Draft Report Concerning
Space Data System Standards

CISLUNAR SPACE
INTERNETWORKING—
ARCHITECTURE

DRAFT INFORMATIONAL REPORT

CCSDS 730.1-G-0

DRAFT GREEN BOOK
December 2006
CCSDS REPORT CONCERNING CISLUNAR SPACE INTERNETWORKING—ARCHITECTURE

AUTHORITY

<table>
<thead>
<tr>
<th>Issue</th>
<th>Draft Green Book, Issue 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>December 2006</td>
</tr>
<tr>
<td>Location</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

(WHEN THIS INFORMATIONAL REPORT IS FINALIZED, IT WILL CONTAIN THE FOLLOWING STATEMENT OF AUTHORITY:)

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and reflects the consensus of technical working group experts from CCSDS Member Agencies. The procedure for review and authorization of CCSDS Reports is detailed in the Procedures Manual for the Consultative Committee for Space Data Systems.

This document is published and maintained by:

CCSDS Secretariat
Office of Space Communication (Code M-3)
National Aeronautics and Space Administration
Washington, DC 20546, USA
FOREWORD

This document is a CCSDS Informational Report to assist readers in understanding the Spacecraft Onboard Interface Services (SOIS) documentation. It has been prepared by the Consultative Committee for Space Data Systems (CCSDS). The concepts described herein are the baseline concepts for the CCSDS standardization activities in respect of communication services and generic support services to be used in the flight segment of spacecraft systems.

This Report describes the challenges posed by spacecraft onboard interfaces, details the service architecture of the SOIS services, and elaborates on the goals and expected benefits of the key SOIS services. It is intended to serve as a reference for both service users and service implementers in order to maximize the potential of standardized onboard interfaces with respect to re-use, interoperability, and interagency cross support.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Report is therefore subject to CCSDS document management and change control procedures, which are defined in the Procedures Manual for the Consultative Committee for Space Data Systems. Current versions of CCSDS documents are maintained at the CCSDS Web site:

http://www.ccsds.org/

Questions relating to the contents or status of this document should be addressed to the CCSDS Secretariat at the address indicated on page i.
At time of publication, the active Member and Observer Agencies of the CCSDS were:

**Member Agencies**
- Agenzia Spaziale Italiana (ASI)/Italy.
- British National Space Centre (BNSC)/United Kingdom.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (Roskosmos)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.

**Observer Agencies**
- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNII Mash)/Russian Federation.
- Centro Tecnico Aeroespacial (CTA)/Brazil.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish Space Research Institute (DSRI)/Denmark.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Hellenic National Space Committee (HNSC)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- KFKI Research Institute for Particle & Nuclear Physics (KFI)/Hungary.
- Korea Aerospace Research Institute (KARI)/Korea.
- MIKOMTEK: CSIR (CSIR)/Republic of South Africa.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic & Atmospheric Administration (NOAA)/USA.
- National Space Organization (NSPO)/Taipei.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- United States Geological Survey (USGS)/USA.
## DOCUMENT CONTROL

<table>
<thead>
<tr>
<th>Document</th>
<th>Title</th>
<th>Date</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCSDS 730.1-G-0</td>
<td>Cislunar Top-Level Architecture and Operations Concept, Draft Informational Report, Issue 0</td>
<td>December 2006</td>
<td>Current draft</td>
</tr>
</tbody>
</table>
# CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  INTRODUCTION</td>
<td>1-1</td>
</tr>
<tr>
<td>1.1 PURPOSE</td>
<td>1-1</td>
</tr>
<tr>
<td>1.2 DEFINITIONS</td>
<td>1-1</td>
</tr>
<tr>
<td>1.3 RATIONALE</td>
<td>1-2</td>
</tr>
<tr>
<td>1.4 SCOPE</td>
<td>1-3</td>
</tr>
<tr>
<td>1.5 OVERVIEW</td>
<td>1-5</td>
</tr>
<tr>
<td>1.6 APPROACH</td>
<td>1-8</td>
</tr>
<tr>
<td>1.7 REFERENCES</td>
<td>1-8</td>
</tr>
<tr>
<td>2  MISSION CHARACTERISTICS AND ENVIRONMENTS</td>
<td>2-1</td>
</tr>
<tr>
<td>2.1 COMMUNICATIONS DELAY AND CONNECTIVITY</td>
<td>2-1</td>
</tr>
<tr>
<td>2.2 DATA TYPES</td>
<td>2-3</td>
</tr>
<tr>
<td>2.3 ENVIRONMENT</td>
<td>2-4</td>
</tr>
<tr>
<td>2.4 ENDPOINTS</td>
<td>2-5</td>
</tr>
<tr>
<td>Deleted: 2-6</td>
<td></td>
</tr>
<tr>
<td>3  COMMUNICATIONS REQUIREMENTS</td>
<td>3-1</td>
</tr>
<tr>
<td>3.1 GENERAL</td>
<td>3-1</td>
</tr>
<tr>
<td>3.2 FLEXIBILITY, SCALABILITY, AND INTEROPERABILITY</td>
<td>3-1</td>
</tr>
<tr>
<td>3.3 PHYSICAL AND DATA LINK REQUIREMENTS</td>
<td>3-2</td>
</tr>
<tr>
<td>3.4 NETWORK LAYER REQUIREMENTS</td>
<td>3-3</td>
</tr>
<tr>
<td>3.5 UPPER LAYER REQUIREMENTS</td>
<td>3-3</td>
</tr>
<tr>
<td>3.6 QUALITY OF SERVICE REQUIREMENTS</td>
<td>3-4</td>
</tr>
<tr>
<td>3.7 TIME DETERMINATION SERVICES</td>
<td>3-4</td>
</tr>
<tr>
<td>3.8 SECURITY</td>
<td>3-5</td>
</tr>
<tr>
<td>3.9 CONTINGENCY OPERATIONS</td>
<td>3-6</td>
</tr>
<tr>
<td>Deleted: 3-5</td>
<td></td>
</tr>
<tr>
<td>4  PROPOSED ARCHITECTURE</td>
<td>4-1</td>
</tr>
<tr>
<td>4.1 ARCHITECTURAL PRINCIPLES</td>
<td>4-1</td>
</tr>
<tr>
<td>4.2 MULTI-HOP, ROUTED, PACKET-SWITCHED COMMUNICATIONS</td>
<td>4-1</td>
</tr>
<tr>
<td>4.3 BASIC ARCHITECTURE</td>
<td>4-2</td>
</tr>
<tr>
<td>4.4 NETWORK LAYER</td>
<td>4-4</td>
</tr>
<tr>
<td>4.5 IP PACKET OVERHEAD</td>
<td>4-6</td>
</tr>
<tr>
<td>4.6 IPV4 / IPV6 INTEROPERABILITY</td>
<td>4-6</td>
</tr>
<tr>
<td>4.7 NETWORK ADDRESS TRANSLATION (NAT)</td>
<td>4-6</td>
</tr>
<tr>
<td>4.8 AUTOMATED DATA FORWARDING</td>
<td>4-7</td>
</tr>
<tr>
<td>4.9 QUALITY OF SERVICE</td>
<td>4-7</td>
</tr>
<tr>
<td>4.10 SECURITY</td>
<td>4-8</td>
</tr>
<tr>
<td>Deleted: 4-5</td>
<td></td>
</tr>
<tr>
<td>Deleted: 4-6</td>
<td></td>
</tr>
</tbody>
</table>
## CONTENTS (continued)

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.11 INTERFACES WITH LEGACY SYSTEMS</td>
<td>4-10</td>
</tr>
<tr>
<td>4.12 TRANSPORT LAYER</td>
<td>4-10</td>
</tr>
<tr>
<td>4.13 OVERLAY NETWORK SERVICES</td>
<td>4-13</td>
</tr>
<tr>
<td>4.14 REQUIREMENTS IMPOSED ON SUBNETWORKS</td>
<td>4-15</td>
</tr>
<tr>
<td>4.15 EMERGENCY COMMANDING</td>
<td>4-16</td>
</tr>
</tbody>
</table>

### 5 OPERATIONS CONCEPTS USING THE NEW ARCHITECTURE ............ 5-1

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 OVERVIEW</td>
<td>5-1</td>
</tr>
<tr>
<td>5.2 ROBOTIC SCENARIO</td>
<td>5-1</td>
</tr>
<tr>
<td>5.3 EXAMPLE APPLICATIONS OF CISLUNAR PROTOCOLS IN ROBOTIC ENVIRONMENT</td>
<td>5-3</td>
</tr>
<tr>
<td>5.4 STORE AND FORWARD TRANSMISSION</td>
<td>5-5</td>
</tr>
</tbody>
</table>

### 6 PHASED INTRODUCTION OF CAPABILITIES                      6-1

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 GENERAL</td>
<td>6-1</td>
</tr>
<tr>
<td>6.2 NON-ROUTING SPACECRAFT</td>
<td>6-1</td>
</tr>
<tr>
<td>6.3 SIMPLE RELAYS</td>
<td>6-1</td>
</tr>
<tr>
<td>6.4 IN-SPACE ROUTING</td>
<td>6-2</td>
</tr>
</tbody>
</table>

### 7 TRANSLUNAR ................................................................ 7-1

### ANNEX A REJECTED ELEMENTS ........................................... A-1
### ANNEX B ENDPOINTS ....................................................... B-1
### ANNEX C ACRONYMS ........................................................ C-1

### Figure

1-1 Earth-Local, Mars-Local, and Deep Space Communications .... 1-4
1-2 Scope of Cislunar Space for this Study, in Terms of Communications Delays (RTT) ... 1-5
1-3 Nominal Cislunar Communications Endpoints ...................... 1-6
1-4 Cislunar Data Paths .................................................. 1-7
4-1 Proposed Architecture and Services .............................. 4-3
4-2 Split-Connection PEPs Break TCP Connections into Three Parts | 4-12   |
4-3 An Overlay Network (Larger, Dark Circles) Sparsely Deployed in an Underlying Network (Smaller, White Circles) ........................... 4-13
4-4 End-To-End Network and Message-Based Store-and-Forward System ... 4-15
5-1 Real-Time Telemetry Transmission .................................. 5-3
5-2 Instrument/User Data Transmission with CFDP Acknowledged Mode ... 5-4

CCSDS 730.1-G-0  
Page vi  
December 2006
## CONTENTS (continued)

<table>
<thead>
<tr>
<th>Figure</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5-3</td>
<td>5-5</td>
</tr>
<tr>
<td>5-4</td>
<td>5-5</td>
</tr>
</tbody>
</table>

### Table

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-1</td>
<td>Approximate Round Trip Times for Communications Endpoints Relevant to Cislunar and Mars Communications</td>
<td>2-2</td>
</tr>
<tr>
<td>5-1</td>
<td>Spaceborne Assets of a Robotic Lunar Architecture</td>
<td>5-1</td>
</tr>
<tr>
<td>5-2</td>
<td>Earthbound Assets of a Robotic Lunar Architecture</td>
<td>5-2</td>
</tr>
</tbody>
</table>
1 INTRODUCTION

1.1 PURPOSE

This document presents a high-level architecture and operations concept for communicating with and among elements in the Earth-moon system (cislunar communications). Communicating elements include terrestrial endpoints such as development and test facilities, launch facilities, and scientists; orbiting endpoints in orbit around Earth or the moon, or in transit from one to the other, including astronauts executing extra-vehicular activities (EVAs); and landed elements on the surface of the moon. The architecture is intended to be reusable in any suitably low-delay environment, such as Low Earth Orbit (LEO) spacecraft, spacecraft in the vicinity of another planet, or among proximate groups of free-flying spacecraft regardless of location.

By standardizing on the architecture in this document and a set of protocols to be provided in subsequent documents, missions will hopefully be able to increase data return volumes while reducing mission operations costs. The increased data return will come from interoperability among many different spacecraft and the ability to use different combinations of spacecraft as relays to forward data to Earth. Reduced mission operations cost will come from automated configuration and management of the communications infrastructure and from the use of standard services that will reduce the amount of custom software needed for each new mission. By agreeing on and implementing a communications infrastructure based on the architecture in this document, common data handling functions can be implemented in standard and hopefully reusable software/hardware. Moving these capabilities into the infrastructure allows mission software to focus on mission-specific functions instead of ‘re-inventing the wheel’ with each mission when it comes to communications.

This document does not attempt to provide a detailed, protocol-level description of how to construct an entire cislunar communications system. A detailed description of the protocols used to populate the architecture described here will be left to subsequent recommendations.

1.2 DEFINITIONS

The protocol layer definitions used here are those of reference [2].

Earth-Moon Lagrangian point 2 (EML2)—An unstable Lagrangian point on the other side of the moon as viewed from Earth. A relay spacecraft in a halo orbit around this point could provide communications between Earth and items on the far side of the moon.

