The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Practices

IP OVER CCSDS SPACE LINKS

DRAFT RECOMMENDED PRACTICE

CCSDS 702.1-R-4

RED BOOK
April 2010

The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Practices

IP OVER CCSDS SPACE LINKS

DRAFT RECOMMENDED PRACTICE

CCSDS 702.1-R-4

RED BOOK

April 2010

AUTHORITY

Issue:	Red Book, Issue 4
Date:	April 2010
Location:	Not Applicable

(WHEN THIS RECOMMENDED PRACTICE 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 represents the consensus technical agreement of the participating CCSDS Member Agencies. The procedure for review and authorization of CCSDS documents is detailed in the *Procedures Manual 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

(WHEN THIS RECOMMENDED PRACTICE IS FINALIZED, IT WILL CONTAIN THE FOLLOWING 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 **Recommendations** and are not in themselves considered binding on any Agency.

CCSDS Recommendations take two forms: **Recommended Standards** that are prescriptive and are the formal vehicles by which CCSDS Agencies create the standards that specify how elements of their space mission support infrastructure shall operate and interoperate with others; and **Recommended Practices** that are more descriptive in nature and are intended to provide general guidance about how to approach a particular problem associated with space mission support. This **Recommended Practice** is issued by, and represents the consensus of, the CCSDS members. Endorsement of this **Recommended Practice** is entirely voluntary and does not imply a commitment by any Agency or organization to implement its recommendations in a prescriptive sense.

No later than five years from its date of issuance, this **Recommended Practice** 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 Practice** is issued, existing CCSDS-related member Practices and implementations are not negated or deemed to be non-CCSDS compatible. It is the responsibility of each member to determine when such Practices or implementations are to be modified. Each member is, however, strongly encouraged to direct planning for its new Practices and implementations towards the later version of the Recommended Practice.

FOREWORD

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 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.
- 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.

Observer Agencies

- Austrian Space Agency (ASA)/Austria.
- Belgian Federal Science Policy Office (BFSPO)/Belgium.
- Central Research Institute of Machine Building (TsNIIMash)/Russian Federation.
- Centro Tecnico Aeroespacial (CTA)/Brazil.
- Chinese Academy of Sciences (CAS)/China.
- Chinese Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/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 (KFKI)/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 and Atmospheric Administration (NOAA)/USA.
- National Space Organization (NSPO)/Chinese Taipei.
- Naval Center for Space Technology (NCST)/USA.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- United States Geological Survey (USGS)/USA.

PREFACE

This document is a draft CCSDS Recommended Practice. Its draft status indicates that the CCSDS believes the document to be technically mature and has released it for formal review by appropriate technical organizations. As such, its technical contents are not stable, and several iterations of it may occur in response to comments received during the review process.

Implementers are cautioned **not** to fabricate any final equipment in accordance with this document's technical content.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 702.1-R-1	IP Over CCSDS Space Links, Draft Recommended Practice, Issue 1	October 2006	Superseded
CCSDS 702.1-R-2	IP Over CCSDS Space Links, Draft Recommended Practice, Issue 2	January 2007	Superseded
CCSDS 702.1-R-3	IP over CCSDS Space Links, Draft Recommended Practice, Issue 3	September 2008	Superseded
CCSDS 702.1-R-4	IP over CCSDS Space Links, Draft Recommended Practice, Issue 4	April 2010	Current draft (note): – replaces options recommended in previous issues with a single recommended method for transferring IP PDUs; – reflects changes in Recommended Standards whose provisions are cited in this Recommended Practice.

NOTE – Changes in this version are too numerous to permit markup/change bars.

CONTENTS

Section Page

1 INTRODUCTION 1-1

1.1 PURPOSE 1-1
1.2 SCOPE 1-1
1.3 CONVENTIONS AND DEFINITIONS 1-2
1.4 REFERENCE DOCUMENTS 1-4

2 OVERVIEW OF TRANSFERRING IP PDUS OVER CCSDS LINK SERVICES 2-1

2.1 GENERAL 2-1
2.2 SERVICE INTERFACE 2-1

3 PDU FORMATS 3-1

3.1 OVERVIEW 3-1
3.2 AOS TRANSFER FRAME 3-1
3.3 TM TRANSFER FRAME 3-3
3.4 TC TRANSFER FRAME 3-4
3.5 PROXIMITY-1 TRANSFER FRAME 3-6
3.6 ENCAPSULATION PACKET STRUCTURE 3-8
3.7 CCSDS INTERNET PROTOCOL EXTENSION (IPE) 3-11
3.8 ISINTERNET PROTOCOL EXTENSION SPECIFICATION 3-12

4 SERVICE PRIMITIVES 4-1

4.1 BASIC MODEL 4-1
4.2 SERVICE PRIMITIVES 4-2

ANNEX A SECURITY (INFORMATIVE) 4-1
ANNEX B MANAGED PARAMETERS FOR CCSDS IP TRANSFER SERVICES (INFORMATIVE) B-1
ANNEX C NETWORK VIEWS (INFORMATIVE) C-1
ANNEX D END-TO-END UPLINK/DOWNLINK FUNCTIONAL CONTEXT DIAGRAMS (INFORMATIVE) D-1
ANNEX E INFORMATIVE REFERENCES (INFORMATIVE) E-1
ANNEX F ACRONYM LIST (INFORMATIVE) F-1

CONTENTS (continued)

Figure Page

1-1 Scope of IP over CCSDS Data Links 1-1
1-2 Bit Numbering Convention 1-4
2-1 Recommended Method for Transferring IP over CCSDS Data Links 2-1
2-2 CCSDS IP Transfer Services Context Diagram 2-2
2-3 Identifiers and Channels Used in the SDLP_Channel Parameter 2-3
2-4 Multiplexing SDUs over AOS Frames 2-6
2-5 Multiplexing SDUs over TM Frames 2-7
2-6 Multiplexing SDUs over TC Frames 2-8
2-7 Multiplexing SDUs over Proximity-1 Frames 2-10
2-8 Concept of Encapsulation Service 2-11
3-1 End-to-End Hierarchy Diagram of IP over CCSDS IPE/Encap 3-1
3-2 AOS Transfer Frame 3-2
3-3 AOS Transfer Frame Primary Header 3-2
3-4 Multiplexing Protocol Data Unit (M_PDU) 3-3
3-5 TM Transfer Frame 3-3
3-6 TM Transfer Frame Primary Header 3-4
3-7 TC Frame Structure 3-5
3-8 TC Frame Primary Header 3-5
3-9 Proximity-1 Transfer Frame 3-6
3-10 Proximity-1 Transfer Frame Header 3-7
3-11 Encapsulation Packet Structural Components 3-8
3-12 Encapsulation Packet Header 3-9
3-13 IPE Header Format and Placement 3-12
4-1 Encapsulation Service Primitives 4-1
C-1 IPv4 over AOS VCP Service Using CCSDS IPE plus Encapsulation Service C-1
C-2 IPv6 over AOS VCP Service Using CCSDS ICE plus Encapsulation Service C-2
D-1 End-to-End Uplink CCSDS Functional Flow for Transferring IP Datagrams D-1
D-2 End-to-End Downlink CCSDS Functional Flow for Transferring IP Datagrams D-2

Table

2-1 Recommended CCSDS IPv4 Transfer Services 2-4
2-2 Key Characteristics of CCSDS Link Layer Protocols 2-5
3-1 Encapsulation Packet Lengths, Depending on the Length of the Packet Header 3-10
3-2 Enumerations for the IPE Header Values 3-14
4-1 Encapsulation Packet Service Primitives 4-2
B-1 Virtual Channel Managed Parameters B-1
B-2 Managed Parameters for Packet Transfer B-1
B-3 Managed Parameters for Encapsulation Service B-2

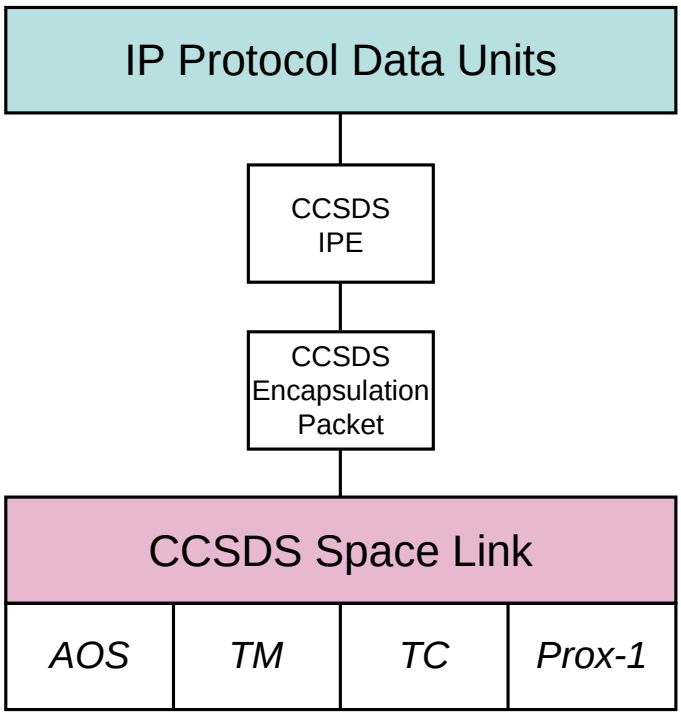
1 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to establish a CCSDS Recommended Practice specification for the implementation of IP over CCSDS Space Data Link layer protocols in both spacecraft and ground systems by the Agencies participating in the CCSDS.

1.2 SCOPE

This document addresses the recommended method for transferring IP Protocol Data Units (PDUs) over CCSDS space links. That method is to prepend the CCSDS Internet Protocol Extension (IPE) byte(s) (see reference [8]) to each IP PDU, encapsulate the result in CCSDS Encapsulation Packets (see reference [7]), and transport the Encapsulation Packets within a CCSDS space link protocol frames (see references [3]-[6] and figure 1-1). This method is recommended for all IP PDUs identified in annex A of reference [8].



NOTE – All CCSDS-recognized IP subprotocols are defined in annex A of reference [8].

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

1.3 CONVENTIONS AND DEFINITIONS

1.3.1 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]. The use of those terms in this document shall be understood in a generic sense; i.e., in the sense that those terms are generally applicable to any of a variety of technologies that provide for the exchange of information between real systems. Those terms are:

a) blocking;

b) connection;

c) Data Link Layer;

d) entity;

e) flow control;

f) protocol data unit;

g) real system;

h) segmenting;

i) service;

j) Service Access Point (SAP);

k) SAP address;

l) service data unit.

1.3.1.2 Definitions from OSI Service Definition Conventions

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

a) confirmation;

b) indication;

c) primitive;

d) request;

e) response;

f) service provider;

g) service user.

1.3.1.3 Terms Defined in This Recommended Practice

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.

asynchronous: not *synchronous* (see below).

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.

Mission Phase: a period of a mission during which specified communications characteristics are fixed. The transition between two consecutive Mission Phases may cause an interruption of the communications services.

periodic: of or pertaining to a sequence of events in which each event occurs at a fixed time interval (within specified tolerance) after the previous event in the sequence.

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.

synchronous: of or pertaining to a sequence of events occurring in a fixed time relationship (within specified tolerance) to another sequence of events. Note that 'synchronous' does not necessarily imply 'periodic' or 'constant rate'.

1.3.2 NOMENCLATURE

The following conventions apply throughout this document:

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.

1.3.3 CONVENTIONS

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 1-2).

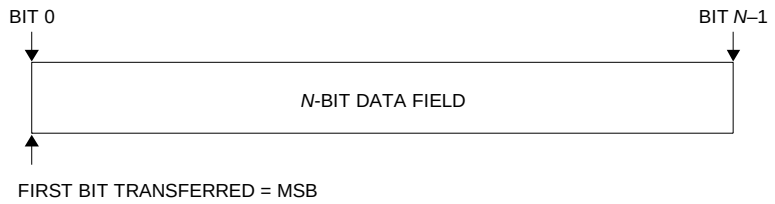


Figure 1-2: Bit Numbering Convention

In accordance with standard data-communications practice, data fields are often grouped into eight-bit 'words' which conform to the above convention. Throughout this Recommended Practice, 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'.

1.4 REFERENCE DOCUMENTS

The following documents contain provisions which, through reference in this text, constitute provisions of this Recommended Practice. At the time of publication, the editions indicated were valid. All documents are subject to revision, and users of this Recommended Practice 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 Documents.

[1] *Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*. International Standard, ISO/IEC 7498-1. 2nd ed. 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] *AOS Space Data Link Protocol*. Recommendation for Space Data System Standards, CCSDS 732.0-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, July 2006.

[4] *TM Space Data Link Protocol*. Recommendation for Space Data System Standards, CCSDS 132.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, September 2003.

[5] *TC Space Data Link Protocol*. Recommendation for Space Data System Standards, CCSDS 232.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, September 2003.

[6] *Proximity-1 Space Link Protocol—Data Link Layer*. Recommendation for Space Data System Standards, CCSDS 211.0-B-4. Blue Book. Issue 4. Washington, D.C.: CCSDS, July 2006.

[7] *Encapsulation Service*. Recommendation for Space Data System Standards, CCSDS 133.1-B-2. Blue Book. Issue 2. Washington, D.C.: CCSDS, October 2009.

[8] *Space Link Identifiers*. Recommendation for Space Data System Standards, CCSDS 135.0-B-4. Blue Book. Issue 4. Washington, D.C.: CCSDS, October 2009.

[9] *Communications Operation Procedure-1*. Recommendation for Space Data System Standards, CCSDS 232.1-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, September 2003.

[10] *Space Packet* Protocol. Recommendation for Space Data System Standards, CCSDS 133.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, September 2003.

[11] M. Degermark, B. Nordgren, and B. Nordgren. *IP Header Compression*. RFC 2507. Reston, Virginia: ISOC, February 1999.

[12] S. Casner and V. Jacobson. *Compressing IP/UDP/RTP Headers for Low-Speed Serial Links*. RFC 2508. Reston, Virginia: ISOC, February 1999.

