



CCSDS

The Consultative Committee for Space Data Systems

Recommendation for Space Data System Standards

IP OVER CCSDS SPACE LINKS

RECOMMENDED STANDARD

CCSDS 702.1-B-1

Note:
This current
issue includes
all updates through
Technical Corrigendum 1,
dated April 2014

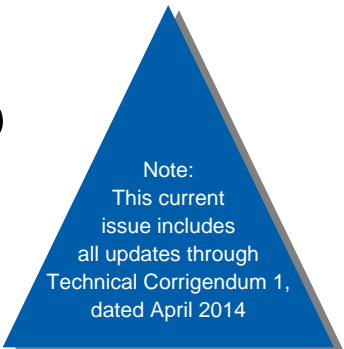
BLUE BOOK
September 2012

Recommendation for Space Data System Standards

IP OVER CCSDS SPACE LINKS

RECOMMENDED STANDARD

CCSDS 702.1-B-1



Note:
This current
issue includes
all updates through
Technical Corrigendum 1,
dated April 2014

BLUE BOOK
September 2012

AUTHORITY

Issue:	Recommended Standard, Issue 1
Date:	September 2012
Location:	Washington, DC, USA

This document has been approved for publication by the Management Council of the Consultative Committee for Space Data Systems (CCSDS) and represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS documents is detailed in *Organization and Processes for the Consultative Committee for Space Data Systems*, and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the address below.

This document is published and maintained by:

CCSDS Secretariat
Space Communications and Navigation Office, 7L70
Space Operations Mission Directorate
NASA Headquarters
Washington, DC 20546-0001, USA

STATEMENT OF INTENT

The Consultative Committee for Space Data Systems (CCSDS) is an organization officially established by the management of its members. The Committee meets periodically to address data systems problems that are common to all participants, and to formulate sound technical solutions to these problems. Inasmuch as participation in the CCSDS is completely voluntary, the results of Committee actions are termed **Recommended Standards** and are not considered binding on any Agency.

This **Recommended Standard** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommendation** is entirely voluntary. Endorsement, however, indicates the following understandings:

- o Whenever a member establishes a CCSDS-related **standard**, this **standard** will be in accord with the relevant **Recommended Standard**. Establishing such a **standard** does not preclude other provisions which a member may develop.
- o Whenever a member establishes a CCSDS-related **standard**, that member will provide other CCSDS members with the following information:
 - The **standard** itself.
 - The anticipated date of initial operational capability.
 - The anticipated duration of operational service.
- o Specific service arrangements shall be made via memoranda of agreement. Neither this **Recommended Standard** nor any ensuing **standard** is a substitute for a memorandum of agreement.

No later than three years from its date of issuance, this **Recommended Standard** will be reviewed by the CCSDS to determine whether it should: (1) remain in effect without change; (2) be changed to reflect the impact of new technologies, new requirements, or new directions; or (3) be retired or canceled.

In those instances when a new version of a **Recommended Standard** is issued, existing CCSDS-related member standards and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each member to determine when such standards or implementations are to be modified. Each member is, however, strongly encouraged to direct planning for its new standards and implementations towards the later version of the Recommended Standard.

FOREWORD

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CCSDS shall not be held responsible for identifying any or all such patent rights.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Standard is therefore subject to CCSDS document management and change control procedures, which are defined in *Organization and Processes for the Consultative Committee for Space Data Systems* (CCSDS A02.1-Y-3). 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.
- Canadian Space Agency (CSA)/Canada.
- Centre National d’Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People’s Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- China Satellite Launch and Tracking Control General, Beijing Institute of Tracking and Telecommunications Technology (CLTC/BITTT)/China.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- CSIR Satellite Applications Centre (CSIR)/Republic of South Africa.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)/Europe.
- European Telecommunications Satellite Organization (EUTELSAT)/Europe.
- Geo-Informatics and Space Technology Development Agency (GISTDA)/Thailand.
- 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 (KFKI)/Hungary.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- National Institute of Information and Communications Technology (NICT)/Japan.
- National Oceanic and Atmospheric Administration (NOAA)/USA.
- National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 702.1-B-1	IP over CCSDS Space Links, Recommended Standard, Issue 1	September 2012	Original issue
CCSDS 702.1-B-1 Cor.1 EC 1	Technical Corrigendum 1 Editorial change 1	April 2014	Cor.1: – clarifies distinction between Protocol ID space for the Encapsulation Service and IPE Header Protocol ID space. EC 1: – updates superseded references with current issues; – updates obsolescent style elements.

CONTENTS

<u>Section</u>	<u>Page</u>
1 INTRODUCTION.....	1-1
1.1 PURPOSE.....	1-1
1.2 SCOPE.....	1-1
1.3 DEFINITIONS.....	1-1
1.4 CONVENTIONS.....	1-2
1.5 REFERENCE DOCUMENTS.....	1-3
2 OVERVIEW.....	2-1
2.1 GENERAL.....	2-1
2.2 SERVICE OVERVIEW.....	2-2
2.3 FUNCTIONS OVERVIEW.....	2-2
3 SERVICE DEFINITION.....	3-1
3.1 OVERVIEW.....	3-1
3.2 SUMMARY OF PRIMITIVES.....	3-1
3.3 SUMMARY OF PARAMETERS.....	3-1
3.4 SERVICE ASSUMED FROM THE UNDERLYING SUBNETWORK.....	3-2
3.5 IPOC SERVICE PRIMITIVES.....	3-3
4 PROTOCOL DEFINITION.....	4-1
4.1 PROTOCOL DATA UNIT.....	4-1
4.2 PROTOCOL PROCEDURES AT THE SENDING END.....	4-2
4.3 PROTOCOL PROCEDURES AT THE RECEIVING END.....	4-2
ANNEX A SECURITY, SANA, AND PATENT CONSIDERATIONS (INFORMATIVE).....	A-1
ANNEX B NETWORK VIEWS (INFORMATIVE).....	B-1
ANNEX C END-TO-END UPLINK/DOWNLINK FUNCTIONAL CONTEXT DIAGRAMS (INFORMATIVE).....	C-1
ANNEX D INFORMATIVE REFERENCES (INFORMATIVE).....	D-1
ANNEX E ACRONYM LIST (INFORMATIVE).....	E-1