Quality of Service (QoS)—Providing different treatment to different data in order to control some characteristic, such as end-to-end delay, loss rate, or jitter.

Sun-Earth Lagrangian point 2 (SEL2)—An unstable Lagrangian point on the other side of Earth as viewed from the Sun.
Forwarding—The act of receiving a Network layer packet, determining to which next-hop recipient the packet should be transmitted, and transmitting the packet. Note that forwarding does not imply any type of autonomous routing decision; the act of determining a packet’s recipient may be controlled entirely via a management interface.

Dynamic Routing—Using an automated protocol to populate the forwarding tables at a set of nodes in the system.

A ‘small-I’ internet—A collection of networks, each of which may use different Data Link layer technologies, joined together by a common OSI layer-3 Network layer.

The ‘capital-I’ Internet—The worldwide IP-based network characterized by hosts with globally routable IPv4 or IPv6 addresses.

Round Trip Time (RTT)—The time it takes to send information to a destination and receive a signal back. Note that the RTT is lower-bounded by the round-trip light time between source and destination.

1.3 RATIONALE

In the 20th century, science and exploration spacecraft were built to communicate primarily with ground stations, with ‘commands’ flowing from ground control center to spacecraft, and ‘telemetry and data’ flowing from spacecraft to ground. There were few cases where a science spacecraft would communicate directly with another spacecraft or with multiple control centers on the ground.

Extensive planning, scheduling, and operational work had to be done to effect each communication session. These activities included scheduling antenna tracking time, tracking the spacecraft, tuning transmitters and receivers to proper frequencies, ensuring that network equipment was operational, and ensuring that data processing systems were ready. In addition, spacecraft usually had to be commanded to transmit their telemetry data; the process was not automatic once the spacecraft established communications with Earth. Communications volumes were carefully scoped during mission design to fit within spectrum and data rate allocations, and there was very little unplanned dynamicity in the traffic flow. If a particular instrument or data source did not need the full bandwidth it was allocated at a particular time, that bandwidth would often go unused.

This approach was successful and has supported many missions. However, in the 21st century, planning is underway for much more elaborate space missions that will involve orders-of-magnitude-more systems and communication links, and human crews. Many missions envision multiple nodes that communicate not only between space and ground but also among systems in space. Manually managing the connectivity and data transfers among this increasing number of systems will become more and more difficult. The situation is reminiscent of the early days of telephones and switchboards. When the number of systems was sufficiently small, human circuit switching with operators in the loop was possible. As the number of users grew, the phone system had to evolve to automated switching systems.
that were fully computer controlled and software upgradeable. The future cislunar communication architecture requires a similar shift from traditional circuit-switched space communication toward a more flexible network architecture for space communication.

The data requirements of humans are also quite different, and harder to regulate, than those of robotic instruments. While humans in space will probably always want to be able to talk to a mission control center, there will be long periods of time when they will not have anything to say. If a voice circuit were permanently established to support the relatively few times when someone wanted to talk, it would result in a considerable waste of spectrum at a time when space agencies around the world are being pressured to return spectrum to the commercial sector.

This document presents an architecture for interoperable communications that can support the number of missions and types of missions that are likely on and around the moon in the coming decades. The architecture is 1) Flexible: able to respond to dynamic changes in connectivity and traffic loading, new applications, and evolution of Data Link layer; 2) Scalable: able to support a wide range in the number of end systems efficiently; and 3) Interoperable: able to provide relatively easy interoperability between different deployed systems and between deployed systems and terrestrial endpoints.

1.4 SCOPE

The scope of this study encompasses an internetworking communications architecture in the cislunar mission domain. It does not prescribe a communications architecture in general, such as relay satellite configurations. However, it makes assumptions about the possible range of options for broader communications architecture configurations, so that the internetworking functions will serve the range of missions (human crewed, robotic, etc.) over the range of communications topologies (with relays, without relays, etc.) that could be part of the mission environment in cislunar space.

A major boundary of the cislunar mission domain is described in terms of communications delays. The architecture is designed to function in the presence of RTTs that might include communications paths of LEO missions with hundreds of milliseconds of delay, through lunar missions, such as relay through geosynchronous satellites, lunar orbiting satellites, and satellites in the vicinity of EML2. These geometries result in delays of 3 to 4 seconds RTT. Deeper space missions are at SEL2 with RTTs in the neighborhood of 10 seconds. Beyond that, the next expected mission set includes interplanetary missions with delays on the order of 4 to 40 minutes. For the purposes of this study it was determined that communications features (protocols, etc.) that function for lunar distances would likely function equally well for SEL2 missions with 10 seconds RTT, but possibly not for the interplanetary distances. Thus the boundary of RTTs for this study is set at 10 seconds to accommodate missions in cislunar space or at SEL2 distances. The rationale for the 10 second RTT boundary is simply to line up with the anticipated technology threshold between the ‘somewhat near Earth’ mission set and the interplanetary mission set.
Wherever possible, the concepts contained in this document should work equally well in any system with round-trip light times that are roughly equivalent to the Earth-moon system. Thus the concepts presented here should hold for the immediate ‘local’ vicinity of most planetary bodies in the Solar System, and in particular should hold for communications between Mars orbit and the planet’s surface.

Figure 1-1 illustrates the basic areas where the communications architecture is intended to function along with both ‘Deep Space’ and ‘Environment-Local’ areas that may employ custom communications tailored to the environment. Figure 1-2 illustrates the boundaries the architecture described in this document is intended to address in terms of communications delays for both the Earth and Mars planetary systems.

Figure 1-1: Earth-Local, Mars-Local, and Deep Space Communications
Figure 1-2: Scope of Cislunar Space for this Study, in Terms of Communications Delays (RTT)

It is also hoped that many of the capabilities developed for cislunar space will work for longer interplanetary missions, including translunar missions’ needs such as Earth-to-Mars communications. When there is a requirement that is different for an Earth-to-Mars mission, or an architectural feature that does not support cis-Martian communications, this document will point it out with a parenthetical note.

This document addresses end-to-end communications assuming an underlying infrastructure of data links. That is, the architecture presented here addresses mainly OSI layers 3 and 4. Higher-layer communications services such as publish-and-subscribe data models that can be constructed from the services described here are not considered.

1.5 OVERVIEW

This document assumes a mission architecture based on current technology (e.g., launch systems, crewed/robotic vehicles, communications relays, etc.). It also assumes the limitations of those technologies, such as incomplete coverage, speed-of-light delays and occasional equipment failures.

This document presents a communications architecture to support reliable, robust, and multi-hop communications among elements. The architecture is designed to take advantage of link heterogeneity, allowing different data link technologies to be tailored to specific environments. Thus data links designed for long-delay deep-space communications (e.g., CCSDS AOS) can be used between an Earth station and a lunar base, while data links...
designed for low-delay wireless communication (e.g., 802.11 or 802.16) can be used for local communications. This architecture provides:

- spanning multiple heterogeneous data links via a common Network layer protocol;
- end-to-end communications across multiple hops;
- easy integration with existing ground networks;
- efficient use of communications resources can be provided.

Figure 1-3 depicts the kinds of communications the architecture has been designed to support.

![Diagram of Cislunar Communications Endpoints]

Figure 1-3: Nominal Cislunar Communications Endpoints

Figure 1-4 depicts the communications paths that are expected to be encountered based on usage of current or anticipated systems. Some important overall characteristics of these missions and this communications architecture are:

- Many communications routes will be multi-hop, across several stations and relays.
- There are many endpoints (terrestrial, in-space, and lunar) and as components navigate cislunar space and the lunar surface, their location and their connectivity may not always be predictable.
- Even though contact may not be predictable, when an element is in range of a communications signal, the network must be capable of being rapidly reconfigured to support the contact.
- The network is complex, and configuration of such a network either will be automated or, if manual, may involve considerable human intervention.
Figure 1-4: Cislunar Data Paths

Notes of explanation for figure 1-4:

1. Session data from other ground facilities / other networks may or may not be required to go through the Mission Control Center (MCC) as a ‘gateway’ to the ground station. This architecture must support both options.

2. Earth-orbiting tracking and data relay satellites can communicate at lunar distances at very low data rates (~5Kbps) by looking past the limb of Earth and may be considered for backup support.

3. The primary communications path, as a vehicle transitions from LEO to lunar orbit is assumed to transition from Earth-orbiting relay satellites to direct-from-Earth communications via ground-based antennas.

4. For landed lunar assets, the primary communications path is either direct-from-Earth via terrestrial-based antennas or via one or more lunar communications relays.

5. A permanent lunar station may or may not be a communications hub for local communications. That is, communications with roving lunar units (rovers, astronauts) may be direct, via orbiting relays, or through a permanent base. This architecture must support all of these options.

6. ‘Other ground facilities’ may include test and integration facilities, science facilities, and public outreach facilities, among others.
Both Earth-orbiting communications relay satellites and lunar communications relay satellites in this illustration are represented as simple one-step hops, but in actuality, the network must support multiple satellite relays and/or constellations of satellite relays with multiple hops through the system before the destination.

Many of the communications paths in the figure may be disrupted. That is, there may be times when a contemporaneous end-to-end path does not exist between source and destination.

1.6 APPROACH

This document presents requirements for the expected set of cislunar missions, an overall architecture for cislunar communication based on the Internet suite of protocols, and the rationale for choosing this particular architecture over others. Future CCSDS recommendations will present additional information about protocols, configurations, and options to detail how this architecture should be implemented in an interoperable fashion.

Because of the nature of space communications, moving directly from the current link-centric model to a network-centric model with multiple spacecraft would be extremely difficult. We thus present a series of phases, starting with the addition of a Network layer protocol but without spacecraft-to-spacecraft routing. That is, the first phase allows for networked communication with spacecraft but not routing through spacecraft. The second phase addresses pairs or groups of spacecraft with simple routing capabilities. Such spacecraft are assumed to have been designed as a unit so that any routing requirements, such as which spacecraft will communicate with Earth and which spacecraft will not, is known. The last phase addresses the more general case where spacecraft not necessarily designed to work together may use each other as Network layer relays to reach other destinations.

1.7 REFERENCES

The following documents are referenced in the text of this Report. At the time of publication, the editions indicated were valid. All documents are subject to revision, and users of this Report are encouraged to investigate the possibility of applying the most recent editions of the documents indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS Recommendations.


2 MISSION CHARACTERISTICS AND ENVIRONMENTS

2.1 COMMUNICATIONS DELAY AND CONNECTIVITY

Communications distances for cislunar missions will vary from LEO distances to Lagrangian distances.

Addressing the effect of time delays (versus disruptions such as Loss Of Signal (LOS) mission segments):

- for LEO missions, the data rates and RTTs between Earth and spacecraft are such that most terrestrial network protocols can cope with the associated bandwidth-delay product;

- at lunar or SEL2 distances, the 2.5–10-second RTTs reduce the effectiveness of some terrestrial protocols. For example, protocols like TCP that use closed loop control will usually not function well with RTTs exceeding five seconds.

Table 2-1 illustrates the RTTs for endpoints relevant to cislunar and Mars communications for various potential cislunar mission segments. The intent is to show the various options for cislunar and other missions associated with Lagrangian points for which this architecture works, and mission segments beyond the domain for this document.
Table 2-1: Approximate Round Trip Times for Communications Endpoints Relevant to Cislunar and Mars Communications

<table>
<thead>
<tr>
<th>RTT</th>
<th>Endpoints</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;0.1 s</td>
<td>Interaction between rovers, landers, etc. (e.g., local planetary surface environment)</td>
</tr>
<tr>
<td>0.1 sec</td>
<td>Earth surface to LEO (a few hundred kilometers one-way)</td>
</tr>
<tr>
<td>0.1 sec</td>
<td>Lunar surface to low-lunar orbit (a few hundred kilometers one-way)</td>
</tr>
<tr>
<td>0.1 sec</td>
<td>Martian surface to low-Mars orbit (a few hundred kilometers one-way)</td>
</tr>
<tr>
<td>0.5 sec</td>
<td>Earth surface to LEO via geosynchronous orbit (72,000 kilometers one-way)</td>
</tr>
<tr>
<td>0.1-2.5 sec</td>
<td>Earth surface to lunar transfer orbit (varies: 200,000-384,000 km one-way)</td>
</tr>
<tr>
<td>2.5 sec</td>
<td>Earth to lunar surface direct (384,000 kilometers one-way)</td>
</tr>
<tr>
<td>3.8 sec</td>
<td>Earth to lunar surface via relay at the EML2 point (570,000 km one-way)</td>
</tr>
<tr>
<td>10.0 sec</td>
<td>Earth surface to missions at SEL2 point (1,500,000 kilometers one-way)</td>
</tr>
</tbody>
</table>

*Limit of cislunar communications domain*

<table>
<thead>
<tr>
<th>6 min</th>
<th>Earth to Mars (closest = 55,000,000 kilometers one-way, 6 minute, RTT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>45 min</td>
<td>Earth to Mars (farthest = 401,000,000 kilometers one-way, 45 minute RTT)</td>
</tr>
</tbody>
</table>

Addressing the effect of connectivity disruptions such as LOS phases:

- For LEO missions, disruptions can be predicted from experience with existing relay satellite configurations, vehicle structure blockages, and other factors that occur in current missions.