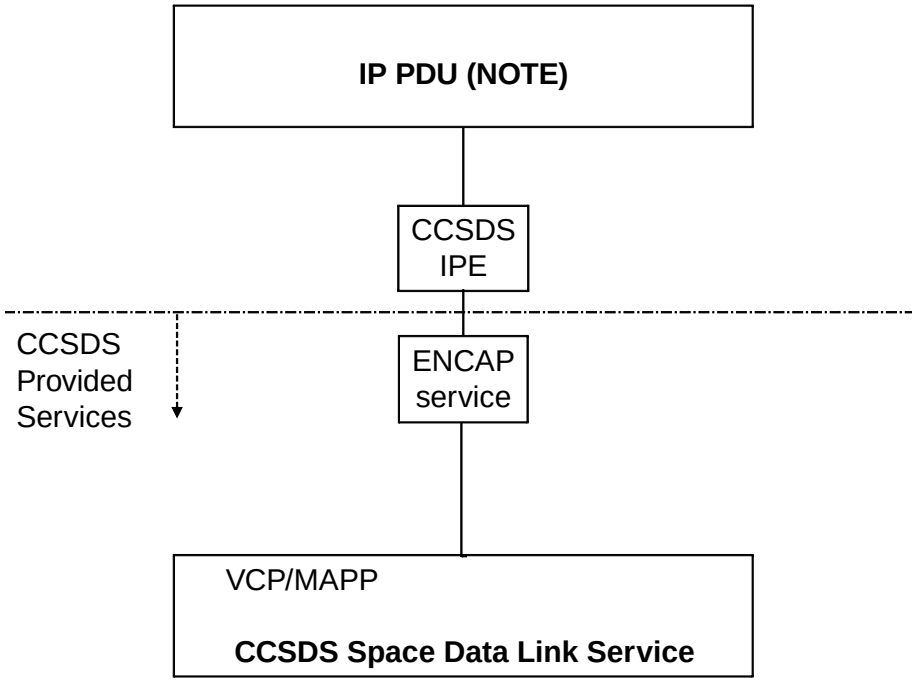
NOTE – Informative references are provided in annex E.

2 OVERVIEW OF TRANSFERRING IP PDUS OVER CCSDS LINK SERVICES

2.1 GENERAL

This section describes the recommended method for transferring IP PDUs over CCSDS Space Data Link Protocols: Telecommand (TC), Telemetry (TM), Advanced Orbiting Systems (AOS), and Proximity-1 (see figure 2-1, below).

IP PDUs enumerated in annex A of reference [8] are transferred by encapsulating them, one-for-one, within CCSDS Encapsulation Packets. The Encapsulation Packets are transferred directly within one or more CCSDS Space Data Link Transfer Frames. This method uses the CCSDS Internet Protocol Extension (IPE) followed by the CCSDS Encapsulation (ENCAP) Service over CCSDS AOS, TM, TC, or Proximity-1 Virtual Channel Packet (VCP) Service.



NOTE – IP PDU enumerated in annex A of reference [8].

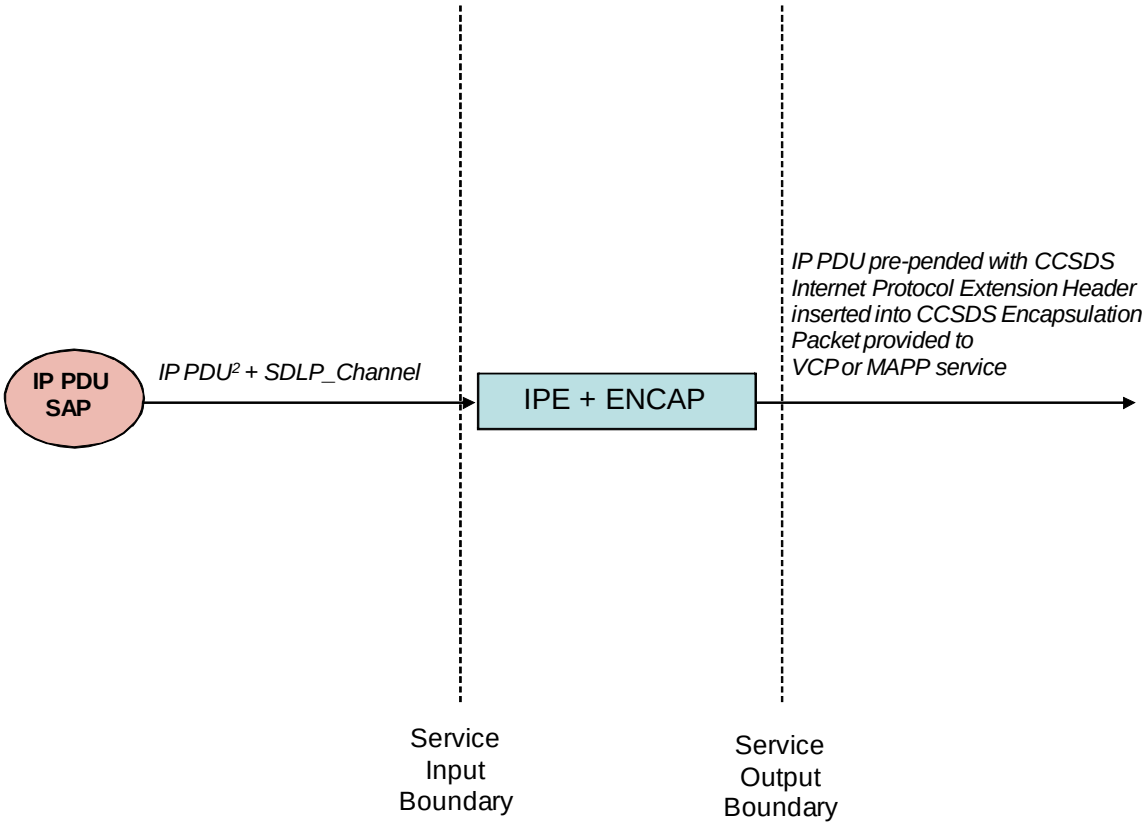
Figure 2-1: Recommended Method for Transferring IP over CCSDS Data Links

2.2 SERVICE INTERFACE

2.2.1 GENERAL

Figure 2-2 describes the interface between the service user, who accesses the transfer service at a Service Access Point (SAP), and the service provider, who performs the service by transferring the data unit across the space link. The user provides an IP PDU as defined in annex A of reference [8] and its associated link layer routing information (i.e., Space Data

Link Protocol Channel, SDLP_Channel) upon input to the Packet SAP. Link layer addressing is explained in terms of the hierarchy of link layer identifiers (e.g., SDLP_Channel) and channels shown in figure 2-3. A complete description of each of the CCSDS IP transfer services is provided in section 4, Service Primitives.



[1] Encapsulation Service Primitives for Proximity-1 have not been formally defined in reference [7], however IP datagrams over Encapsulation Service over Proximity-1 are transferred analogously to TC except the functionality of Virtual channel IDs is replaced with Port IDs.
[2] See annex A in reference [8] for the list of enumerated IP protocol data units.

Figure 2-2: CCSDS IP Transfer Services Context Diagram

In order to transfer IP PDUs over a CCSDS Space Data Link, upon input to the service provider, the service user provides the appropriate link layer address over which the data unit traverses. The generic term for this link layer address for all of the CCSDS Space Link layer protocols is called 'SDLP_Channel'. The contents of the SDLP_Channel parameter is defined based upon the underlying service of the CCSDS Data Link Layer Protocol:

- for VCP services of TM, TC or AOS: Global Virtual Channel ID (GVCID);
- for Multiplexer Access Point Packet (MAPP) service of TC: GVCID and MAP ID;
- for Proximity-1: Transfer Frame Version Number (TFVN), Spacecraft ID (SCID), Physical Channel ID (PCID), Data Field Construction Identifier (DFC_ID) and Port ID.

For the VCP data transfer service, the user supplies the Global Virtual Channel ID (GVCID). The GVCID is a concatenation of the Transfer Frame Version Number (TFVN), Spacecraft ID (SCID), and Virtual Channel ID (VCID)[1] fields within the Transfer Frame Header of a CCSDS link layer protocol. By specifying the GVCID, the user assigns the contents of the frame to a specific TFVN, to or from a specific SCID, over a specific VCID.[2] For the MAPP transfer service, the user supplies the Global MAP ID or GMAP ID. The GMAP ID is a concatenation of GVCID and MAP ID. The MAP ID supports the multiplexing of MAP Channels over a given Virtual Channel to provide an additional level of multiplexing. In addition, the MAPP service can handle the segmentation and reassembly of datagrams larger than the maximum transmission unit of the Transfer Frame Data Field. MAP channels are supported only by the TC Space Data Link Protocol. (See figure 2-3.)

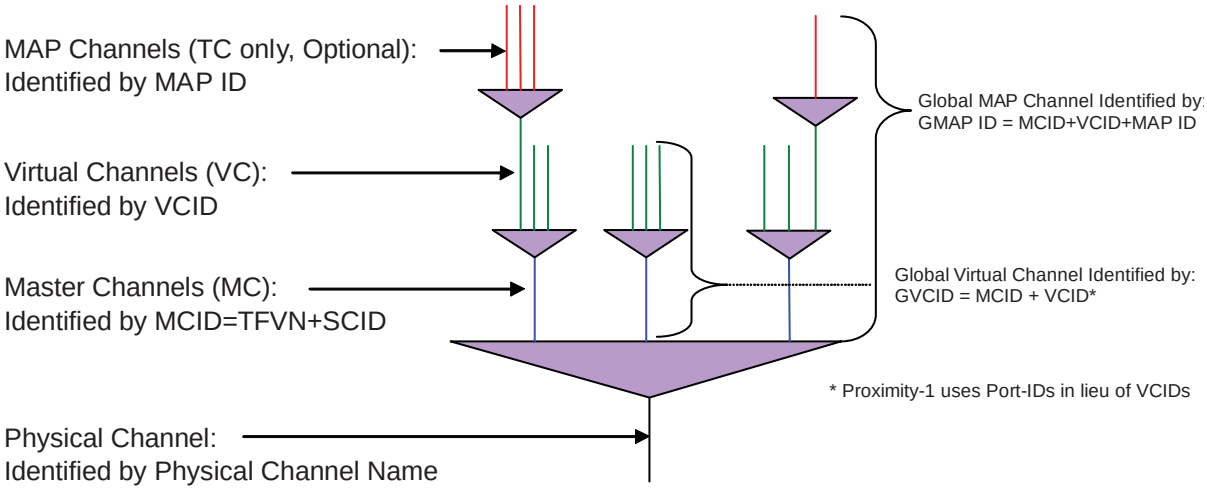


Figure 2-3: Identifiers and Channels Used in the SDLP_Channel Parameter

2.2.2 RECOMMENDED CCSDS IP TRANSFER SERVICES

2.2.2.1 Using CCSDS IPE plus Encapsulation Service to transfer IP over CCSDS Space Links

The recommended CCSDS method of transferring an IP PDU (enumerated in annex A of reference [8]) over a CCSDS space link is to prepend the IP PDU with the CCSDS IPE header and then incorporate the result into the Encapsulation Packet defined in the CCSDS Encapsulation Service (reference [7]). Figure 3-11 shows how the IPE header is prepended to the IP PDU before it is encapsulated into the Encapsulation packet. The Encapsulation Service is cross-supported by CCSDS Member Agencies at the Network layer. The CCSDS Encapsulation Service provides a mechanism for transferring protocol data units of protocols recognized by CCSDS to a protocol handler over a space link. The service user inputs an IP PDU and its associated link layer address to the IP PDU SAP. The Encapsulation Packet may

[1] Proximity-1 does not have the concept of Virtual Channel IDs.

be split across several CCSDS Transfer Frames, depending upon the size of the encapsulated IP PDU, and the CCSDS Date Link layer protocol used.

2.2.2.2 Recommended CCSDS IP Transfer Service

CCSDS Encapsulation Service is the exclusive CCSDS service for transferring IP PDUs across the CCSDS Space Link. Table 2-1 describes the CCSDS recommended IP transfer service over AOS, TM, TC, and Proximity-1 Space Data Link Protocols.

Table 2-1: Recommended CCSDS IPv4 Transfer Services

CCSDS IPv4 Transfer Service	Applicable Space Data Link	Service Access Point (SAP) Address	Service Data Unit
Virtual Channel Packet (VCP)	AOS, TM, TC, Proximity-1	GVCID + PVN	Packet
MAP Packet (MAPP)	TC	GVCID + PVN + MAP ID	Packet
Encapsulation (ENCAP) over VCP[1]	AOS, TM, TC, Proximity-1	GVCID	Packet

2.2.3 MULTIPLEXING SERVICE DATA UNITS OVER CCSDS LINKS

2.2.3.1 General

This subsection provides a tutorial on how CCSDS-recognized service data units, i.e., CCSDS Space Packets, SCPS-NP datagrams, Encapsulation Packets are inserted and multiplexed at the sending end and demultiplexed, extracted, and routed at the receiving end for each CCSDS Space Data Link Protocol. An executive summary of the key characteristics for each CCSDS Data Link layer protocol is provided below in table 2-2.

Table 2-2: Key Characteristics of CCSDS Link Layer Protocols

CCSDS Link Layer Protocol	Transmission Features	Reception Features	Multiplexing Features	Packet Types Transferred
AOS	1. Fixed-length frame (2048 octet maximum) 2. Used for high rate uplink or downlink 3. Isochronous Data 4. No frame ARQ	First Header Pointer provides for packet resynchronization within the frame stream	Frame routing based upon 64 VCIDs	SCPS-NP, CCSDS Space Packet, Encapsulation Packet
TM	1. Fixed-length frame (2048 octet maximum) 2. Used for low rate downlink 3. No isochronous Data 4. No frame ARQ	First Header Pointer provides for packet resynchronization within the frame stream	Frame routing based upon 8 VCIDs	SCPS-NP, CCSDS Space Packet, Encapsulation Packet
TC	1. Variable-length frame (1024 octet maximum) 2. Used for low rate uplink 3. No isochronous data 4. COP-1 go-back-*N* protocol provides frame ARQ	Frame length in transfer frame header delimits frame contents	1. Frame routing based upon 64 VCIDs 2. Routing at segmentation sublayer up to 64 MAP IDs	SCPS-NP, CCSDS Space Packet, Encapsulation Packet
Proximity-1	1. Variable-length frame (2048 octet maximum) 2. Used for moderate rate uplink/downlink 3. No isochronous data 4. COP-P go-back-*N* protocol provides frame ARQ	Frame length in transfer frame header delimits frame contents	Contents of frame routed to either 8 physical or logical entities via Port IDs per Physical Channel	SCPS-NP, CCSDS Space Packet, Encapsulation Packet
NOTE – Low rate downlink is defined here to mean ≤ 100 kb/s; efficient low rate uplink is bounded by 1 Mb/s.				