Figure

1-1 Bit Numbering Convention.....	1-3
2-1 Scope of IP over CCSDS Data Links.....	2-1

CONTENTS (continued)

<u>Figure</u>	<u>Page</u>
2-2 CCSDS IP Transfer Services Context Diagram	2-2
2-3 Relationship of IPE to the Encapsulation Service	2-3
4-1 IPE Header Format and Placement.....	4-1
B-1 IP over AOS VCP Service Using CCSDS IPE plus Encapsulation Service	B-1
C-1 Conceptual End-to-End Uplink CCSDS Functional Flow for Transferring IP PDUs.....	C-1
C-2 Conceptual End-to-End Downlink CCSDS Functional Flow for Transferring IP PDUs.....	C-2

Table

3-1 Recommended CCSDS Transfer Services for Transferring IP PDUs.....	3-2
---	-----

1 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to establish a CCSDS Recommended Standard specification for the implementation of Internet Protocol (IP) over CCSDS (IPoC) Space Data Link Protocols (SDLPs) in both spacecraft and ground systems by the Agencies participating in the CCSDS. In essence, this book constitutes a prescriptive profile on the one method recommended by CCSDS as the best practice for implementing IPoC.

1.2 SCOPE

This document addresses the recommended method for transferring IP Protocol Data Units (PDUs) over CCSDS space links.

1.3 DEFINITIONS

1.3.1.1 Definitions from the Open Systems Interconnection (OSI) Basic Reference Model

This document makes use of a number of terms defined in reference [1]. These terms are to be understood in a generic sense, i.e., in the sense that the terms are generally applicable to any of a variety of technologies that provide for the exchange of information between real systems. The terms are:

- a) Data Link Layer;
- b) protocol data unit;
- c) real system;
- d) service;
- e) Service Access Point (SAP);
- f) SAP address;
- g) Service Data Unit (SDU).

1.3.1.2 Definitions from OSI Service Definition Conventions

This document makes use of a number of terms defined in reference [2]. These terms are to be understood in a generic sense, i.e., in the sense that the terms are generally applicable to any of a variety of technologies that provide for the exchange of information between real systems. The terms are:

- a) indication;

- b) primitive;
- c) request;
- d) service provider;
- e) service user.

1.3.1.3 Terms Defined in This Recommended Standard

For the purposes of this document, the following definitions also apply. Many other terms that pertain to specific items are defined in the appropriate sections.

delimited: having a known (and finite) length; applies to data in the context of data handling.

IP PDU: Internet Protocol Protocol Data Unit; includes all IP data types e.g., IPV4, IPV6, compressed header IP PDUs.

Physical Channel: a stream of bits transferred over a space link in a single direction.

space link: a communications link between a spacecraft and its associated ground system or between two spacecraft. A space link consists of one or more Physical Channels in one or both directions.

1.4 CONVENTIONS

1.4.1 NOMENCLATURE

The following conventions apply for the normative specifications in this Recommended Standard:

- a) the words ‘shall’ and ‘must’ imply a binding and verifiable specification;
- b) the word ‘should’ implies an optional, but desirable, specification;
- c) the word ‘may’ implies an optional specification;
- d) the words ‘is’, ‘are’, and ‘will’ imply statements of fact.

NOTE – These conventions do not imply constraints on diction in text that is clearly informative in nature.

1.4.2 INFORMATIVE TEXT

In the normative sections of this document (sections 3 and 4), informative text is set off from the normative specifications either in notes or under one of the following subsection headings:

- Overview;
- Background;
- Rationale;
- Discussion.

1.4.3 BIT NUMBERING

In this document, the following convention is used to identify each bit in an N -bit field. The first bit in the field to be transmitted (i.e., the most left justified when drawing a figure) is defined to be ‘Bit 0’; the following bit is defined to be ‘Bit 1’ and so on up to ‘Bit $N-1$ ’. When the field is used to express a binary value (such as a counter), the Most Significant Bit (MSB) shall be the first transmitted bit of the field, i.e., ‘Bit 0’ (see figure 1-1).

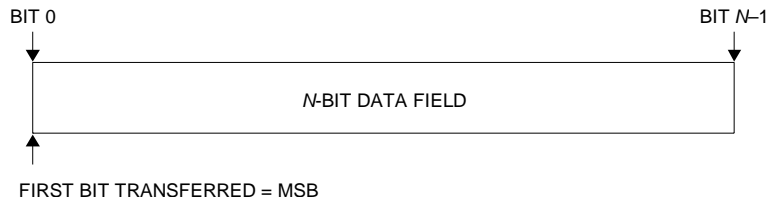


Figure 1-1: Bit Numbering Convention

In accordance with standard data-communications practice, data fields are often grouped into eight-bit ‘words’ that conform to the above convention. Throughout this Recommended Standard, such an eight-bit word is called an ‘octet’.

The numbering for octets within a data structure starts with zero. By CCSDS convention, all ‘spare’ bits shall be permanently set to ‘0’.

1.5 REFERENCE DOCUMENTS

The following publications contain provisions which, through reference in this text, constitute provisions of this document. At the time of publication, the editions indicated were valid. All publications are subject to revision, and users of this document are encouraged to investigate the possibility of applying the most recent editions of the publications indicated below. The CCSDS Secretariat maintains a register of currently valid CCSDS publications.

- [1] *Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*. 2nd ed. International Standard, ISO/IEC 7498-1:1994. Geneva: ISO, 1994.