- At lunar or SEL2 distances, but not in lunar orbit or lunar surface locations, disruptions are expected to be reduced (compared to LEO) because of the more continuous line-of-sight connectivity provided by Earth-based communications stations. Disruptions due to scheduling of spacecraft and/or terrestrial antennas may still be present.

- For lunar orbit or lunar surface locations, communications disruptions will be more frequent and the characteristics are difficult to project. They will vary with the communications architecture that is ultimately provided in terms of relay satellites, ground station locations, design characteristics of vehicles, and lunar topology at lunar landing sites that have not yet been selected. This communications architecture must support the worst case of no relay satellites (long disruptions for lunar orbiters or far-side stations) and the best case of complete relay satellite coverage, in either slow-moving or fast-moving constellations. It must also support the intermediate cases of partial relay satellite coverage.
Cislunar missions will need to address these communications outages and disruptions. Current missions often store data until a communications session can be established to transmit the data to either a relay spacecraft or to Earth. A cislunar example of this is a lunar mapping satellite that must store images while on the far side of the moon and transmit them when Earth is in view.

Even with relays, it is likely that there will still be periods where there is no end-to-end path between data source and destination. While crewed missions may be able to invest in infrastructure to support continuous communications, robotic missions to the far side of the moon might not be able to justify that level of infrastructure investment. Local communications to and among elements on the surface of the moon may also not be able to maintain 100% connectivity because of shadowing and multipath effects.

To address the full range of possible delay and disruption characteristics for cislunar communications, the cislunar architecture must be able to tolerate delays of up to 10 seconds and disruptions that are not known in advance.

2.2 DATA TYPES

While mission characteristics drive the data types that must flow through the communications architecture, it is not feasible to project new data types that will emerge as lunar exploration programs evolve. The set of data types that will need to be supported will include, as a minimum, the data types that are typical of current advanced orbital systems such as the International Space Station. However, it is anticipated that new data types will also be needed as 21st century humans move into cislunar space expecting to take with them the Internet-based tools with which they are familiar. In general, these new data types will be supported by the public communications architecture on Earth, and compatible protocols and architecture characteristics will be needed in the cislunar environment.

The architecture capabilities should not preclude the delivery of any data types to any location. Even though today’s mission characteristics may not require a certain data type for a given mission, future cislunar missions may evolve to require it. For example, one would initially expect that no voice data type is needed on unmanned vehicles. Later, human voice control of robotic rovers may be needed between lunar crew and a rover, and MCC operators may need a downlink of the voice commands from the rover for troubleshooting.

The following data types are considered to apply to all types of spacecraft systems (core systems, science payloads, manned and unmanned systems, etc.). Also, most data types are expected to exist in both real-time and playback forms.

- command, including program uploads;
- telemetry;
- digital voice and video (including HDTV);
- multi-party videoconference data.
mission planning and scheduling data;
- file transfer of all types of computer files (binary, executable, database, etc.);
- data quality messages (communications link quality messages);
- data for remote control and monitoring of ground systems;
- crew family and private communications (email, text chat, videoconference, biomedical data);
- hailing/neighbor discovery;
- time synchronization and distribution;
- crew and robotic access to Internet and WWW services.

2.3 **ENVIRONMENT**

This environment description explains the external forces that must be dealt with by the architecture.

**NETWORK ENVIRONMENT**

- Terrestrial links between major control facilities will be primarily on interagency or intra-agency private networks. Other terrestrial links will make maximum usage of public networks, using secure encapsulation technologies to protect critical control functions or sensitive data. The architecture must not preclude and should easily accommodate use of common commercial services (Internet, Frame Relay, etc.) and anticipated emerging commercial technologies (WiMax, etc.).

- Space-to-ground links need to be able to use orbital relay satellites when they are available. The architecture must efficiently enable communications across multiple hops between nodes, accommodating anticipated dynamic changes in the topology of the connections between nodes, whether the nodes are on orbiting spacecraft, planetary bodies, or moons.

**GEOPOLITICAL ENVIRONMENT**

- International operations will drive the need for common tools that can be used at multiple control centers and other types of ground facilities. Components of the networking architecture are usually inherently end-to-end, and those components must not use technologies which cannot be used between different agencies.

- The architecture must enable the cross-support operation of control facilities in various countries, each using a different Mission Control System (MCS) while sharing their tools and data between facilities.
COMMUNICATIONS SYSTEMS PHYSICAL ENVIRONMENT AND TOPOLOGY

- The various data links in the system may be heterogeneous, ranging from high-bandwidth, low-latency links in control centers and between tethered launch vehicles and control centers, to long-haul space links to medium and short-range wireless links. The various links will exhibit a wide range of speeds and reliabilities.

- Remote teams for special operations may be deployed to isolated locations with sparse communications. Such teams, performing functions such as water landing support or disaster recovery, will need access to real-time and historical operations data from control facilities.

- The connectivity between elements may change over time and the routing of data will need to respond to those changes.

- There will be times when there is no end-to-end connectivity between elements (e.g., reentry blackout, far-side-of-the-moon rover with no relay asset visible).

COMPUTING ENVIRONMENT

- For ground systems, services and protocols must function in widely available computing platforms and operating systems.

- For onboard systems, services and protocols must function in currently available avionics platforms, and also those anticipated in the near future.

COST CONSTRAINED ENVIRONMENT

- Cost constraints will require maximum usage of automation, with minimal manual intervention for any function that can be automated. Example: Manual configuration of networks for multi-hop communications should be minimized in favor of automated configuration as much as technology permits. This is particularly critical for multi-decade missions and campaigns where manually configured systems will have long-term cost implications.

2.4 ENDPOINTS

The communications architecture is bounded by the endpoints serviced by the communications systems. For readability, this section includes only a high-level list compatible with figure 1-2. A more comprehensive list of endpoints is presented in annex B, and they provide a deeper insight into the complexity of communications of cislunar missions.

- Terrestrial users on the global networks—Includes remote science users in universities, commercial payload control facilities, normal flight control operations, displaced flight controllers performing contingency operations, and a very wide range of other user types scattered around the globe. Some of these users are performing command and control, while others, like the general public, are monitoring only.
- Mission control facilities—Mission control centers, payload operations centers, and other centers that act as hubs for mission operations. These facilities may or may not be the entry point for all data to and from spacecraft, depending on mission and program requirements.

- Earth orbiting tracking and relay ground stations that communicate through Earth-orbiting relay satellites.

- Earth communications stations—Ground stations that communicate directly with spacecraft or other spaceborne facilities.

- Earth ascent/descent vehicles—Launch vehicles and their payloads during the transition phase from atmospheric to orbital flight and vice-versa. This also includes terrestrial Earth communications stations.

- Earth orbiting vehicles—Vehicles in Earth orbit, generally up to geosynchronous orbit.

- Earth orbiting communications and tracking satellites—Data relay and tracking satellites that are communications ‘hops’ for both Earth orbiting vehicles and vehicles in transit to lunar trajectories. These vehicles are endpoints for some communications management data types.

- Transit/Lagrangian vehicles—Vehicles between Earth geosynchronous orbit and lunar orbit. These include earthbound and moonbound vehicles, as well as vehicles at Lagrangian points such as communications relay satellites, fuel depots, or other components of lunar mission support.

- Lunar communications and tracking relay satellites—Data relay and tracking satellites in lunar orbit that are communications ‘hops’ for both lunar orbiting vehicles and possibly for vehicles in transit between the Earth and the moon. These vehicles are endpoints for some communications management data types.

- Lunar orbiting vehicles.

- Lunar ascent/descent vehicles.

- Lunar surface endpoints—Includes multiple endpoints at a lunar outpost, lunar crew on EVA, robotic lunar rovers, robotic lunar stations, deployed science payloads, deployed lunar surface communications relay stations, and other TBD elements.
3 COMMUNICATIONS REQUIREMENTS

3.1 GENERAL

The following subsections discuss requirements on the cislunar architecture in a layered manner. The discussion starts with a description of the high-level goals of interoperability, flexibility, and scalability of the network. The next subsection discusses features the Physical and Data Link layers need to support in order to service the envisioned set of data types. The next subsection discusses requirements of the Network layer, OSI layer 3, which provides the key functionality in modern large-scale networks. Following subsections discuss the requirements for upper layer protocols to provide a suite of services with different characteristics implemented over the Network layer. Finally, the last subsection discusses security issues that must also be addressed as the network grows.

3.2 FLEXIBILITY, SCALABILITY, AND INTEROPERABILITY

3.2.1 FLEXIBILITY

Voice, video, and data in the form of at least file transfers, electronic mail, and possibly instant messaging will be applications that need to be supported for crewed missions. Each of these has different requirements for service in terms of latency, jitter, and correctness of the data. In addition, any number of applications, with yet different service requirements, may be developed over the next few decades.

Historically, space communications systems have carefully managed data volumes and data paths, sometimes tying particular applications to specific physical resources. This tight coupling of applications to physical communications makes it difficult to add new applications or new types of physical connectivity, and can make it difficult for multiple applications to share physical resources efficiently.

The above argues for an isolation function separating applications from the underlying communications resources. Ideally, this isolation function should provide a powerful upper-layer (service) interface to applications, efficient multiplexing of multiple applications onto multiple physical resources, and the ability to arbitrate among competing application demands. To function in the full range of envisioned communications environments, the isolation layer needs to be able to provide at least some level of service over unidirectional data links, function across a wide range of delays, and accommodate situations where end-to-end connectivity is not always present.

3.2.2 SCALABILITY

If one were to attempt to engineer custom interfaces between each pair of communicating elements, and then to manage multi-hop data flows through the resulting infrastructure, the complexity would grow at least as the square of the number of elements. This would quickly
become unmanageable after just a few elements. Thus for efficiency the system needs to be scalable with the number of interfaces. Similar reasoning suggest that the system should be scalable with the total number of endpoints and applications as well, since future lunar bases might contain local area networks with tens or hundreds of computers, each running multiple applications.

### 3.2.3 INTEROPERABILITY

The main benefits of interoperability are to reduce complexity, to increase software and hardware reuse, to increase reliability, and to enable inter-provider and interagency cross support. By implementing one common standard for network data communications, that standard can be codified in flight hardware and software and will hopefully become a commodity item for future mission developers. This will reduce cost by shortening mission development time, and should also increase reliability as the standard mechanisms will experience constant testing and improvement. The scalability arguments above militate for a single interoperability standard.

In summary, the basic communication requirements for a cislunar communications system are:

- ability to support a wide range of applications with different requirements, including voice, video, and data;
- ability to operate effectively over a range of link and end-to-end delays;
- ability to function in the presence of simplex, half-duplex, and full-duplex links and data paths;
- support for interoperability between agencies;
- ability to support configurations from a few end systems to hundreds or thousands of end systems efficiently;
- a single interoperability standard.

### 3.3 PHYSICAL AND DATA LINK REQUIREMENTS

Even with an automated, routed network service for data transmission, spacecraft scheduling and physical link availability will dictate when communications are possible. Thus communications may be constrained by spacecraft pointing to carry out science experiments, by availability of terrestrial antennas, and by power/thermal considerations. Different environments will also favor different Data Link layers. For example, terrestrial LAN connections will likely use Ethernet, while space links will possibly include some form of space data link service.
3.4 NETWORK LAYER REQUIREMENTS

The Network layer needs to provide a common way to address data to each element of the cislunar network. In fitting with the overall requirements, the Network layer must also be able to function in simplex, half-duplex, and full-duplex environments. The network function should also be flexible and extensible in that it will need to support a number of different applications, including applications that are currently unknown.

3.5 UPPER LAYER REQUIREMENTS

3.5.1 GENERAL

A cislunar network that supports end-to-end addressing of packets across a variety of space and ground links provides the basic packet delivery network that can be used to support the end systems and traffic types described in section 2. While all nodes need to use a common Network layer to provide a large, scalable network, the Transport and Application layer protocols only need to be coordinated between end systems.

