The Consultative Committee for Space Data Systems

Recommendation for Space Data System Standards

ENCAPSULATION PACKET PROTOCOL

RECOMMENDED STANDARD

CCSDS 133.1-B-3

BLUE BOOK

May 2020

The Consultative Committee for Space Data Systems

Recommendation for Space Data System Standards

ENCAPSULATION PACKET PROTOCOL

RECOMMENDED STANDARD

CCSDS 133.1-B-3

BLUE BOOK

May 2020

AUTHORITY

Issue:	Recommended Standard, Issue 3
Date:	May 2020
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* (CCSDS A02.1-Y-4), and the record of Agency participation in the authorization of this document can be obtained from the CCSDS Secretariat at the e-mail address below.

This document is published and maintained by:

CCSDS Secretariat
National Aeronautics and Space Administration
Washington, DC, USA
Email: secretariat@mailman.ccsds.org

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:

- 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.
- 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.
- 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 five 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

This document is a **Recommended Standard** for use in developing flight and ground systems for space missions and has been prepared by the **Consultative Committee for Space Data Systems** (CCSDS). The Encapsulation Service described herein is intended for missions that are cross-supported between Agencies of the CCSDS.

This **Recommended Standard** specifies a communications service to be used by space missions to transfer protocol data units that are not directly transferred by the Space Data Link Protocols (references [1]–[5]) over a ground-to-space, space-to-ground, or space-to-space communications link. The data units transferred with this service are encapsulated in Encapsulation Packets, defined in this document.

This **Recommended Standard** is developed from the Encapsulation Service that was defined in the Advanced Orbiting Systems (AOS) Recommended Standard (reference [C2]). In this **Recommended Standard**, that service is re-defined so that it can be used with any of the Space Data Link Protocols (references [1]–[5]).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CCSDS has processes for identifying patent issues and for securing from the patent holder agreement that all licensing policies are reasonable and non-discriminatory. However, CCSDS does not have a patent law staff, and 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-4). 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 sent to the CCSDS Secretariat at the email 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 (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 (BFSPO)/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.
- China Academy of Space Technology (CAST)/China.
- Commonwealth Scientific and Industrial Research Organization (CSIRO)/Australia.
- Danish National Space Center (DNSC)/Denmark.
- Departamento de Ciência e Tecnologia Aeroespacial (DCTA)/Brazil.
- Electronics and Telecommunications Research Institute (ETRI)/Korea.
- 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.
- Hellenic Space Agency (HSA)/Greece.
- Indian Space Research Organization (ISRO)/India.
- Institute of Space Research (IKI)/Russian Federation.
- Korea Aerospace Research Institute (KARI)/Korea.
- Ministry of Communications (MOC)/Israel.
- Mohammed Bin Rashid Space Centre (MBRSC)/United Arab Emirates.
- 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.
- Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
- Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
- South African National Space Agency (SANSA)/Republic of South Africa.
- Space and Upper Atmosphere Research Commission (SUPARCO)/Pakistan.
- Swedish Space Corporation (SSC)/Sweden.
- Swiss Space Office (SSO)/Switzerland.
- United States Geological Survey (USGS)/USA.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 133.1-B-1	Encapsulation Service, Recommended Standard, Issue 1	June 2006	Original issue, superseded
CCSDS 133.1-B-2	Encapsulation Service, Recommended Standard, Issue 2	October 2009	Issue 2, superseded
CCSDS 133.1-B-3	Encapsulation Packet Protocol, Recommended Standard, Issue 3	May 2020	Current issue: – removes the Space Packet from available encapsulation formats; – changes name from Encapsulation Service to Encapsulation Packet Protocol; – adds USLP to supported Space Data Link protocols
EC 1	Editorial Change 1	November 2020	Updates obsolete text in page header

NOTE – Changes from the previous issue are too extensive to permit meaningful change bars.

CONTENTS

CONTENTS (continued)

Figure Page

Table

1 INTRODUCTION

1.1 PURPOSE

The purpose of this Recommended Standard is to specify the Encapsulation Packet Protocol (EPP). This protocol is used to encapsulate higher-layer protocol data units that are recognized by CCSDS over applicable ground-to-space, space-to-ground, or space-to-space communications links using Space Data Link Protocols (references [1]–[5]).

1.2 SCOPE

This Recommended Standard defines the EPP in terms of

a) the service primitives provided to the users of this protocol;

b) the protocol data units employed by the service provider; and

c) the procedures performed by the service provider.