- [2] *Information Technology—Open Systems Interconnection—Basic Reference Model—Conventions for the Definition of OSI Services*. International Standard, ISO/IEC 10731:1994. Geneva: ISO, 1994.
- [3] *Encapsulation Service*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 133.1-B-2. Washington, D.C.: CCSDS, October 2009.
- [4] *AOS Space Data Link Protocol*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 732.0-B-2. Washington, D.C.: CCSDS, July 2006.
- [5] *TM Space Data Link Protocol*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 132.0-B-1. Washington, D.C.: CCSDS, September 2003.
- [6] *TC Space Data Link Protocol*. Recommendation for Space Data System Standards, CCSDS 232.0-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, September 2010.
- [7] *Proximity-1 Space Link Protocol—Data Link Layer*. Issue 5. Recommendation for Space Data System Standards (Blue Book), CCSDS 211.0-B-5. Washington, D.C.: CCSDS, December 2013.
- [8] “Space Assigned Number Authority (SANA) Registry: Internet Protocol Extension Header.” Space Assigned Numbers Authority. Consultative Committee for Space Data Systems. http://sanaregistry.org/r/ipe_header/.

NOTE – Informative references are provided in annex D.

2 OVERVIEW

2.1 GENERAL

This document describes the recommended method for transferring IP PDUs over CCSDS SDLPs: Telecommand (TC), Telemetry (TM), Advanced Orbiting Systems (AOS), and Proximity-1 (Prox-1). IP PDUs are transferred by encapsulating them, one-for-one, within CCSDS Encapsulation Packets. The Encapsulation Packets are transferred directly within one or more CCSDS SDLP Transfer Frames. This method uses the CCSDS Internet Protocol Extension (IPE) convention in conjunction with the CCSDS Encapsulation Service over CCSDS AOS, TM, or TC Virtual Channel Packet (VCP) Service, TC Multiplexer Access Point Packet (MAPP) Service, or Prox-1.

The CCSDS IPE convention is to prepend the CCSDS IPE octet(s) to each IP PDU, encapsulate the result in a CCSDS Encapsulation Packet (see reference [3]), and transport the Encapsulation Packet within one or more CCSDS SDLP frames (see references [4]-[7] and figure 2-1). This method is recommended for all IP PDUs identified in reference [8].

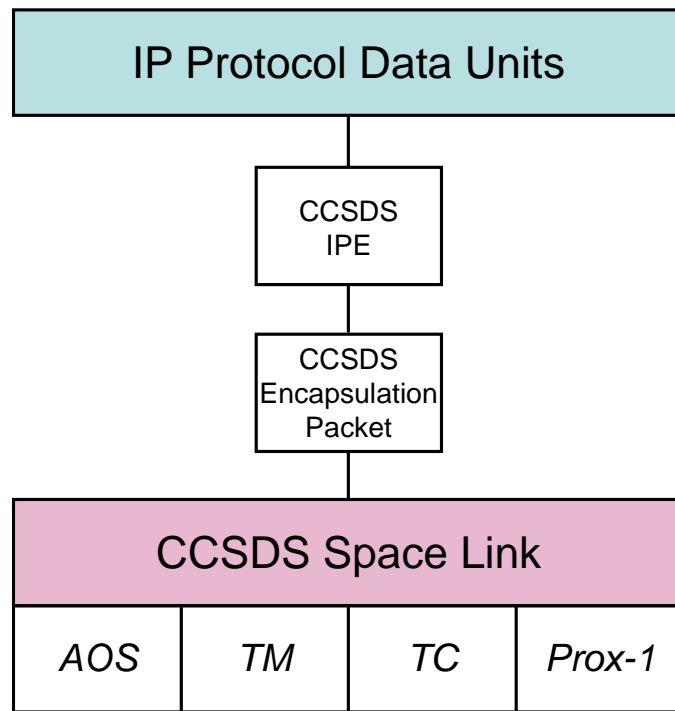


Figure 2-1: Scope of IP over CCSDS Data Links

2.2 SERVICE OVERVIEW

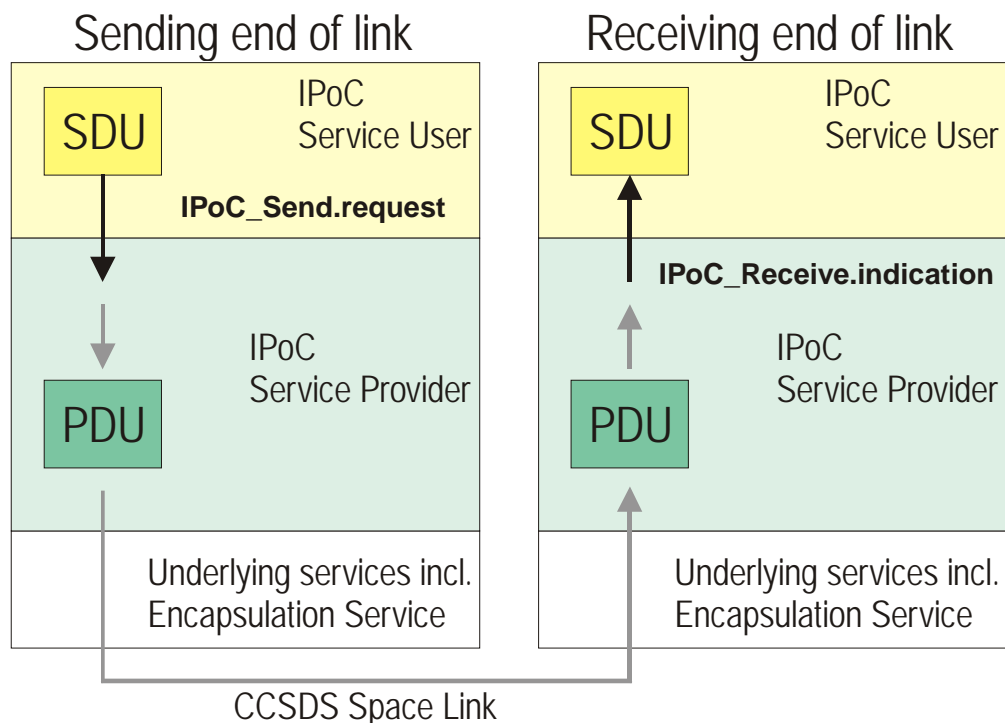


Figure 2-2: CCSDS IP Transfer Services Context Diagram

Figure 2-2 describes the interface between the service user, which provides the SDU, and the service provider, which performs the service of transferring the PDU across the space link. The service user provides an IP PDU as the SDU along with its associated IPE header value (values defined in reference [8]) and its associated Data Link Layer routing information (i.e., Space Data Link Protocol Channel [SDLP_Channel]) to the service provider.

