The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Practices

CFDP UNITDATA TRANSFER LAYERS

DRAFT RECOMMENDED PRACTICE

CCSDS 722.1-P-1.1

PINK BOOK

December 2024

The Consultative Committee for Space Data Systems

Draft Recommendation for
Space Data System Practices

CFDP UNITDATA TRANSFER LAYERS

DRAFT RECOMMENDED PRACTICE

CCSDS 722.1-P-1.1

PINK BOOK

December 2024

AUTHORITY

Issue:	Pink Book, Issue 1.1
Date:	December 2024
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 *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 email 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

(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 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

This document is a technical **Recommended Practice** 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 **Recommended Practice** described herein is intended for missions that are cross-supported between Agencies of the CCSDS.

This **Recommended Practice** specifies methods for operating the CCSDS File Delivery Protocol (CFDP) over the CCSDS Space Packet Protocol, the CCSDS Encapsulation Packet Protocol, the CCSDS Bundle Protocol, the CCSDS Licklider Transmission Protocol, UDP/IP, and TCP/IP.

Through the process of normal evolution, it is expected that expansion, deletion, or modification of this document may occur. This Recommended Practice is therefore subject to CCSDS document management and change control procedures, which are defined in the *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 Science Policy Office (BELSPO)/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.
- Egyptian Space Agency (EgSA)/Egypt.
- 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.
- Netherlands Space Office (NSO)/The Netherlands.
- 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.

PREFACE

This document is a draft CCSDS Recommended Practice. Its 'Pink Book' 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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

DOCUMENT CONTROL

Document	Title	Date	Status
CCSDS 722.1-M-1	Operation of CFDP over Encapsulation Service, Recommended Practice, Issue 1	March 2014	Original issue
CCSDS 722.1-P-1.1	CFDP Unitdata Transfer Layers, Draft Recommended Practice, Issue 1.1	December 2024	Current draft update: addresses the change from Encapsulation Service to Encapsulation Packet Protocol (CCSDS 133.1-B-3) and extends supported underlying transport layers.

NOTE – Changes from the original issue are too numerous to permit meaningful markup.

CONTENTS

1 INTRODUCTION

1.1 PURPOSE AND SCOPE OF THIS DOCUMENT

The CCSDS File Delivery Protocol (CFDP, reference [1]) has been designed to support the transfer of files in a variety of mission scenarios. CFDP offers different qualities of service ranging from best effort to fully reliable and has been specifically optimized for long delay, noisy, and disjoint links. CFDP requires a simple minimum service from the underlying protocols, operating over any link providing a communication service.

The purpose of this document is to specify the operation of CFDP over the CCSDS Encapsulation Packet Protocol (EPP) (reference [2]), CCSDS Space Packet Protocol (SPP) (reference [3]), CCSDS Bundle Protocol (BP) (reference [4]), and CCSDS Licklider Transmission Protocol (LTP) (reference [5]) as provided for Earth-to-spacecraft, spacecraft-to-Earth, and spacecraft-to-spacecraft communications. In addition, it specifies CFDP UT Layers for UDP and TCP, which might be used in terrestrial testing or in combination with CCSDS IP Encapsulation (reference [6]).

1.2 APPLICABILITY

This document applies to any mission or equipment claiming to provide a CCSDS-compliant CFDP capability between two CFDP entities.

1.3 RATIONALE

This document is needed to clarify how CFDP should be used with SPP, EPP, BP, LTP, UDP, and TCP.

1.4 DOCUMENT STRUCTURE

The document has three major sections and two annexes:

- section 1 (this section), containing administrative information, definitions, and references;
- section 2, describing the communications architecture of CFDP operating over an underlying communication protocol;
- section 3, defining CFDP UT Layers for SPP, EPP, BP, LTP, UDP, and TCP;
- annex A, listing informative references;
- annex B, providing security, SANA/IANA and patent considerations;
- annex C, expanding abbreviations used in the document.

1.5 CONVENTIONS AND DEFINITIONS

1.5.1 DEFINITIONS

1.5.1.1 General

For the purpose of this document the following definitions apply.

1.5.1.2 Definitions from the OSI Basic Reference Model

This document is defined using the style established by the Open Systems Interconnection (OSI) Basic Reference Model (reference [B1]). This model provides a common framework for the development of standards in the field of systems interconnection.