It does not specify

a) individual implementations or products;

b) the implementation of service interfaces within real systems;

c) the methods or technologies required to perform the procedures; or

d) the management activities required to configure and control the service.

1.3 APPLICABILITY

This Recommended Standard applies to the creation of Agency standards and to the future data communications over space links between CCSDS Agencies in cross-support situations. The Recommended Standard includes comprehensive specification of the service for inter-Agency cross support. It is neither a specification of, nor a design for, real systems that may be implemented for existing or future missions.

The Recommended Standard specified in this document is to be invoked through the normal standards programs of each CCSDS Agency, and is applicable to those missions for which cross support based on capabilities described in this Recommended Standard is anticipated. Where mandatory capabilities are clearly indicated in sections of the Recommended Standard, they must be implemented when this document is used as a basis for cross support. Where options are allowed or implied, implementation of these options is subject to specific bilateral cross support agreements between the Agencies involved.

1.4 RATIONALE

The CCSDS Space Data Link protocols were primarily defined to carry Application Layer data that could be directly inserted into the data field of the protocol. In order to allow these space data link protocols to carry other protocol data units, such as internetworking protocols, or file transfer or message transfer protocols, a 'shim' protocol was devised to specify unambiguously how this is to be performed.

1.5 DOCUMENT STRUCTURE

This document is divided into five numbered sections and three annexes:

a) Section 1 presents the purpose, scope, applicability, and rationale of this Recommended Standard and lists the conventions, definitions, and references used throughout the document;

b) Section 2 provides an overview of the EPP;

c) Section 3 defines the service primitives provided for this protocol;

d) Section 4 specifies the protocol data units and procedures employed by the service provider;

e) Section 5 lists the managed parameters associated with this protocol;

f) Annex B lists all abbreviations and acronyms used within this document;

g) Annex C provides a list of informative references.

1.6 CONVENTIONS AND DEFINITIONS

1.6.1 DEFINITIONS

1.6.1.1 Definitions from the Open Systems Interconnection Basic Reference Model

This Recommended Standard makes use of a number of terms defined in Open Systems Interconnection (OSI) Basic Reference Model (reference [6]). The use of those terms in this Recommended Standard is to be understood in a generic sense, that is, 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) connection;

b) entity;

c) flow control;

d) protocol data unit;

e) real system;

f) service;

g) Service Access Point (SAP);

h) SAP address;

i) service data unit.

1.6.1.2 Definitions from OSI Service Definition Conventions

This Recommended Standard makes use of a number of terms defined in reference [7]. The use of those terms in this Recommended Standard is to be understood in a generic sense, that is, 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) indication;

b) primitive;

c) request;

d) service provider; and

e) service user.

1.6.1.3 Terms Defined in This Recommended Standard

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

asynchronous: Not *synchronous* (see **synchronous**, below).

Encapsulation Idle Packet: An Encapsulation Packet that is identified by a reserved Encapsulation Protocol ID value and that contains idle data.

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.

1.6.1.4 Definition from CCSDS 232.0-B-3 (Reference [2])

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

1.6.1.5 Definition from CCSDS 732.0-B-3 (Reference [3])

idle data: A fixed-length, project-specified 'idle' pattern of binary digits, whose assignment is a project design choice.

1.6.2 NOMENCLATURE

1.6.2.1 Normative Text

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.

1.6.2.2 Informative Text

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

– Overview;

– Background;

– Rationale;

– Discussion.

1.6.3 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, that is, 'Bit 0' (see figure 1-1).

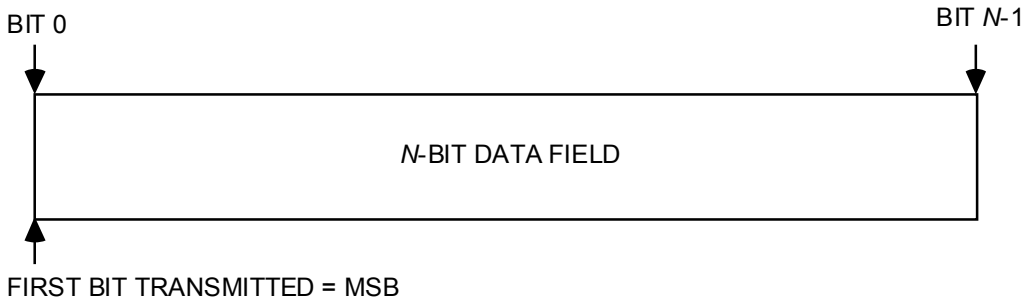

Figure 1-1: Bit Numbering Convention

In accordance with standard data-communications practice, data fields are often grouped into 8-bit 'words' that conform to the above convention. Throughout this Recommended Standard, such an 8-bit word is called an 'octet'.

