4303, IP Encapsulating Security Payload (ESP), at all Internet Protocol (IP) based intersystem data exchange interfaces.

The ESP provides authentication of the source of IP packets (the source is the node that secures a packet via the ESP, and this may be a security gateway rather than the original source of a packet), detection of changes to the payload (but not the header) of IP packets, and encryption of IP packet payloads and (optionally) the original header. If the original header is encrypted (i.e., tunnel mode), the ESP adds a clear header to the packet in order to facilitate routing and other layer 3 services. Using the ESP in tunnel mode provides partial traffic flow confidentiality because the IP addresses of internal networks can be hidden behind the IP addresses of security gateways. The ESP also provides a transport mode that protects traffic from original source to ultimate destination (rather than between two gateways). The ESP is part of the IPsec architecture, which provides the ability to configure (for each source-destination pair) if the ESP is used, which security services of the ESP are used, and which cryptographic keys are used. The ESP protocol does not interfere with routing or the processing of IP datagrams.

Projects must implement, at a minimum, all of the MUST algorithms, except Triple-DES-CBC, listed in RFC 4835, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), at all Internet Protocol (IP) based intersystem data exchange interfaces.

There is a need to support multiple cryptographic modes to cover the range of likely uses of the Advanced Encryption Standard (AES) algorithm. The required modes of operation are typically included in commercial products and are consistent with Internet standards associated with the use of AES.

Projects must implement RFC 4106, The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP), at all Internet Protocol (IP) based intersystem data exchange interfaces.

RFC 4106 describes the use of Advanced Encryption Standard (AES) in GCM in IPsec ESP mechanism to provide confidentiality, data origin authentication, and connectionless integrity. This mode provides an efficient mode that combines integrity checking and encryption (confidentiality protection) using the same (AES-based) algorithm.

4.3.1 INTERNET KEY EXCHANGE (IKE)

The Internet Key Exchange (IKE) provides a mechanism for systems to securely negotiate traffic encryption/authentication keys as needed.

Projects must implement RFC 4306, Internet Key Exchange Version 2 (IKEv2) Protocol, for all intersystem management of security associations (SAs) and keys used by IPsec.

The ability for network nodes to negotiate IPsec SAs and keys as described in RFC 4306 increases security by reducing the amount of information authenticated/encrypted with the same key, and decreases or eliminates the need to distribute keying material via a key management infrastructure. Reducing the use and distribution of cryptographic keys reduces the likelihood of the keys being compromised.

Projects must implement RFC 4307, Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2).

Systems will not be able to perform IKEv2 negotiations unless the systems use the same authentication and encryption algorithms. RFC 4307 is the Internet standard that specifies which algorithms are used in the IKEv2 protocol. Adopting RFC 4307 facilitates wide-scale interoperability and the use of commercial products for IKEv2 negotiations.

4.4 OPERATIONAL CONFIGURATIONS

A description of the operations engineering aspects, management practices and operability features that need to be engineered into the end-to-end IP network

Projects must implement the Internet Control Messaging Protocol (ICMP) per RFC 792.

ICMP is needed to inform hosts/routers when destinations are not reachable, when packets have timed out, and to carry other diagnostic information.

Projects must resolve symbolic names to IP addresses using static host table.

While Domain Name Services (DNS) may be available in addition to static host tables, static host tables will provide high-reliability mechanisms for mapping important DNS names to addresses. Using tables at each host relieves the need for connectivity to a DNS server. Some laboratory work will be needed to determine the best way to manage DNS zone transfers among intermittently connected systems, and how, or if, an appropriate DNS hierarchy can be set up.

Projects must accept changes to the static host table via the network.

4.4.1 HEADER COMPRESSION

This section defines how IP network communication traffic will be compressed in lossless fashion for transmission over resource constrained links, to maximize the volume of meaningful data conveyed by means of these limited resources.

Projects must implement RFC 2507, IP Header Compression.

On low-bandwidth links, IP headers can consume a significant percentage of total traffic, and also compresses the IP headers of non-TCP traffic.

Projects must implement RFC 2508, Compressing IP/UDP/RTP Headers for Low-Speed Serial Links.

On low-bandwidth links, RTP headers can consume a significant percentage of total traffic. RFC 2508 header compression will reduce the IP/UDP/RTP header from a typical length of 40 bytes to from 2 to 4 bytes.

4.4.2 TRAFFIC PRIORITIZATION

One of the tenets of using IP for networking is that it will not require all data flow volumes and paths to be planned ahead of time or strictly managed. There may be times when there is more data trying to traverse a particular link than that link can handle. If this condition persists, the IP packet queues in the router transmitting data will fill up and the router will be forced to discard packets (packets that are already in queue or new packets coming in). With Differentiated Services (diffserv), users will indicate relative priorities among packets, which state which packets are preferred to have dropped when congestion occurs. Network management can override users' requests or act on behalf of users to assert priorities for certain traffic types. If the network can support a user's request and the user traffic stays within its allocated bandwidth, the user should see minimal latency and jitter, with no congestion loss.

Projects must implement RFC 2474.