2.2.3.2 AOS Space Data Link

Figure 2-4 provides a tutorial on how Service Data Units (SDU)s are input into AOS frames, how SDUs are extracted upon output, and how multiple types of service data units can be multiplexed over the AOS frame. The AOS protocol can be used in either forward or return links to transfer relatively high rate data (multiple Mb/s) without Automatic Repeat Queuing (ARQ).

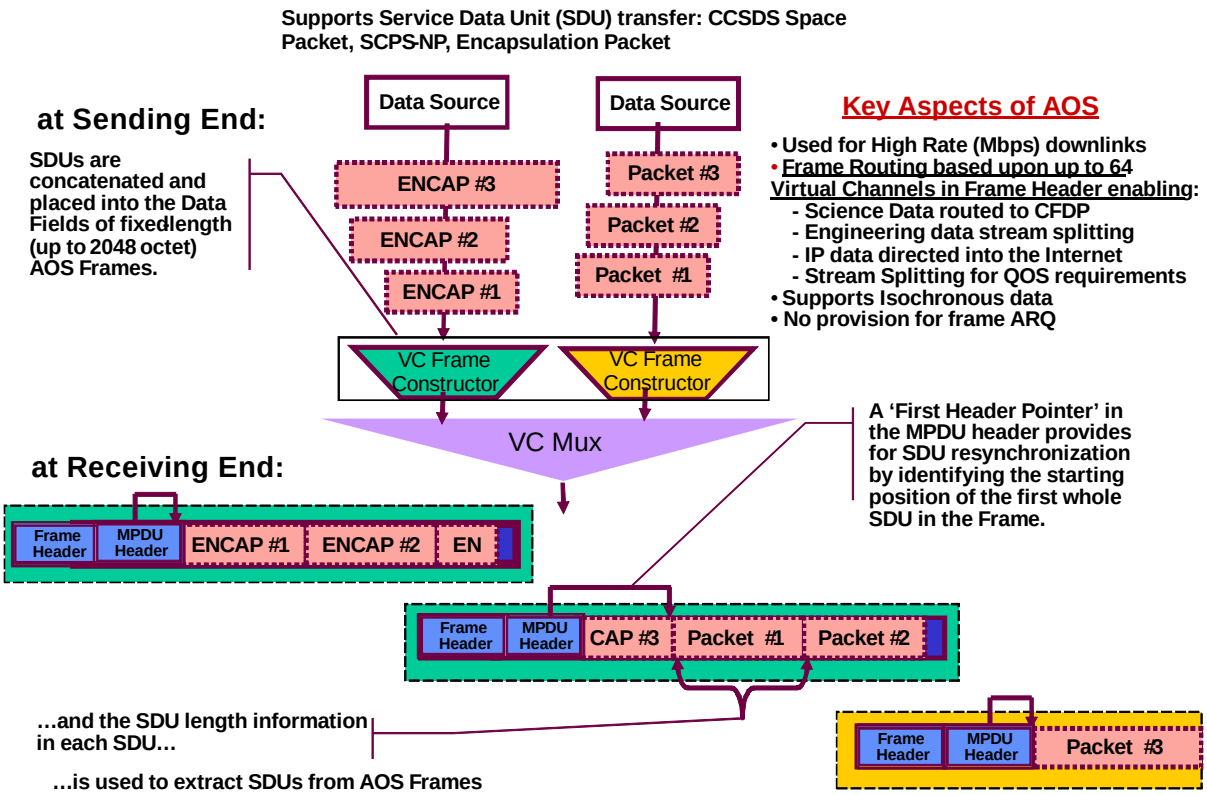


Figure 2-4: Multiplexing SDUs over AOS Frames

In this example, a data source is producing IPv6 datagrams contained one-for-one within CCSDS Encapsulation Packets (ENCAP), while concurrently a second data source is producing CCSDS Space Packets. CCSDS provides the capability of multiplexing both of these SDUs onto the same master channel in two separate ways. Option 1, as shown above, assigns a unique VCID to each SDU type (i.e., CCSDS Space Packets, Encapsulation Packets). Assigning separate VCIDs may be done in order to split out and route these data directly at the ground receiving station. A second option, not shown above, but equally viable, would be to assign a single VCID for both SDU types and multiplex both Encapsulation Packets and Space packets onto it. The receiving system can extract the SDUs from the frame, since each SDU has a defined length field based upon its Packet Version Number (PVN) in the packet header. For the set of requirements and constraints associated with transferring data units over the AOS Space Data Link, see reference [3].

2.2.3.3 TM Space Data Link

Figure 2-5 provides a tutorial on how SDUs are input into TM frames, how SDUs are extracted upon output, and how multiple types of service data units can be multiplexed over the TM frame. The TM frame is used to transfer relatively low rate telemetry (multiple kb/s) directly to Earth without ARQ.

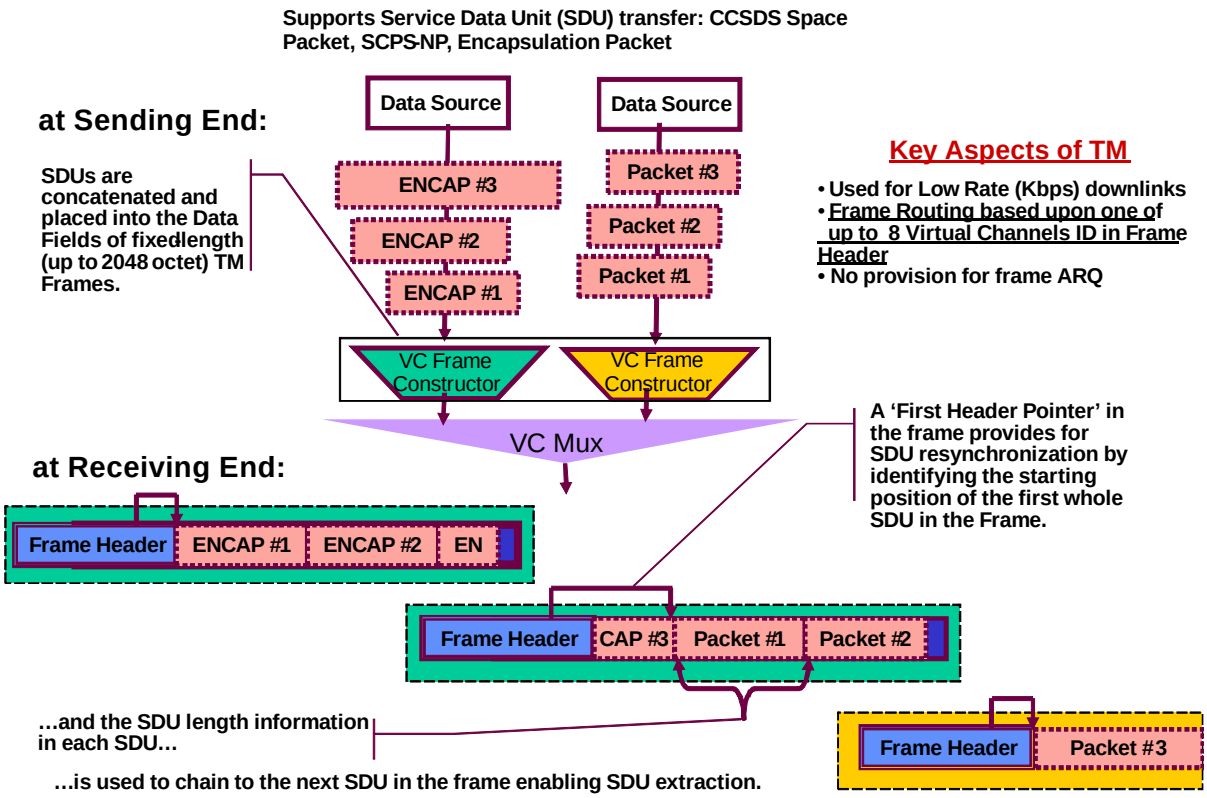


Figure 2-5: Multiplexing SDUs over TM Frames

In this example, a data source is producing IPv6 datagrams contained one-for-one within a CCSDS Encapsulation Packet (ENCAP), while concurrently a second data source is producing CCSDS Space Packets. CCSDS provides the capability of multiplexing both of these SDUs onto the same master channel in two separate ways. Option 1, as shown above, assigns a unique VCID to each SDU type (i.e., Space Packets, Encapsulation Packets). Assigning separate VCIDs may be done in order to split out and route these data directly at the ground receiving station. A second option, not shown above, but equally viable, would be to assign a single VCID for both types and multiplex both Encapsulation Packets and Space Packets onto the same virtual channel. The receiving system can extract the SDUs from the frame, since each SDU has a defined length field based upon its PVN in the packet header. For the overall set of requirements and constraints associated with transferring data units over the TM Space Data Link, see reference [4].

2.2.3.4 TC Space Data Link

Figure 2-6 provides a tutorial on how SDUs are input into TC frames, how SDUs can be segmented, how both packets and segments are extracted upon output, and how multiple types of service data units can be multiplexed over the TC frame. The TC frame is used to transfer relatively low rate telecommand (multiple kb/s) directly from Earth with optional frame ARQ, using the COP-1 protocol (see reference [9]).

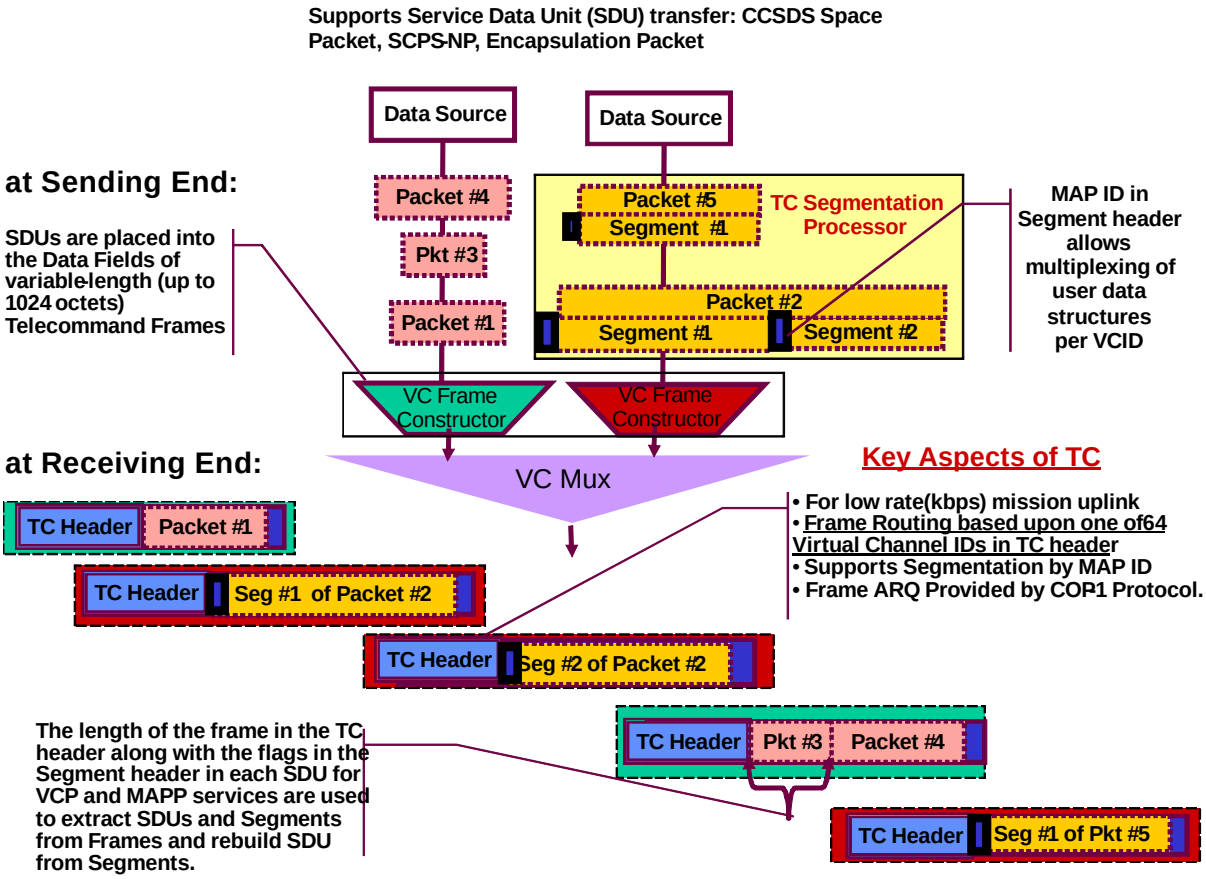


Figure 2-6: Multiplexing SDUs over TC Frames

In this example, a data source is producing packets smaller than the maximum TC frame size (i.e., link layer Maximum Transmission Unit [MTU]) over one VC while a second data source is concurrently producing packets mostly larger than the MTU over a second independent VC. TC provides the capability of both aggregating and subdividing SDUs into segments. CCSDS requires that, once segmentation occurs on a VC, every TC frame assigned to that VC contain a segment. Therefore, as figure 2-6 shows, even packets smaller than the MTU are encapsulated into a segment for transmission over that VC. For the set of requirements associated with transferring data units over the TC Space Data Link, see reference [5].

A MAP is a mechanism provided within the TC segmentation sublayer to allow different user data structures to be multiplexed for transmission over one VC provided by the link layer. Multiplexing at the segment sublayer allows user data structures with different delivery priorities to be multiplexed onto the same VC. The SDU arriving at the sending end can optionally be allocated to a MAP and transferred to the corresponding MAP at the receiving end of the segment layer. Similar to AOS and TM, TC also provides the independent capability of multiplexing SDUs at the link layer using VCIDs.

The receiving system can extract the SDUs from the frame, since each SDU has a defined length field based upon its PVN in the packet header. For the overall set of requirements and constraints associated with transferring data units over the TC Space Data Link, see reference [5].