The numbering for octets within a data structure starts with 0.

By CCSDS convention, all 'spare' bits shall be permanently set to value 'zero'.

1.7 REFERENCES

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] *TM Space Data Link Protocol*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 132.0-B-2. Washington, D.C.: CCSDS, September 2015.

[2] *TC Space Data Link Protocol*. Issue 3. Recommendation for Space Data System Standards (Blue Book), CCSDS 232.0-B-3. Washington, D.C.: CCSDS, September 2015.

[3] *AOS Space Data Link Protocol*. Issue 3. Recommendation for Space Data System Standards (Blue Book), CCSDS 732.0-B-3. Washington, D.C.: CCSDS, September 2015.

[4] *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.

[5] *Unified Space Data Link Protocol*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 732.1-B-1. Washington, D.C.: CCSDS, October 2018.

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

[7] *Information Technology—Open Systems Interconnection—Basic Reference Model—Conventions for the Definition of OSI Services*. International Standard, ISO/IEC 10731:1994. Geneva: ISO, 1994.

[8] "Packet Version Number." Space Assigned Numbers Authority. http://sanaregistry.org/r/packet_version_number/.

[9] "Protocol Identifier for Encapsulation Service." Space Assigned Numbers Authority. http://sanaregistry.org/r/protocol_id/.

[10] "Extended Protocol Identifiers." Space Assigned Numbers Authority. http://sanaregistry.org/r/extended_protocol_id/.

NOTE – Informative references are listed in annex C.

2 OVERVIEW

2.1 CONCEPT OF THE ENCAPSULATION PACKET PROTOCOL

The EPP is used to transfer protocol data units recognized by CCSDS (references [9] and [10]) that are *not directly transferred* by the Space Data Link Protocols (references [1]–[5]) over an applicable ground-to-space, space-to-ground, or space-to-space communications link.

Data units that can be directly transferred by the Space Data Link Protocols have a Packet Version Number (PVN) authorized by CCSDS. (A list of the Packet Version Numbers presently authorized by CCSDS is contained in reference [8].) The main purpose of the EPP is to provide a mechanism to transfer protocol data units without an authorized PVN over a space link.

The EPP is a 'shim' protocol that utilizes the packet services of the Space Data Link Protocols of the Data Link Layer defined in references [1]–[5], and therefore is intended to be used together with one of these references.

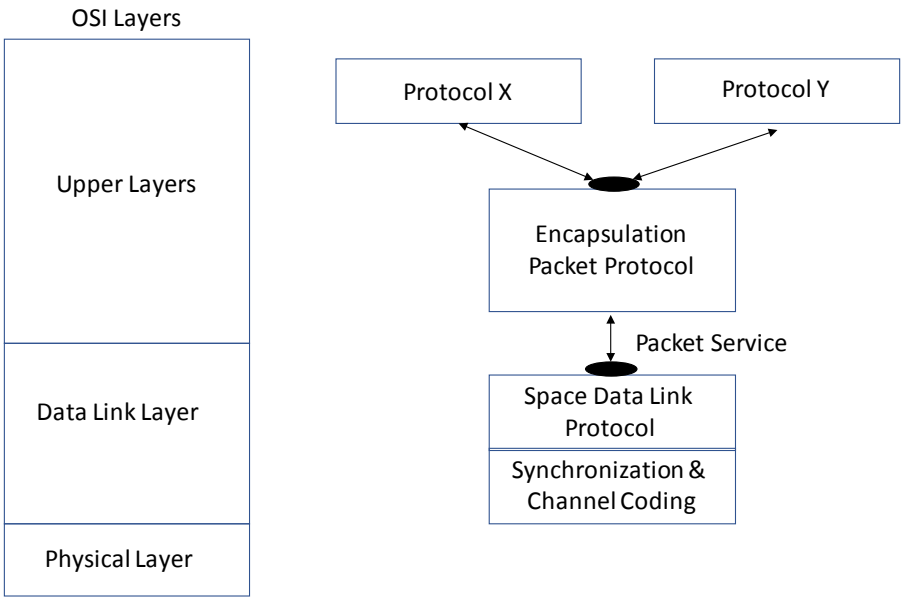

Figure 2-1: Concept of Encapsulation Packet Protocol

Figure 2-1 illustrates the concept of this protocol. Protocol data units of Protocols X and Y, which do not have an authorized PVN, are transferred with the EPP within the Data Link Layer. Protocol data units of Protocols X and Y are encapsulated in Encapsulation Packets, defined in 4.1 of this document, and are eventually transferred using one of the VC/MAP/Proximity-1 Packet Services of a Space Data Link Protocol. Management shall establish which Space Data Link Protocol is to be used to transfer encapsulated protocol data units.