This is necessary to specify how to mark packets to comply with the IP Differentiated Services (DiffServ) architecture. DiffServ provides a scalable mechanism for providing differentiated treatment for different data. As such, certain data can be marked as higher priority than other data, with lower priority data discarded first in the case of network congestion. Support for any specific version of IP is not implied by this requirement. RFC 2474 is updated by RFC 3168, The Addition of Explicit Congestion Notification (ECN) to IP, and RFC 3260, New Terminology and Clarifications for Diffserv. RFC 3168 specifies how the 2 bits marked as unused in RFC 2474 should be used to implement Explicit Congestion Notification (ECN). This document does not specify the use of ECN, so RFC 3168 is not required. RFC 3260 is an informational RFC that clarifies terminology for differentiated services.

Projects must implement RFC 3140, Per Hop Behavior Identification Codes.

This is necessary to identify behaviors in order to comply with the IP Differentiated Services (DiffServ) architecture.

Projects must implement RFC 3246, An Expedited Forwarding PHB (Per-Hop Behavior).

This is necessary to identify an additional behavior in order to comply with the IP Differentiated Services (DiffServ) architecture.

Projects must implement RFC 2597, Assured Forwarding PHB Group.

The Assured Forwarding (AF) Per-Hop Behavior (PHB) Group provides delivery of IP packets in four independently forwarded AF classes. Within each AF class, an IP packet can be assigned one of three different levels of drop precedence. This PHB provides the flexibility to control both the transmission priorities across multiple AF classes such as motion imagery, telemetry, file transfer, etc., and the buffering allocations assigned to data flows within a single AF class. AF PHB will deliver the desired end-to-end quality of service while providing automated protection of critical data flows in the event of unplanned drop in space link capacity.

4.4.3 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

The SNMP provides a standard mechanism for using an IP network to control IP systems such as routers and hosts. The SNMP provides a simple request/response interface to access parameters on IP network devices. The SNMP provides for traps, which are gratuitous messages generated when specified network events occur. The SNMP also provides for a set operation, which allows network operations to configure specified network parameters.

Projects must implement STD-0062, RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP).

SNMP is the industry standard for managing network elements. There is an abundance of software that uses SNMP to harvest information and display network status to operators. STD-0062 includes RFCs 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), with RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework being an informational RFC. SNMP runs over a wide range of transport protocols, including UDP.

5. Future Planned Networks (TBD)

Material from NASA programs relative to this section do exist and will be provided at a future time. Further, we invite participation in developing this section from all interested parties.

APPENDIX A

A-1 TRANSPORTING IP OVER CCSDS LINKS

IP protocols actually depend on control protocols that have to be separately identified at the link layer. For this reason - and the ability to not depend on which link protocols are favored on the line card interfaces of a desired router – simply encapsulating the link layer used at the routers egress in CCSDS ENCAP has significant merits. The down side is that the link layers used in spacecraft would not be forced to be interoperable because they are router dependent. To reduce this interoperability constraint, and because CCSDS already defined packet encapsulation, the approach chosen was to use AOS/ENCAP as the CCSDS standardized method of transporting IP datagrams between routers. Since AOS/ENCAP is not available as part of ground COTS routers – typically it is Ethernet, but it can also be MPoFR or PPP - a link layer translation bridge was required on the ground. This is shown in Figure 7. The reliability of a custom developed bridge in a human spaceflight environment was a point of discussion. The desire was to make the bridge translation functions as simple and stateless as possible. However, the bridge will have to provide some form of support for certain link layer protocols, such as header compression.

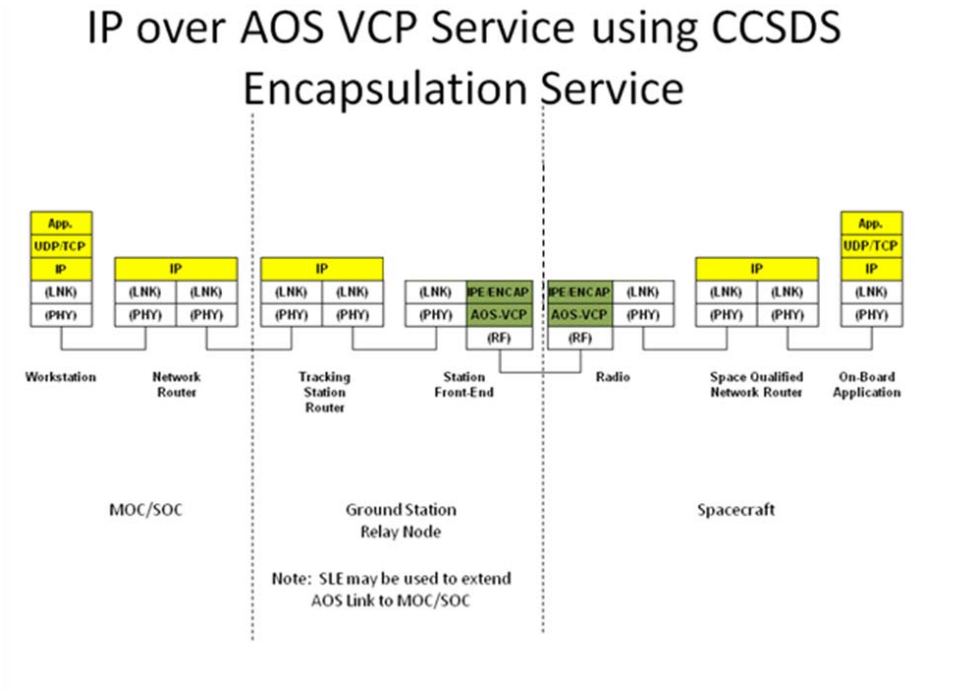


Figure 7 Use of bridge to translate commercial router interface protocols to CCSDS standard