2.3 FUNCTIONS OVERVIEW

It is the task of the IPoC service provider to generate the IPE header and prepend it to the IP PDU on the sending end. On the receiving end, the IPoC service provider extracts the IPE header and uses the IPE value to route the IP PDU to the applicable IP protocol handler for transfer across the receiving end.

2.4 IPE CONCEPT AND RATIONALE

2.4.1 GENERAL

The primary purpose of the CCSDS IPE convention is to provide an interoperable way of identifying the Internet protocols being encapsulated by the CCSDS Encapsulation Service

(reference [3]) when this service is being used to provide a Data Link Layer for IP. The IPE header uses one and optionally more than one shim octet to logically extend the CCSDS Encapsulation Packet header. Reference [8] lists the CCSDS recommended protocols to be encapsulated and their enumerations for the content of the IPE header.

Using this convention, the Encapsulation service provides a Data Link Layer for the IP protocols identified in reference [8]. IPE uses the Encapsulation service primitives defined and the service described in reference [3]. The additional service provided through the IPE is a protocol multiplexing/demultiplexing capability.

The IPE convention allows demultiplexing of subprotocols used in IP. It provides a unique protocol ID space distinct from that used by the Encapsulation Service itself. This abstracts, and allows the separation of, protocols originally supported by the Encapsulation Service and IP data transfer over it. No additional processing is performed at the multiplexing/demultiplexing layer affiliated with the IPE convention. The multiplexing/demultiplexing services know nothing of the formats or conventions of the protocols they are multiplexing or demultiplexing.

NOTE – The Relationship of IPE to the Encapsulation Service is shown in figure 2-3.

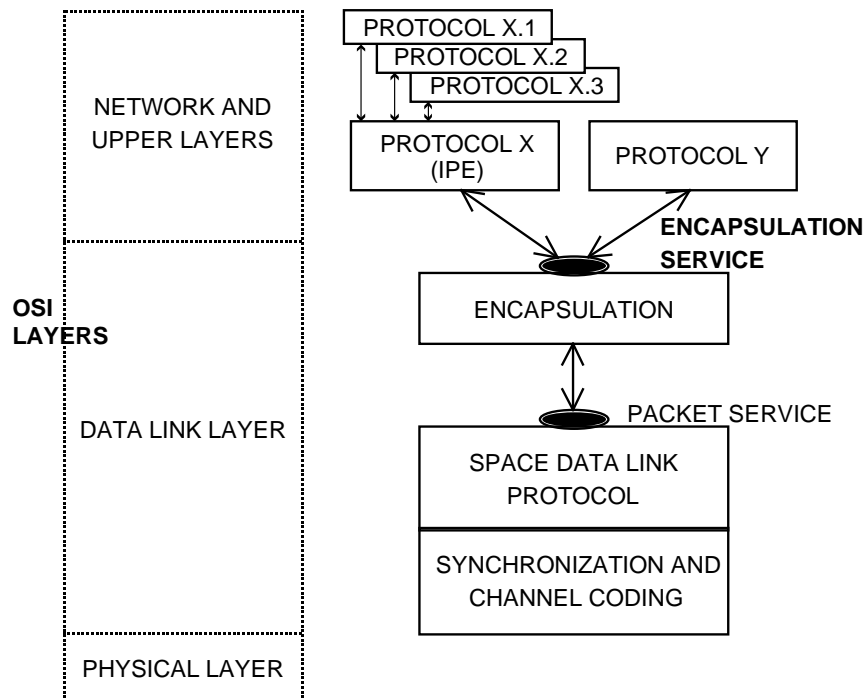


Figure 2-3: Relationship of IPE to the Encapsulation Service

2.4.2 IPE HEADER ENUMERATIONS AND MAPPINGS

There often are many IP data types that require encapsulation. The exact number of protocols depends on the mission and its requirements. These protocols are fully defined in other data standards. Thus the intent here is to identify only auxiliary PDU formats that are often used in support of IP. As a comparison, serial links between routers often carry the 16-bit Point-to-Point Protocol (PPP) protocol field, and the Ethernet PDUs carry a 16-bit Ethernet type field. In these cases, the enumerations of the protocols are defined by the Internet Assigned Numbers Authority (IANA) and the Institute of Electrical and Electronics Engineers (IEEE), respectively. The tables containing the enumerations then point to the standards that define the protocols themselves.

The alternative approach would have been to encapsulate a conventional link layer, such as Multiprotocol over Frame Relay, and use its methods for identifying the auxiliary PDU formats.

Auxiliary protocols nominally identified at the Data Link Layer in support of IP include IPv4, IPv6, IP compressed header formats, the address resolution protocol for multi-access link layers, link layer control protocols including link metrics exchange and link health monitoring, various Data Link and Network Layer configuration protocols, and authentication protocols.

Addressing and routing protocols often tie into these protocols via initial configuration exchanges and link state up/down information. It should be noted, however, that routing protocols such as Open Shortest Path First (OSPF), Protocol-Independent Multicast (PIM), and Border Gateway Protocol (BGP) also maintain their own adjacency or state via hello exchanges or refreshes at the Network Layer.

Most of these protocols are built around bidirectional links and require bidirectional exchanges. Since in the space environment it is expected that Network Layer protocols will have to be able to use one-way links, it is not recommended that these protocols be required. It is believed that if fairly simple networks are involved, and they are monitored in a transparent manner, it is possible to use prearranged static settings rather than dynamic exchanges to verify and maintain correct configuration. However, if appropriate for the mission, use of these protocols is not prohibited.

3 SERVICE DEFINITION

3.1 OVERVIEW

This section provides service definition in the form of primitives, which present an abstract model of the logical exchange of data and control information between the service provider and the service user. The definitions of primitives are independent of specific implementation approaches.