2.2 FEATURES OF THE ENCAPSULATION PACKET PROTOCOL

The EPP transfers a sequence of variable-length, delimited, octet-aligned protocol data units within the data field of a Space Data Link Protocol over a space link. A user of this protocol is a protocol entity that sends or receives protocol data units that do not have an authorized PVN.

A data unit supplied by the protocol user is encapsulated unchanged into an Encapsulation Packet, and a single data unit is encapsulated into a single packet.

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

The point at which an instance of this protocol is provided to a user is called a Service Access Point (SAP) (reference [6]). 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 an 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 EPP are as follows:

The Encapsulation Packet Protocol entity at the source end system generates Encapsulation Packets from protocol data units supplied by the source user application. The transfer of data is one-way, that is, 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. 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. Furthermore, there are no timing relationships between the transfer of protocol 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 underlying service provider on the data generation rate. Although the Encapsulation.indication primitive acknowledges the receipt of the Encapsulation.request from the user, the sending user does not receive confirmation from the receiving end indicating that data has been received. Moreover, there is no guarantee that the data was completely transferred, but the service provider may signal gaps in the sequence of data units delivered to the receiving user. Finally, 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.

2.3 ADDRESSING

A user of the EPP is identified by the Encapsulated Protocol Identifier (EPI). The Encapsulation Packet is a protocol data unit defined in section 4 of this document.

Encapsulation Protocol Identifiers are registered as 'defined Protocol IDs' in reference [9].

A SAP is identified by the combination of a PVN, an EPI, and a Space Data Link Protocol (SDLP) channel through which the data units supplied by the user are to be transferred.

2.4 PROTOCOL DESCRIPTION

The EPP is described in terms of

a) the primitives provided to the users of this protocol;

b) the protocol data units employed by the protocol for encapsulation; and

c) the procedures performed by the protocol.

The 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 unit (i.e., the Encapsulation Packet) defines 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 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.

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 PARAMETERS

NOTE – The parameters used by the EPP primitives are described in subsections 3.2.1 through 3.2.3.

3.2.1 DATA UNIT

3.2.1.1 The parameter Data Unit is the service data unit transferred by the EPP, and it shall be a delimited, octet-aligned data unit.

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

3.2.2 SDLP_CHANNEL

3.2.2.1 The parameter SDLP_Channel is part of the SAP address of the EPP, and it shall uniquely identify the channel of the underlying SDLP through which the protocol data unit is to be transferred.

3.2.2.2 The contents of SDLP_Channel depend on the underlying SDLP service:

a) for the Virtual Channel Packet (VCP) service of TM (reference [1]), TC (reference [2]), or AOS (reference [3]), SDLP_Channel shall contain the Global Virtual Channel Identifier (GVCID);

b) for the MAP Packet (MAPP) service of TC (reference [2]) and USLP (reference [5]), SDLP_Channel shall contain the Global MAP ID (GMAP ID);

c) for the Packet Service of Proximity-1 (reference [4]), SDLP_Channel shall contain the Transfer Frame Version Number, the Spacecraft Identifier (SCID), the Physical Channel Identifier (PCID), the Data Field Construction ID (DFC_ID), and the Port ID.

NOTE – Definitions of Virtual Channel, MAP, GVCID, GMAP ID, Transfer Frame Version Number, SCID, PCID, and Port ID can be found in references [1]–[5].

3.2.3 EPI

The EPI is part of the SAP address of the EPP. It identifies the external protocol data unit to be encapsulated by this protocol. It is registered in SANA as the 'Encapsulation Protocol Identifier' in reference [9] and defined in section 4 of this document.

3.3 SERVICE PRIMITIVES

3.3.1 GENERAL

The service primitives associated with this service are:

a) ENCAPSULATION.request. The ENCAPSULATION.request primitive shall be passed from the protocol user at the sending end to the service provider to request that a protocol data unit be transferred, through the underlying Space Data Link Protocol, to the user at the receiving end.

b) ENCAPSULATION.indication. The ENCAPSULATION.indication shall be passed from the service provider to the protocol user at the receiving end in order to deliver a protocol data unit.

