

**DRAFT Recommendation for Space Data System Standards**

|  |
| --- |
| **CCSDS Bundle Protocol Specification** |

**DRAFT Recommended Standard**

**CCSDS ????**

**Red Book**

**Month Year**

**Dedication**

**AUTHORITY**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | Issue: | Red Book, Issue 1 |  |
|  | Date: | Month Year |  |
|  | Location: | Washington, DC, USA |  |
|  |  |  |  |

**(WHEN THIS RECOMMENDED STANDARD 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 e-mail address below.

This document is published and maintained by:

CCSDS Secretariat

National Aeronautics and Space Administration

Washington, DC, USA

E-mail: secretariat@mailman.ccsds.org

**STATEMENT OF INTENT**

**(WHEN THIS RECOMMENDED STANDARD 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 **Recommended Standards** and are not considered binding on any Agency.

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

o Whenever a member establishes a CCSDS-related **standard**, this **standard** will be in accord with the relevant **Recommended Standard**. Establishing such a **standard** does not preclude other provisions which a member may develop.

o Whenever a member establishes a CCSDS-related **standard**, that member will provide other CCSDS members with the following information:

 -- The **standard** itself.

 -- The anticipated date of initial operational capability.

 -- The anticipated duration of operational service.

o Specific service arrangements shall be made via memoranda of agreement. Neither this **Recommended Standard** nor any ensuing **standard** is a substitute for a memorandum of agreement.

No later than 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.

**PREFACE**

This document is a draft CCSDS Recommended Standard. Its ‘Red 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.

**FOREWORD**

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 e-mail 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.
* Chinese 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.
* Indian Space Research Organization (ISRO)/India.
* Institute of Space Research (IKI)/Russian Federation.
* KFKI Research Institute for Particle & Nuclear Physics (KFKI)/Hungary.
* Korea Aerospace Research Institute (KARI)/Korea.
* Ministry of Communications (MOC)/Israel.
* National Institute of Information and Communications Technology (NICT)/Japan.
* National Oceanic and Atmospheric Administration (NOAA)/USA.
* National Space Agency of the Republic of Kazakhstan (NSARK)/Kazakhstan.
* National Space Organization (NSPO)/Chinese Taipei.
* Naval Center for Space Technology (NCST)/USA.
* Scientific and Technological Research Council of Turkey (TUBITAK)/Turkey.
* 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 ??? | CCSDS Bundle Protocol Specification, Draft Recommended Standard, Issue 2 | Month Year | Current Draft |
|  |  |  |  |
|  |  |  |  |

**CONTENTS**

[**1.**](#_heading=h.4d34og8) **INTRODUCTION** 10

[**1.1**](#_heading=h.2p2csry) **PURPOSE** 10

[**1.2**](#_heading=h.147n2zr) **SCOPE** 10

[**1.3**](#_heading=h.37m2jsg) **ORGANIZATION OF THE RECOMMENDED STANDARD** 10

[**1.4**](#_heading=h.1mrcu09) **DEFINITIONS** 11

[**1.5**](#_heading=h.46r0co2) **REFERENCES** 13

[**2.**](#_heading=h.2lwamvv) **OVERVIEW** 14

[**2.1**](#_heading=h.111kx3o) **GENERAL** 14

[**2.3**](#_heading=h.3l18frh) **SERVICES PROVIDED BY BP** 16

[**2.4**](#_heading=h.206ipza) **QUALITIES OF SERVICE NOT PROVIDED BY BP** 16

[**3.**](#_heading=h.4k668n3) **CCSDS PROFILE OF RFC 9171** 16

[**3.1**](#_heading=h.2zbgiuw) **GENERAL** 16

[**3.2**](#_heading=h.1egqt2p) **NAMING SCHEMES** 16

[**3.3 Bundle Creation** 17](#_heading=h.3ygebqi)

[**4**](#_heading=h.2dlolyb) **SERVICE DESCRIPTION** 17

[**5**](#_heading=h.sqyw64) **SERVICES BP REQUIRES OF THE SYSTEM** 25

[**5.1**](#_heading=h.3cqmetx) **SYSTEM REQUIREMENTS** 26

[**5.2**](#_heading=h.1rvwp1q) **UNDERLYING COMMUNICATION SERVICE REQUIREMENTS** 26

[**6**](#_heading=h.4bvk7pj) **CONFORMANCE REQUIREMENTS** 28

[**6.2**](#_heading=h.2r0uhxc) **BUNDLE PROTOCOL REQUIREMENTS** 28

[**ANNEX A PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT PROFORMA (NORMATIVE)** 30](#_heading=h.1664s55)

[**A1**](#_heading=h.3q5sasy) **NOTATION** 31

[**A2**](#_heading=h.25b2l0r) **REFERENCED BASE STANDARDS** 31

[**A3**](#_heading=h.kgcv8k) **GENERAL INFORMATION** 32

[**ANNEX B CONVERGENCE LAYER ADAPTERS (NORMATIVE)** 38](#_heading=h.34g0dwd)

[**B1**](#_heading=h.1jlao46) **OVERVIEW** 38

[**B2**](#_heading=h.43ky6rz) **CONVERGENCE LAYER ADAPTERS** 38

[**ANNEX C BP MANAGED INFORMATION** 41](#_heading=h.2iq8gzs)

[**C1**](#_heading=h.xvir7l) **BASIC REQUIREMENTS** 41

[**C2**](#_heading=h.3hv69ve) **BUNDLE STATE INFORMATION** 41

[**C3**](#_heading=h.1x0gk37) **NODE ERROR AND REPORTING INFORMATION** 43

[**C4**](#_heading=h.4h042r0) **REGISTRATION INFORMATION** 45

[**C5**](#_heading=h.2w5ecyt) **NODE STATE INFORMATION** 45

[**ANNEX D SECURITY, SANA, AND PATENT CONSIDERATIONS** 47](#_heading=h.1baon6m)