2.2.3.5 Proximity-1 Data Link

Figure 2-7 provides a tutorial on how SDUs are input into Proximity-1 frames, how SDUs can be segmented, how both packets and segments are extracted upon output, and how multiple types of service data units can be multiplexed over the Proximity-1 frame. The Proximity-1 frame is used to transfer moderate rate telecommand and telemetry (up to 2 Mb/s) in proximate environments with optional frame ARQ, using the COP-P protocol (reference [6]).

In this example, a data source is producing packets smaller than the maximum Proximity-1 frame size (i.e., link layer MTU) over one Port ID, while a second data source is concurrently producing packets mostly larger than the MTU over a second independent Port. Proximity-1 provides the capability of both aggregating and subdividing SDUs into segments by assigning a ‘pseudo packet ID’ to each segment. Unlike the multiplexer functionality of the TC MAP ID, the pseudo packet ID is a temporary packet ID assigned to enable the protocol to account for the segments of multiple SDUs during transmission. In order to reconstruct the SDU on the receive side, Proximity-1 requires that segments of the same SDU be sent in frames containing the same physical channel ID and Port ID. However, segments from another packet may be interspersed but only in frames containing a different physical channel ID or Port ID.

The receiving system can extract SDUs of multiple CCSDS-recognized protocols from the frame, since each SDU has a defined length field based upon its PVN in the packet header. Reference [6] contains the overall set of requirements associated with transferring data units over the Proximity-1 Space Data Link.

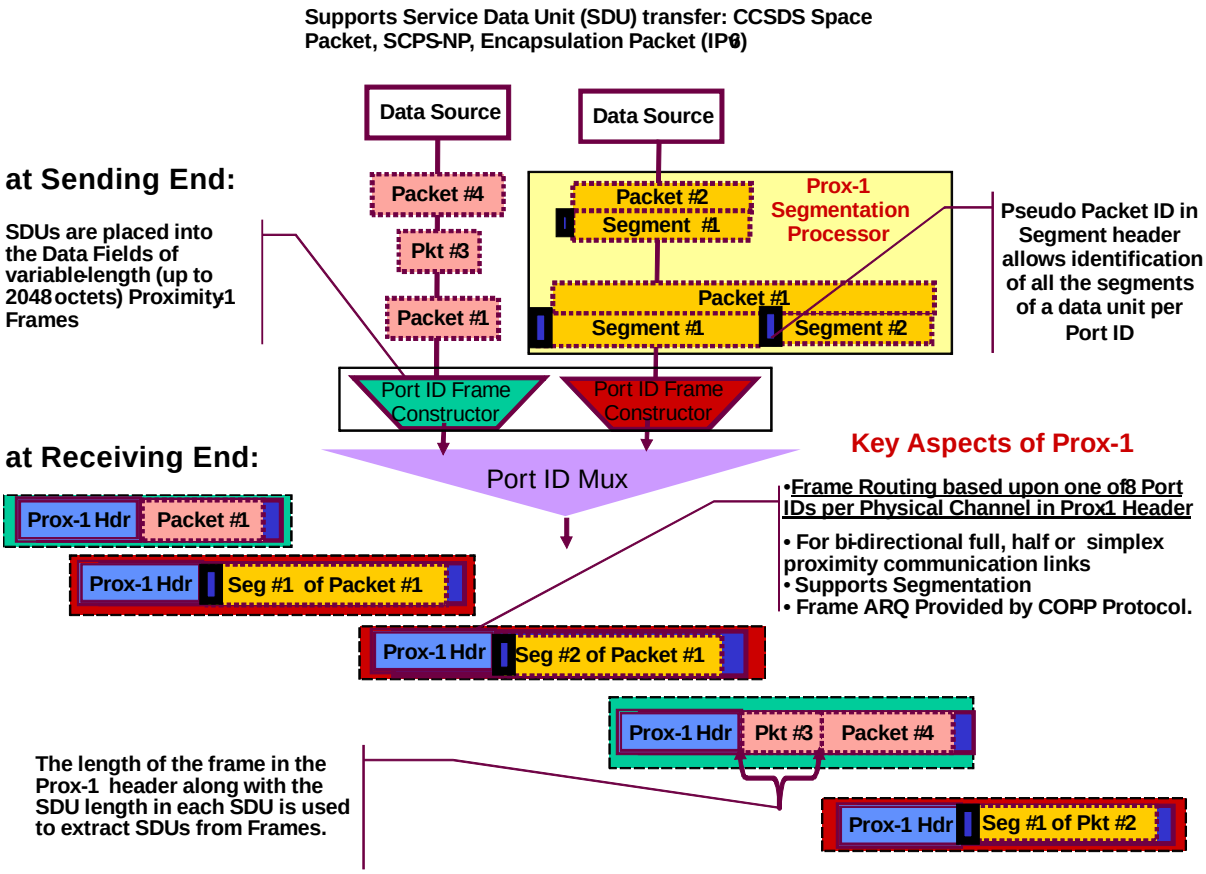


Figure 2-7: Multiplexing SDUs over Proximity-1 Frames

2.2.4 CCSDS ENCAPSULATION SERVICE

2.2.4.1 Concept of Encapsulation Service

The Encapsulation Service provides a mechanism for transferring protocol data units of protocols recognized by CCSDS to a protocol handler over a space link. It is the recommended practice to use this service to transfer all IP PDUs across CCSDS space links,. The Encapsulation Service is a service provided by the Data Link Layer of the OSI Basic Reference Model (reference [1]). (See figure 2-8.) It is used together with the Space Data Link Protocols defined in references [3]-[6] and therefore is to be used together with one of these references.

The Encapsulation Service can encapsulate into Space Packets or into Encapsulation Packets. It is recommended that only the CCSDS Encapsulation Packet be used to transfer IP protocol data units.

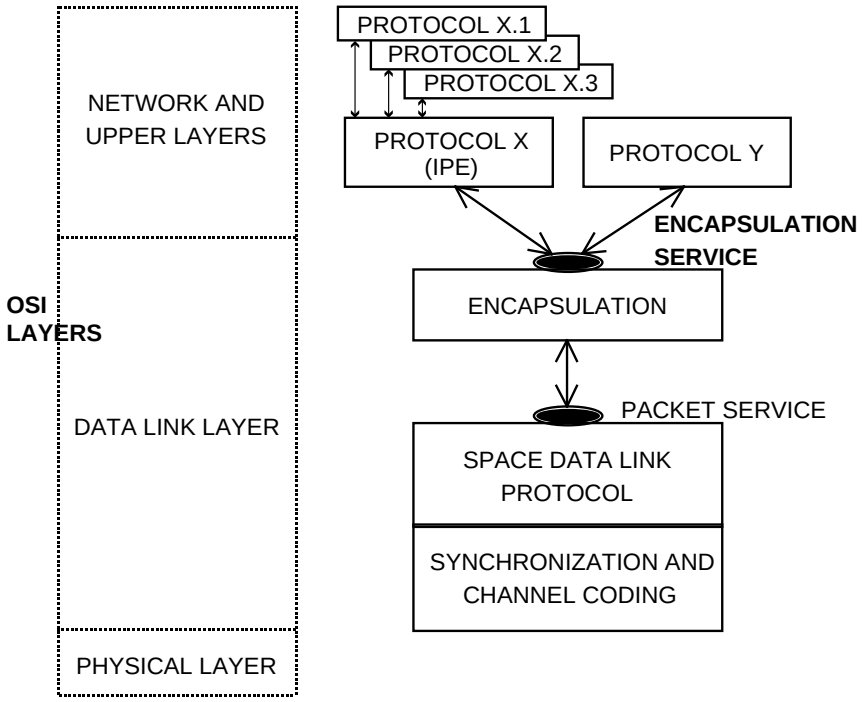


Figure 2-8: Concept of Encapsulation Service

Figure 2-8 illustrates the concept of the Encapsulation Service. The primary purpose of the CCSDS Internet Protocol Extension (IPE) convention is to provide an interoperable way of identifying the Internet protocols being encapsulated by the CCSDS Encapsulation Service when this service is being used to provide a Data Link layer for IP. This protocol convention uses one and optionally more than one 'shim' byte placed in front of the IP PDU. Using this convention, the Encapsulation service provides a Data Link layer for IP. It supports IP PDU formats shown table 3-2. IPE uses the Encapsulation service primitives defined and the service described in reference [7]. The additional service provided through the IPE is a protocol multiplexing/demultiplexing capability.

The IPE convention allows demultiplexing of subprotocols used in IP. It offers a sizable protocol identifier space while not impacting the protocol ID space used by the Encapsulation Service itself. 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.

2.2.4.2 Features of the Encapsulation Service

The Encapsulation Service transfers a sequence of variable-length, delimited, octet-aligned data units with a Space Data Link Protocol over a space link. The format and content of data units transferred with this service are unknown to the service provider.

A data unit supplied by the service user is encapsulated unchanged into an Encapsulation Packet, and no more than one data unit is encapsulated into a single packet. That is, segmenting or blocking of data units is not performed by the service provider.

The service permits a data unit to be of any length which is an integral number of octets, and which is subject to the maximum and minimum sizes established by the project organization. Although the length of a data unit that can be accommodated by an encapsulating packet ranges from 0 to 4,294,967,287 octets if the Encapsulation Packet is used, individual project organizations may establish the maximum and minimum sizes for the encapsulated data unit.

The point at which an instance of this service is provided to a user is called a Service Access Point (SAP) (see reference [1]). Data units submitted to a SAP are processed in the order of submission. No processing order is maintained for data units submitted to different SAPs.

NOTE – Implementations may be required to perform flow control at a SAP between the service user and the service provider. However, CCSDS does not recommend a scheme for flow control between the user and the provider.

Features of the Encapsulation Service are as follows:

a) Unidirectional (one way) service: One end of a connection can send, but not receive, data through the space link, while the other end can receive, but not send, data through the space link.

b) Asynchronous service: There are no timing relationships between the transfer of data units supplied by the user and any data transmission mechanism within the Data Link Layer. The user may request data transfer at any time, but there may be restrictions imposed by the service provider on the data generation rate.

c) Unconfirmed service: The sending user does not receive confirmation from the receiving end indicating that data has been received.

d) Incomplete service: The service does not guarantee completeness, but the service provider may signal gaps in the sequence of data units delivered to the receiving user.

e) Sequence preserving service: The sequence of data units supplied by the sending user is preserved through the transfer over the space link, although there may be gaps in the sequence of data units delivered to the receiving user.

2.2.4.3 ADDRESSING

A user of the Encapsulation Service is identified by the combination of the following:

a) a PVN that indicates that Encapsulation Packets are used for encapsulation; and

b) an Encapsulated Protocol Identifier (EPI) that indicates that the IPE Protocol is used.

NOTE – Both the PVN and the EPI are defined in reference [8] and are provided in table B-3, Managed Parameters for Encapsulation Service.

2.2.4.4 SERVICE Description

The Encapsulation Service is described in terms of:

a) the service primitives provided to the users of this service (see 4.2);

b) the protocol data units employed by the service provider for encapsulation (see 3.5);

c) the procedures performed by the service provider (see 2.2).

The service primitives 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.

The protocol data units (i.e., the Encapsulation Packet) define the data structure in which data units supplied by the service user are encapsulated.

The procedure specifications define the procedures performed by the service provider for the transfer of data units. The definitions of procedures are independent of specific implementation methods or technologies.

3 PDU FORMATS

3.1 OVERVIEW

This section provides a tutorial on the PDUs used in the transfer of IP PDUs over CCSDS Space Data Link Protocols. For each Data Link layer protocol, the PDUs and key fields within them are identified and described. In addition, the recommended Encapsulation Service PDU applicable to encapsulating all CCSDS recognized IP PDUs (see table 3-2), i.e., the Encapsulation Packet, is described.

Figure 3-1 describes the prepending of the IP PDU by the IPE header and further incorporation of that result into the CCSDS Encapsulation Packet, which is required for transfer of all CCSDS recognized IP PDUs.

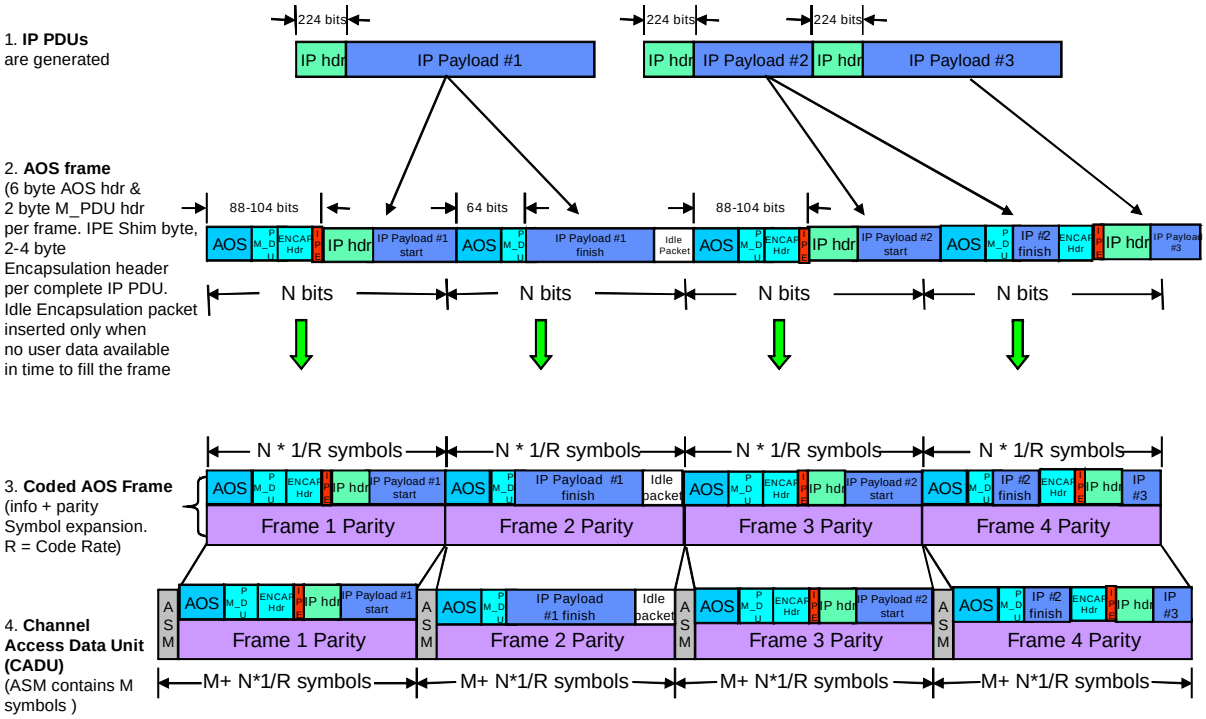


Figure 3-1: End-to-End Hierarchy Diagram of IP over CCSDS IPE/Encap

3.2 AOS TRANSFER FRAME

Figures 3-2, 3-3, and 3-4 show the components of the AOS Transfer Frame applicable to the transfer of IP over the AOS Space Data Link. The AOS Transfer Frame is the CCSDS Version 2 frame, having a TFVN of '01' binary.