3.3.2 ENCAPSULATION.REQUEST

3.3.2.1 Function

The ENCAPSULATION.request primitive shall be the service request primitive for the EPP.

3.3.2.2 Semantics

The ENCAPSULATION.request primitive shall provide parameters as follows:

ENCAPSULATION.request	(Data Unit, SDLP_Channel, EPI)

NOTE – Information on the management of the SDLP_Channel, on the management of EPI parameters, and on where applicable values are defined is contained in 3.2.2, reference [8], and reference [9], respectively.

3.3.2.3 When Generated

The ENCAPSULATION.request primitive shall be passed to the service provider to request it to send the protocol data unit.

3.3.2.4 Effect on Receipt

Receipt of the ENCAPSULATION.request primitive shall cause the service provider to transfer the protocol data unit.

3.3.2.5 Additional Comments

The ENCAPSULATION.request primitive shall be used to transfer protocol data units across the space link through the underlying Space Data Link Protocol.

3.3.3 ENCAPSULATION.INDICATION

3.3.3.1 Function

The ENCAPSULATION.indication primitive shall be the service indication primitive for the EPP.

3.3.3.2 Semantics

The ENCAPSULATION.indication primitive shall provide parameters as follows:

ENCAPSULATION.indication	(Data Unit, SDLP_Channel, EPI)

NOTE – Information on the management of the SDLP_Channel, on the management of EPI parameters, and on where applicable values are defined is contained in 3.2.2, reference [8], and reference [9], respectively.

3.3.3.3 When Generated

The ENCAPSULATION.indication primitive shall be passed from the service provider to the protocol user at the receiving end in order to deliver a protocol data unit.

3.3.3.4 Effect on Receipt

The effect on receipt of the ENCAPSULATION.indication primitive by the protocol user is undefined.

3.3.3.5 Additional Comments

The ENCAPSULATION.indication primitive shall be used to deliver protocol data units to the protocol user identified by the SDLP_Channel and EPI.

4 DATA UNITS AND PROCEDURES

4.1 ENCAPSULATION PACKET

4.1.1 GENERAL

4.1.1.1 An Encapsulation Packet shall encompass the major fields, positioned contiguously, in the following sequence:

a) Packet Header (1 to 8 octets, mandatory);

b) Encapsulated Data Field (from 0 to 4,294,967,287 octets, optional).

4.1.1.2 An Encapsulation Packet shall consist of at least 1 and at most 4,294,967,295 octets.

NOTES

1 The maximum Encapsulation Packet length allowed by a particular spacecraft or ground implementation may be less than the maximum specified here.

2 The structural components of the Encapsulation Packet are shown in figure 4-1.

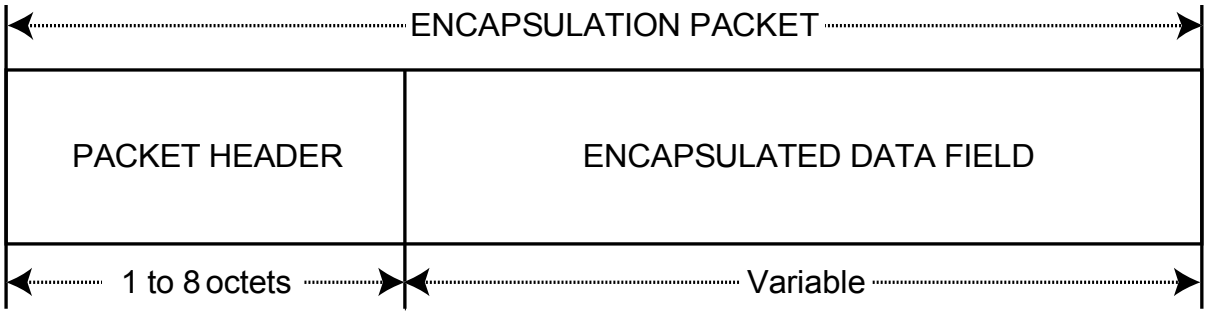

Figure 4-1: Encapsulation Packet Structural Components

4.1.2 ENCAPSULATION PACKET HEADER

4.1.2.1 General

4.1.2.1.1 The Packet Header is mandatory and it shall have a length of one, two, four, or eight octets. The Packet Header shall consist of three, four, six, or seven fields, positioned contiguously, in the following sequence:

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

b) Encapsulation 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 4-2);

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

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

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

NOTE – The format of the Packet Header is shown in figure 4-2.