A further discussion involved how projects interpreted the CCSDS link layer specifications. Several issues were discussion. For one, CCSDS does not have a maximum transmission unit (MTU) size inherit in the link – progressively larger ENCAP headers are used. No project opted to support the largest ENCAP header size. Some projects decided not to support the small ENCAP header size. The IPE shim

is defined to be extensible by using the low bit to signal extensions. All needed IPE protocols were covered with a single byte, so no project opted to implement the extension capability in their hardware. The placement of IP packets in AOS frames was another discussion. In an actual implementations, the data is pulled and then an AOS frame is constructed. If at that moment, there is not enough data to fully populate the AOS frame, there frame will be constructed as is. The implication is that once ENCAP idle packets start, no useful data will follow in that frame. For this reason, projects declared that upon finding and ENCAP idle, they'd stop processing the rest of the AOS frame. Finally, there originally were multiple ways of putting an IP packet into an AOS frame. Recently the CCSDS deprecated all but one approach, justifying projects that had opted to only include the IPE approach.

It is noted that the above implementation choices actually can hurt interoperability. An example is a system that generates 2-byte encap headers when small IP packets are encountered, but a receiving system that only understands 4-byte encap headers.

A-2 Applicability Matrix for CCSDS Blue books

The following are a sample of the total applicability tables. More to follow.

CCSDS 133.1-B1

CCSDS 133.1-B-1	Encapsulation Service, Blue Book June 2006	Primary Communications		
Section Number	Section Title	DRM Compliancy	Lunar Compliancy	Notes
1	INTRODUCTION			
1.1	PURPOSE	n/a	n/a	
1.2	SCOPE	n/a	n/a	
1.3	APPLICABILITY	yes	yes	
1.4	RATIONALE	n/a	n/a	
1.5	DOCUMENT STRUCTURE	n/a	n/a	
1.6	CONVENTIONS AND DEFINITIONS	yes	yes	
1.7	REFERENCES	n/a	n/a	
2	OVERVIEW			
2.1	CONCEPT OF ENCAPSULATION SERVICE	yes	yes	
2.2	FEATURE OF ENCAPSULATION SERVICE	yes	yes	
2.3	ADDRESSING	yes	yes	PVN = 8, section 4
2.4	SERVICE DESCRIPTION	n/a	n/a	
3	SERVICE DEFINITIONS			
3.1	OVERVIEW			
3.2	SERVICE PARAMETERS	n/a	n/a	
3.2.1	DATA UNIT	yes	yes	IP is Octet aligned
3.2.2	GVCID	no	no	This is handled in the AOS fra
3.2.3	PVN	yes	yes	
3.2.4	EPI	yes	yes	Protocol ID
3.2.5	DATA UNIT LOSS FLAG	no	no	
3.3	SERVICE PRIMITIVES	no	no	
3.3.1	GENERAL	no	no	Only utilizing the ENCAP Head
3.3.2	ENCAPSULATION.REQUEST	no	no	Only utilizing the ENCAP Head
3.3.2.1	Function			
3.3.2.2	Semantics			
3.3.2.3	When Generated			
3.3.2.4	Effect on Receipt			
3.3.2.5	Additional Comments			
3.3.3	ENCAPSULATION.INDICATION	no	no	Only utilizing the ENCAP Head
3.3.3.1	Function			
3.3.3.2	Semantics			
3.3.3.3	When Generated			
3.3.3.4	Effect on Receipt			
3.3.3.5	Additional Comments			
4	DATA UNITS AND PROCEDURES			

4.1	SPACE PACKET	no	no	
4.2	ENCAPSULATION PACKET	n/a	n/a	
4.2.1	GENERAL	yes	yes	
4.2.2	ENCAPSULATION PACKET HEADER	n/a	n/a	
4.2.2.1	General	yes	yes	6 Octets
4.2.2.2	Packet Version Number	yes	yes	mandatory
4.2.2.3	Protocol ID	yes	yes	mandatory
4.2.2.4	Length of Length	yes	yes	mandatory
4.2.2.5	User Defined Field	yes	yes	possibly needed to carry head info
4.2.2.6	Protocol ID Extension	yes	yes	
4.2.2.7	CCSDS Defined Field	no	no	
4.2.2.8	Packet Length	yes	yes	
4.2.3	ENCAPSULATED DATA FIELD	yes	yes	
4.3	PROCEDURES AT THE SENDING END	yes	yes	
4.4	PROTOCOL PROCEDURES AT THE RECEIVING END	yes	yes	
5	**MANAGED PARAMETERS**			
ANNEX A	ACRONYMS	n/a	n/a	
ANNEX B	INFORMATIVE REFERENCES	n/a	n/a	
ANNEX C	CHANGES FROM REFERENCES	n/a	n/a	
C1	GENERAL	n/a	n/a	