The following terms, used in this Recommended Practice, are adapted from definitions given in reference [B1]:

layer: A subdivision of the architecture, constituted by subsystems of the same rank.

protocol data unit, PDU: A unit of data specified in a protocol and consisting of protocol-control information and possibly user data.

protocol ID: An identifier that specifies the layer-(*N+1*) protocol (type of service data unit) encapsulated within a PDU at layer *N*.

service: The capability of a layer (service provider) together with the layers beneath it, provided to the service users.

service data unit, SDU: A set of data that is sent by a user of the services of a given layer and is transmitted to a peer service user semantically unchanged.

1.5.1.3 Definitions of Terms as Used in this Recommended Practice

packet: A delimited, octet-aligned data unit.

1.6 NOMENCLATURE

1.6.1 NORMATIVE TEXT

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

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 INFORMATIVE TEXT

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

– Overview;

– Background;

– Rationale;

– Discussion.

1.7 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] *CCSDS File Delivery Protocol (CFDP)*. Issue 5. Recommendation for Space Data System Standards (Blue Book), CCSDS 727.0-B-5. Washington, D.C.: CCSDS, July 2020.

[2] *Encapsulation Packet Protocol*. Issue 3. Recommendation for Space Data System Standards (Blue Book), CCSDS 133.1-B-3. Washington, D.C.: CCSDS, May 2020.

[3] *Space Packet Protocol*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 133.0-B-2. Washington, D.C.: CCSDS, June 2020.

[4] *CCSDS Bundle Protocol Specification*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 734.2-B-1. Washington, D.C.: CCSDS, September 2015.

[5] *Licklider Transmission Protocol (LTP) for CCSDS*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 734.1-B-1. Washington, D.C.: CCSDS, May 2015.

[6] *IP over CCSDS Space Links*. Issue 1. Recommendation for Space Data System Standards (Blue Book), CCSDS 702.1-B-1. Washington, D.C.: CCSDS, September 2012.

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

[8] "LTP Client Service Identifiers." Internet Assigned Numbers Authority. https://www.iana.org/assignments/ltp-parameters/ltp-parameters.xhtml#client-service-ids.

2 OVERVIEW

2.1 GENERAL

The specification of CFDP is provided by reference [1]. The standard is supplemented by three informational reports, references [B2], [B3], and [B4], and the reader is directed to these for a more detailed explanation of the protocol and its intended targets.

CFDP is designed to run over an Underlying Transport (UT) service that provides to CFDP the following primitives:

– `UNITDATA.request` (UT_SDU, UT address);

– `UNITDATA.indication` (UT_SDU, UT address).

The services required of the UT Layer are discussed in reference [1].

This document maps the primitives that CFDP requires onto those provided by SPP, EPP, BP, and LTP, and it specifies the sending of CFDP PDUs over UDP and TCP (section 3).

2.2 CONTEXT AND GUIDELINES

The protocol configuration for CFDP communication is shown in figure 2-1. CFDP entities communicate with each others via means of Unitdata.requests and Unitdata.indications using appropriate communication protocols over available communication links.