ENCAPSULATION PACKET HEADER

PACKET VERSION NUMBER 3 bits	ENCAPSULATION PROTOCOL ID 3 bits	LENGTH OF LENGTH 2 bits	USER DEFINED FIELD 0 or 4 bits	ENCAPSULATION 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 4-2: Packet Header

4.1.2.1.2 An implementation of the EPP shall be capable of receiving Encapsulation Packets with fixed- or variable-length headers.

NOTE – An implementation on the transmitting end may choose to use either a fixed Packet Header size or adaptively/dynamically adjust the Packet Header size according to the payload size in order to optimize bandwidth use (minimize header overhead).

4.1.2.2 Packet Version Number

4.1.2.2.1 Bits 0-2 of the Packet Header shall contain the (Binary Encoded) Packet Version Number.

4.1.2.2.2 This 3-bit field shall identify the data unit as an Encapsulation Packet defined by this subsection; it shall be set to '111'.

NOTE – The Version Number is used to reserve the possibility of introducing other packet structures. This subsection defines 'Encapsulation Packet (Version 8 CCSDS Packet)', whose Binary Encoded Version Number is '111'.

4.1.2.3 Encapsulation Protocol ID

4.1.2.3.1 Bits 3-5 of the Packet Header shall contain the EPI.

4.1.2.3.2 The EPI shall be used to identify the protocol whose data unit is encapsulated within the Encapsulation Packet.

4.1.2.3.3 The EPIs recognized by CCSDS for the Encapsulation Packet shall be registered in reference [9].

NOTES

1 The value '000' in the Encapsulation Protocol ID field signals that the packet is an Encapsulation Idle Packet. Encapsulation Idle Packets may be used to fill space in a fixed-length Transfer Frame used in references [1], [3], and [5].

2 The value '110' in the Encapsulation Protocol ID field signals that the 4-bit Encapsulation Protocol ID Extension field is used for protocol identification.

3 The value '111' in the Encapsulation Protocol ID field signals that the Encapsulated Data field contains mission-specific, privately defined data.

4.1.2.4 Length of Length

4.1.2.4.1 Bits 6-7 of the Packet Header shall contain the Length of Length field.

4.1.2.4.2 The Length of Length field shall define the length of the Packet Length field.

4.1.2.4.3 The value of this field shall be interpreted as shown in table 4-1.

Table 4-1: Interpretation of Length of Length Field

Value of 'Length of Length' Field (binary)	Length of 'Packet Length' Field
00	0
01	1 octet
10	2 octets
11	4 octets

4.1.2.4.4 If the Length of Length field has the value '00' then the Protocol ID field shall have the value '000', indicating that the packet is an Encapsulation Idle Packet.

NOTE – If the Length of Length field has the value '00', then the Packet Length field and the Encapsulated Data Unit field are both absent from the packet. In this case, the length of the Encapsulation Packet is one octet.

4.1.2.5 User Defined Field

4.1.2.5.1 If present, the User Defined field shall be four bits in length and shall follow, without gap, the Length of Length field.

4.1.2.5.2 The User Defined field shall be used for sending mission-specific, privately defined header data.

4.1.2.6 Encapsulation Protocol ID Extension

4.1.2.6.1 If present, the Encapsulation Protocol ID Extension field shall be four bits in length and shall follow, without gap, the User Defined field.

4.1.2.6.2 If the Encapsulation Protocol ID field contains the value '110', then this field shall be used to identify the protocol whose data unit is encapsulated within the Encapsulation Packet.

4.1.2.6.3 If the Encapsulation Protocol ID field does not contain the value '110', then the Encapsulation Protocol ID Extension field shall be set to 'all zeros'.

4.1.2.6.4 The extended Encapsulation Protocol IDs shall be registered in reference [10].

4.1.2.7 CCSDS Defined Field

4.1.2.7.1 If present, the CCSDS Defined field shall be two octets in length and shall follow, without gap, the Encapsulation Protocol ID Extension field.

4.1.2.7.2 The CCSDS Defined field is reserved for future use by CCSDS and is by convention set to 'all zeros'.

4.1.2.8 Packet Length

4.1.2.8.1 If present, the Packet Length field shall be the final field in the Encapsulation Packet Header (see figure 4-2).

4.1.2.8.2 If the value of the Length of Length field is '00', the Packet Length field shall be absent. Otherwise, the Packet Length field shall contain a binary number corresponding to the total length of the Encapsulation Packet (in octets), including the Packet Header. See table 4-2.