CCSDS 732

CCSDS 732.0-B-2	**AOS Space Data Link Protocol**	**Primary Communications**		
Section Number	**Section Title**	**DRM Compliancy**	**Lunar Compliancy**	**Notes**
1	**INTRODUCTION**			
1.1	PURPOSE	n/a	n/a	
1.2	SCOPE	n/a	n/a	
1.3	APPLICABILITY	yes	yes	
1.4	RATIONALE	n/a	n/a	
1.5	DOCUMENT STRUCTURE	n/a	n/a	
1.6	CONVENTIONS AND DEFINITIONS	yes	yes	
1.7	REFERENCES	n/a	n/a	
2	**OVERVIEW**			
2.1	CONCEPT OF AOS SPACE DATA LINK PROTOCOL			
2.1.1	ARCHITECTURE	n/a	n/a	
2.1.2	PROTOCOL FEATURES	n/a	n/a	
2.1.3	ADDRESSING	n/a	n/a	
2.1.4	PROTOCOL DESCRIPTION	n/a	n/a	
2.2	OVERVIEW OF SERVICES			
2.2.1	COMMON FEATURES OF SERVICES			
2.2.2	SERVICE TYPES			
2.2.2.1	Overview			
2.2.2.2	Asynchronous Service	no	no	
2.2.2.3	Synchronous Service	no	no	

2.2.2.4	Periodic Service	yes	yes	One Master channel in the Phy
2.2.3	SUMMARY OF SERVICES			
2.2.3.1	Overview			
2.2.3.2	Packet Service	yes	yes	I believe this is going to be VC
2.2.3.3	Bitstream Service	no	no	
2.2.3.4	Virtual Channel Access (VCA) Service	no	no	
2.2.3.5	Virtual Channel Operational Control Field (VC_OCF) Service	no	no	
2.2.3.6	Virtual Channel Frame (VCF) Service	no	no	
2.2.3.7	Master Channel Frame (MCF) Service	no	no	
2.2.3.8	Insert Service	no	no	
2.2.4	RESTRICTIONS ON SERVICES	yes	yes	
2.3	OVERVIEW OF FUNCTIONS	yes	yes	
2.3.1	GENERAL FUNCTIONS	yes	yes	excluding c) multiplexing/dem
2.3.2	INTERNAL ORGANIZATION OF PROTOCOL ENTITY	n/a	n/a	informational
2.4	SERVICES ASSUMED FROM LOWER LAYERS			
2.4.1	SERVICES ASSUMED FROM THE SYNCHRONIZATION AND CHANNEL CODING SUBLAYER	yes	yes	
2.4.2	PERFORMANCE REQUIREMENTS TO LOWER LAYERS	no	no	mission has not specified spec (further discussions necessary
3	**SERVICE DEFINITIONS**			
3.1	OVERVIEW	n/a	n/a	
3.2	SOURCE DATA			
3.2.1	SOURCE DATA OVERVIEW	yes	yes	a) Packet
3.2.2	PACKET	yes	yes	ENCAP Packet
3.2.3	BITSTREAM DATA	no	no	
3.2.4	VIRTUAL CHANNEL ACCESS SERVICE DATA UNTI (VCA_SDU)	no	no	
3.2.5	OPERATIONAL CONTROL FIELD SERVICE DATA UNIT (OCF_SDU)	no	no	
3.2.6	AOS TRANSFER FRAME	yes	yes	
3.2.7	INSERT SERVICE DATA UNIT (IN_SDU)	no	no	
3.3	PACKET SERVICE	yes	yes	
3.3.1	OVERVIEW OF PACKET SERVICE	n/a	n/a	
3.3.2	PACKET SERVICE PARAMETERS	n/a	n/a	
3.3.2.1	General	n/a	n/a	
3.3.2.2	Packet	yes	yes	ENCAP Packet
3.3.2.3	GVCID	yes	yes	In the AOS Header field, althou be the VCID
3.3.2.4	Packet Version Number	yes	yes	In the ENCAP header field
3.3.2.5	Packet Quality Indicator	no	no	only complete packets will be t
3.3.3	PACKET SERVICE PRIMITIVES	no	no	No Primitives will be used
3.4	BITSTREAM SERVICE	no	no	
3.5	VIRTUAL CHANNEL ACCESS (VCA) SERVICE	no	no	
4	**PROTOCOL SPECIFICATION**			
4.1	PROTOCOL DATA UNIT			
4.1.1	AOS TRANSFER FRAME			
4.1.1.1	no heading	yes	yes	following the header field conv
4.1.1.2	no heading	yes	yes	maintaining a constant length f
4.1.2	TRANSFER FRAME PRIMARY HEADER			