When the IPoC service is used for the transfer of IP PDUs, then

- the IPoC service SDU is the IP PDU;
- the IPoC service PDU is the IPE Header + IP PDU.

The parameters of the primitives are specified in an abstract sense and specify the information to be made available to the user of the primitive. The way in which a specific implementation makes this information available is not constrained by this specification. In addition to the parameters specified in this section, an implementation may provide other parameters to the service user (e.g., parameters for controlling the service, monitoring performance, facilitating diagnosis, and so on).

3.2 SUMMARY OF PRIMITIVES

The IPoC service shall consume the following primitives:

- **IPoC_Send.request;**
- **IPoC_Receive.indication.**

3.3 SUMMARY OF PARAMETERS

3.3.1 The **Unitdata** parameter is the SDU transferred by the IPoC service:

- it shall contain a delimited, octet-aligned IP PDU;
- the maximum length of an IP PDU accommodated by this service shall be constrained by the maximum SDU size of the underlying Encapsulation Service minus the size of the IPE Header used by this service.

NOTE – The maximum value of the Encapsulation Service SDU is given by the Maximum Data Unit Length managed parameter of the Encapsulation Service (section 5 of reference [3]).

3.3.2 The **IPE_Header_Value** parameter shall contain one of the values specified in reference [8].

NOTE – The IPE header is an extension to the Encapsulation Packet header in that it effectively expands the number of IP protocols that can have a standardized definition for transport over CCSDS Space Data Links.

3.3.3 The **SDLP_Channel** parameter shall identify the SAP of the underlying CCSDS Data Link Layer service:

- for Encapsulation over VCP services of TM, TC, or AOS: GVCID;
- for MAPP service of TC: GVCID and MAP ID;
- for Prox-1: TFDN, SCID, Port ID, DFC_ID and Physical Channel ID (PCID).

3.4 SERVICE ASSUMED FROM THE UNDERLYING SUBNETWORK

3.4.1 OVERVIEW

CCSDS Encapsulation Service (ENCAP) is the exclusive CCSDS service for transferring IP PDUs across the CCSDS space link. Table 3-1 describes the CCSDS recommended IP transfer service over AOS, TM, TC, and Prox-1 SDLPs. The Encapsulation Packet is the only recommended CCSDS packet type to encapsulate IP PDUs. Therefore the Packet Version Number (PVN) can only equal ‘Encapsulation packet’, i.e., binary ‘111’.

Table 3-1: Recommended CCSDS Transfer Services for Transferring IP PDUs

CCSDS Transfer Service	Applicable Space Data Link	SAP Address	SDU
Encapsulation	AOS, TM, TC, Prox-1	SDLP_Channel	Packet

3.4.2 CCSDS ENCAPSULATION SERVICE

3.4.2.1 The CCSDS Encapsulation Packet specified in reference [3] shall be used to encapsulate the IPE header and IP PDU for transfer over the CCSDS Space Data Link.

3.4.2.2 One CCSDS Encapsulation Packet shall contain one IPE header and one IP PDU.

NOTE – Since the Encapsulation Packet is the only CCSDS recommended packet type to carry an IPE header and IP PDU, and it is the only CCSDS recommended data structure to carry an IP PDU, the Encapsulation Packet is the only packet type that CCSDS recommends for the transport of IP PDUs.

3.4.2.3 There are no restrictions on the use of an Encapsulation Packet to carry the IPE header and IP PDU.

3.4.2.4 Only CCSDS AOS, TM, TC, and Prox-1 Transfer Frames shall be used to carry a CCSDS Encapsulation Packet containing an IPE header and IP PDU.

3.4.2.5 There are no restrictions on the use of an AOS, TM, TC, or Prox-1 transfer frame to carry an Encapsulated IP PDU.

3.4.2.6 For transferring IP datagrams over the CCSDS Space Link, the Encapsulation Packet Protocol ID shall be set to the value for the IPE ID, i.e., '010'.

NOTE – The Protocol ID space for the Encapsulation Service (see reference [D2]) is distinct from that of the IPE Header Protocol ID space (see reference [8]).

3.5 IPOC SERVICE PRIMITIVES

3.5.1 IPOC_SEND.REQUEST

3.5.1.1 Function

The **IPoC_Send.request** primitive shall be used by the user IP entity to request delivery of an IP PDU to a remote IP entity.

3.5.1.2 Semantics

IPoC_Send.request shall provide parameters as follows:

IPoC_Send.request (Unitdata, IPE_Header_Value, SDLP_Channel)

3.5.1.3 When Generated

IPoC_Send.request is generated by the IPoC user at any time.

3.5.1.4 Effect on Receipt

Receipt of **IPoC_Send.request** causes the IPOC entity to initiate the procedures described in 4.2.

3.5.1.5 Additional Comments

None.

3.5.2 IPOC_RECEIVE.INDICATION

3.5.2.1 Function

The **IPoC_Receive.indication** primitive shall be used to deliver an IP PDU to the user Internet Protocol entity.

3.5.2.2 Semantics

IPoC_Receive.indication shall provide parameters as follows:

IPoC_Receive.indication (Unitdata, IPE_Header_Value, SDLP_Channel)

3.5.2.3 When Generated

IPoC_Receive.indication is generated by the IPoC entity in response to the arrival of an IPoC PDU.

3.5.2.4 Effect on Receipt

The effect of receipt of **IPoC_Receive.indication** on the IPoC user is undefined.

3.5.2.5 Additional Comments

None.

4 PROTOCOL DEFINITION

4.1 PROTOCOL DATA UNIT

4.1.1 The IP PDU to be encapsulated shall follow, without gap, the IPE header.

4.1.2 The concatenation of IPE header and IP PDU shall be the Data Unit parameter of the Encapsulation Service (see reference [7], section 3).

NOTES

- 1 The Encapsulation Packet length field in the Encapsulation Packet header consists of the sum of the sizes of the Encapsulation Packet header, the IPE header, and the PDU to be encapsulated.
- 2 The format and placement of the IPE header are shown in figure 4-1.