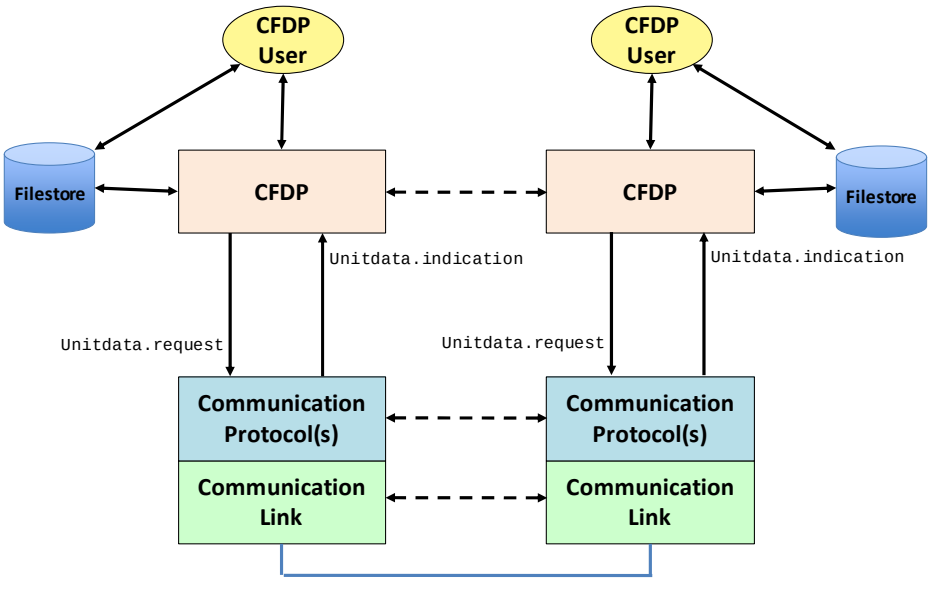

Figure 2-1: CFDP Communication Using Unitdata Requests and Indications

3 CFDP UNITDATA TRANSFER LAYERS

3.1 GENERAL

3.1.1 For CCSDS-compliant space links, CFDP shall operate over EPP, SPP, BP, or LTP (references [2], [3], [4], and [5]).

3.1.2 For CCSDS space links, CFDP may also operate using TCP/IP or UDP/IP with CCSDS IP Encapsulation (reference [6]).

3.1.3 For terrestrial links, CFDP may also operate using TCP/IP or UDP/IP.

3.1.4 An aggregation of CFDP PDU shall be a single CFDP PDU or a concatenation of several complete CFDP PDU with the same destination entity ID without any additional data.

NOTE – The aggregated CFDP PDU can belong to different CFDP transactions. Aggregation is used for some UT Layers (BP, LTP) for efficiency reasons.

3.2 ENCAPSULATION PACKET PROTOCOL UT LAYER

3.2.1 DISCUSSION

The Encapsulation Packet Protocol (reference [2]) provides the following service primitives and parameters:

– `ENCAPSULATION.request` (data unit, SDLP_Channel, EPI);

– `ENCAPSULATION.indication` (data unit, SDLP_Channel, EPI).

where:

– data unit is the Service Data Unit (SDU) transferred by the EPP.

– SDLP_Channel is part of the SAP address of the EPP. It uniquely identifies the channel of the underlying Space Data Link Protocol (SDLP) through which the PDU is to be transferred. Reference [2] describes the SDLP_Channel semantics, of which the exact semantics depend on the underlying SDLP services.

– The Encapsulation Protocol Identifier (EPI) is part of the SAP address of the encapsulation service; it identifies the external PDU to be encapsulated by this protocol.

3.2.2 EQUIVALENCES

3.2.2.1 To reconcile the service required by CFDP and the service provided by EPP, the following equivalences shall be used:

- CFDP UT_SDU = encapsulation data unit;
- CFDP UT address = encapsulation SAP address;
  = encapsulation SDLP_Channel + EPI.

3.2.2.2 A CFDP UNITDATA.request shall generate an ENCAPSULATION.request where:

- the encapsulation data unit shall be a single, complete CFDP PDU;
- the CFDP UT address shall contain SDLP_Channel and EPI.

3.2.2.3 An ENCAPSULATION.indication shall generate a CFDP UNITDATA.indication where:

- the CFDP PDU UT_SDU shall contain the received encapsulation data unit;
- the CFDP UT address shall contain the SDLP_Channel and EPI.

3.2.2.4 The EPI value shall be set to the CCSDS EPI for CFDP as registered in SANA (reference [7]).

NOTE – The SDLP_Channel used by CFDP for encapsulation packets are configured as part of the CFDP Remote Entity Configuration Information in the CFDP MIB.

3.3 SPACE PACKET PROTOCOL UT LAYER

3.3.1 DISCUSSION

The Space Packet Protocol (reference [2]) provides service primitives for a PACKET service and for an OCTET_STRING service. For CFDP, the OCTET_STRING service providing the following service primitives and parameters is recommended:

`OCTET_STRING.request`	(octet string, APID, secondary header indicator, packet type, packet sequence count/packet name)
`OCTET_STRING.indication`	(octet string, APID, secondary header indicator, data loss indicator [optional])

where:

- octet string is the SDU transferred by SPP;
- APID uniquely identifies the source, destination, or type of the space packet;
- secondary header indicator indicates the presence or absence of a packet secondary header;
- packet type is used to distinguish packets used for telemetry (or reporting) from packets used for telecommand (or requesting);

- packet sequence count provides the sequential binary count of each space packet generated by the user application identified by the APID;
- packet name is only allowed for telecommand packets and will not be used for CFDP;
- (optional) data loss indicator may be used to alert the user in a destination end system that one or more octet strings have been lost during transmission, as evidenced by a discontinuity in the packet sequence count.

In principle, the PACKET service can be used for CFDP if CFDP provides space packets to that service which are confirming to the following specifications.