4.1.2.1	General	yes	yes	
4.1.2.2	Master Channel Identifier	yes	yes	01 and SCID determined by m
4.1.2.3	Virtual Channel Identifier	yes	yes	determined by management
4.1.2.4	Virtual Channel Frame Count	yes	yes	
4.1.2.5	Signaling Field	yes	yes	except replay flag
4.1.2.6	Frame Header Error Control	no	no	optional field
4.1.3	TRANSFER FRAME INSERT ZONE	no	no	
4.1.4	TRANSFER FRAME DATA FIELD			
4.1.4.1	Overview			
4.1.4.1.1	no heading	yes	yes	
4.1.4.1.2	no heading	yes	yes	
4.1.4.1.3	no heading	yes	yes	M_PDU
4.1.4.1.4	no heading	yes	yes	M_PDU
4.1.4.1.5	no heading	yes	yes	support for idle transfer frames
4.1.4.2	Multiplexing Protocol Data Unit	yes	yes	
4.1.4.2.1	Overview			
4.1.4.2.1.1		yes	yes	
4.1.4.2.1.2		yes	yes	
4.1.4.2.1.3		yes	yes	
4.1.4.2.1.4		yes	yes	
4.1.4.2.1.5		yes	yes	
4.1.4.2.2	Reserved Spare			
4.1.4.2.2.1		yes	yes	
4.1.4.2.2.2		yes	yes	
4.1.4.2.3	First Header Pointer			
4.1.4.2.3.1		yes	yes	
4.1.4.2.3.2		yes	yes	
4.1.4.2.3.3		yes	yes	
4.1.4.2.3.4		yes	yes	
4.1.4.2.3.5		no	no	at this point, there is only a pla a AOS fill frame or a M_PDU fi
4.1.4.2.4	M_PDU Packet Zone			
4.1.4.2.4.1		yes	yes	
4.1.4.2.4.2		yes	yes	only packet data,no fill
4.1.4.2.4.3		yes	yes	
4.1.4.2.4.4		no	no	again, only one type of fill fram
4.1.4.3	Bitstream Protocol Data Unit	no	no	
4.1.5	OPERATIONAL CONROL FIELD	no	no	
4.1.6	FRAME ERROR CONTROL FIELD	no	no	Recommended by CCSDS but from by NASA
4.2	PROTOCOL PROCEDURES AT THE SENDING END			
4.2.1	OVERVIEW			
4.2.2	PACKET PROCESSING FUNCTION			
4.2.3	BITSTREAM PROCESSING FUNCTION			
4.2.4	VIRTUAL CHANNEL GENERATION FUNCTION			
4.2.4.1	no heading	yes	yes	M_PDU
4.2.4.2	no heading	no	no	
4.2.4.3	no heading	no	no	

4.2.5	VIRTUAL CHANNEL MULTIPLEXING FUNCTION	no	no	
4.2.6	MASTER CHANNEL MULTIPLEXING FUNCTION	no	no	
4.2.7	ALL FRAMES GENERATION FUNCTION	no	no	
4.3	PROTOCOL PROCEDURES AT THE SENDING END			
4.3.1	OVERVIEW			
4.3.2	PACKET EXTRACTION FUNCTION	yes	yes	
4.3.2.1		yes	yes	
4.3.2.2		yes	yes	
4.3.2.3		yes	yes	
4.3.2.4		yes	yes	
4.3.2.5		yes	yes	
4.3.2.6		yes	yes	in our case, only one PVN
4.3.3	BITSTREAM EXTRACTION FUNCTION	no	no	
4.3.4	VIRTUAL CHANNEL RECEPTION FUNCTION			
4.3.4.1	no heading	yes	yes	
4.3.4.2	no heading	yes	yes	Packet Extraction
4.3.4.3	no heading	n/a	n/a	
4.3.4.4	no heading	no	no	frame count in telemetry will si packet
4.3.4.5	no heading	n/a	n/a	
4.3.5	VIRTUAL CHANNEL DEMULTIPLEXING FUNCTION	no	no	
4.3.6	MASTER CHANNEL DEMULTIPLEXING FUNCTION	no	no	
4.3.7	ALL FRAMES RECEPTION FUNCTION	no	no	
5	**MANAGED PARAMETERS**			
5.1	OVERVIEW OF MANAGED PARAMETERS			
5.2	MANAGED PARAMETERS FOR A PHYSICAL CHANNEL			
5.3	MANAGED PARAMETERS FOR A MASTER CHANNEL			
5.4	MANAGED PARAMETERS FOR A VIRTUAL CHANNEL	yes	yes	version number, SCID, VCID,
5.5	MANAGED PARAMETERS FOR PACKET TRANSFER	no	no	
ANNEX A	ACRONYMS	n/a	n/a	
ANNEX B	INFORMATIVE REFERENCES	n/a	n/a	
ANNEX C	CHANGES FROM REFERENCES			
C1	GENERAL			
C2	TECHNICAL CHANGES			
C2.1	PACKETS WITH DIFFERENT VERSION NUMBERS	yes	yes	version 1
C2.2	MULTIPLEXING AND DEMULTIPLEXING OF PACKETS WITH DIFFERENT APPLICATION IDENTIFIERS	n/a	n/a	
C2.3	MULTIPLEXING OF CODED AND NON-CODED TRANSFER FRAMES	yes	yes	no multiplexing of coded and u coding is either "on" or "off" for
C2.4	INPUT TO THE VIRTUAL CHANNEL FRAME SERVICE	n/a	n/a	
C2.5	MASTER CHANNEL FRAME SERVICE	n/a	n/a	
C2.6	INTERNET AND ENCAPSULATION SERVICES	n/a	n/a	
C2.7	OPERATIONAL CONTROL FIELD SERVICES	n/a	n/a	
C2.8	PARAMETERS OF SERVICE PRIMITIVES	n/a	n/a	
C2.9	SLAP	n/a	n/a	
C2.10	GRADES OF SERVICE	n/a	n/a	
C3	TERMINOLOGY CHANGES	n/a	n/a	