AOS TRANSFER FRAME				
TRANSFER FRAME PRIMARY HEADER	TRANSFER FRAME INSERT ZONE (Optional)	TRANSFER FRAME DATA FIELD	TRANSFER FRAME TRAILER (Optional)	
			OPERA-TIONAL CONTROL FIELD (Optional)	FRAME ERROR CONTROL FIELD (Optional)
6 or 8 octets	Varies	Varies	4 octets	2 octets

Figure 3-2: AOS Transfer Frame

TRANSFER FRAME PRIMARY HEADER								
MASTER CHANNEL ID		VIRTUAL CHANNEL ID	VIRTUAL CHANNEL FRAME COUNT	SIGNALING FIELD				FRAME HEADER ERROR CONTROL (Optional)
TRANSFER FRAME VERSION NUMBER	SPACECRAFT ID			REPLAY FLAG	VC FRAME COUNT USAGE FLAG	RSVD. SPARE	VC FRAME COUNT CYCLE	
2 bits	8 bits	6 bits		1 bit	1 bit	2 bits	4 bits	
2 octets			3 octets	1 octet				2 octets

Figure 3-3: AOS Transfer Frame Primary Header

The length of the AOS Transfer Frame is fixed and is a managed parameter. The maximum Transfer Frame length is dependent upon the coding used and is defined in reference [E9].

The AOS Transfer Frame key fields used by the CCSDS IP transfer services (see section 4) are:

a) Transfer Frame Version Number (TFVN), a two-bit field at the start of the Transfer Frame Header, containing the binary value '01';

b) Spacecraft ID (SCID), an eight-bit field that immediately follows the TFVN field;

c) Virtual Channel ID (VCID), a six-bit field that immediately follows the SCID field.

For a complete description of all of the fields within the AOS frame, see reference [3].

The AOS Transfer Frame Data Field consists of one Multiplexing Protocol Data Unit (M_PDU) into which the spacecraft application data is placed.

M_PDU HEADER		M_PDU PACKET ZONE				
RSVD. SPARE 5 bits	FIRST HEADER POINTER 11 bits	END OF PREVIOUS CCSDS PACKET #k	CCSDS PACKET #k+1	. . . . .	CCSDS PACKET #m	START OF CCSDS PACKET #m+1

Figure 3-4: Multiplexing Protocol Data Unit (M_PDU)

An IP PDU inserted into a CCSDS Encapsulation packet is carried using the (M_PDU) shown in figure 3-4. The M_PDU may contain more than one data unit (as shown above) or only a partial data unit depending on the length of the data unit. Data Units of multiple protocols recognized by CCSDS may be multiplexed in the same M_PDU and in the same Virtual Channel. The first bit of the M_PDU aligns with the first bit of the AOS Transfer Frame Data Field. For a complete description of the M_PDU, see reference [3].

Note that if there is insufficient user data available to complete the frame, then an idle packet, i.e., a packet containing idle data, is created to complete the frame so that the frame can be released in time.

3.3 TM TRANSFER FRAME

Figures 3-5 and 3-6 show the components of the TM Transfer Frame, i.e., the CCSDS Version 1 frame, having a TFVN of ‘00’ binary.

TM TRANSFER FRAME				
TRANSFER FRAME PRIMARY HEADER	TRANSFER FRAME SECONDARY HEADER (Optional)	TRANSFER FRAME DATA FIELD	TRANSFER FRAME TRAILER (Optional)	
			OPERA-TIONAL CONTROL FIELD (Optional)	FRAME ERROR CONTROL FIELD (Optional)
6 octets	Up to 64 octets	Varies	4 octets	2 octets

Figure 3-5: TM Transfer Frame

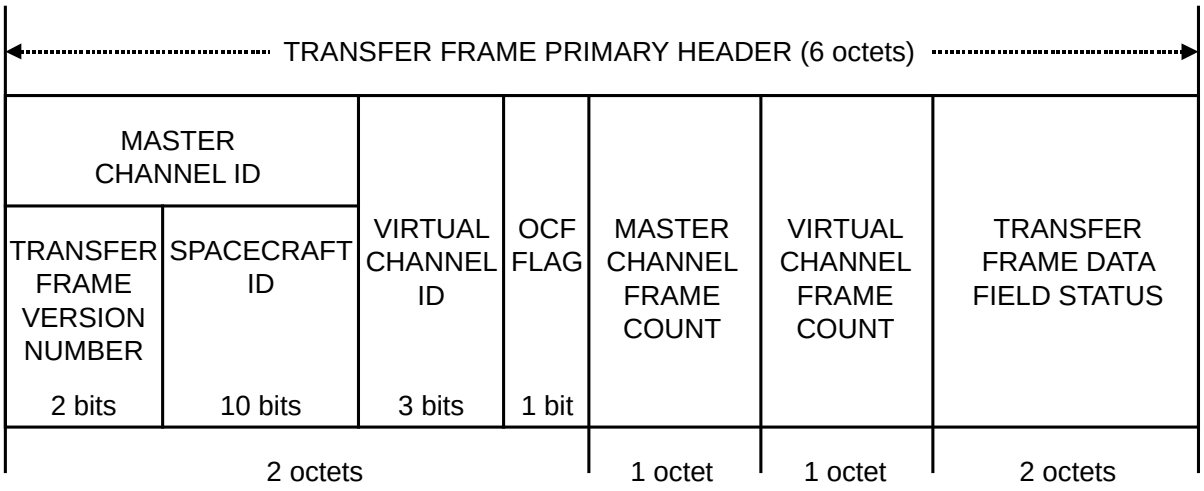


Figure 3-6: TM Transfer Frame Primary Header

The length of the Transfer Frame Data Field into which the spacecraft application data is placed varies and is a managed parameter. The maximum Transfer Frame length is dependent upon the coding used and is defined in reference [E9].

The TM Transfer Frame key fields used by CCSDS IP transfer services (see section 4) are:

a) Transfer Frame Version Number (TFVN), a two-bit field at the start of the Transfer Frame Header, containing the binary value '00';

b) Spacecraft ID (SCID), a ten-bit field that immediately follows the TFVN field;

c) Virtual Channel ID (VCID), a three-bit field that immediately follows the SCID field.

An IP PDU inserted into a CCSDS Encapsulation packet is carried within the Transfer Frame Data Field shown in figure 3-5. This field may contain more than one data unit or only a partial data unit depending on the length of the data unit. Data Units of multiple protocols recognized by CCSDS may be multiplexed in the same Transfer Frame Data Field within the same Virtual Channel.

Note that when there is insufficient user data available to complete the frame, then a packet containing idle data is created to complete the frame so that it can be released. For a complete description of all of the fields within the TM frame, see reference [4].

3.4 TC TRANSFER FRAME

Figures 3-7 and 3-8 show the components of the TC Transfer Frame, i.e., the CCSDS Version 1 frame, having a TFVN of '00' binary.

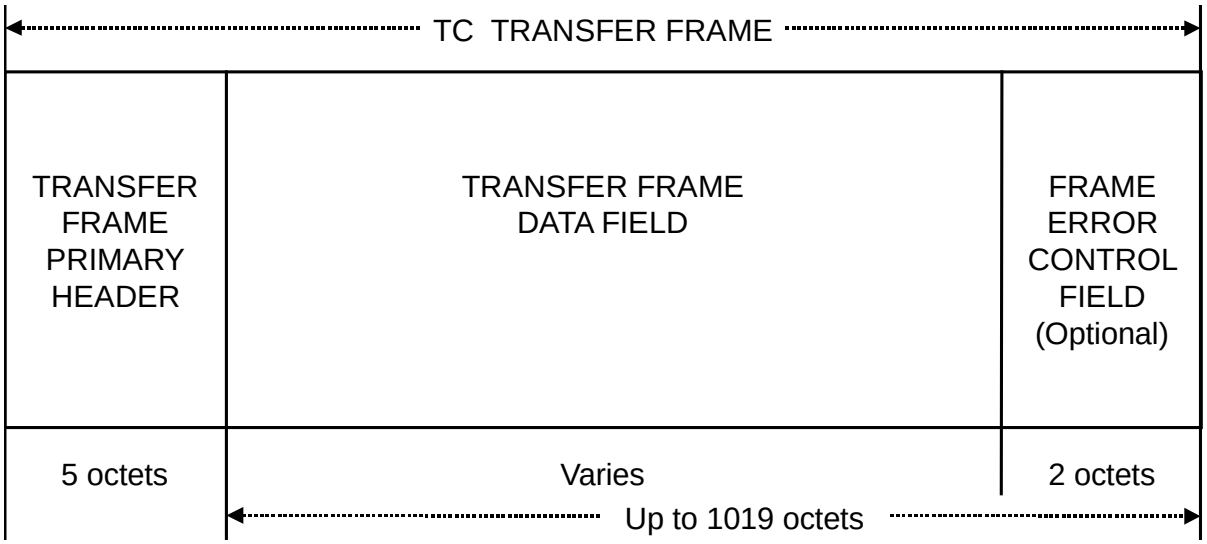


Figure 3-7: TC Frame Structure

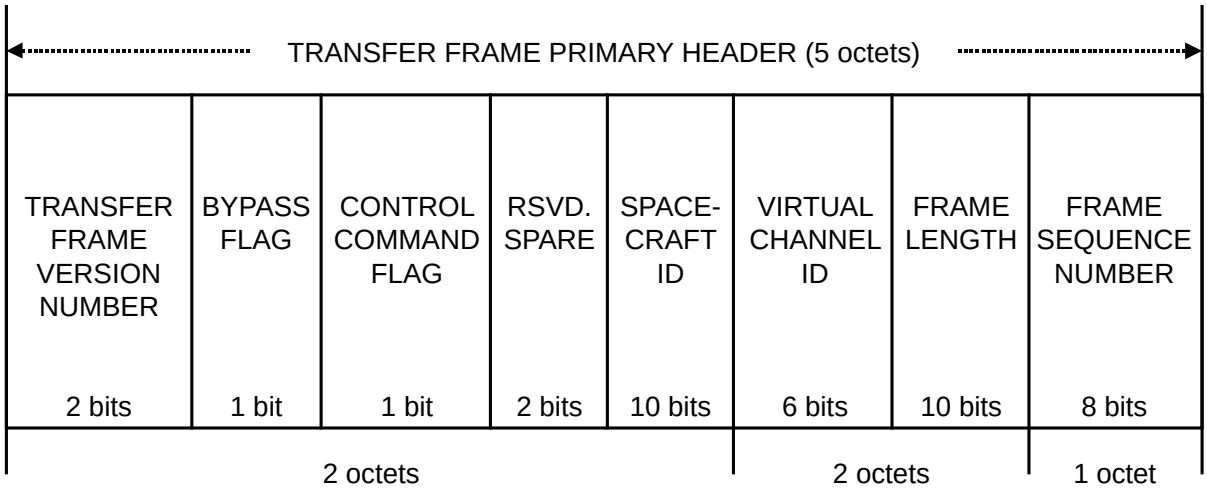


Figure 3-8: TC Frame Primary Header

The length of the Transfer Frame Data field varies according to the length of the spacecraft application data that is placed in it. If the MAPP Service is used for the Virtual Channel, the field contains a segment. If the VCP Service is used for the Virtual Channel, the field contains one or more complete packets. The length of the Transfer Frame Data field can be calculated from the value contained in the Frame Length field. The maximum TC frame length is 1024 octets.

The TC Transfer Frame key fields used by CCSDS IP transfer services (see section 4) are:

a) Transfer Frame Version Number (TFVN), a two-bit field at the start of the Transfer Frame Header, containing the binary value ‘00’;

b) Spacecraft ID (SCID), a ten-bit field within the Transfer Frame Header;

c) Virtual Channel ID (VCID), a six-bit field that immediately follows the SCID field.

An IP PDU inserted into a CCSDS Encapsulation packet is carried within the Transfer Frame Data Field shown in figure 3-7:

– If the MAPP Service is used for the Virtual Channel, then the field contains a segment, which can carry one or more complete packets, or part of one packet. Packets of multiple protocols recognized by CCSDS may be multiplexed within a MAP channel, and may be carried in the same segment if length constraints are not exceeded.

– If the VCP Service is used for the Virtual Channel, then the field contains one or more complete packets. Packets of multiple protocols recognized by CCSDS may be multiplexed within a Virtual Channel, and may be carried in the same frame if length constraints are not exceeded.

TC frames are generated asynchronously when there is data to be sent, and the length of a TC frame is adjusted to fit the data it is carrying. Therefore, in general, TC frames do not carry idle data. Procedures are defined for the Physical Layer of a TC link, which specify the sending of an idle sequence to maintain symbol synchronization on the link.

For a complete description of all of the fields within the TC frame, see reference [5].

3.5 PROXIMITY-1 TRANSFER FRAME

Figures 3-9 and 3-10 show the components of the Proximity-1 Transfer Frame, i.e., the CCSDS Version 3 frame, having a TFVN of '10' binary.