3.3.2 EQUIVALENCES

3.3.2.1 To reconcile the service required by CFDP and the service provided by the OCTET_STRING service, the following equivalences shall be used:

- CFDP UT_SDU = octet string;
- CFDP UT address = SAP address;
  = APID.

3.3.2.2 A CFDP UNITDATA.request shall generate an OCTET_STRING.request where:

- the octet string shall be a single, complete CFDP PDU;
- the CFDP UT address shall be an APID.

NOTE – As the OCTET_STRING service is used, the sequence flags in the packet primary header will always be set to ‘11’ (unsegmented user data).

3.3.2.3 An OCTET_STRING.indication shall generate a CFDP UNITDATA.indication where:

- the CFDP PDU UT_SDU shall contain the received octet string;
- the CFDP UT address shall contain the APID.

3.3.2.4 The packet secondary header indicator shall be set to absent.

NOTE – Packet secondary headers will not be used when sending CFDP PDU, and the secondary header flag will be ‘0’.

3.3.2.5 The packet sequence count shall always be used instead of a packet name.

3.3.2.6 The optional data loss indicator shall be ignored.

NOTE – The APID and packet type to be used for space packets are configured as part of the CFDP Remote Entity Configuration Information.

3.4 BUNDLE PROTOCOL UT LAYER

NOTE – The service interface description below is based on the service interface of CCSDS 734.2-B-1defining the CCSDS profile of BPv6. This standard is currently being updated to provide a profile for BPv7. While there may be slight changes to the service interfaces, the same principles as described below apply to BPv7.

3.4.1 DISCUSSION

The BP (reference [4]) provides service primitives for transmission of an application data unit from a source communications endpoint to a destination communications endpoint with the following service primitives and parameters:

`Send.request` (source communications endpoint ID, destination communications, endpoint ID, report-to communications endpoint ID, class-of-service, IsSingletonEID, delivery options, lifetime, application data unit)

`BundleDelivery.indication` (header information, application data unit)

where:

- source communications endpoint ID uniquely identifies the communications endpoint from which the bundle was sent;
- destination communications endpoint ID identifies the communications endpoint to which the bundle is to be sent;
- report-to communications endpoint ID parameter identifies the communications endpoint to which any bundle status reports pertaining to the bundle are to be sent;
- class-of-service parameter indicates which class of standard procedures is to be followed when transmitting and delivering the bundle;
- IsSingletonEID parameter is ‘True’ if the destination communications endpoint ID is a singleton endpoint;
- delivery options indicate which optional procedures are additionally to be followed when transmitting and delivering the bundle;
- lifetime indicates the length of time, following initial creation time of a bundle, after which BP agents may discard the bundle;
- application data unit parameter shall indicate the application data conveyed by the bundle;
- header information uniquely identifies the delivered bundle and indicates the delivered bundle’s remaining time to live and the time of delivery to the application agent.

3.4.2 EQUIVALENCES

3.4.2.1 To reconcile the service required by CFDP and the service provided by the BP, the following equivalences shall be used:

- CFDP UT_SDU = application data unit;
- CFDP UT address = destination endpoint ID.

3.4.2.2 A CFDP UNITDATA.request shall generate a Send.request where:

- the application data unit shall be an aggregation of CFDP PDU according to 3.1.4;
- the CFDP UT address shall be a destination endpoint ID.

3.4.2.3 A BundleDelivery.indication shall generate a CFDP UNITDATA.indication where:

- the CFDP PDU UT_SDU shall contain the application data unit, an aggregation of CFDP PDU according to 3.1.4;
- the CFDP UT address shall contain the source endpoint ID which can be obtained from the header information.

NOTE – Source node ID, destination node ID, report-to endpoint ID, and any other send request parameters are configured as part of the CFDP Remote Entity Configuration Information in the MIB.

3.5 LTP UT LAYER

3.5.1 DISCUSSION

LTP (reference [5]) provides service primitives for transmission of client service data from one LTP engine to another with the following service primitives and parameters:

- `Transmission.request` (destination client service ID, destination LTP engine ID, client service data to send, length of the red-part of the data);

  NOTE – LTP provides reliable (the ‘red’ part of the data) and unreliable (the ‘green’ part) transmission of data. However, using ‘green’ data does not guarantee reception of complete CFDP PDU. The definition of the CFDP LTP UT Layer does require use of ‘red’ data only.