A-3 Applicability Matrix for IETF RFCs

Formatted: Font: 16 pt, Bold, Italic

RFC 2507

RFC-2507	IP Header Compression (IPHC)				
Section Number	Section Title	DRM Compliancy	Lunar Compliancy	Rationale/Comments/Assumptions	Additional Comm
1	Introduction	Yes	Yes		
2	Terminology	Yes	Yes		
3	Compression method	Partially Yes (See Column E, IPHC supported only in WAN (RF) interfaces)	Partially Yes (See Column E, IPHC supported only in WAN (RF) interfaces)	The following links/interfaces on the C3I router will employ IPHC: 3 WAN (RF) links: YES 1 Hardline (CCN): NO 1 802.11g WLAN: NO 2 Host interfaces: NO **Rationale:** Of these, only the WAN links can drop to low speeds (10s of kbps (e.g. during launch) and can exhibit higher errors. The much higher speeds of the other links (e.g. hardline at 100Mbs and 802.11g at 54Mbps) and/or low error rates imply that any gains from IPHC would be insignificant. The link layer is required to provide the following for IPHC to work correctly: 1. Link layer packet length indication 2. Link layer packet type indication 3. Link layer packet loss/error indication (checksum protection) **Configuration:** Router software will configure a link to enable or disable IPHC.	
3.1.	Packet types	Partially Yes (See Column E, IPHC not supported for TCP traffic)	Partially Yes (See Column E, IPHC not supported for TCP traffic)	The following packet types would be supported: FULL_HEADER: YES (required to establish and maintain contexts) COMPRESSED_NON_TCP: YES (to support UDP/IP streams) COMPRESSED_TCP: NO (there is no TCP traffic envisaged and this entails significant state maintanence and protocol complexity COMPRESSED_TCP_NO_DELTA: NO (same rationale as COMPRESSED_TCP) CONTEXT_STATE: NO (Used to repair broken TCP contexts. Same rationale as COMPRESSED_TCP)	COMPRESSED_TCP, COMPRESSED_TCP_ packet types are not M CONTEXT_STATE is
3.2.	Lost packets in TCP packet streams	No	No	See rationale for Section 3.1 in cell 6E.	

3.3.	Lost packets in UDP and non-TCP packet streams	Yes	Yes	**Configuration:** MIN_WRAP, F_MAX_PERIOD, F_MAX_TIME. Will be configured per-link (rather than per-context). Router software will configure the hardware. Router software will present a command interface for configuration (similar to one for IPsec configuration).
4	Grouping packets into packet streams	Yes	Yes	See note about configuration mechanism in cell 8E. Links would be configured by router software for enabling or disabling IPHC. Router software will also provide the means to identify packets belonging to a particular packet stream (to establish context).
4.1.	Guidelines for grouping packets	Yes	Yes	**Configuration:** Choice of defining fields (DEF) in the header chain include: Flow Label, Source and Destination IP addresses, Source and Destination UDP Ports, Next Header fields (for IPv6), Protocol field (IPv4), SPI (for AH and ESP), SSRC (RTP). Trade-off between too few and too many fields used. Router software will configure the links for defining fields for the contexts.
5	Size Issues	Yes	Yes	
5.1.	Context identifiers	Yes	Yes	Both 8-bit and 16-bit CID formats will be supported. **Rationale:** Even though IPHC envisaged to be used for limited number of RT/UDP/IP streams and some UDP/IP streams, for inter-operability with ground systems, both CID formats will be supported.
5.2.	Size of the context	Yes	Yes	**Configuration:** MAX_HEADER defines the maximum size of the context that can be compressed or decompressed. The chain of headers less than or equal in size to MAX_HEADER bytes will be compressed. Software will configure the link for this parameter.
5.3.	Size of full headers	Yes	Yes	Since we assume that the link layer implementation provides the length of packets, we can use the length fields in full headers to pass the values of the CID and the generation to the decompressor.
5.3.1.	Length fields in full TCP headers	No	No	See rationale for Section 3.1 in cell 6E. TCP headers not supported.
5.3.2.	Length fields in full non-TCP headers	Yes	Yes	Full non-TCP headers with both 8-bit and 16-bit CID formats supported. See cell 12E.