3.5.2 SPACE TRANSPORT LAYER REQUIREMENTS

The cislunar Transport layer(s) need to support both ‘unreliable’ and ‘reliable’ data transport. Applications that do not require reliability often function better without the added latency that reliability introduces. For applications that require reliable communications, it is often better if that reliability is implemented in a common way that can be shared by all of the applications rather than having the reliability function replicated in each application. Both reliable and unreliable transport layer(s) need to provide mechanisms for multiplexing multiple Application layer data streams.

The ‘unreliable’ transport protocol(s) should provide an unreliable data delivery service without any guarantee of orderliness, completeness, timeliness, duplication, flow control, or congestion control. These protocols would provide a service somewhat similar to traditional space communication using TDM and CCSDS Space Packets (reference [4]). Because they do not require feedback from the receiver, unreliable transport protocols can operate over simplex, half-duplex, and duplex links, and can work independently of any propagation delays. Unreliable services are also free to deliver data as it comes in without waiting to fill ‘holes’ in the data stream. This allows them to be more responsive in errored environments. The unreliable transport protocol(s) should also support an end-to-end mechanism to detect data corruption.

Transport layer error detection may seem like extra overhead if the various data links in the path also support ‘per-hop’ error detection, but it is prudent to provide the error detection at both layers. Data Link layer error detection can quickly identify link-layer frames that are bad and prevent the Network layer from using communications resources from relaying what is essentially bad data. However, it may be that not all data links in a path provide sufficiently strong error detection, in which case Transport layer error detection is the only

Deleted: The main requirements on the cislunar architecture are thus:

Deleted: The ability to function in the presence of intermittent (though possibly scheduled) connectivity;

Formatted: Bullets and Numbering
Deleted: The ability to function over a set of possibly heterogeneous data links;

Deleted: wide range of layers
Deleted: capabilities similar to UDP and TCP, respectively, on the Internet
Deleted: The terms "unreliable" and "reliable" refer to whether the network service simply attempts to deliver packets without error detection and retransmission, or provides mechanisms for detecting missing data and retransmitting packets as necessary to provide guaranteed complete delivery. Other functions may include capabilities for multiplexing multiple data streams, flow control, and a standard or de facto standard application programming interface.

Deleted: protocols
Deleted: [4]
Deleted: to detect missing data
Deleted: protocols
Deleted: provide
Deleted: for multiplexing multiple data streams to one or more remote hosts and also
Deleted: optional
guardian against delivering corrupted data to applications. Transport layer error detection also protects against errors that might be introduced while packets are being manipulated within intermediate routers, errors that are not protected by Data Link layer error detection.

The ‘reliable’ transport protocol(s) should ensure complete delivery to the destination application of all data sent, in the order it was submitted to the sending transport agent and without duplicates. If the ‘reliable’ mechanism provides for a service that may deliver incomplete data, ‘holes’ in the received data must be signaled to the receiving application. These protocols may also include mechanisms for adjusting the rate of data transmission to provide flow control and congestion control.

Any ‘reliable’ options that require feedback and interaction between the sender and receiver can only be supported when a duplex path exists between the sender and receiver. This interaction also means that the protocol performance may be impacted by longer propagation delays that interfere with the protocol’s feedback loop.

In summary, the basic Transport layer requirements for cislunar networking are:

– support both reliable and unreliable transport protocols;
– support multiplexing of multiple Application Layer data flows;
– provide end-to-end error detection;

3.6 QUALITY OF SERVICE REQUIREMENTS

The cislunar architecture needs to provide mechanisms to differentiate between, and to provide different levels of service to, different types of data. The QoS mechanisms should at least provide for relative treatment of different data classes, including a very high reliability mechanism to handle critical traffic.

There is a strong desire from the mission operations community to have some level of data accountability, to be able to determine, for instance, whether data is actually being transmitted, and even into which Data Link layer frame a particular piece of information is placed. To the extent possible, the cislunar architecture will need to address this desire.

3.7 TIME DETERMINATION SERVICES

Time protocols must allow periodic ability to determine the relative differences between clocks located in different systems that may be many light seconds apart in the Cislunar regime, or several light minutes apart for cis-Martian operations. The level of precision provided needs to be on the order of hundreds of milliseconds. Such precision is suitable for overall scheduling of spacecraft operations, including network configuration and loose synchronization of cryptography, but may not be precise enough to support navigational services. If precise time information is available from navigational sources, it can be used to assist in time determination.
Determining the relative difference between clocks does not necessarily imply synchronizing one clock with another. The goal of the time determination service is to determine accurately the difference (offset) between two or more clocks. Separate mechanisms may be used to synchronize two or more clocks.

3.8 SECURITY

Cislunar missions will include a mix of robotic and crewed missions with varying security requirements. Traditional space science and some crewed missions have been able to rely on the sheer difficulty of physical communications to deter intruders. Future missions will need to be more interoperable, communicating among space assets and with more elements on the ground. Heterogeneous data types will require different security measures for different data types during the same mission. For example, while science data may have limited security requirements, authentication of spacecraft and instrument command and control traffic may be required, and astronaut personal data will likely require confidentiality/privacy. Some science data may be proprietary for initial analysis by the principal scientist and may therefore also require confidentiality. These services will have to work under the delay and connectivity requirements described above as well as among/between international partners.

The International Space Station program developed the capability for science users to exercise command and control over their payloads from remote locations at universities, commercial locations, and other facilities far removed from centralized mission control centers. This trend is expected to continue, as even greater capabilities of public infrastructure are realized. Therefore, security measures must be capable of establishing end-to-end security across these commercial network implementations.

The Application of CCSDS Protocols to Secure Systems (reference [5]) describes various security mechanisms and how they can be applied to missions. Other CCSDS works in progress describe security threats against various representative classes of space missions. These documents provide valuable material on which security requirements and services can be based as well as how/where they can be applied.

Authentication may be accomplished via either a Message Authentication Code (MAC) or a digital signature. The MAC is created by the use of a keyed hash. That is, a hash algorithm such as SHA-1 is taken over the data to be authenticated plus a shared secret known only to the communicating entities. The digital signature is also created through the use of a hash over the data but the hash is then encrypted using the initiator’s private key. Digital signatures imply the use of public key encryption technology whereas MACs do not.

Confidentiality or privacy may be accomplished by the use of encryption. As is shown in the above-mentioned CCSDS 350.0-G-2, encryption may be applied at various layers or at multiple layers if so desired. When applied at lower layers of the OSI model, more of the packet is hidden. For example, if encryption is applied between the Network and Transport layers, all of the Transport layer and above are made opaque. However, the use of encryption at the Network layer requires access to the protocol suite, which may be a problem in some
cases. Therefore, applications may apply their own confidentiality by encrypting the payload data, leaving all of the lower-layer protocol headers in the clear. In this case the application developer takes on the responsibility for ensuring that the encryption service has been implemented correctly. Either public key, symmetric key, or a combination of both may be utilized.

### 3.9 CONTINGENCY OPERATIONS

Portability of Operations—When a major control facility goes down, the system must accommodate transfer of control to a backup location. This means that control functions that were securely restricted to one location can be quickly reprogrammed to be provided from a new location, whether a ground terminal, a hotel room, or another non-standard site. In the more general case, this scenario may apply to any facility, including less critical payload or user facilities.

Communications services must allow for contingency operations features, such as commanding in the blind (commanding over a simplex path), and commanding in emergency situations such as a tumbling spacecraft.
4 PROPOSED ARCHITECTURE

4.1 ARCHITECTURAL PRINCIPLES

Given the above discussion of the scope, goals, and motivation, a set of principles to guide the design of the cislunar architecture can be presented.

- Existing protocols and standards should be reused where possible; they should be adapted when necessary to fit the environment; new protocols and standards should be invented as a last resort.

- The cislunar environment encompasses elements that are five light seconds apart or less. This does NOT necessarily imply bi-directional connectivity or continuous connectivity between elements.

- The cislunar architecture should apply relatively unchanged to any comparable environment, regardless of location (e.g., around another planet).

- Interoperability with existing terrestrial equipment and standards will help reduce costs (design / development / testing / integration / operations).

- Multi-hop communications should rely on layer-3 (Network) services. Services specific to particular data links cannot necessarily be counted on end-to-end.

- All endpoints need to be individually addressable.

- Local optimizations should be used in regions where they make sense, and end-to-end communications should be built by gatewaying between regions.

- The cislunar architecture should be flexible enough to support a wide range of current and future applications.

- The path and/or bandwidth between any two endpoints may be dynamically varying and shared with other data flows. Carefully tuning each application’s output to avoid congestion loss is not a scalable solution.

- The architecture will need to support different qualities / classes of service.

- The architecture will need to support confidentiality and authentication. These services need to address interagency and international data paths.

4.2 MULTI-HOP, ROUTED, PACKET-SWITCHED COMMUNICATIONS

A multi-hop, routed, packet-switched communications infrastructure can efficiently support the communications requirements of the previous section. This section briefly describes the terms multi-hop, routed, and packet-switched as they are used here, and then describes an architecture based on the Internet Protocol (IP—reference [6]) as a common end-to-end Network layer packet. In the context of the above discussion, IP provides the "isolation
function’ between applications and physical communications resources, and is capable of supporting a wide array of traffic types with varying requirements.

This section is not meant to provide a complete protocol-level solution, but only to present the high-level concepts of an IP-based architecture. A complete, protocol-level set of specifications is left to later documents. For some important concepts such as security, QoS, and emergency commanding, this section provides brief overviews of approaches supported by IP, the details of which will be formalized in later documents.

Annex A contains a list of rejected architectures and a short rationale for why each was discarded in favor of the IP-based architecture described here.

**Multi-Hop:** Communications paths will typically be several ‘hops’ long, allowing different data links to be used in different environments. For instance, a typical data path might use Ethernet and SONET on Earth, space link protocols between Earth and the moon, and Ethernet (wired or wireless) inside a lunar base.

**Packet-Switched:** Packet-switched communications allow for efficient multiplexing of many data sources onto a particular Physical layer link. Each application’s data is broken into a series of packets containing information about the destination, and these packets are individually switched onto the various links in the end-to-end path. Packet switching based on individual packet addresses allows a data source to send data to many different destinations without having to worry about the mechanics of how the data will get there. Efficient use of communications resources will be important in the cislunar environment because of spectrum restrictions mentioned above.

**Routed:** In a routed network, each node along the path makes its own decision regarding which outgoing link the data should take. In a packet-switched network, this routing is generally done on a per-packet basis. Ensuring that there are multiple paths to a particular destination from a given node generally increases the robustness of flows to that destination; if one path fails, the intermediate node can route subsequent packets along another, working path. Routing allows intelligent decisions about resource (bandwidth) use to be made inside the network. For example, a human on the moon might want to use a lunar relay satellite to send data both to a lunar base and to Earth. If the satellite is capable of routing the data, the human can send two data streams to the satellite and they will be split apart there, with only the stream destined for Earth consuming the relay-to-Earth channel capacity.

### 4.3 BASIC ARCHITECTURE

The basic architecture is illustrated in figure 4-1. The rationale for standardizing a networked architecture rather than simply standardizing a set of Data Link layers is that inclusion of a Network layer provides additional services that greatly reduce the complexity of the overall system with very little overhead. Without a Network layer, applications themselves would be responsible for any global naming and addressing, for example. This means that an application would only be able to address peer applications sitting on the same layer-2 (Data
Link) segment. Using this method, multi-hop data transfers would have to be managed hop-by-hop by the applications themselves. This is the method employed by the Mars Exploration Rovers when transmitting data via the orbiters. The rover-to-orbiter links use the CCSDS Proximity-1 protocol (reference [7]), while the long-haul links to Earth use CCSDS TM/TC (references [8] and [9]). Special forwarding software on the orbiters is responsible for accepting telemetry from the rovers and forwarding that data to Earth.

IP provides standardized global addressing, along with multi-hop packet forwarding and routing capabilities, plus the ability to use QoS markings to prioritize data. These functions allow applications to focus on the data they want to send without having to worry about the details of each transmission of the data across multiple hops; destinations that may be multiple hops away are as easily accessible as those that are link-local. Standard Transport layer protocols such as TCP, SCPS-TP, and SCTP provide reliable stream and datagram services with congestion control, relieving applications from having to implement these features. The result is that an application using a reliable Transport layer need only worry about its Application layer data; reliability, duplicate suppression, and the mechanics of moving data to and from the peer application anywhere on the network, are all handled transparently to the application.

IP has been implemented over a number of different data links, and requires very little in terms of Data Link layer services. Subsection 4.14 discusses implementation guidelines for subnetwork designers who wish to support IP traffic.