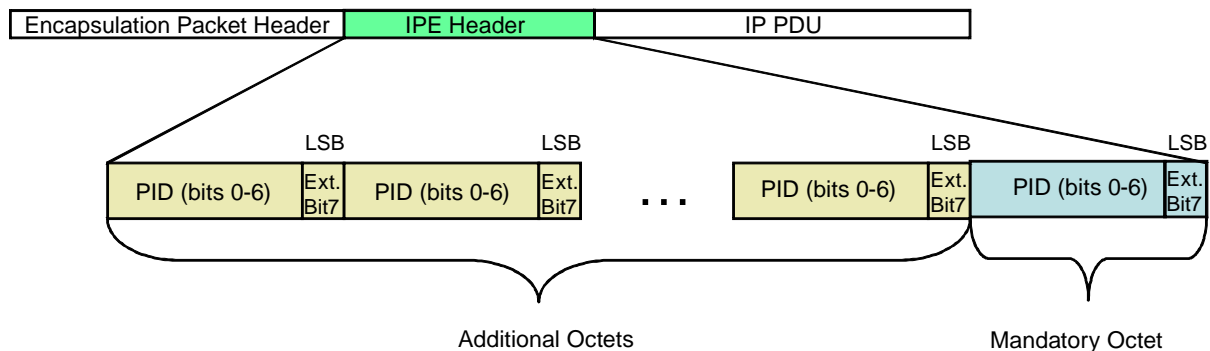


Figure 4-1: IPE Header Format and Placement

4.1.3 The IPE header shall be an integral number of octets in length, with a minimum length of one octet.

4.1.4 Bit and octet ordering of the IPE header shall follow the conventions given in 1.4.3.

4.1.5 The IPE header shall be extendable by adding more significant octets to the first octet. The use of one or more additional octets is signaled by setting the LSB of each octet of the header except the final (least significant) octet to '0'; the LSB of the IPE header shall be set to '1'.

EXAMPLE – For an IPE header value of 33 (decimal) for a two octet header, the most significant octet would contain all zeros.

4.1.6 The IPE header shall be interpreted as an unsigned integer value, per the convention given in 1.4.3.

4.1.7 The IPE header shall contain one of the values given in reference [8].

4.1.8 The IPE header value shall be the decimal value of the contents of the entire IPE header.

NOTE – Only the odd IPE header values are valid, since the LSB of the least significant octet must have a value of ‘1’.

If the IPE header consists of a single octet, then only odd IPE header values from 1 to 255 are valid.

If the IPE header consists of two or more octets, then

- odd IPE header values from 1 to 255 are valid;
- no IPE header values from 256 to 511 are valid (since the value of the LSB in the second least significant octet must have a value of ‘0’);
- odd IPE header values from 513 to 767 are valid;
- no IPE header values from 768 to 1023 are valid (since the value of the LSB in the second least significant octet must have a value of ‘0’).

This pattern continues across the entire IPE header space.

4.2 PROTOCOL PROCEDURES AT THE SENDING END

The IPoC entity at the sending end shall:

- build the IPE Header relevant to the given IP PDU received from the user, as defined by the IPE_Header_Value parameter;
- prepend the IPE Header to the IP PDU;
- pass this result to the Encapsulation Service as the SDU.

4.3 PROTOCOL PROCEDURES AT THE RECEIVING END

The IPoC entity at the receiving end shall:

- receive the SDU from the Encapsulation Service;
- extract and decode the IPE Header;
- deliver the IP PDU to the user.

ANNEX A

SECURITY, SANA, AND PATENT CONSIDERATIONS

(INFORMATIVE)

A1 SECURITY CONSIDERATIONS

A1.1 SECURITY BACKGROUND

It may be required that security services be applied to the payloads carried by IP datagrams over CCSDS space links. The specification of such security services is outside the scope of this document but is discussed in the following subsections.

If there is a reason to believe that non-authorized entities might be able to view or obtain the payload data, and if there is a need to ensure that non-authorized entities not be able to view or obtain the data, then confidentiality needs to be applied. If there is a need to ensure that the payload data has not been modified in transit without such modification being recognized, then integrity needs to be applied. If the authenticity of the source of the payload data is required (e.g., the payload contains a command), then authentication needs to be applied. It is possible for a single datagram to require all three security services to ensure that the payload is not disclosed, not altered, and authentic.

A1.2 SECURITY CONCERNS

As stated in the previous subsection, various security services might need to be applied to the IP datagram depending on the threat, the mission security policy(s), and the desire of the mission planners. While these security concerns are valid, they are outside the scope of this document. This document assumes that either upper or lower layers of the OSI model will provide the security services. That is, if authenticity at the granularity of a specific user is required, it is best applied at the Application Layer. If less granularity is required, it could be applied at the Network or Data Link Layers. If integrity is required, it can be applied at either the Application, Network, or Data Link Layer. If confidentiality is required, it can be applied at either the Application Layer, the Network Layer, or the Data Link Layer. Reference [D1] provides more information regarding the choice of service and where it can be implemented.

A1.3 POTENTIAL THREATS AND ATTACK SCENARIOS

Without authentication, unauthorized commands or software might be uploaded to a spacecraft or data retrieved from a source masquerading as the spacecraft. Without integrity, corrupted commands or software might be uploaded to a spacecraft. Without integrity, corrupted telemetry might be retrieved from a spacecraft, and the result could be that an

incorrect course of action is taken. Sensitive or private information might be disclosed to an eavesdropper if confidentiality is not applied to the data.

A1.4 CONSEQUENCES OF NOT APPLYING SECURITY

The security services are out of scope of this document and should be applied at layers above or below those specified in this document. However, should there be a requirement for authentication, and if it is not implemented, unauthorized commands or software might be loaded onto a spacecraft. If integrity is not implemented, erroneous commands or software might be loaded onto a spacecraft, potentially resulting in the loss of the mission. If confidentiality is not implemented, data flowing to or from a spacecraft might be visible to unauthorized entities, resulting in disclosure of sensitive or private information.