6	Compressed Header Formats	Partially Yes (See Column E, IPHC not supported for TCP traffic)	Partially Yes (See Column E, IPHC not supported for TCP traffic)	a) COMPRESSED_TCP format: NO b) COMPRESSED_TCP_NODELTA header format: NO c) Compressed non-TCP header, 8 bit CID: YES d) Compressed non-TCP header, 16 bit CID: YES Rationale: For a) and b) See cell 6E. For c) and d) see cell 12E.
7	Compression of subheaders	Partially Yes (See below)	Partially Yes (See below)	
7.1.	IPv6 Header	No	Yes	**Rationale:** IPv6 not a requirement in DRM
7.2.	IPv6 Extension Headers	No	Yes	**Rationale:** IPv6 not a requirement in DRM
7.3.	Options	No (See Column E)	No (See Column E)	Recommendation is No, based on assumption of low volume of this type of subheader. Gains from compression expected to be insignificant.
7.4.	Hop-by-hop Options Header	No (See Column E)	No (See Column E)	Recommendation is No, based on assumption of low volume of this type of subheader. Gains from compression expected to be insignificant.
7.5.	Routing Header	No (See Column E)	No (See Column E)	**Rationale:** Routing Protocol supported in s/w. Routing Protocol headers will not be compressed by h/w. h/w is expected to be agnostic to Routing Protocol headers. Also, Routing Headers are expected to be low volume and not expected to gain significantly by IPHC.
7.6.	Fragment Header	No (See Column E)	No (See Column E)	**Rationale:** Fragments supported only in software. Router h/w does not handle IP fragmentation. Fragment Headers will not be compressed by h/w. h/w is agnostic to Fragment headers. Also, Fragment Headers are expected to be low volume and not expected to gain significantly by IPHC.
7.7.	Destination Options Header	No	No	**Rationale:** Destination software processes this header.
7.8.	No Next Header	Yes	Yes	Covered by rules for Row 20 (IP Extension Headers)
7.9.	Authentication Header	Yes	Yes	
7.10.	Encapsulating Security Payload Header	Yes	Yes	
7.11.	UDP Header	Yes	Yes	

Meaning, the payload cannot be padded with

Will this ever happen i environment?

there must not be any after the UDP payload covered by the IP Leng

7.12.	TCP Header	No (See Column E, IPHC not supported for TCP traffic)	No (See Column E, IPHC not supported for TCP traffic)	Rationale: See cell 6E.
7.13.	IPv4 Header	Yes	Yes	
7.14	Minimal Encapsulation header	No (See Column E)	No (See Column E)	**Rationale:** This type of subheader is used by Mobile IP. Mobile IP is not a requirement for the C3I Router and therefore this type of subheader will not be supprted for compression.
8	Changing context identifiers	Yes	Yes	
9	Rules for dropping or temporarily storing packets	Partially Yes (See coumn E)	Partially Yes (See coumn E)	**TCP:** Not supporting rules for dropping or storing TCP packets. **Rationale:** See cell 6E. **UDP:** Rules for dropping/storing UDP packets: **Recommend:** Drop packets when: A decompressor receives a packet with a compressed non-TCP header with CID C and generation G, the header must not be decompressed using the current context when: a) the decompressor has been disconnected from the compressor for more than MIN_WRAP seconds, because the context might be obsolete even if it has generation G. b) the context for C has a generation other than G. **Rationale:** Minimize context overhead and complexity.
10	Low-loss header compression for TCP	No	No	**Rationale:** See 6E (not supporting TCP packet types).
10.1.	The "twice" algorithm	No	No	Rationale: See cell 35E.
10.2.	Header Requests	No	No	Rationale: See cell 35E. Packet Type CONTEXT_STATE not supported (see cell 6E).
11	Links that reorder packets	No	No	**Rationale:** Reordering will not happen on point to point links in the Constellation. Multi-hop (layer-2) radio links are not being used so reordering is not going to happen. Egress scheduling of packets is FIFO per priority class and we are not supporting QoS remarking.
11.1.	Reordering in non-TCP packet streams	No	No	**Rationale:** See cell 38E. Also see cell 34E. Packets arriving out of order (due to potential errors) will be dropped.
11.2.	Reordering in TCP packet streams	No	No	**Rationale:** See cell 38E and cell 6E.
12	Hooks for additional header compression	Yes (See Column E)	Yes (See Column E)	Note: Only supported for RTP packets (RFC 2508)

13	Demultiplexing	Yes	Yes	Link layer support required as noted in cell 5E. Will support for WAN RF interfaces only as noted in cell 5E. AOS ENCAP has draft specification for this support.
14	Configuration Parameters	Yes	Yes	**Configuration:** Will be done per-link (not per context) MIN_WRAP (default 3 seconds) F_MAX_PERIOD (default 256) Range: 1 - 65535 F_MAX_TIME (default 5) Range: 1 - 255 F_MAX_HEADER (168 octets) Range: 60 - 65535 TCP_SPACE - Maximum CID value for TCP (not supported) NON_TCP_SPACE - Maximum CID value for non-TCP (default 15) Range: 3 - 65535 EXPECT_REORDERING (default No) Other configuration entities as noted in cells 5E and 10E.
15	Implementation Status	Yes	Yes	
16	Acknowledgments	Yes	Yes	
17	Security Considerations	Yes	Yes	

RFC 2508

RFC-2508	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links			
Section Number	Section Title	DRM Compliancy	Lunar Compliancy	Rationale/Comments/Assumptions
1	Introduction	Yes	Yes	
2	Assumptions and Tradeoffs	Yes	Yes	No segmentation and preemption of large packets assumed. Performs best on links with low round trip delays.
2.1.	Simplex vs. Full Duplex	Yes	Yes	Since this would be used for RTP/UDP/IP header compression, the periodic refresh method listed in Section 3.3 of RFC 2507 (UDP compression slow start) is recommended to be used rather than an explicit error signal from the decompressor.
2.2.	Segmentation and Layering	Yes	Yes	Segmentation expected to be handled as a separate layer. This IPHC scheme does not deal with segmentation. The link layer is assumed to provide the following for IPHC to work correctly: 1. Link layer packet length indication 2. Link layer packet type indication 3. Link layer packet loss/error indication (checksum protection)
3	The Compression Algorithm	Yes	Yes	