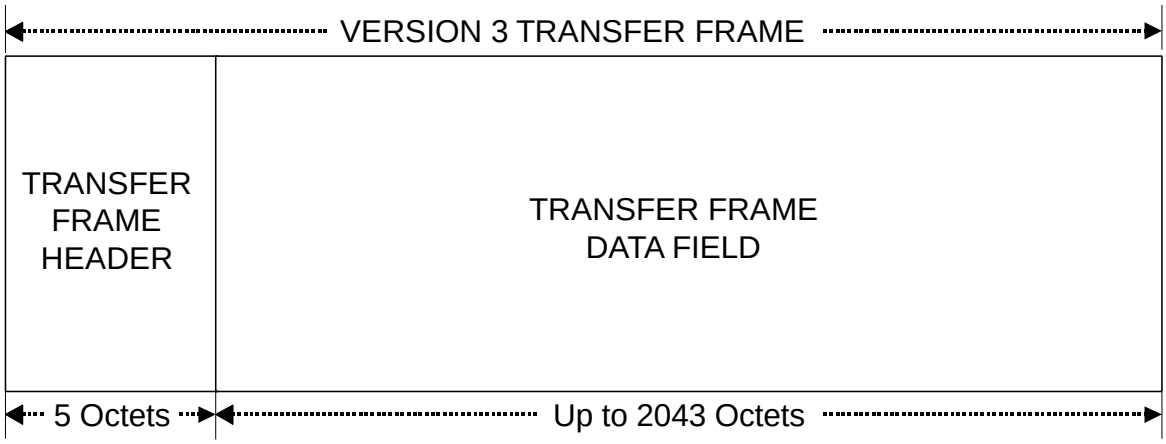


Figure 3-9: Proximity-1 Transfer Frame

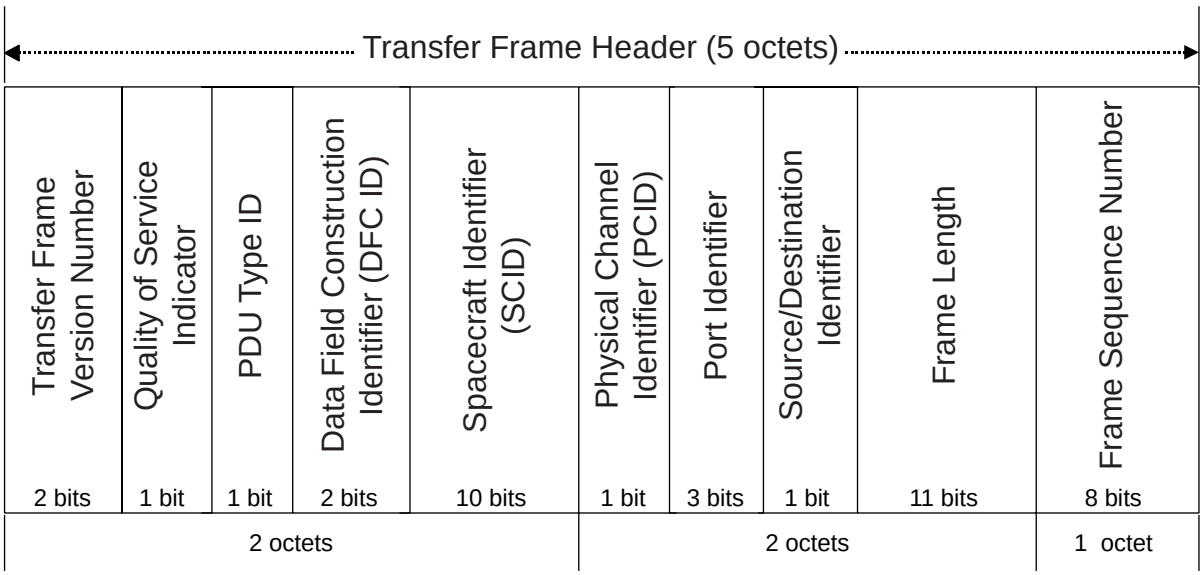


Figure 3-10: Proximity-1 Transfer Frame Header

The length of the Transfer Frame Data Field into which the spacecraft application data is placed varies with the size of the packet or SDU and is defined by the Frame Length Field. The maximum Proximity-1 frame size is 2048 octets.

The Proximity-1 Transfer Frame key fields used by CCSDS IP transfer services (see section 4) are:

a) Transfer Frame Version Number (TFVN), a two-bit field at the start of the Transfer Frame Header, containing the binary value '10';

b) Spacecraft ID (SCID), a ten-bit field within the Transfer Frame Header;

c) Physical Channel Identifier (PCID), a one-bit field that immediately follows the SCID field.

An IP PDU inserted into a CCSDS Encapsulation packet is carried within the Transfer Frame Data Field shown in figure 3-9. This field may contain one or more complete data units. Data Units of multiple protocols recognized by CCSDS may be multiplexed in the same Transfer Frame Data Field within the same Physical Channel/Port ID.

When the Data Link layer has no frames for transmission, then the Physical layer transmits an idle sequence to maintain symbol synchronization on the link.

For a complete description of all of the fields within the Proximity-1 frame, see reference [6].

3.6 ENCAPSULATION PACKET STRUCTURE

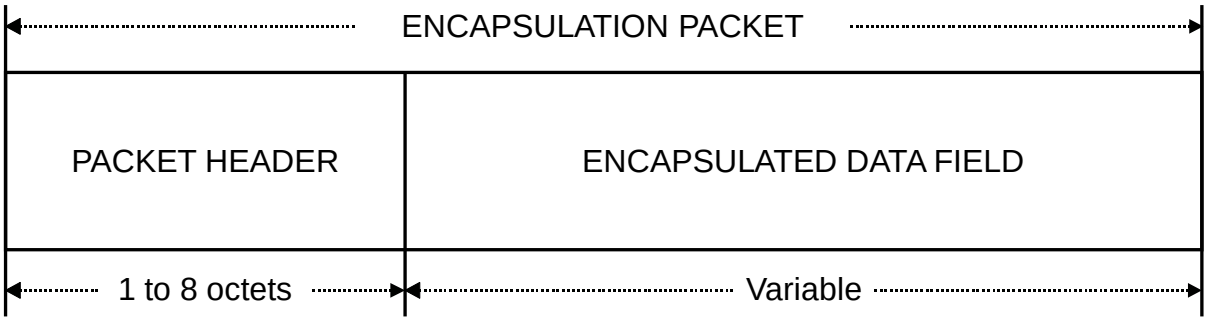


Figure 3-11: Encapsulation Packet Structural Components

3.6.1 ENCAPSULATION PACKET HEADER

3.6.1.1 General

The Encapsulation Packet Header is mandatory and has a length of one, two, four or eight octets. The Encapsulation Packet Header consists of three, four, six, or seven fields, positioned contiguously, in the following sequence:

a) Packet Version Number (3 bits, mandatory);

b) Protocol ID (3 bits, mandatory);

c) Length of Length (2 bits, mandatory);

d) User Defined Field (4 bits; mandatory in 4- and 8-octet headers; not used in 1- and 2-octet headers—see figure 3-12);

e) Protocol ID Extension Field (4 bits; mandatory in 4- and 8-octet headers; not used in 1- and 2-octet headers—see figure 3-12);

f) CCSDS Defined Field (2 octets; mandatory in 8-octet headers; not used in 1-, 2-, and 4-octet headers—see figure 3-12);

g) Packet Length (1, 2, or 4 octets; mandatory in 2-, 4-, and 8-octet headers; not used in 1-octet headers—see figure 3-12).

The format of the Encapsulation Packet Header is shown in figure 3-12.

ENCAPSULATION PACKET HEADER

PACKET VERSION NUMBER 3 bits	PROTOCOL ID 3 bits	LENGTH OF LENGTH 2 bits	USER DEFINED FIELD 0 or 4 bits	PROTOCOL ID EXTENSION 0 or 4 bits	CCSDS DEFINED FIELD 0 or 2 octets	PACKET LENGTH 0 to 4 octets
'111'	'XXX'	'00'	0 bits	0 bits	0 octets	0 octets
'111'	'XXX'	'01'	0 bits	0 bits	0 octets	1 octet
'111'	'XXX'	'10'	4 bits	4 bits	0 octets	2 octets
'111'	'XXX'	'11'	4 bits	4 bits	2 octets	4 octets

Figure 3-12: Encapsulation Packet Header

The Encapsulation Packet key addressing fields used by the CCSDS IP transfer services (see section 4) are:

a) Packet Version Number, a three-bit field at the start of the Encapsulation Packet Header, containing the binary value '111';

b) Protocol ID, a three-bit field defined in table 2-5. The recommended practice for transferring an IP PDU shall set the the Encapsulation Packet Protocol Identifier, i.e., PID to '010' (CCSDS IPE).

NOTE – An implementation on the transmitting end may choose to either use a fixed Encapsulation header size or adaptively/dynamically adjust the size of the Encapsulation Header size according to the payload size in order to optimize bandwidth use (minimize header overhead). Therefore, an implementation needs the capability of receiving encapsulation packets implementing either case.

For a complete description of all of the fields within the Encapsulation Packet Header, see reference [6].

3.6.2 ENCAPSULATED DATA FIELD

If present, the Encapsulated Data Field follows, without gap, the Packet Length field. It consists of an integral number of octets.

The Encapsulated Data Field contains the protocol data as indicated by the Protocol ID field as well as by the Protocol ID Extension field if present.

If the Protocol ID field contains the value '000', then the Encapsulated Data Field contains idle data.

Under the following conditions, the Encapsulated Data Field is absent:

a) when the value of the Length of Length field is '00'; or

b) when the value of the Length of Length field is other than '00', and the packet length as indicated by the Packet Length field is equal to the length of the Encapsulation Packet Header.

If the Encapsulated Data Field is absent, then the Protocol ID field contains the value '000'.

NOTES

1 When the Encapsulation Packet is generated as a result of an ENCAPSULATION.request to the Encapsulation Service, then the Encapsulated Data Field contains the Data Unit supplied by the service user.

2 If the Protocol ID field contains the value '000', then the packet is an Encapsulation Idle Packet. Encapsulation Idle Packets may be used by the TM Space Data Link Protocol (reference [4]) and by the AOS Space Data Link Protocol (reference [3]). These protocols generate Idle Packets in the absence of sufficient user data to maintain synchronization of the data transport processes.

3 CCSDS does not specify the pattern of idle data.

Table 3-1: Encapsulation Packet Lengths, Depending on the Length of the Packet Header

Length (*) of Packet Header	Number of octets in Packet Length Field	Minimum packet length	Maximum packet length	Minimum length of Encapsulated Data Field	Maximum length of Encapsulated Data Field (**)
1	Packet Length Field is absent	1	1	Encapsulated Data Field is absent	
2	1	2	255	0	253
4	2	4	65 535	0	65 531
8	4	8	4 294 967 295	0	4 294 967 287

(*) All lengths are given in octets.
(**) An implementation may establish a lower value for the maximum length of the Encapsulated Data field. The length of the Encapsulated Data Unit is the same as the length of the Encapsulated Data field.

3.7 CCSDS INTERNET PROTOCOL EXTENSION (IPE)

3.7.1 OVERVIEW

The primary purpose of the CCSDS Internet Protocol Extension (IPE) convention is to provide an interoperable way of identifying the Internet protocols being encapsulated by the CCSDS Encapsulation Service (reference [7]) when this service is being used to provide a data link layer for the Internet Protocol (IP). Table A-1 in reference [8] contains a listing of the CCSDS recommended protocols to be encapsulated and their enumerations for the content of the IPE Header.

IPE uses the Encapsulation service primitives defined and the service described in reference [7]. The additional service provided through the IPE is a protocol multiplexing/demultiplexing capability.

The IPE convention allows demultiplexing of subprotocols used in IP. It offers a sizable protocol identifier space while not impacting the protocol ID space 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 2-8.

3.7.2 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 Protocol Data Unit (PDU) formats that are often used in support of IP. As a comparison, serial links between routers often carry the 16-bit PPP protocol field, and the Ethernet protocol data units carry a 16-bit Ethernet type field. In these cases, the enumerations of the protocols are defined by 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 alternate 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 link and network layer configuration protocols, and authentication protocols.

3.8 ISINTERNET PROTOCOL EXTENSION SPECIFICATION

3.8.1 GENERAL

3.8.1.1 The IP PDU to be encapsulated follows, without gap, the IPE header.

3.8.1.2 The concatenation of IPE Header and IP PDU is 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 3-13.

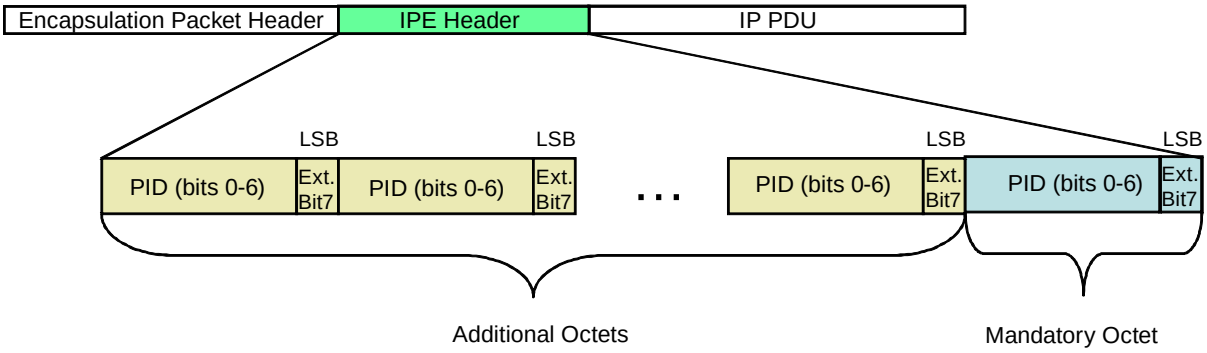


Figure 3-13: IPE Header Format and Placement

3.8.2 INTERNET PROTOCOL EXTENSION HEADER

3.8.2.1 The IPE header is an integral number of octets in length, with a minimum length of one octet.

3.8.2.2 Bit and octet ordering of the IPE header follow the conventions given in 1.3.3.

3.8.2.3 The IPE header is 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 is 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.

3.8.2.4 The IPE header is interpreted as an unsigned integer value, per the convention given in 1.3.3.

3.8.2.5 The IPE Header contains one of the values given in table 3-2.

3.8.2.6 The IPE Header Value is the decimal value of the contents of the entire IPE Header.

3.8.2.7 Only the odd IPE Header Values are valid, since the LSB of the least significant octet must have a value of "1".

3.8.2.8 If the IPE Header consists of a single octet, then only odd IPE Header Values from 0 to 255 are valid.

3.8.2.9 If the IPE Header consists of two or more octets, then:

- Odd IPE Header Values from 0 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 512 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.