A2 SANA CONSIDERATIONS

The specifications of this Recommended Standard do not require any action from SANA.

A3 PATENT CONSIDERATIONS

The specifications of this Recommended Standard are not known to be the subject of patent rights.

ANNEX B

NETWORK VIEWS

(INFORMATIVE)

This annex contains an example protocol stack recommending how to transfer IP over the CCSDS AOS SDLP depending upon the routing capability and needs of the on-board network. It could be noted that the diagram is bidirectional.

IP over AOS VCP Service using CCSDS Encapsulat on Service

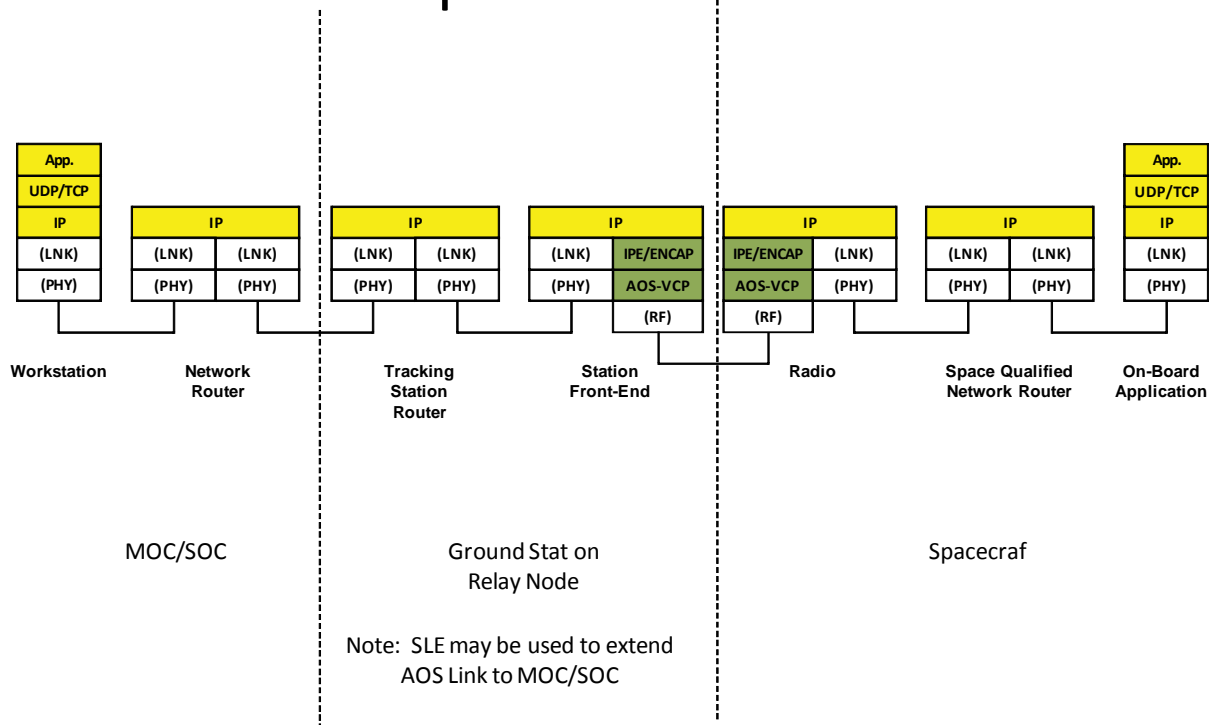


Figure B-1: IP over AOS VCP Service Using CCSDS IPE plus Encapsulation Service

ANNEX C

END-TO-END UPLINK/DOWNLINK
FUNCTIONAL CONTEXT DIAGRAMS

(INFORMATIVE)

Figure C-1 describes the end-to-end information system processing functions needed to transfer IP PDUs on the uplink.

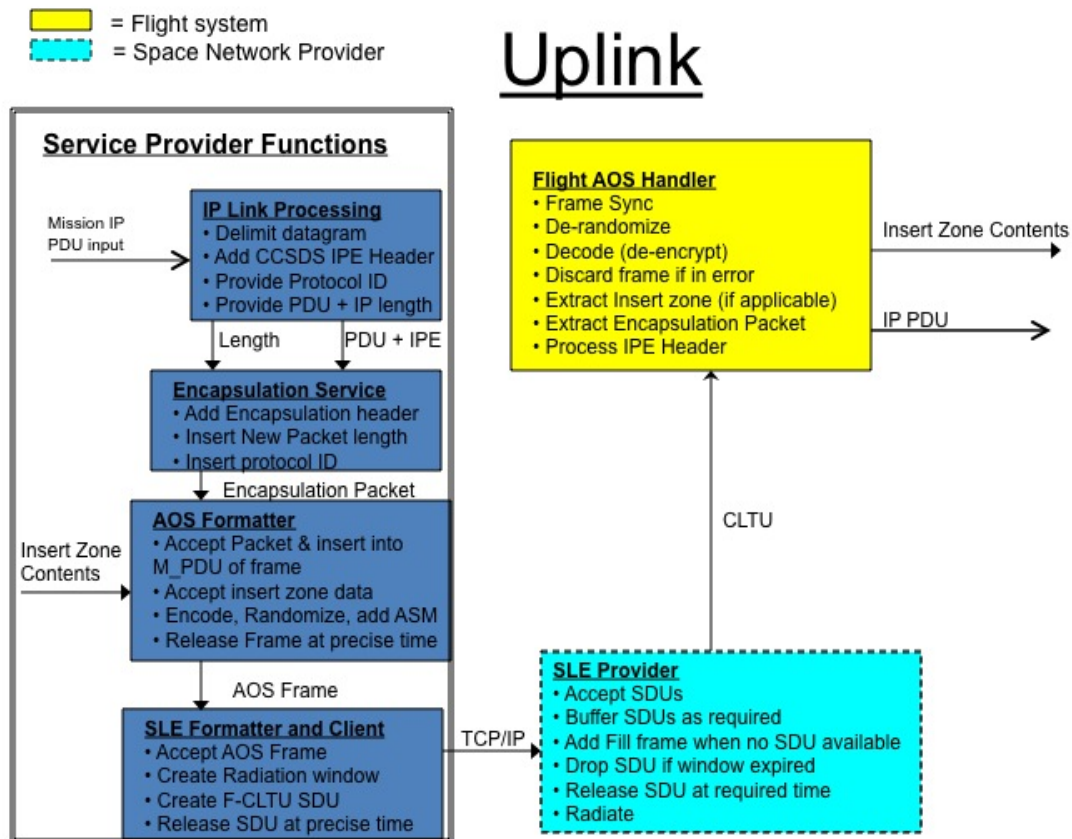


Figure C-1: Conceptual End-to-End Uplink CCSDS Functional Flow for Transferring IP PDUs

Figure C-2 describes the end-to-end information system processing functions needed to transfer IP PDUs on the downlink.