NOTES

1 Although unlikely to be used in space, a 4-octet Packet Length field permits accommodating IPv6 (reference [C7]) 'Jumbograms' up to 4,294,967,287 ($=2^{32}$-5) octets in length.

2 If the Packet Length field is absent (i.e., the value of the Length of Length field is '00'), then the length of the Encapsulation Packet is one octet.

Table 4-2: 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.					

4.1.3 ENCAPSULATED DATA FIELD

4.1.3.1.1 If present, the Encapsulated Data field shall follow, without gap, the Packet Length field. It shall consist of an integral number of octets.

4.1.3.1.2 The Encapsulated Data field shall contain the protocol data as indicated by the Encapsulation Protocol ID field, and by the Encapsulation Protocol ID Extension field if present.

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

4.1.3.1.4 Under the following conditions, the Encapsulated Data field shall be 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.

4.1.3.1.5 If the Encapsulated Data field is absent, then the Encapsulation Protocol ID field shall contain the value '000'.

NOTES

1 When the Encapsulation Packet is generated as a result of an ENCAPSULATION.request to the EPP, then the Encapsulated Data field contains the protocol data unit supplied by the protocol 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 as Idle Packets by the TM Space Data Link Protocol (reference [1]) and by the AOS Space Data Link Protocol (reference [3]) and Unified Space Data Link Protocol (reference [5]). These protocols generate Idle Packets when needed to maintain synchronization of the data transport processes.

3 CCSDS does not specify the bit pattern of idle data.

4.2 PROCEDURES AT THE SENDING END

NOTE – This subsection describes procedures for providing the EPP at the sending end (see figure 4-3). The procedures described here are defined in an abstract sense and are not intended to imply any particular implementation approach of the service.

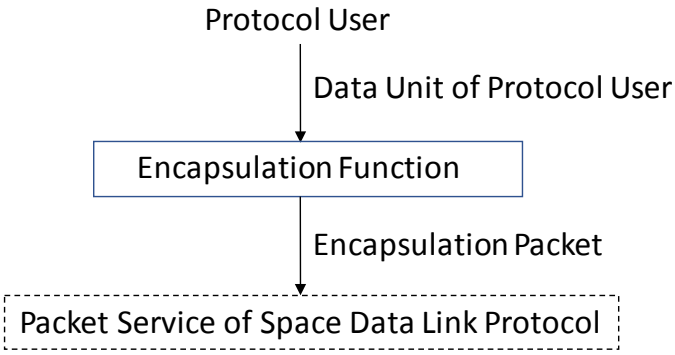

Figure 4-3: Internal Organization of Encapsulation Packet Protocol (Sending End)

4.2.1.1.1 The Encapsulation Function (see figure 4-3) shall be used to encapsulate data units supplied by the service users.

4.2.1.1.2 The Encapsulation Function receives data units from the protocol users. Any data unit that violates the limits of the size shall be rejected.

4.2.1.1.3 Each valid data unit shall be encapsulated in an Encapsulation Packet and passed to the Packet Service of the underlying Space Data Link Protocol.

4.3 PROTOCOL PROCEDURES AT THE RECEIVING END

NOTE – This subsection describes procedures for providing the EPP at the receiving end (see figure 4-4). The procedures described here are defined in an abstract sense and are not intended to imply any particular implementation approach of the service.

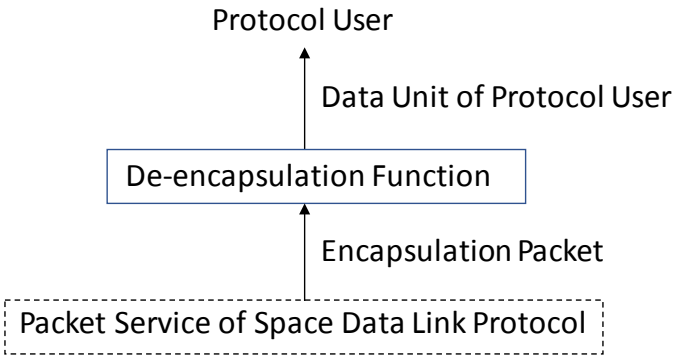

Figure 4-4: Internal Organization of Encapsulation Packet Protocol (Receiving End)

4.3.1.1.1 The De-encapsulation Function (see figure 4-4) shall be used to extract data units supplied by the service users.

4.3.1.1.2 The De-encapsulation Function shall receive Encapsulation Packets, from the Packet Service of the underlying Space Data Link Protocol, and extract original data units by stripping the headers of the Encapsulation packets.