Table 3-2: Enumerations for the IPE Header Values

IPE Header Value	Protocol Encapsulated	Reference
33	IPv4 datagram	[H6]
35	Frame_Relay_IP_Header_Control (FRIHCP)	[H13]
87	IPv6 datagram	[H7]
97	FULL_HEADER	[11]
99	COMPRESSED_TCP	[11]
101	COMPRESSED_TCP_NO_DELTA	[11]
103	COMPRESSED_NON_TCP	[11]
105	COMPRESSED_RTP_8	[12]
107	COMPRESSED_RTP_16	[12]
109	COMPRESSED_UDP_8	[12]
111	COMPRESSED_UDP_16	[12]
113	CONTEXT_STATE	[11], [12]

NOTES

1 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.

2 Since the most significant octets occur first, octets with the value of zero are effectively fill octets.

3 All IPE header numbers will by definition be odd. A consequence of signaling additional octets in the IPE Header by setting the extension bit to ‘0’, results in discontinuities in the IPE header value as discussed in 3.8.2.9.

4 To support the IPE header, processing and parsing of the header is required. Besides multiplexing and demultiplexing, which can subsequently involve stateless mapping between link layer conventions used on other link layers, no additional processing is intended. Such processing would be considered to be specific to the protocols that are identified via this header.

4 SERVICE PRIMITIVES

4.1 BASIC MODEL

This subsection 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.

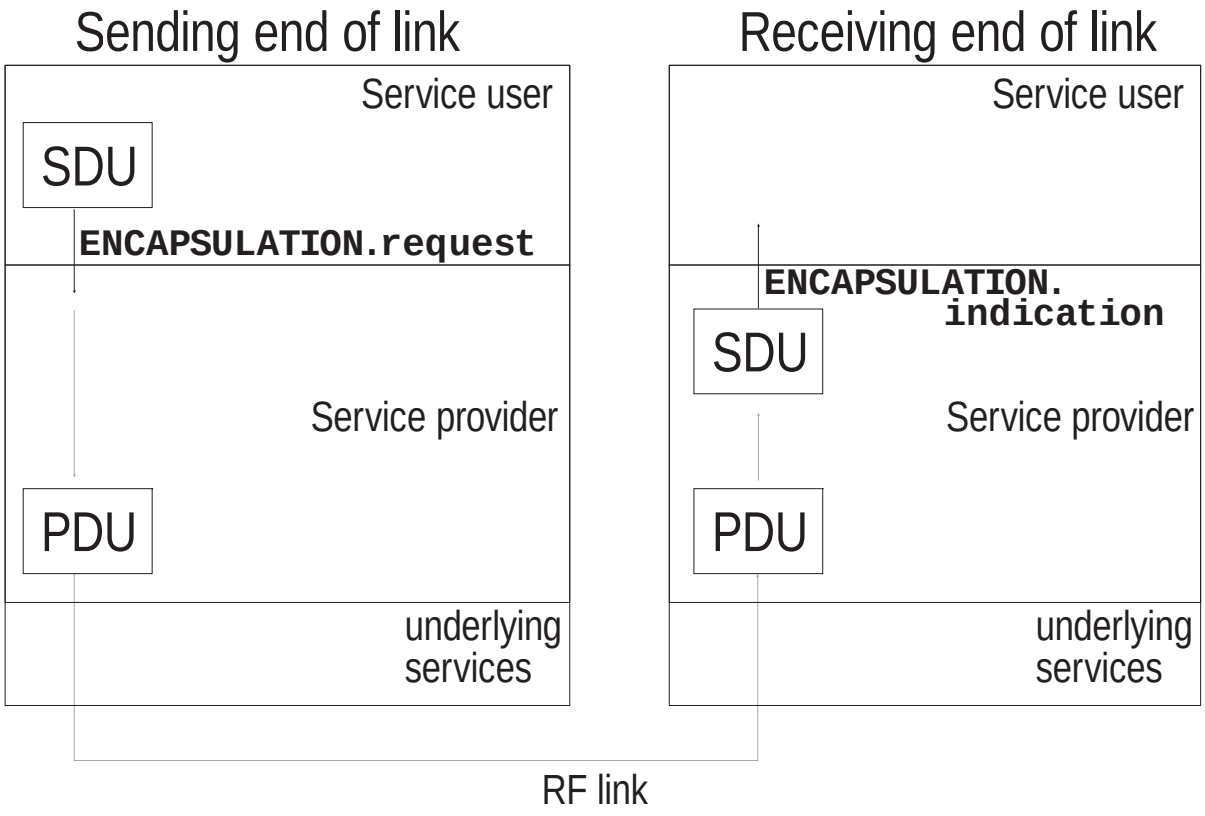


Figure 4-1: Encapsulation Service Primitives

Figure 4-1 shows the primitives of the Encapsulation Service. When the Encapsulation Service is used for the transfer of IP PDUs, then

- the Encapsulation Service PDU is the Encapsulation Packet
- the Encapsulation Service SDU 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 subsection, an implementation may provide other parameters to the service user (e.g., parameters for controlling the service, monitoring performance, facilitating diagnosis, and so on).

4.2 SERVICE PRIMITIVES

4.2.1 GENERAL

The service primitives associated with the Encapsulation Service are shown in table 4-1.

Table 4-1: Encapsulation Packet Service Primitives[2]

Data Link	Service Type	Service Primitive	Function	Semantics
AOS, TM, TC, Prox-1	*Encapsulation*	Request	Service user requests a data unit be transferred into an Encapsulation Packet over a Space Data Link layer protocol.	ENCAPSULATION.request(data unit, `SDLP_Channel`, PVN, EPI)
AOS, TM, TC, Prox-1	*Encapsulation*	Indication	When an Encapsulation Packet arrives, the data unit contained in the packet is extracted. The function of the Indication primitive is to deliver the data unit to the service user	ENCAPSULATION.indication(data unit, `SDLP_Channel`, PVN, EPI, Data Unit Loss Flag (optional))

4.2.2 ENCAPSULATION SERVICE PARAMETERS

4.2.2.1 Data Unit

Data Unit is the service data unit transferred by the Encapsulation Service; it is a delimited, octet-aligned data unit.

Although the maximum length of a data unit that can be accommodated in an encapsulating packet is 4,294,967,287 octets if the Encapsulation Packet is used, individual project organizations may establish the maximum and minimum sizes for the encapsulated data unit.

4.2.2.2 SDLP_Channel

The contents of the SDLP_Channel identifier is defined based upon the underlying service of the CCSDS Data Link Layer Protocol:

- for VCP services of TM, TC or AOS: GVCID;

- for Multiplexer Access Point Packet (MAPP) service of TC: GVCID and MAP ID;

[2] Encapsulation Service Primitives for Proximity-1 have not been formally defined; however, IP datagrams over Encapsulation Service over Proximity-1 are transferred analogously to TC, except that Port IDs are used in lieu of Virtual Channels.

- for Proximity-1: TFVC, SCID, Port ID, DFC_ID and Physical Channel ID (PCID);

It identifies the address or SAP of the underlying Space Data Link Protocol through which the Data Unit is to be transferred.

4.2.2.3 PVN

The PVN is part of the SAP address of the Encapsulation Service; it indicates whether the Space Packet or the Encapsulation Packet is to be used for encapsulating the Data Unit (see table B-3).

4.2.2.4 EPI

The Encapsulated Protocol Identifier (EPI) is part of the SAP address of the Encapsulation Service. It represents either an Application ID (APID) of a CCSDS Space Packet or the protocol ID of an Encapsulation packet. See table 2-5 for CCSDS-recognized protocol IDs.

4.2.2.5 Data Unit Loss Flag

The Data Unit Loss Flag is an optional parameter that may be used to notify the user at the receiving end of the Encapsulation Service that a sequence discontinuity has been detected and that one or more Data Units have been lost.

ANNEX A

SECURITY

(INFORMATIVE)

A1 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 subsequent sections.

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.

A2 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 [E10] provides more information regarding the choice of service and where it can be implemented.

A3 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.

A4 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.

ANNEX B

MANAGED PARAMETERS FOR CCSDS IP TRANSFER SERVICES

(INFORMATIVE)

B1 GENERAL

Table B-1 lists the managed frame-related parameters of the CCSDS link layer protocols which are relevant to the CCSDS IP transfer services.

Table B-1: Virtual Channel Managed Parameters

Managed Parameter	TM	TC	AOS	Prox-1
Transfer Frame Version Number (binary value)	'00'	'00'	'01'	'10'
Spacecraft ID	Integer	Integer	Integer	Integer
VCID	0,1,…7	0,1,…63	0, 1, …, 63	PCID[3] 0,1

B2 MANAGED PARAMETERS FOR PACKET TRANSFER

Table B-2 lists the additional managed parameters associated with transferring packets over a Virtual Channel.

Table B-2: Managed Parameters for Packet Transfer

Managed Parameter	Allowed Values
Valid Packet Version Numbers	Set of integers selected from table 7-6 of reference [8]
Maximum Packet Length (octets)	Integer
Whether incomplete Packets are required to be delivered to the user at the receiving end	Not required

[3] Proximity-1 contains a PCID field and not a Virtual Channel ID.

B3 MANAGED PARAMETERS FOR ENCAPSULATION SERVICE

In order to conserve bandwidth on the space link, some parameters associated with the Encapsulation Service are handled by management, rather than by inline communications protocol. The managed parameters are those which tend to be static for long periods of time, and whose change generally signifies a major reconfiguration of the service provider associated with a particular mission. Through the use of a management system, management conveys the required information to the service provider.

The managed parameters used for the Encapsulation Service are listed in table B-3, showing the values specific to the use of the Encapsulation Service for transfer of IP PDUs. These parameters are defined in an abstract sense, and are not intended to imply any particular implementation of a management system.

NOTE – Service Data Unit is the data unit encapsulated by the Encapsulation Packet and transferred by the Encapsulation Service.

Table B-3: Managed Parameters for Encapsulation Service

Managed Parameter	Allowed Values
Minimum Service Data Unit Length (octets)	0
Maximum Service Data Unit Length (octets)	4,294,967,287
Valid Packet Version Number	‘111’ binary (Encapsulation packet)
Valid Protocol Identifier	‘010’ binary (CCSDS IPE)

ANNEX C

NETWORK VIEWS

(INFORMATIVE)

This annex contains example implementations corresponding to the list of options in 2.1 recommending how to transfer both IPv4 and IPv6 over CCSDS data links depending upon the routing capability and needs of the on-board network. Note that the diagrams are bi-directional.