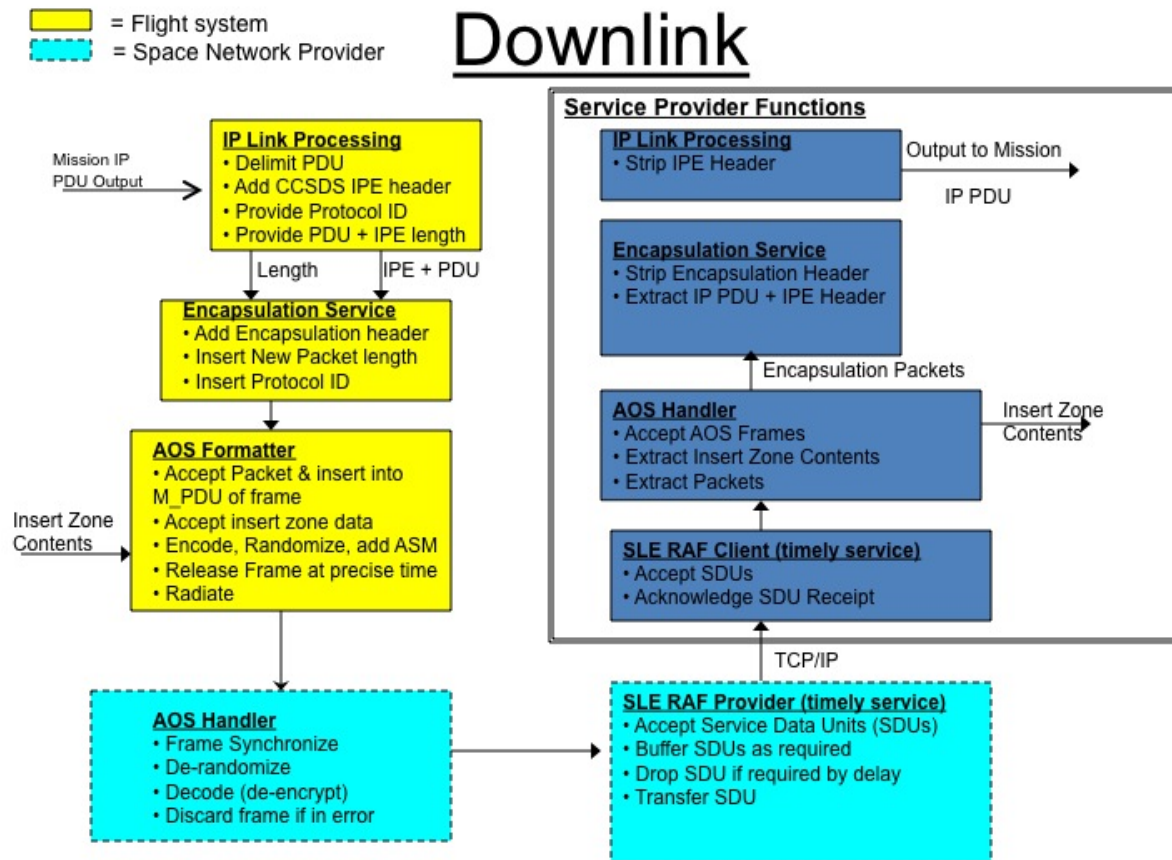


Figure C-2: Conceptual End-to-End Downlink CCSDS Functional Flow for Transferring IP PDUs

ANNEX D

INFORMATIVE REFERENCES

(INFORMATIVE)

- [D1] *The Application of CCSDS Protocols to Secure Systems*. Issue 2. Report Concerning Space Data System Standards (Green Book), CCSDS 350.0-G-2. Washington, D.C.: CCSDS, January 2006.
- [D2] “Space Assigned Number Authority (SANA) Registry: Protocol Identifier for Encapsulation Service.” Space Assigned Numbers Authority. Consultative Committee for Space Data Systems. http://sanaregistry.org/r/protocol_id/.

NOTE – Normative references are provided in 1.5.

ANNEX E

ACRONYM LIST

(INFORMATIVE)

AOS	Advanced Orbiting Systems
CCSDS	Consultative Committee for Space Data System
DFC_ID	Data Field Construction Identifier
ENCAP	Encapsulation (Packet Service)
GVCID	Global Virtual Channel Identifier
IP	Internet Protocol
IPE	Internet Protocol Extension
IPoC	IP over CCSDS
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
MAP ID	Multiplexer Access Point Identifier
MAPP	Multiplexer Access Point Packet (Service)
MSB	Most Significant Bit
OSI	Open Systems Interconnection
PDU	Protocol Data Unit
Prox-1	Proximity-1
PVN	Packet Version Number
RFC	Request for Comment
SANA	Space Assigned Numbers Authority
SAP	Service Access Point
SDLP	Space Data Link Protocol
SDLP_Channel	Space Data Link Protocol Channel
SDU	Service Data Unit

TC	Telecommand (pertains to TC SDLP)
TFVN	Transfer Frame Version Number
TM	Telemetry (pertains to TM SDLP)
VCP	Virtual Channel Packet (Service)
SCID	Spacecraft ID
PCID	Physical Channel ID