- `RedPartReception.indication` (session ID, red-part bytes, indication as to whether or not the last byte of the red-part is also the last byte of the block, source LTP engine ID).

where:

- service ID number identifies the layer-(N+1) service to which the segment is to be delivered by the receiving LTP engine that is providing the N-layer service; this service ID should be fixed per CFDP entity;
- destination LTP engine ID is the LTP engine ID of the LTP engine that is to be the receiver of data blocks;
- client service data to Send is the client data to be transmitted;
- length of the red-part of the data indicates the size of the part of the data which is to be transmitted reliably; for CFDP this will be set to the total length of the data to be sent allowing only reliable transmission;
- session ID uniquely identifies a transmission session;
- red-part bytes is the part of the client service data which has been sent reliably; for CFDP this will be the complete client data;
- indication as to whether or not the last byte of the red-part is also the last byte of the block will always indicate that the last byte of the red-part is the last byte of the block for CFDP;
- source LTP engine ID is the LTP engine ID of the LTP engine that has transmitted the client service data.

3.5.2 EQUIVALENCES

3.5.2.1 To reconcile the service required by CFDP and the service provided by the LTP the following equivalences shall be used:

- CFDP UT_SDU = client service data;
- CFDP UT address = destination client service ID + destination LTP engine ID.

3.5.2.2 A CFDP UNITDATA.request shall generate a Transmission.request where:

- the client service data to send shall contain an aggregation of CFDP PDU according to 3.1.4;
- the CFDP UT address shall be the destination client ID and the destination LTP engine ID;
- length of red-part shall be set to the size of the aggregation of CFDP PDU.

NOTE – IANA (reference [8]) has assigned LTP Client Service ID ‘3’ to CCSDS File Delivery Service.

3.5.2.3 A RedPartReception.indication shall generate a CFDP UNITDATA.indication where:

– the CFDP PDU UT_SDU shall contain the red-part bytes, that is, a complete aggregation of CFDP PDU according to 3.1.4;

– the CFDP UT address shall contain source LTP engine ID.

NOTE – Destination client service ID and destination LTP engine ID are configured as part of the CFDP Remote Entity Configuration Information in the CFDP MIB.

3.6 UDP/IP UT LAYER

3.6.1 DISCUSSION

UDP/IP does not provide an abstract service interface.

3.6.2 EQUIVALENCES

3.6.2.1 To reconcile the service required by CFDP and the service provided by UDP/IP the following equivalences shall be used:

– CFDP UT_SDU = data part of an UDP datagram;

– CFDP UT address = destination port and IP address.

3.6.2.2 A CFDP UNITDATA.request shall send a single UDP datagram with a single, complete CFDP PDU included in the data part.

3.6.2.3 Only CFDP PDU shall be sent to the UDP port of the listening CFDP application.

3.6.2.4 Reception of a UDP datagram at a listening port of a CFDP application shall generate a CFDP UNITDATA.indication where:

– the CFDP PDU UT_SDU shall contain the data contained in the UDP datagram;

– the CFDP UT address shall contain the source IP address and port.

NOTE – Destination IP address and port are configured as part of the CFDP Remote Entity Configuration Information in the MIB.

3.7 TCP/IP UT LAYER

3.7.1 DISCUSSION

TCP/IP does not provide an abstract service interface.

3.7.2 EQUIVALENCES

3.7.2.1 To reconcile the service required by CFDP and the service provided by UDP/IP, the following equivalences shall be used:

- CFDP UT_SDU = data sections of TCP segments;
- CFDP UT address = destination port and IP address.

3.7.2.2 A CFDP UNITDATA.request shall initiate sending the complete CFDP PDU via a TCP connection.

NOTE – The establishment of the TCP connection is an implementation matter. TCP connections can be initiated by the CFDP source or destination. They can be established some time in advance or only when a specific file is to be sent.

3.7.2.3 As TCP is a stream-oriented protocol, there is no alignment between CFDP PDU and TCP segments.

3.7.2.4 No non-CFDP data shall be sent over a TCP connection used by CFDP.

3.7.2.5 Reception of a TCP segment at a listening port of a CFDP application shall generate a CFDP UNITDATA.indication where:

- the CFDP PDU UT_SDU shall contain the received data;
- the CFDP UT address shall contain the source IP address and port.

NOTE – In practice, TCP sockets are typically polled to obtain received data that may contain data from several TCP segments. It is an implementation matter when to poll the socket and generate the UNITDATA.indication.

3.7.2.6 CFDP implementations implementing a TCP/IP UT Layer must be able to accept partial CFDP PDU contained in UT_SDU, which will continue in subsequent UT_SDU.