**Figure 4-1: Proposed Architecture and Services**

While this architecture envisions providing direct access by applications to Data Link layer services, it does not propose to standardize services based on such access. The rationale for this is that each of the data links in a given path may be different, and may provide different...
services such that a given service available on one link may not be achievable end-to-end. CCSDS AOS (reference [3]), for example, provides an isochronous data insert service that is well suited to carrying a low-rate voice channel in addition to packetized data; IEEE 802.3 (Ethernet) does not support isochronous traffic, whereas IEEE 1394 supports both isochronous and asynchronous traffic.

It is important to note that applications that want direct access to Data Link layer services are still free to use them. There may well be advantages to direct Data Link layer communications between a high-speed instrument and a data recorder, for example. A data recorder might receive and package data, then forward it to the ground at a later date. In this case the data recorder is acting as an Application layer peer to the instrument, buffering data before sending it on.

4.4 NETWORK LAYER

4.4.1 IP NETWORK PACKET FORMAT

The communications systems of most current scientific space missions use the CCSDS Space Packet as the common Network layer encapsulation format, which has greatly simplified operations since its introduction in missions in the 1980s. While CCSDS Space Packets could be used as the basis of a multi-hop routed approach, there are some disadvantages. These include the lack of both source and destination addresses in the packets, lack of a suitable QoS field in the packets, lack of a developed multi-hop routing protocol, and lack of wide-scale terrestrial support for forwarding CCSDS Space Packets. While these drawbacks argue for a more capable networking layer, experience with using CCSDS Space Packets vs. custom-built telemetry formats argues for maintaining a common Network layer packet format for simplicity, interoperability, and economies of scale in software/hardware development.

There are currently two widely deployed versions of IP (IPv4 and IPv6). The main differences between the two lie in the number of end systems they can address, and whether support for services like autoconfiguration, security, and mobility are mandatory or optional. The rate at which IPv6 will replace IPv4 in operational networks is not clear at this time. Fortunately, systems can opt for a mix of IPv6 and IPv4, and there are a number of other solutions, including tunneling each protocol across the other and/or gateways between the two. Both IPv4 and IPv6 support hop-by-hop (Data Link layer) header compression mechanisms to reduce the headers from their native sizes to around 2-4 bytes. The currently defined header compression mechanisms all assume that the Data Link layer can provide the IP packet length and that this length does not need to be transmitted as part of the compressed IP header.

In cases where the overhead of either version of IP is too great, alternate low-bandwidth network protocols may be employed. The Space Communications Protocol Specification: Network Protocol (SCPS-NP) is a highly bit-efficient network protocol capable of supporting many of the features of IP. SCPS-NP gets its overhead reduction from including only those
fields necessary, and by compressing network addresses or pairs of network addresses. Thus a single-byte SCPS-NP address might refer to a pair of 16-byte IPv6 addresses. While no commercial network hardware currently routes SCPS-NP packets, Network layer gateways can be used to convert between IP-based and SCPS-NP-based networks.

Note that the use of the IP packet format says nothing about how packets are forwarded and/or routed. In particular, all data movement can still be commanded from a mission control center on Earth.

4.4.2 FLEXIBILITY, SCALABILITY, AND INTEROPERABILITY OF IP

The Internet Protocol itself is mostly a format for identifying the source and destination of data packets, along with information about which upper-layer transport protocol is being used and space to hold QoS information. Because it makes very few assumptions about the nature of the higher-level data (Transport and Application), IP provides a very strong buffer between applications and underlying communication hardware. IP does not have any sort of closed-loop control between data source and destination, and hence can be used to carry information across simplex links. The main disadvantage of IP in a cislunar context is that all known IP implementations are intolerant of disconnection. That is, if there is not a continuous end-to-end path from the source to the destination, IP packets will be dropped at the point where they cannot be forwarded. This deficiency is addressed below by current work in Delay/Disruption Tolerant Networking (DTN), a form of overlay network discussed in more detail later in 4.13.

IPv4 allows for the use of private address spaces that are $2^{24}$ bits, or 16,777,216 hosts; IPv6 does not provide for private addresses but because of IPv6’s larger address space, allocations of $2^{32}$ bits could be made to single missions. This would be enough to support cislunar operations for a long time. Another aspect of IP’s scalability is in the way it supports upper-layer protocols through the Protocol ID field. While TCP and UDP are by far the most popular transport protocols in the terrestrial Internet, there is ample room to define new transport protocols for cislunar operation should they be required. Multiplexing of applications over particular Transport layers is handled by the Transport layers, via 16-bit port numbers in TCP and UDP.

Standardizing on IP (or any) network protocol for cislunar communications will provide interoperability between deployed elements. The advantage of IP over any other network protocol comes from the large-scale deployment of IP on Earth, particularly the Internet and many private networks. Choosing IP for cislunar also has the advantage that it brings with it support for the huge array of applications that are seen on the Internet, including many that will probably be useful for crewed missions, such as electronic mail, web browsing, and instant messaging.
4.5 IP PACKET OVERHEAD

Uncompressed IPv4 headers require 20 bytes plus options, and uncompressed IPv6 headers (reference [10]) require 40 bytes plus any extension headers. Typical IP packet sizes tend to be either around 40 bytes (for TCP acknowledgements carrying no data), or 1500 bytes for full-sized TCP segments that traverse Ethernets. A typical TCP header is between 20 and 32 bytes, depending on the options used. This means that uncompressed TCP/IP headers on a full-sized (1500-byte) data segment are about 3.5% overhead. Note that for TCP acknowledgements that do not carry any data, the packet is essentially 100% overhead but is required in order to provide TCP’s reliable delivery service.

A number of header compression mechanisms have been defined for both IPv4 and IPv6 that drastically reduce header overhead by compressing the IP and sometimes additional headers into a single one- or two-octet context identifier. This has the effect of reducing the effective size of an IP header to one or two bytes, rather than 20 (uncompressed IPv4) or 40 (uncompressed IPv6) bytes. For full-sized IP packets, this amounts to a header overhead of less than 1%.

4.6 IPV4 / IPV6 INTEROPERABILITY

IP version 4 (IPv4) is the most common version of IP in use today. IPv6 is being deployed, with many institutions requiring IPv6 changeover, or at least IPv6 compatibility, within the next few years. This document does not recommend either version over the other, but whichever version(s) is(are) used, it is likely that the architecture described here will have to interface with both IPv4 and IPv6 networks and systems. A number of mechanisms exist to support tunneling of IPv4 packets across IPv6 networks and vice-versa, and many routers and end systems support running both IPv4 and IPv6 simultaneously.

4.7 NETWORK ADDRESS TRANSLATION (NAT)

In addition to the version of IP used to communicate, IP addresses can be either public or private. Public addresses are those that are globally routable by the terrestrial Internet and are allocated by a central authority. Private IP addresses are not globally routable. That is, private addresses may be reused at multiple institutions, but packets with private destination addresses cannot be sent over the Internet.

Network Address Translation (reference [11]) is a mechanism that allows hosts with private addresses to connect to the Internet via a NAT gateway with at least one publicly routable address. The NAT gateway modifies the headers of IP packets flowing through it to allow the hosts with private addresses to communicate with other hosts via the Internet.
4.8 AUTOMATED DATA FORWARDING

4.8.1 GENERAL

The next step in advancing the efficiency of the infrastructure is to allow for automated forwarding of data packets. Enabling automated data forwarding will decrease operations costs, since less human intervention will be required. This will become increasingly important as the number of deployed elements grows, and will allow mission operations to focus more on data collection and analysis rather than the mechanics of data transport.

Note that all decisions about the paths packets take can still be made manually at this stage. Mission managers can still set up which routes data packets will take via a management interface, and then allow the various elements to send data automatically along those routes.

4.8.2 FORWARDING, ROUTING, AND DIFFERENT TYPES OF RELAYS

While the Internet uses routing protocols to update the forwarding tables of intermediate routers automatically and dynamically, the same need not be the case for space missions. While dynamic routing may one day be used, either because it is needed to deal with the number of systems or simply to reduce operations costs, initial operations can choose to manage all forwarding tables via management interfaces. What this amounts to is telling each router, for each destination IP address, where packets for that destination address should be sent. This will allow mission operations personnel to maintain absolute control over the forwarding process while still not having to manage each data transfer across each link.

The management of the data forwarding tables takes place at the network (IP) level, and is insensitive to data link and physical connectivity underneath. Specifically, bent-pipe relays are ‘invisible’ to the IP forwarding and routing mechanisms, and may be intermixed in the system along with other types of links (e.g., 802.11G, switched Ethernet, etc.).

4.9 QUALITY OF SERVICE

One of the issues in using a packet-switched network to support critical operations is that if the network becomes congested, packets can be dropped. For certain classes of traffic, data loss could be catastrophic, leading to loss of life or spacecraft.

IP provides a number of QoS mechanisms, ranging from Differentiated Services (DiffServ—see reference [12]) to Integrated Services (RSVP—see reference [13]) to traffic engineering (reference [14]). Of these, DiffServ is probably the best suited for ‘everyday’ operations, as it allows applications to request particular treatment for packets belonging to specific data flows, flexibility to the network in meeting those requests where possible, and shaping of traffic where necessary.

DiffServ allows for different treatment of packets based on a field in the IP header. Packets are typically grouped into four forwarding classes, with three drop precedences per
forwarding class. Other schemes are possible, as the interpretation of the DiffServ CodePoint (DSCP) is up to the individual routers. Note also that the DSCP allows a point where policy can be imposed on applications by the network (typically the first-hop router for the data flow). That is, network routers can rewrite the DSCPs of application packets. Thus if a particular application is allowed, by policy, to transmit XMbps of high-priority (e.g., AF1) traffic, and the application emits 2XMbps of traffic, the first-hop router can re-mark half of the application’s traffic as AF2 or AF3. This allows policy to protect the network and other applications from a single rogue application.

DiffServ is typically implemented via Class-Based Queuing (CBQ) mechanisms, where traffic with different DSCP markings is first sorted into different classes, and different queuing/forwarding mechanisms are invoked on the classes. Alternately, CBQ can be directly applied to the IP packets, using fields from the TCP/IP headers such as the source/destination addresses and port numbers to classify packets. Special treatment of packets can come at the IP layer by altering the packet queuing and scheduling and/or at other layers. For example, packets marked with a particular DSCP may invoke special treatment by the Data Link layer, such as a reliable contention-free service.

Of particular interest for emergency operations is the expedited forwarding traffic class defined in reference [15]. Routers implementing expedited forwarding should provide a guaranteed minimum forwarding rate for Expedited Forwarding (EF) packets, regardless of other traffic that may be present at the router. This would allow emergency traffic a guaranteed minimum forwarding rate which, when combined with limited injection of EF-marked traffic, would provide a very low-latency and high-reliability solution.

4.10 SECURITY

4.10.1 GENERAL

There are two different aspects to security: security policy and security implementation. Security policy defines what members of the system are allowed to perform what actions with other members, such as commanding or monitoring telemetry. The security implementation defines how the various policy rules are implemented and enforced. In a networked system of the kind discussed here, security can be implemented at many different protocol layers. As previously discussed, reference [5] describes a number of ways to provide security services with CCSDS protocols at the Application, Network, Data Link, and Physical (bulk encryption) layers of the network stack.

Internet Protocol Security (IPSec—reference [16]) is a framework of open standards for ensuring secure private communications over the Internet or any IP-based network. It is based on standards developed by the Internet Engineering Task Force (IETF), which provide confidentiality, integrity, and authenticity of data communications across a public network. IPSec provides a standards-based, flexible solution for deploying a network wide security policy. IPSec is a Network layer security mechanism providing an authentication-only service via the Authentication Header (AH) protocol, or a confidentiality service via the...
Encapsulating Security Payload (ESP) protocol. Key management is accomplished in IPSec via the use of the Internet Key Exchange (IKE) protocol. This internationally recognized protocol suite is especially useful for implementing virtual private networks. Because IPSec works by appending additional header information after the standard 20-byte IP header, it can be routed through any IP network, even if the internal routing nodes are not IPSec aware. Because IPSec was designed for the IP protocol, it has wide industry support and is becoming the standard for virtual private networks on the Internet. IPSec implementation is mandated for IPv6 conformance and is optional for IPv4.

4.10.2 AUTHENTICATION

Authentication is a security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information. IPSec implements authentication by the use of an Authentication Header (AH). This is an extension header that protects the upper layer headers and contents. These upper layer headers can be either Transport layer (such as UDP or TCP) or tunneling headers, such as ESP (used for VPNs) or Generic Routing Encapsulation (GRE—used for Mobile IP). AH typically uses keyed Message Authentication Codes (MACs) based on symmetric encryption algorithms (e.g., AES) or on one-way hash functions (e.g., MD5 or SHA-1). For multicast communication, one-way hash algorithms combined with asymmetric signature algorithms are appropriate, subject to performance considerations. The mandatory-to-implement authentication algorithms consist of hashed-MAC (HMAC) with MD5, and HMAC with SHA-1. These two MUST be implemented in order to ensure interoperability. Other algorithms MAY be supported.