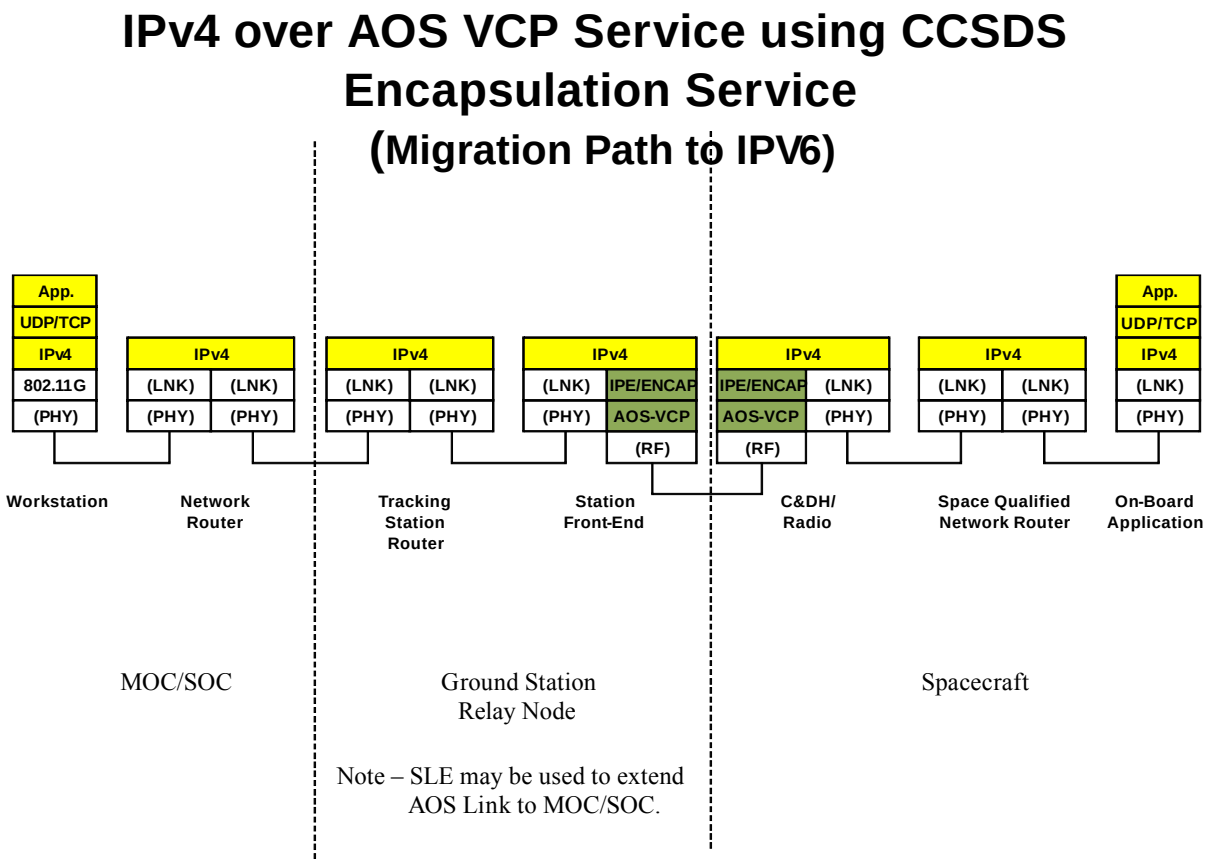


Figure C-1: IPv4 over AOS VCP Service Using CCSDS IPE plus Encapsulation Service

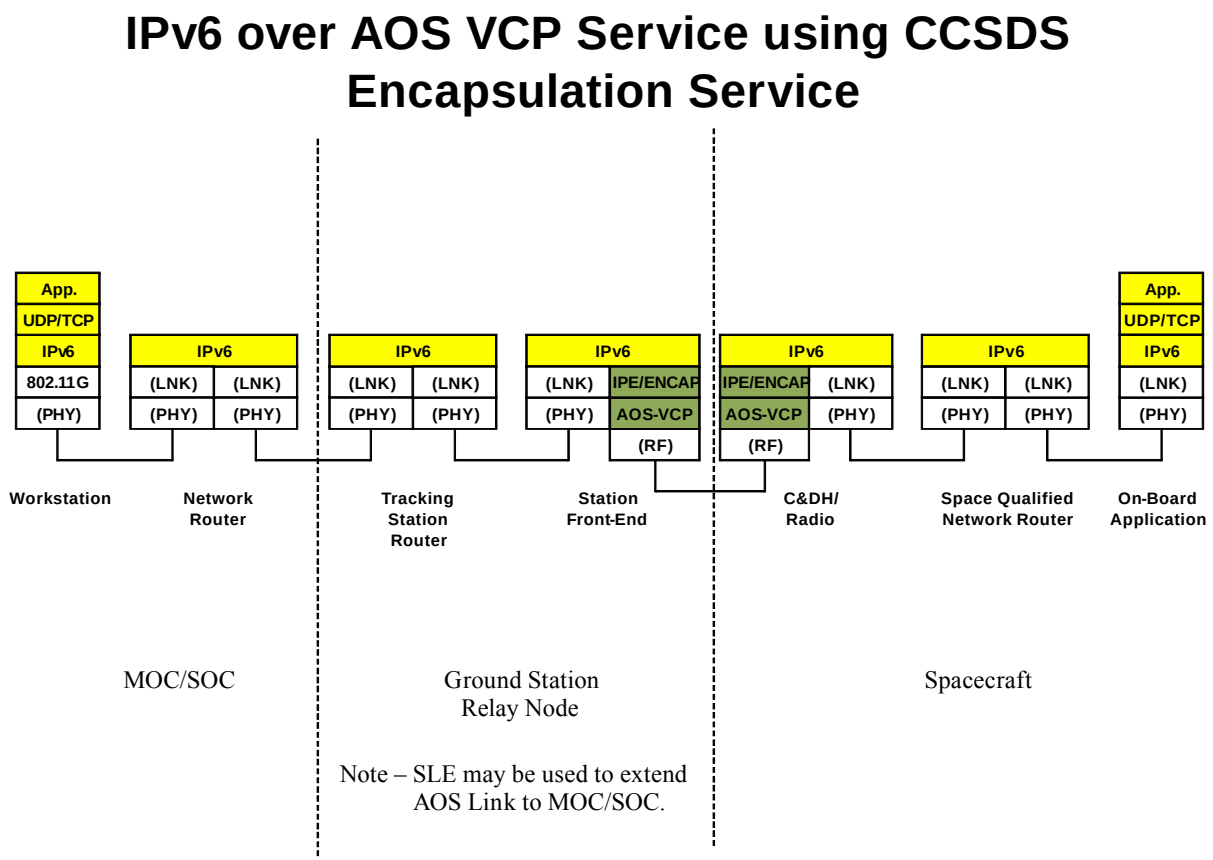


Figure C-2: IPv6 over AOS VCP Service Using CCSDS ICE plus Encapsulation Service

ANNEX D

END-TO-END UPLINK/DOWNLINK FUNCTIONAL CONTEXT DIAGRAMS

(INFORMATIVE)

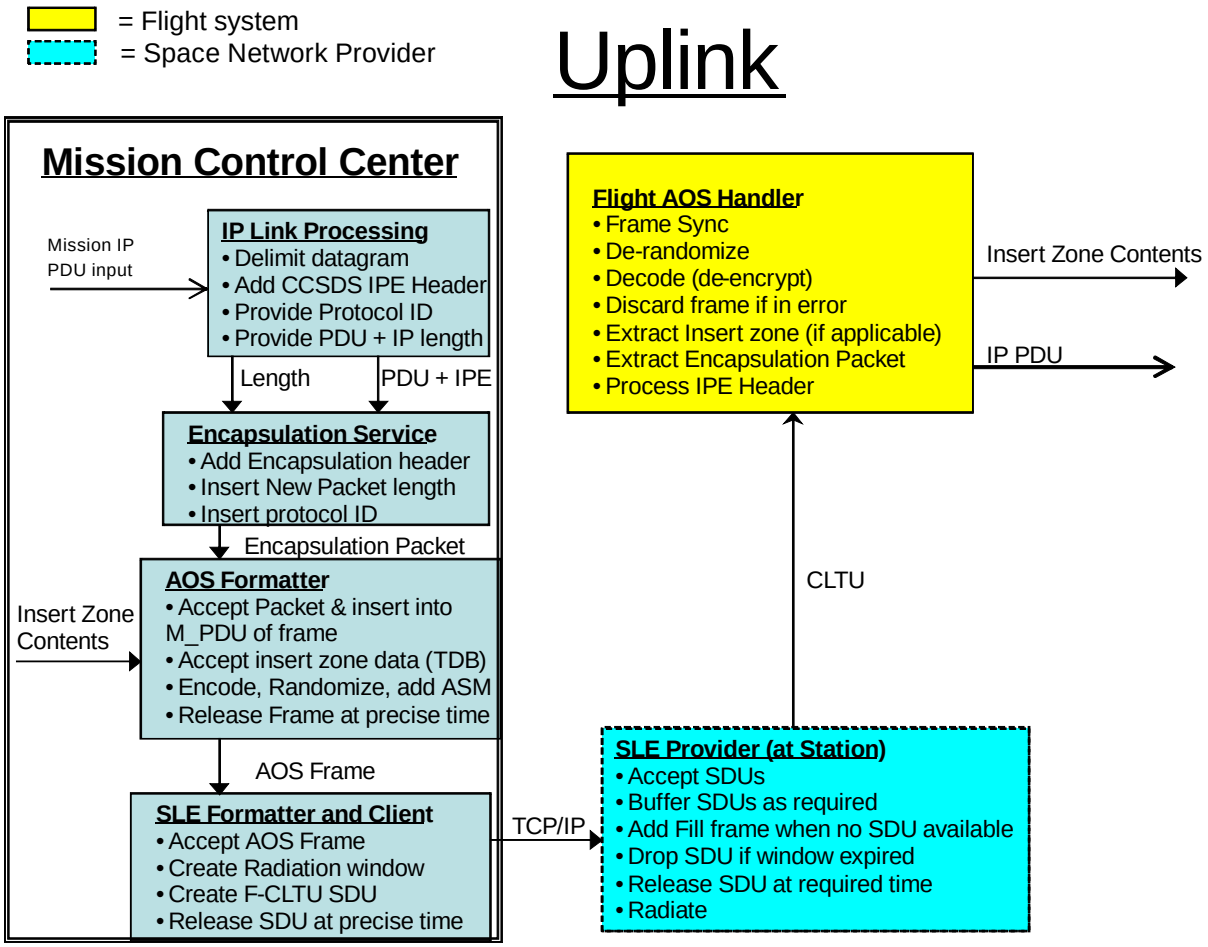


Figure D-1: End-to-End Uplink CCSDS Functional Flow for Transferring IP PDUs

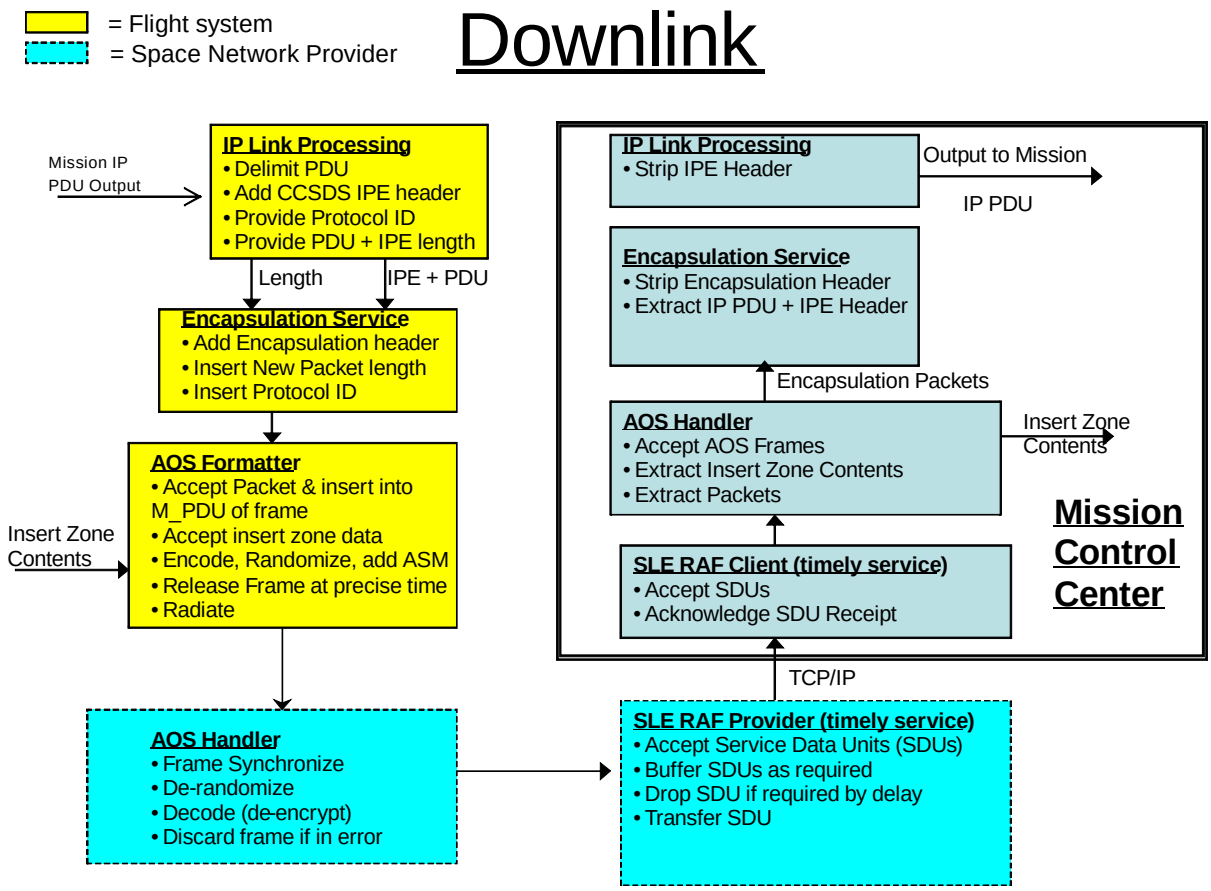


Figure D-2: End-to-End Downlink CCSDS Functional Flow for Transferring IP PDUs

ANNEX E

INFORMATIVE REFERENCES

(INFORMATIVE)

[E1] *Space Data Link Protocols—Summary of Concept and Rationale*. Report Concerning Space Data System Standards, CCSDS 130.2-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, December 2007.

[E2] *TC Synchronization and Channel Coding—Summary of Concept and Rationale*. Report Concerning Space Data System Standards, CCSDS 230.1-G-1. Green Book. Issue 1. Washington, D.C.: CCSDS, June 2006.

[E3] W. Simpson. *PPP in Frame Relay*. RFC 1973. Reston, VA: ISOC, June 1996.

[E4] C. Brown and A. Malis. *Multiprotocol Interconnect over Frame Relay*. STD 55. Reston, VA: ISOC, September 1998.

[E5] P. Karn, Ed. *Advice for Internet Subnetwork Designers*. BCP 89. Reston, VA: ISOC, July 2004.

[E6] J. Postel. *Internet Protocol*. STD 5. Reston, VA: ISOC, September 1981.

[E7] S. Deering and R. Hinden. *Internet Protocol, Version 6 (IPv6) Specification*. RFC 2460. Reston, VA: ISOC, December 1998.

[E8] *Space Communications Protocol Specification (SCPS)—Network Protocol (SCPS-NP)*. Recommendation for Space Data System Standards, CCSDS 713.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, May 1999.

[E9] *TM Synchronization and Channel Coding*. Recommendation for Space Data System Standards, CCSDS 131.0-B-1. Blue Book. Issue 1. Washington, D.C.: CCSDS, September 2003.

[E10] *The Application of CCSDS Protocols to Secure Systems*. Report Concerning Space Data System Standards, CCSDS 350.0-G-2. Green Book. Issue 2. Washington, D.C.: CCSDS, January 2006.

[E11] *CCSDS File Delivery Protocol (CFDP)*. Recommendation for Space Data System Standards, CCSDS 727.0-B-4. Blue Book. Issue 4. Washington, D.C.: CCSDS, January 2007.

[E12] Frame Relay IP Header Compression Implementation Agreement FRF.20, Frame Relay Forum Technical Committee, June 2001.

NOTE – Normative references are provided in 1.3.

ANNEX F

ACRONYM LIST

(INFORMATIVE)

AOS	Advanced Orbiting Systems
ARQ	Automatic Repeat Request
BGP	Border Gateway Protocol
CCSDS	Consultative Committee for Space Data System
ENCAP	Encapsulation (Packet Service)
ENCAP_SDU	Encapsulation Packet Service Data Unit
EPI	Encapsulated Protocol Identifier
GMAP ID	Global Multiplexer Access Point Identifier
SDLP_Channel	Space Data Link Protocol Channel Identifier
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPE	Internet Protocol Extension
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
MAP ID	Multiplexer Access Point Identifier
MAP_SDU	Multiplexer Access Point Service Data Unit
MAPP	MAP Packet (Service)
MCID	Master Channel Identifier
MTU	Maximum Transmission Unit
OSI	Open Systems Interconnection

OSPF	Open Shortest Path First
PCID	Physical Channel Identifier (Proximity-1)
PDU	Protocol Data Unit
PIM	Protocol-Independent Multicast
Prox-1	Proximity-1
PVN	Packet Version Number
RAF	Return All Frames Service (SLE Service)
RCF	Return Channel Frames Service (SLE Service)
RFC	Request for Comment
SAP	Service Access Point
SCPS-NP	Space Communication Protocol Standards – Network Protocol
SLE	Space Link Extension
SCID	Spacecraft Identifier
SDU	Service Data Unit
SLE	Space Link Extension
TC	Telecommand (pertains to TC Space Data Link Protocol)
TCP	Transmission Control Protocol
TFVN	Transfer Frame Version Number
TM	Telemetry (pertains to TM Space Data Link Protocol)
UDP	User Datagram Protocol
VC	Virtual Channel
VCDU	Virtual Channel Data Unit
VCID	Virtual Channel Identifier
VCP	Virtual Channel Packet (Service)
VCID	Virtual Channel Identifier