NOTES

1 TCP/IP does not guarantee that only complete CFDP PDUs will be contained in the UT_SDU. However, it does guarantee completeness and in-order delivery. The CFDP implementation can determine the length of each CFDP PDU by reading the CFDP header. If a CFDP PDU is not completely contained in an UT_SDU, the partial PDU has to be retained and completed when the next UT_SDU arrives.

2 Destination IP address and port are configured as part of the CFDP Remote Entity Configuration Information in the CFDP MIB.

ANNEX A

SECURITY, SANA, AND PATENT CONSIDERATIONS

(INFORMATIVE)

A1 SECURITY

A1.1 INTRODUCTION

As these Recommended Practices do not define a new protocol but rather the use of CFDP with existing protocols, no specific security mechanisms are included.

However, the security considerations regarding the underlying protocols used within the UT Layer apply also in the scope of this recommendation.

A1.2 ENCAPSULATION PACKET PROTOCOL/SPACE PACKET PROTOCOL UT LAYERS

EPP (reference [2]) and SPP (reference [3]) do not provide any security functions. Nevertheless, security functions (authentication, confidentiality, and integrity) can be implemented at the data link layer using Space Data Link Security (SDLS) protocols (references [B5] and [B6]).

A1.3 BUNDLE PROTOCOL UT LAYER

BP security, according to the upcoming CCSDS profile of reference [B7], can be applied for confidentiality, authenticity, and integrity with the BP (reference [4]) UT Layer.

Additionally, security can be applied on the layers below BP depending on the chosen BP Convergence Layers.

A1.4 LTP PROTOCOL UT LAYER

LTP, as specified in reference [5], does not provide any mechanism for confidentiality, integrity, and non-repudiation of data. As LTP is typically using EPP or SPP for space links, the same considerations as in B1.1 apply; that is, application of Space Data Link Security on the Space Data Link Layer is possible.

A1.5 UDP/IP AND TCP/IP UT LAYER

Standard considerations for IP security, for example, the use of IPSEC, apply.

A2 SANA/IANA CONSIDERATIONS

The CCSDS Encapsulation Protocol ID used in the EPP UT Layer (section 3.2) is registered in SANA (reference [7]).

The LTP Client Service IDs used in the LTP UT Layer (section 3.5) are registered in IANA (reference [8]).

A3 PATENTS

The recommended practices within this document are not protected by any known patents.

ANNEX B

INFORMATIVE REFERENCES

(INFORMATIVE)

[B1] *Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*. 2nd ed. International Standard, ISO/IEC 7498-1:1994. Geneva: ISO, 1994.

[B2] *CCSDS File Delivery Protocol (CFDP)—Part 1: Introduction and Overview*. Issue 4. Report Concerning Space Data System Standards (Green Book), CCSDS 720.1-G-4. Washington, D.C.: CCSDS, May 2021.

[B3] *CCSDS File Delivery Protocol (CFDP)—Part 2: Implementers Guide*. Issue 4. Report Concerning Space Data System Standards (Green Book), CCSDS 720.2-G-4. Washington, D.C.: CCSDS, May 2021.

[B4] *CCSDS File Delivery Protocol (CFDP)—Part 3: Interoperability Testing Final Report*. Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 720.3-G-1. Washington, D.C.: CCSDS, September 2007.

[B5] *Space Data Link Security Protocol*. Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 355.0-B-2. Washington, D.C.: CCSDS, July 2022.

[B6] *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 2020.

[B7] E. Birrane and K. McKeever. *Bundle Protocol Security (BPSec)*. RFC 9172. Reston, Virginia: ISOC, January 2022.

ANNEX C

ABBREVIATIONS

(INFORMATIVE)

APID	Application Process Identifier
BP	Bundle Protocol
CCSDS	Consultative Committee for Space Data Systems
CFDP	CCSDS File Delivery Protocol
EPI	Encapsulated Protocol Identifier
EPP	Encapsulation Packet Protocol
IANA	Internet Assigned Numbers Authority
ID	identifier
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISO	International Organization for Standardization
LTP	Licklider Transmission Protocol
MIB	Management Information Base
OSI	Open Systems Interconnection
PDU	protocol data unit
SANA	Space Assigned Numbers Authority
SAP	service access point
SDLP	Space Data Link Protocol
SDLS	Space Data Link Security
SDU	service data unit
SPP	Space Packet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UT	Underlying Transport