4.3.1.1.3 Extracted protocol data units shall be delivered to the service user identified by the EPI or the extended EPI.

5 MANAGED PARAMETERS

In order to conserve bandwidth on the space link, some parameters associated with the EPP 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 are listed in table 5-1. These parameters are defined in an abstract sense, and are not intended to imply any particular implementation of a management system.

Table 5-1: Managed Parameters for Encapsulation Packet Protocol (Encapsulation Packet Used)

Managed Parameter	Allowed Values	Defined In
Minimum Data Unit Length (octets)	Integer	4.1
Maximum Data Unit Length (octets)	Integer	4.1
Valid Encapsulation Protocol Identifiers	Set of integers	Reference [9]
Valid Extended Encapsulation Protocol Identifiers	Set of integers	Reference [10]

ANNEX A

SECURITY, SANA, AND PATENT CONSIDERATIONS

(INFORMATIVE)

A1 SECURITY CONSIDERATIONS

The Encapsulation protocol does not provide any security function. Nevertheless, security functions (authentication, confidentiality, and integrity) can be implemented either at the data link layer using Space Data Link Security (SDLS) protocols (references [C3], [C4]) or at the network layer using Bundle Security Protocol (reference [C5]).

A2 SANA CONSIDERATIONS

A2.1 GENERAL

This section contains two modified SANA registry requests for the EPP.

A2.2 NEW REGISTRY REQUESTS

None.

A2.3 MODIFIED REGISTRIES

A2.3.1 The working group requests that SANA change the descriptive name of the registry currently called ‘Protocol Identifier for Encapsulation Service’ to ‘Protocol Identifier for Encapsulation Packet Protocol’. The registry itself is not to be changed.

Reference: CCSDS 133.1-B-2

A2.3.2 The working group requests that SANA change the descriptive name in the registry currently called ‘Extended Protocol Identifier for Encapsulation Service’ to ‘Extended Protocol Identifier for Encapsulation Packet Protocol’. The registry itself is not to be changed.

Reference: CCSDS 133.1-B-2

ANNEX B

ABBREVIATIONS AND ACRONYMS

(INFORMATIVE)

This annex lists the abbreviations and acronyms used in this Recommended Standard.

AOS	Advanced Orbiting Systems
CCSDS	Consultative Committee for Space Data Systems
DFC_ID	Data Field Construction Identifier
EPI	Encapsulated Protocol Identifier
EPP	Encapsulation Packet Protocol
GVCID	Global Virtual Channel Identifier
IPv6	Internet Protocol, Version 6
OSI	Open Systems Interconnection
MSB	Most Significant Bit
PVN	Packet Version Number
SAP	Service Access Point
SDLP	Space Data Link Protocol
TFVN	Transfer Frame Version Number

ANNEX C

INFORMATIVE REFERENCES

(INFORMATIVE)

[C1] *Organization and Processes for the Consultative Committee for Space Data Systems*. Issue 4. CCSDS Record (Yellow Book), CCSDS A02.1-Y-4. Washington, D.C.: CCSDS, April 2014.

[C2] *Advanced Orbiting Systems, Networks and Data Links: Architectural Specification*. Issue 3-S. Recommendation for Space Data System Standards (Historical), CCSDS 701.0-B-3-S. Washington, D.C.: CCSDS, (June 2001) August 2005.

[C3] *Space Data Link Security Protocol*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 355.0-B-1. Washington, D.C.: CCSDS, September 2015.

[C4] *Space Data Link Security Protocol—Extended Procedures*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 355.1-B-1. Washington, D.C.: CCSDS, February 2019.

[C5] *CCSDS Streamlined Bundle Security Protocol Specification*. Issue 1. Draft Recommendation for Space Data System Standards (Red Book), CCSDS 734.5-R-1. Washington, D.C.: CCSDS, March 2018.

[C6] *Space Data Link Protocols—Summary of Concept and Rationale*. Issue 3. Report Concerning Space Data System Standards (Green Book), CCSDS 130.2-G-3. Washington, D.C.: CCSDS, September 2015.

[C7] S. Deering and R. Hinden. *Internet Protocol, Version 6 (IPv6) Specification*. RFC 1883. Reston, Virginia: ISOC, December 1995.

[C8] *The Application of Security to CCSDS Protocols*. Issue 3. Report Concerning Space Data System Standards (Green Book), CCSDS 350.0-G-3. Washington, D.C.: CCSDS, March 2019.

NOTE – Normative references are listed in subsection 1.7.