4.10.3 CONFIDENTIALITY

IPSec provides confidentiality through the use of the ESP protocol. ESP may be applied alone, in combination with the IP Authentication Header (AH), or in a nested fashion, through the use of tunnel mode. The ESP header is inserted after the IP header and before the upper layer protocol header (transport mode) or before an encapsulated IP header (tunnel mode). ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality. The set of services provided depends on options selected at the time of Security Association establishment. Confidentiality may be selected independent of all other services; however, use of confidentiality without integrity/authentication (either in ESP or separately in AH) may subject traffic to certain forms of active attacks that could undermine the confidentiality service.

4.10.4 VIRTUAL PRIVATE NETWORKS

Virtual Private Network (VPN) refers to the practice of using a public network such as the Internet to transmit private data. The standard for VPNs is the layer 3 (Network) IP IPSec. IPSec VPNs leverage the free/public long-haul IP transport service and the proven IPSec
protocol to provide a more flexible, cost-effective solution for secure access than previous techniques such as leased lines (layer 1), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Tunneling Protocol (L2TP). IPSec VPNs are best used to secure fixed infrastructure virtual networks, or ones with a limited, controlled number of mobile nodes.

4.10.5 TRANSPORT LAYER SECURITY (TLS)

Transport Layer Security (TLS) is applied between the Application and Transport layers, so that in particular the application data content is protected but the Network and Transport layer headers are not. This has the advantage of leaving information about the source and destination addresses, the protocol, and the application (via the port numbers) available to intermediate nodes in the network. Networks that include a large number of uncontrolled mobile nodes may be better served by an Application layer VPN built upon TLS or Secure Socket Layer (SSL) technology.

4.10.6 KEY EXCHANGE

Key exchange protocols form another vital part of all IPSec-based security solutions. IPSec uses IKE. When traffic wishes to use a tunnel, IKE is used to set up an IPSec Security Association (SA). IKE provides authentication of the IPSec peers, negotiates IPSec SAs, and establishes IPSec keys before the data SAs are established. This allows for dynamic SAs and dynamic rekeying so that keys can be expired and recreated, reducing the chance of an attacker’s gaining advantage by cracking one key. If key exchange is considered unnecessary or undesirable, IPSec also supports static keys based on a pre-shared secret.

4.11 INTERFACES WITH LEGACY SYSTEMS

At least in the initial stages of deployment, there will continue to be elements (perhaps both space and ground) that do not use the IP Network Layer format. Using the layered model described above, communications with such ‘legacy’ devices would still be possible, provided the new devices:

- a) are physically capable of communicating with the legacy devices;
- b) know about the legacy device framing/addressing mechanisms.

4.12 TRANSPORT LAYER

4.12.1 GENERAL

The standard transport protocols used with the Internet protocol suite are Transmission Control Protocol (TCP—reference [17]), which provides a reliable byte-stream service, and user Datagram Protocol (UDP—reference [18]), which provides an unreliable datagram service. Other services such as overlay services that provide reliability without the...
requirement for bidirectional end-to-end paths, or that provide reliable multicast, can be built on top of TCP and UDP.

### 4.12.2 UDP

UDP provides an unreliable data delivery service comparable to standard TDM and CCSDS Space Packet delivery systems currently used for space communication. UDP packets may be lost or duplicated in the network, and no feedback of such events is provided to the sender. Because UDP does not implement reliability or require any signaling from the recipient to the sender, it can function over paths with arbitrary delays and/or simplex paths. UDP is commonly used for data delivery where completeness is not required, such as cyclic telemetry. If a UDP packet containing one or a set of telemetry measurements is lost, it may be enough simply to wait for the next packet, which will contain more up-to-date information.

While it is possible to use UDP for data transport and to implement reliability at the Application layer, care should be taken in doing so, especially in a network that concurrently carries other Internet protocol traffic such as TCP. Applications using UDP would need (in a mixed network) to ensure that they did not congest the network, either by implementing some sort of congestion control mechanism or by careful management of all link volumes. Note that this is not considered a problem if the application sends small amounts of data such as small and relatively infrequent telemetry samples. It becomes an issue only when a UDP-based application might want to send large amounts of data that could, if sent all at once, overwhelm a router in the middle of the network. The IETF is currently investigating a Datagram Congestion Control Protocol (DCCP) for such applications, though DCCP requires bidirectional communications.

### 4.12.3 TCP

#### 4.12.3.1 Overview

TCP provides a reliable, in-order bytestream delivery service without duplication. This means that when applications send data using TCP, the sending TCP endpoint will attempt to detect lost data and will retransmit data until it is acknowledged by the receiver. TCP also provides congestion control to attempt to keep from overloading the network with too much traffic. Because of the way reliability and congestion control are implemented within the protocol, TCP performance can suffer in stressed environments characterized by large bandwidth-delay products, high bit-error rates, and significant asymmetries in data rate. The round trip light time from Earth to the moon is on the order of three seconds, and an overall RTT including intermediate relays of on the order of five seconds will probably be more typical. Such delays are enough to cause degradation in TCP performance, especially if ‘stock’ end systems are used.

In the 1990s, CCSDS developed the Space Communications Protocol Standards Transport Protocol (SCPS-TP) extensions to TCP to attempt to extend the operating range over which...
TCP can perform efficiently. While SCPS-TP provides a compatible application programming interface to TCP, deploying the SCPS-TP extensions in every end host may be impractical. Terrestrially, Performance Enhancing Proxies that translate between TCP and SCPS-TP are often used to isolate the high bandwidth*delay links that can lower TCP performance.

4.12.3.2 Using Performance Enhancing Proxies to Improve TCP Performance

Some of the performance problems of end-to-end TCP can be ameliorated with the use of Performance Enhancing Proxies (PEPs). For TCP traffic, a PEP is a device that is in the network but that interacts with the end-to-end TCP flow in order to improve its performance. There are a number of different kinds of PEPs discussed in reference [19], but one of the most common types is a split-connection PEP. Split connection PEPs break end-to-end TCP connections into multiple pieces, with the pieces traversing the stressed portion of the network using technologies specifically designed and/or tuned for those environments.

![Figure 4-2: Split-Connection PEPs Break TCP Connections into Three Parts](image)

Figure 4-2 illustrates a pair of split-connection PEPs bracketing a stressed link. The PEP on the left terminates the TCP connection from the left-hand host, and uses a separate transport connection (in this case, SCPS-TP) to communicate with the PEP on the right. The right hand PEP terminates the SCPS-TP connection and shuttles data between it and a TCP connection with the destination host.

Note that to terminate TCP connections the PEPs must be able to see and modify the TCP headers. This requires that the TCP headers be ‘in the clear’ as they pass through the PEP, and not encrypted. Network security mechanisms such as IPSec encrypt the transport (TCP) headers, preventing the use of performance enhancing proxies. It is worth noting that most PEPs will pass IPSec traffic, but it will not benefit from the PEP’s enhancement. This means that IPSec can still be used if the security benefits it provides override the performance degradation.

It is also worth mentioning that most of the benefits of IPSec can be obtained from TLS mechanisms.
Finally, TCP requires an end-to-end bi-directional path.

### 4.13 OVERLAY NETWORK SERVICES

While TCP and UDP provide enough services to cover most terrestrial communications needs, there are times when neither is in itself particularly well suited to an environment or application. Perhaps the two most common situations that require more support are reliable multicast communication and communication when no end-to-end path exists. TCP’s control loops that provide reliability and congestion control are necessarily peer relationships between a single sender and a single receiver. Thus TCP is not suited to multicast traffic. While UDP can support multicast traffic, it does not provide any reliability or congestion control. Finally, both TCP and UDP rely on IP, which assumes that network paths run uninterrupted from sender to receiver. While this is a good assumption in most terrestrial environments, it may not hold for space applications, as spacecraft pointing, antenna/communications scheduling, and obscurations may conspire to interrupt communications.

The common approach to providing enhanced services such as reliable multicast or communication without an end-to-end path is to create a new layer of protocol on top of either TCP or UDP. This new layer of protocol defines an overlay network as shown in figure 4-3. It may be the case that only the end systems, some nodes in the network (as shown in the figure), or all nodes implement the overlay protocol. Nodes in the overlay then use TCP, UDP, or Data Link layer communications to exchange data. The overlay may provide a reliable file replication service or a reliable (unicast) file delivery service over intermittently connected links; or it may look like a Transport layer protocol itself.

![Overlay Network Diagram](image)

#### Figure 4-3: An Overlay Network (Larger, Dark Circles) Sparsely Deployed in an Underlying Network (Smaller, White Circles)

The Asynchronous Layered Coding (ALC) protocol (reference [20]) forms the basis for a number of overlay protocols, including NACK-Oriented Reliable Multicast (NORM—reference [21]), a general-purpose reliable multicast data distribution protocol, and File Delivery over Unidirectional Transport (FLUTE—reference [22]), a file delivery protocol that can be used over simplex data paths.
The CCSDS File Delivery Protocol (CFDP—reference [23]) with its Store-and-Forward Overlay (SFO) procedures also implements an overlay network focused on file delivery. CFDP can run over TCP or UDP, or can be configured to run directly over data link protocols such as AOS and Proximity-1.

A slightly different type of overlay network is Delay/Disruption Tolerant Networking (DTN—reference [24]). DTN provides an optionally reliable datagram delivery service to applications, regardless of whether end-to-end paths exist or not. Reliable message delivery is accomplished by a sequence of custody transfers from node to node in the overlay rather than with end-to-end reliability as with TCP. Custody transfers are a function of the overlay protocol and do not depend on contemporaneous bidirectional connectivity between overlay nodes. Thus a DTN node might transmit a message on Tuesday using UDP over AOS and receive an indication that some other node has taken custody of the message on Wednesday, with that indication coming by way of a TCP connection over Proximity-1.

Unlike the overlays above, DTN is designed to accommodate changing connectivity in addition to intermittency. The DTN overlay is designed to run its own routing protocol(s) independent of the underlying network. These DTN routing protocols can account for things the underlying network does not, such as scheduled future periods of connectivity. Thus a DTN node might decide to break a message it is currently forwarding into two parts, one to be sent now over UDP and another to be sent over a future scheduled Proximity-1 connection. The various pieces are then reassembled at the destination (or can be reassembled at another intermediate node if they happen to meet).

To illustrate how overlay services can improve performance in intermittently connected environments, figure 4-4 shows two views of a notional four-hop network path. The top view uses end-to-end networking such as IP between the source at the top and the destination at the bottom. Time in the figure progresses to the right, and up/down timelines for each link are shown. A heavy bar centered on the thin line for a link indicates that a particular link is up at a particular time, and a thin line without a bar indicates that the link is down. Data is represented by the heavy boxes that are above link connectivity indicators, and the source is assumed always to have data to send.
NOTE – End-to-end networking requires a full path between source and destination before any data can be sent. A long-term store-and-forward system can use individual links as they are available.

Figure 4-4: End-To-End Network and Message-Based Store-and-Forward System

In the end-to-end (top) portion of the figure, the source has to wait until there is a complete path to the destination before any data can be sent, thereby increasing the latency and reducing throughput. The message-based store-and-forward system, on the other hand, gets the first bit to the destination much faster, and has a higher overall throughput.

4.14 REQUIREMENTS IMPOSED ON SUBNETWORKS

IP makes use of subnetwork services to transfer packets between IP routers. In the parlance of reference [25], subnetworks are layer-2 networks that do not require the use of IP routers to forward packets. Note that subnetworks may include (or be entirely composed of) layer-1 switching fabrics such as the Tracking and Data Relay Satellite System (TDRSS). RFC 3819, also known as BCP89, provides advice to subnetwork designers who wish to support Internet protocols so that the subnetworks can efficiently support the Internet protocols without undue duplication of services. For example, RFC 3819 includes sections on:

- Maximum Transmission Units (MTUs);
- framing over connectionless and connection-oriented networks;
- support for broadcast, multicast, and discovery;
– reliability and error control;
– qos;
– delay;
– asymmetry;
– compression;
– packet reordering;
– mobility;
– routing;
– fairness.

These recommendations should be considered in the design and configuration of the various data links supporting the cislunar architecture described here.

4.15 EMERGENCY COMMANDING

4.15.1 GENERAL

Emergency commanding of spacecraft in a networked environment poses a number of challenges. For spacecraft that are tumbling, for instance, an important metric is the number of bits required to effect a basic command, such as ‘safe the spacecraft’. For a spacecraft that is on station but has a damaged receiver, transmitting a command such that it arrives at the damaged spacecraft with the highest power might be more important.