3.1.	The basic idea	Yes	Yes	A session context is defined by the combination of the IP source and destination addresses, the UDP source and destination ports, and the RTP SSRC field. Maintain negative cache (?) (for packets that fail to compress). Recommend not supporting. Also no support for IP fragmentation.
3.2.	Header Compression for RTP Data Packets	Yes	Yes	
3.3.	The protocol	Partially Yes (see below)	Partially Yes (see below)	The following packet types would be supported: FULL_HEADER: YES (required to establish and maintain contexts) COMPRESSED_UDP: YES (Even though COMPRESSED_NON_TCP (RFC 2507) already supports UDP/IP streams, we support COMPRESSED_UDP for interoperability with ground systems). COMPRESSED_RTP: YES CONTEXT_STATE: NO (See cell 15E below)
3.3.1.	FULL_HEADER (uncompressed) packet format	Yes	Yes	Both 8-bit and 16-bit CID formats supported. **Rationale:** See cell 12E for RFC 2507 (Sheet 1)
3.3.2.	COMPRESSED_RTP packet format	Yes	Yes	
3.3.3.	COMPRESSED_UDP packet format	Yes	Yes	**Rationale:** See cell 10E above.
3.3.4.	Encoding of differences	Yes	Yes	
3.3.5.	Error Recovery	No (See Column E)	No (See Column E)	**Recommend:** All packets for an invalid context will be discarded. **Rationale:** Pre-configured RTP streams, low-error probability and to keep complexity low.
3.4.	Compression of RTCP Control Packets	No (See Column E)	No (See Column E)	**Rationale:** RTCP is not a requirement. Therefore no need to tailor a spearate compression scheme for RTCP control packets.
3.5.	Compression of non-RTP UDP Packets	Yes	Yes	**Rationale:** See cell 10E above.
4	Interaction With Segmentation	No (See Column E)	No (See Column E)	**Rationale:** Segmentation dealt with in software.
5	Negotiating Compression	No (Static configuration)	No (Static configuration)	**Rationale:** Handled through configuration. **Configuration:** Requires the following: 1. The size of the context ID. 2. The maximum size of the stack of headers in the context. 3. A context-specific table for decoding of delta values.

		Compliancy		
1	Introduction	Yes	Yes	
1.1	Terminology	Yes	Yes	
2	RTP and RTCP Packet Forms and Protocol Behavior	Partial	Partial	Congestion: "...RTP are dropped (Note: Verify HW wil
3	Registering Additional Encodings	Partial	Partial	"Systems that expect not make their own a types." - We need a
4	Audio	Yes	Yes	
4.1	Encoding-IndependentRules	Yes	Yes	AI: need to determin to PTT reqt. Mb - Nice to have.
4.2	Operating Recommendations	Yes	Yes	
4.3	Guidelines for Sample-Based Audio Encodings	NA	NA	
4.4	Guidelines for Frame-Based Audio Encodings	Yes	Yes	
4.5	Audio Encodings	Yes	Yes	
4.5.1	DVI4	NA	NA	
4.5.2	G722	NA	NA	
4.5.3	G723	NA	NA	
4.5.4	G726-40, G726-32, G726-24, and G726-16	NA	NA	
4.5.5	G728	NA	NA	
4.5.6	G729	Partial	Partial	"A voice activity dete Annex B of G.729 is
4.5.7	G729D and G729E	NA	NA	
4.5.8	GSM	NA	NA	
4.5.9	GSM-EFR	NA	NA	
4.5.10	L8	NA	NA	
4.5.11	L16	NA	NA	
4.5.12	LPC	NA	NA	
4.5.13	MPA	NA	NA	
4.5.14	PCMA and PCMU	NA	NA	
4.5.15	QCELP	NA	NA	
4.5.16	RED	NA	NA	
4.5.17	VDVI	NA	NA	
5	Video	Partial	Partial	"For most of these vi instant of the video ir occupies more than and "Most of these v header should be se zero."
5.1	CelB	NA	NA	
5.2	JPEG	NA	NA	
5.3	H261	NA	NA	
5.4	H263	NA	NA	
5.5	H263-1998	NA	NA	
5.6	MPV	NA	NA	
5.7	MP2T	NA	NA	
5.8	nv	NA	NA	
6	Payload Type Definitions	Partial	Partial	"Audio applications c and/or receive payloa

7	RTP over TCP and Similar Byte Stream Protocols	NA	NA	
8	Port Assignment	Yes*	Yes*	follow the rule that R
9	Changes from RFC 1890	Yes	Yes	
10	Security Considerations	Yes	Yes	
11	IANA Considerations	NA	NA	
12	References	NA	NA	
12.1	Normative References	NA	NA	
12.2	Informative References	NA	NA	
13	Current Locations of Related Resources	NA	NA	
14	Acknowledgments	NA	NA	
15	Intellectual Property Rights Statement	NA	NA	
16	Authors' Addresses	NA	NA	
17	Full Copyright Statement	NA	NA	

Yes* indicates that this section applies, but since RTCP is unimplemented those aspects are ignored.