Traditionally, emergency commands have been handled by a hardware command decoder that is very close to the RF front end of the spacecraft. Thus a particular bit string is included in a Data Link layer frame, and a correlator immediately following the demodulation process detects the bit string and acts on it. An advantage of this approach is that none of the rest of the spacecraft command and control system (including any network stack onboard) needs to be functioning. Indeed, hardware commands to reboot the main spacecraft command and data handling system are usually considered in spacecraft design.

This architecture admits three basic mechanisms for emergency commanding:

a) Emergency commanding via IP. This option relies on the ‘standard’ communications mechanisms to get an emergency command to a particular spacecraft and to have it recognized. Such a command could be identified with a special transport protocol type, or could be included as the payload of a standard UDP packet. Using IP to route the command allows emergency commanding of elements that are not proximate to the element doing the commanding (multi-hop communications). Drawbacks of this approach are that it requires that either the full IP (and possibly UDP) headers be transmitted, or that the header compression mechanisms at the receiver be working.
In either case, a hardware detection mechanism could be used to detect a ‘special’ bit pattern and act on it accordingly so that the full networking stack would not have to be functional. Measures would need to be taken to ensure that the ‘trigger’ bit pattern did NOT show up as the payload of any data transmitted by the spacecraft. One way to achieve this would be to make use of the Data Link layer synchronization mechanisms to search for a trigger pattern only immediately following a Data Link layer synchronization marker. Using the data link frame marker to bound the search for a trigger bit sequence would rely on there being a single IP packet per Data Link layer frame. If multiple IP packets can be aggregated together into a single data link frame, the packet containing the trigger could be placed after some other packet and hence not proximate to the Data Link layer frame marker.

b) Emergency commanding via link layer mechanisms. It may be possible to use Data Link layer mechanisms to effect emergency commanding. CCSDS data links support a number of virtual channels (VCs) that are commonly used to segregate traffic of different types, including emergency commands. Variable-length Data Link layers such as the CCSDS Telecommand (TC) standard are particularly good for this, since a short frame header can be followed by a VC identifier and then the emergency command itself. The main drawback of this approach for the architecture presented here is that it is not routable; emergency commands must be transmitted by a link-local neighbor. Also, fixed-length Data Link layer frames like CCSDS AOS tend to be long, impairing the ability to get a short command into a tumbling spacecraft.

c) A third mechanism would be to use a combination of the above, using Internet-based protocols to get an emergency command to a special application resident at the penultimate IP hop, and to use link layer mechanisms to get it to the destination. This has the advantage of being able to use link-specific mechanisms that may allow very short commands while still allowing those commands to traverse multiple hops in the network. The main disadvantage of this mechanism is that it requires the ‘special application’ to be standardized and resident at each node.

4.15.2 EMERGENCY COMMANDING SECURITY

The requirements for emergency commanding are somewhat at odds with the requirements for security. On one hand, emergency commands want to be as short as possible to maximize the chance of being received by a tumbling spacecraft. On the other hand, emergency commands probably need some form of security, at least authentication, which adds overhead. Of course, if power delivered to the ultimate destination is an issue, then any node could conceivably be directed to form a data link connection with the destination and forward emergency commands in this manner. Emergency commands are usually implemented entirely in hardware, with no software or processor involvement, in order to be able to recover from a crashed processor, but this often results in fixed, repeatable bit sequences that are susceptible to a replay attack. At a minimum, emergency commands should have some form of authentication.
5 OPERATIONS CONCEPTS USING THE NEW ARCHITECTURE

5.1 OVERVIEW

The following two scenarios give examples of how the guidelines presented in this document would be used for future architectures for lunar missions. The examples are derived from the various endpoints described in section 3 and the architecture described in section 4. The first example showcases an architecture consisting of robotic missions and the second is a crewed scenario. The protocols and technologies used in these examples and the links shown are for illustrative purposes only and should not be construed as recommendations.

5.2 ROBOTIC SCENARIO

The robotic scenario describes an established architecture that makes use of a mature lunar communications infrastructure consisting of multiple international missions. It consists of the spaceborne assets shown in table 5-1 and the Earth entities shown in table 5-2. In the case of the earthbound nodes, there may be multiple instances of each. For instance, each mission may have its own Mission Operations Center (MOC) or a given MOC may control multiple spacecraft. It is assumed that in all instances there will be greater than one of each type.

Table 5-1: Spaceborne Assets of a Robotic Lunar Architecture

<table>
<thead>
<tr>
<th>Spacecraft</th>
<th>Location</th>
<th>Quantity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Science Mission</td>
<td>Lunar Orbit</td>
<td>3</td>
<td>Science asset with multiple instruments onboard the spacecraft</td>
</tr>
<tr>
<td>Lander</td>
<td>Lunar Surface</td>
<td>2</td>
<td>Robotic lander with multiple instruments</td>
</tr>
<tr>
<td></td>
<td>(near and far side)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rover</td>
<td>Lunar Surface</td>
<td>2</td>
<td>Robotic rover with multiple instruments</td>
</tr>
<tr>
<td></td>
<td>(near and far side)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spacecraft (either lander or rover)</td>
<td>En Route</td>
<td>1</td>
<td>A spacecraft en-route to the either orbit or land on the moon</td>
</tr>
<tr>
<td>TDRSS</td>
<td>Earth Orbit</td>
<td>Multiple</td>
<td>Used for relay of communications</td>
</tr>
</tbody>
</table>
Table 5-2: Earthbound Assets of a Robotic Lunar Architecture

<table>
<thead>
<tr>
<th>Node</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ground Stations</td>
<td>Multiple ground stations. Either the Deep Space Network (DSN) or commercial antennas.</td>
</tr>
<tr>
<td>Missions Operations Center</td>
<td>Mission operations centers for the various missions. Each MOC may control one or more spacecraft. The MOC is responsible for the health and safety of the spacecraft and coordination of science operations with the SOC.</td>
</tr>
<tr>
<td>Science Operations Center</td>
<td>Science Operations Centers for the various missions. Each SOC may be responsible for one or more instruments on one or more spacecraft.</td>
</tr>
<tr>
<td>Spacecraft Development Facilities</td>
<td>Spacecraft engineers at commercial/government/university facilities monitor health and safety of the spacecraft.</td>
</tr>
<tr>
<td>Remote locations</td>
<td>These nodes consist of scientists or operations personnel who are not in their home facility.</td>
</tr>
</tbody>
</table>

A common denominator of these robotic spacecraft is that they process various types of input and output either from or to other nodes in the cislunar network. Input to a node will typically take the form of commands to control the platform or payload, configuration data for operating the spacecraft or instruments, or data destined for another node in the cislunar network. Spacecraft output may consist of payload telemetry consisting of spacecraft status or data, science data in files, video streams, or other formats, and the aforementioned data being relayed to other nodes. Transmission of this data can be either one-to-one as in Earth ground station to spacecraft or one-to-many such as telemetry that may be received by a single Earth antenna but end in various location such as an operations center, an archiver, and a science workstation. How this data travels throughout the system may also vary. Some data, such as real-time housekeeping data or navigation images, have an innate time sensitivity that requires delivery as quickly as possible. Other types of data may be delay tolerant and able to be transmitted in a store-and-forward fashion.
5.3 EXAMPLE APPLICATIONS OF CISLUNAR PROTOCOLS IN ROBOTIC ENVIRONMENT

5.3.1 OVERVIEW

The following list of examples describes methods and protocol interactions for typical operations and applications that may be seen in a robotic lunar architecture.

5.3.2 REAL-TIME NETWORK TELEMETRY FROM A SPACECRAFT

Unmanned spacecraft typically produce real-time telemetry containing information about the health and welfare of the spacecraft and other data. Using the cislunar network architecture, this telemetry could be formatted into CCSDS Space Packets and transported to the ground via UDP and IP. Upon receipt by the ground, the packets would then be routed to various destinations including the SOC and MOC across standard terrestrial communication.

![Figure 5-1: Real-Time Telemetry Transmission](image-url)
5.3.3 RELIABLE FILE TRANSMISSION FROM INSTRUMENT TO USER

Reliable file transmission from instrument to user uses the transfer of a data file from an instrument to a user on the ground. The protocol stack for this transfer is shown in figure 5-2. In this example, the CCSDS File Delivery Protocol (CFDP) is used to perform the file transfer. The process begins with the user’s initiating a file transfer by contacting the CFDP engine on the spacecraft. The transfer uses CFDP’s Acknowledged Mode, which provides for reliable delivery of CFDP information between endpoints. Since delivery is ensured by CFDP, UDP is chosen at the next layer, and the appropriate IP packets are created with the address of the sender and the address of the instrument on the spacecraft. This information is then sent within the user’s facility via a Physical layer protocol followed by a transmission across the Internet via the same or a different Physical layer mechanism to the ground station. The packet is then placed into the appropriate Data Link layer protocol frames and sent to a lunar orbiter functioning as relay via R/F. Upon receipt by the spacecraft, the spacecraft determines appropriate communication capability and timing with the lander and initiates a transmission by placing the IP packet in a selected Data Link layer frame for transmission to the lander. When the lander receives this information, it determines the destination of the packet through its routing information and transmits the packet across its internal bus to the instrument. At this time, the instrument software extracts the CFDP information from the packet. The CFDP engine determines what was requested, communicates with the CFDP client application, and initiates the appropriate action. Communication back the sending entity is started in the reverse of that described above but perhaps through a different series of nodes using a different Data Link layer where appropriate.

Figure 5-2: Instrument/User Data Transmission with CFDP Acknowledged Mode
5.3.4 COMMANDING A SPACECRAFT VIA END-TO-END IP

Standard commands in the cislunar network would travel along a path similar to that in the two examples above. Assuming the commanding of a lander via an orbiter, mission operations personnel would format a command via their command software and the data would travel via UDP and IP through the local router to the ground station. The command would then be formatted in the appropriate Data Link layer frame for transmission to the orbiter, which would then route it to the lander. Software or hardware onboard the lander would direct the command to the appropriate subsystem, in this case the Command & Data Handling (C&DH) processor.

![Figure 5-3: Spacecraft Commanding](image)

5.4 STORE AND FORWARD TRANSMISSION

In some instances in the cislunar network, it may not be possible to transmit data from a spacecraft immediately. Under these circumstances, a store and forward mechanism will be required to enable data to reach Earth. Store and forward transmission uses the Delay Tolerant Networking bundling layer discussed in section 6. Data transfer takes the form of a bundle from the corresponding application on the spacecraft. It is sent from lander to the orbiter, where it can be stored until necessary bandwidth is available. Upon receipt on the ground it is forwarded to the SOC where the data is extracted from the bundle.

![Figure 5-4: Store and Forward Using Delay Tolerant Networking](image)
6 PHASED INTRODUCTION OF CAPABILITIES

6.1 GENERAL

Moving from traditional operations to a completely IP-based system in one step would be jarring at best. While the concepts of automated data forwarding, routing, and network QoS are mature and have operational experience terrestrially, their applicability to a ‘MANET of networks’ composed of orbiting satellites, orbiting relays, lunar outposts, and lunar transit vehicles leaves several questions. One of the largest open questions is how to structure a dynamic routing protocol to handle the changing connectivity among various spacecraft. Identification and development the protocols to populate the architecture presented here should be done in three phases:

a) simple spacecraft without in-space routing;

b) simplified in-space routing among cooperating spacecraft;

c) advanced in-space routing among multiple spacecraft.

6.2 NON-ROUTING SPACECRAFT

In the first phase, spacecraft will not be required to use other spacecraft as IP routers in order to reach the ground. This admits the use of layer-2 relays such as TDRSS, but greatly simplifies Network layer routing. Because the spacecraft may use different ground stations and hence change their points of attachment to the Internet, routing from ground-based systems to space-based systems is an issue (routing toward the ground-based systems, which do not move within the Internet topology, is trivial). Techniques such as MobileIP would work here, as would a more managed approach where GRE tunnels from the spacecraft’s ‘home’ location to the correct ground station are configured and maintained from a mission operations center.

6.3 SIMPLE RELAYS

The second phase will consider simple routing among spacecraft that are designed to know of each other’s existence and where the in-space routing does not require a full dynamic routing protocol to manage connectivity. An example of such a situation would be an orbiter-lander mission, where the lander could route data via the orbiter to reach Earth. This situation is not much more complex than the first phase, since the only thing changing from the point of view of the terrestrial routing is the orbiter’s point of attachment to the ground.
6.4 IN-SPACE ROUTING

The third phase will consider the general case of spacecraft-to-spacecraft routing where two spacecraft, A and B, can use zero or more other spacecraft as relays to communicate either with different spacecraft or with the ground. This becomes more complicated when spacecraft A is directly attached to the ground (via a DTE/DFE link), in which case packets from locations on the ground to spacecraft A should be routed to spacecraft A’s home (assuming some form of tunneling is used). Spacecraft A’s point of attachment could also be via spacecraft B, in which case packets to spacecraft A would need to be routed toward spacecraft B’s home (again, assuming some form of tunneling from spacecraft B’s home location to the current ground station serving spacecraft B). Full dynamic routing would alleviate the tunneling problem but would introduce route convergence issues that would need to be addressed.
7 TRANSLUNAR

Some elements of the cislunar communications architecture cannot readily be applied to mission operations beyond the moon, i.e., in ‘translunar’ space. Since signal propagation delay increases with distance, end-to-end delays similar in effect to those discussed in section 2 are encountered even when the end-to-end path between source and destination is continuous. Moreover, communication with vehicles in deep space is typically discontinuous for other reasons: orbital mechanics may result in periodic occultation of the spacecraft, and resource constraints both on the spacecraft and on Earth typically restrict communications to planned, limited contact periods. The episodic nature of deep-space communication imposes additional round-trip delay; i.e., the response to a message received at the end of one episode cannot be transmitted until the beginning of the next.

Among the implications of long and highly variable delay in the end-to-end communication round trip are the following:

- At the extreme, the data exchange required for establishment of a connection could consume the entire communications opportunity. Therefore only connectionless protocols should be used.

- Transmission history cannot be used to predict RTTs, so communication timeout interval computation should rely on link state information rather than timing statistics.

- End-to-end retransmission would reserve resources (the retransmission buffer) at the message originator for the entire duration of the transaction, possibly for days or weeks. Therefore retransmission should be between relay points within the network rather than end-to-end.

- Reliable in-order stream communications would delay delivery of byte \( N \) until successful delivery of byte \( N-1 \). If byte \( N-1 \) were lost in transmission, the delivery of byte \( N \) and all subsequently received data would be retarded by at least one RTT while awaiting retransmission of that lost byte. Therefore out-of-transmission-order delivery is preferable for reliable communications: data should be structured in individually identifiable transmission blocks, rather than streams, to enable concurrent retransmission.

These effects argue for the use, over the direct ‘deep space’ links between Earth and vehicles in translunar space, of store-and-forward protocols, such as the DTN system described in 4.13 above, in place of the standard cislunar network and transport protocols discussed in 4.12.2 and 4.12.3.

However, communications among vehicles remotely deployed at a single remote point in the solar system, such as a system of orbiters and surface rovers cooperatively exploring Mars, will not be characterized by the same long and highly variable delay as communications between those vehicles and the mission operations center on Earth. Within such a system, delay and connectivity will be much as in the cislunar environment, and all elements of the cislunar communications architecture can again be applied.
In effect, this discontinuity in the applicability of the standard cislunar architecture to translunar mission operations forms an environment in which the only protocols that can all operate effectively within all segments (cislunar, circum-Mars, and the deep space links in between) of any end-to-end path are the DTN protocols. Applications designed to utilize DTN will require no alternation in order to communicate anywhere within the translunar environment. Applications designed to rely on the capabilities of the standard cislunar architecture, on the other hand, will need DTN capability added in order to communicate across the end-to-end translunar environment’s deep-space discontinuity in ‘cislunar-ness’.
ANNEX A

REJECTED ELEMENTS

A1 NON-NETWORKED COMMUNICATIONS

In non-networked communications, data to different destinations is differentiated at the Data Link or Physical layers. This can be accomplished through the use of a particular physical property of the transmission (time offset within a TDMA frame, a particular CDMA code, etc.) or a Data Link layer address (as in Ethernet). The primary disadvantage of this approach is that multi-hop data transmissions such as from a laptop to a wireless access point onboard a vehicle to a trunk line to Earth are not directly supported.

With a non-networked architecture, multi-hop transfers could be achieved using specialized Application layer software at each hop along the path to replicate the forwarding/routing capabilities of a Network layer. Since a non-networked architecture approach assumes that ‘non-networked communications’ is the baseline, the special forwarding software would presumably be used on a per-mission or per-application basis. Per-mission Network layers would impose the added overhead of designing, implementing, and testing networking capability on each new mission. With no expectation that two different implementations would be able to exchange data, there would be no way to leverage existing assets (orbiters, landed elements) for future missions.

A2 CIRCUIT-SWITCHED COMMUNICATIONS

Circuit-switched systems rely on circuits (physical or virtual) that are established between the communicating endpoints. Circuit establishment traditionally (though not always) brings with it resource reservation. There are a number of advantages to this approach, including guaranteed QoS, little or no congestion loss (depending on the circuit-switched mechanisms used), and very high switching capacities. The major drawbacks to this approach are inefficiency and a lack of robustness to changes in connectivity.

As an example, one could design a system that used out-of-band signaling to set up multi-hop data paths. Data could then be deposited into those paths and forwarded to the destination, with forwarding decisions at intermediate hops made simple as a result of the path setup procedure. Such an approach can provide exquisite QoS because, once set up, a data connection has reserved and exclusive access to resources (bandwidth) along the path. It suffers from the inability to take advantage of statistical multiplexing to fill the unused portions of circuits, however. Tagging individual pieces of data with destination information so that they can ‘fill the holes’ in pre-existing connections is essentially the same as adding a ‘packet header’ to the data.
ANNEX B

ENDPOINTS

B1 OVERVIEW

While section 2 had a higher-level abbreviated list of endpoints, this section provides an expanded comprehensive list of endpoints that more fully characterizes the potential scope of cislunar missions.

B2 TERRESTRIAL ENDPOINTS

The terrestrial endpoints to the communications network are the most complex and diverse of the network. This list is intended to describe the breadth of the end users and endpoints, but it cannot be comprehensive.

- spacecraft development facilities;
- spacecraft test & evaluation facilities;
- ground processing facilities;
- launch facilities (pad, etc.);
- launch control facilities (LCC, etc.);
- range safety facilities;
- launch vehicles on the ground;
- planning facilities (office environment);
- planners at remote locations;
- crew trainers and simulators;
- MCC facilities;
- backup operations personnel at remote locations;
- off-duty operations personnel with pagers;
- relay through one MCC to another MCC;
- communications stations and network control centers;
- payload development & test facilities;
- data archive facility;
– science operations facilities;
– science user facilities (universities, etc.);
– ground network facilities (antenna complexes, etc.);
– any of above facilities may sometimes be ‘lights-out’;
– remote scientists at home;
– public and news media;
– local civil authorities;
– astronauts’ families at home;
– landing facilities;
– other agencies: FAA, NOAA, DoD, the White House;
– water recovery facilities (navy ships, etc.);
– search and rescue teams;
– accident investigation teams.

Notes on the above list of terrestrial endpoints:

1  Some of these facilities may be ‘lights out’ unattended facilities at time, continuing to operate and exchange data with spacecraft.

2  Some of the distribution of data to these endpoints must be assumed to take place on terrestrial public and private networks.

B3  EARTH ASCENT/DESCENT ENDPOINTS

Earth ascent/descent endpoints are:

– launch vehicles (w/o crews);
– launch vehicles with crews;
– payloads reporting health;
– descent vehicles (w/o crews);
– descent vehicles (with crews).

B4  EARTH ORBIT ENDPOINTS

Earth orbit endpoints are:
– space network facilities (communications and tracking relay satellites, etc.);
– upper stage propulsion vehicles;
  • free-flyer unmanned vehicles (science, cargo, etc.);
  • payloads on free-flyer unmanned vehicles;
  • manned vehicles (Crew Exploration Vehicle [CEV], etc.);
  • crew on manned vehicles;
  • payloads on manned vehicles;
– crew in EVA suits;
– multiple spacecraft in rendezvous (automated, crew controlled);
– multiple spacecraft docked to each other;
– relay through one vehicle to another;
– communications relay and tracking satellites.

B5 LUNAR TRANSIT ENDPOINTS

Lunar transit endpoints are:
– upper stage propulsion vehicles;
  • free-flyer unmanned vehicles (science, cargo, etc.);
  • payloads on free-flyer unmanned vehicles;
  • manned vehicles (CEV, etc.);
  • crew on manned vehicles;
  • payloads on manned vehicles;
  • crew in EVA suits;
  • multiple spacecraft in rendezvous (automated, crew controlled);
– multiple spacecraft docked to each other;
– relay through one vehicle to another;
– vehicles at Lagrangian points, including communications relays, fuel depots and other TBD components of lunar mission support.
B6 LUNAR ORBIT ENDPOINTS

Lunar orbit endpoints are:
- space network facilities (lunar relay orbiter, etc.);
- upper stage propulsion vehicles;
  - free-flyer unmanned vehicles (science, cargo, etc.);
  - payloads on free-flyer unmanned vehicles;
  - manned vehicles (CEV, etc.);
  - crew on manned vehicles;
  - payloads on manned vehicles;
  - crew in EVA suits;
  - multiple spacecraft in rendezvous (automated, crew controlled);
  - multiple spacecraft docked to each other;
  - relay through one vehicle to another.

B7 LUNAR ASCENT/DESCENT ENDPOINTS

Lunar ascent/descent endpoints are:
- launch vehicles (w/o crews);
- launch vehicles with crews;
- payloads reporting health;
- descent vehicles (w/o crews);
- descent vehicles (with crews).

B8 LUNAR SURFACE ENDPOINTS

Lunar surface endpoints are:
- crew in LSAM or habitat;
- lunar habitat systems (occupied or vacant);
- multiple endpoints at a lunar outpost (core systems, payloads, crew entertainment systems, multiple communications systems, etc.);
- crew during EVA;
- crew mobility system (moonbuggy);
- unmanned lunar stations;
- autonomous robotic systems (stationary and rovers);
- human-guided robotic systems;
- communications hubs as standalone stations or part of larger stations;
- science systems (at habitat, station or standalone);
- crew or systems in safe haven (‘escape pods’), in emergency mode.
ANNEX C

ACRONYMS

This annex identifies and defines the acronyms that have been adopted in this Report.

AES Advanced Encryption Standard
ALC Asynchronous Layered Coding
AOS Advance Orbiting Systems
API Applications Program Interface
C&DH Command and Data Handling
CBQ Class-Based Queuing
CDMA Code Division Multiple Access
CEV Crew Exploration Vehicle
CFDP CCSDS File Delivery Protocol
DCCP Datagram Congestion Control Protocol
DiffServ Differentiated Services
DoD (U.S.) Department of Defense
DSCC DiffServ Codepoint
DSN Deep Space Network
DTE/DFE Direct-To-Earth/Direct-From-Earth
DTN Delay Tolerant Networking
EF expedited forwarding
EVA Extra-vehicular activity
FLUTE File Delivery over Unidirectional Transport
GRE Generic Routing Encapsulation
HMAC Hashed-MAC
IETF Internet Engineering Task Force
EML2 Earth-Moon Lagrangian point 2
IKE Internet Key Exchange
IPSec Internet Protocol Security
ISO International Organization for Standardization
L2TP Layer 2 Tunneling Protocol
LEO Low Earth Orbit
LCC Launch Control Facilities
LSAM Lunar Surface Access Module
MAC Message Authentication Code
MANET Mobile Ad-hoc Network
MCC Mission Control Center
MTU Maximum Transmission Unit
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>NACK</td>
<td>Negative-Acknowledgment</td>
</tr>
<tr>
<td>NORM</td>
<td>NACK-Oriented Reliable Multicast</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>PEP</td>
<td>Performance Enhancing Proxy</td>
</tr>
<tr>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RTT</td>
<td>Round Trip Time</td>
</tr>
<tr>
<td>SA</td>
<td>Security Association</td>
</tr>
<tr>
<td>SCPS</td>
<td>Space Communications Protocol Specification</td>
</tr>
<tr>
<td>SCPS-TP</td>
<td>SCPS Transport Protocol</td>
</tr>
<tr>
<td>SCTP</td>
<td>Stream Control Transmission Protocol</td>
</tr>
<tr>
<td>SEL2</td>
<td>Sun-Earth Lagrangian point 2</td>
</tr>
<tr>
<td>SFO</td>
<td>Store-and-Forward Overlay</td>
</tr>
<tr>
<td>SLE</td>
<td>Space Link Extension</td>
</tr>
<tr>
<td>SONET</td>
<td>Synchronous Optical Network</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>TC</td>
<td>Telecommand</td>
</tr>
<tr>
<td>TDM</td>
<td>Time Division Multiplexing</td>
</tr>
<tr>
<td>TDMA</td>
<td>Time Division Multiple Access</td>
</tr>
<tr>
<td>TDRSS</td>
<td>Tracking and Data Relay Satellite System</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TM</td>
<td>Telemetry</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WiMax</td>
<td>Worldwide Interoperability for Microwave Access</td>
</tr>
</tbody>
</table>