[**D1**](#_heading=h.3vac5uf) **SECURITY** 47

[**D2**](#_heading=h.2afmg28) **SANA CONSIDERATIONS** 48

[**D3**](#_heading=h.pkwqa1) **PATENT CONSIDERATIONS** 48

[**ANNEX E SANA Registry Considerations** 49](#_heading=h.39kk8xu)

[**E1 Encapsulation Protocol** 49](#_heading=h.1opuj5n)

[**ANNEX F BP ELEMENT SPECIFICATION** 50](#_heading=h.48pi1tg)

[**F1 BP Block Tables** 50](#_heading=h.2nusc19)

[**ANNEX G INFORMATIVE REFERENCES (INFORMATIVE)** 53](#_heading=h.1302m92)

[**ANNEX H ABBREVIATIONS AND ACRONYMS (INFORMATIVE)** 54](#_heading=h.3mzq4wv)

# **1. INTRODUCTION**

## PURPOSE

The purpose of this document is to establish a recommended standard for CCSDS Bundle Protocol (BP), based on the bundle protocol of RFC 9171 (reference [1]), which defines end-to-end protocol, bundle structure, and block types for the exchange of messages (bundles) that support Delay Tolerant Networking (DTN). This document includes abstract service descriptions for the application services provided by BP.

## SCOPE

This Recommended Standard is designed to be applicable to any space mission infrastructure that might benefit from delay and disruption tolerance, regardless of resources, latencies, or complexity. It is intended that this Recommended Standard become a uniform standard among all CCSDS Agencies.

This Recommended Standard is intended to be applied to all systems that claim conformance to the CCSDS Bundle Protocol version 7.

BP is agnostic to the choice of underlying transmission protocol in that BP can function over TC, TM, AOS, USLP, Proximity-1 Space Link Protocol, Encapsulation Packet Protocol, Space Packet, and various Internet and ground-based protocols.

The CCSDS believes it is important to document the rationale underlying the recommendations chosen, so that future evaluations of proposed changes or improvements will not lose sight of previous decisions. The concept and rationale for the use of bundle protocol in space links may be found in reference [G1].

## ORGANIZATION OF THE RECOMMENDED STANDARD

This recommended Standard is organized as follows:

* Section 2 contains an overview of the Bundle Protocol and the references from which it is derived.
* Section 3 contains the CCSDS modification to RFC 9171.
* Section 4 contains the service descriptions.
* Section 5 contains services BP requires of the system.
* Section 6 contains conformance requirements.
* Annex A contains the Implementation Conformance Statement for the protocol.
* Annex B contains the Convergence Layer Adapters (CLAs).
* Annex C contains BP managed information
* Annex D contains Security, Space Assigned Numbers Authority (SANA), and Patent considerations.
* Annex E contains SANA Registry Considerations
* Annex F contains BP Element Specification
* Annex G contains Informative References
* Annex H contains abbreviations and acronyms used in this document.

## DEFINITIONS

**1.4.1 Definitions From Open Systems Interconnection (OSI) Service Definition Conventions**

This Recommended Standard makes use of a number of terms defined in reference [2]. As used in this Recommended Standard those terms are to be interpreted 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:

* Indication;
* Primitive;
* Request;
* Response;

**1.4.2 Definitions From OSI Basic Reference Model**

This Recommended Standard makes use of a number of terms defined in reference [3]. As used in this Recommended Standard those terms are to 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:

* Entity;
* Protocol Data Unit (PDU);
* Service;
* Service Data Unit (SDU);

**1.4.3 Definitions From RFC 9171**

***1.4.3.1 Overview***

This Recommended Standard makes use of a number of terms defined in reference [1]. Some of the definitions needed for section 2 of this document are reproduced here for convenience.

A graphical representation of a bundle node is given in figure 1-1. A bundle node is any entity that can send and /or receive bundles.

Each bundle node has three conceptual components described in more detail below: a ‘bundle protocol agent’, a set of zero or more ‘convergence layer adapters’, and an ‘application agent’. The major components are illustrated in figure 1-1 (“CLx PDUs” are the PDUs of the convergence-layer protocols used in individual networks).



**Figure 1-1: Graphical Representation of a Bundle Node**

It should be noted that there is *one* application agent per conceptual bundle node. That application agent may provide communication services to multiple applications and the node may register in multiple endpoints (may provide multiple endpoint identifiers to the bundle protocol agent, requesting delivery of bundles to any of those endpoints).

**1.4.3.2 RFC 9171 Terms**

**Bundle**: A bundle is a protocol data unit of BP, so named because negotiation of the parameters of a data exchange may be impractical in a delay-tolerant network: it is often better practice to “bundle” with a unit of application data all metadata that might be needed in order to make the data immediately usable when delivered to the application. Each bundle comprises a sequence of two or more “blocks” of protocol data, which serve various purposes.

**Bundle Node**: A bundle node (or, in the context of this document, simply a “node”) is any entity that can send and/or receive bundles. Each bundle node has three conceptual components: a “bundle protocol agent”, a set of zero or more “convergence layer adapters”, and an “application agent”.

**Bundle Protocol Agent**: The bundle protocol agent (BPA) of a node is the node component that offers the BP services and executes the procedures of the bundle protocol.

**Application Agent**: The application agent (AA) of a node is the node component that utilizes the BP services to effect communication for some user purpose. The application agent in turn has two elements, an administrative element and an application-specific element.

**Administrative Element**: The administrative element of an AA is the node component that constructs and requests transmission of administrative records (defined below), including status reports, and accepts delivery of and processes any administrative records that the node receives.

**Application-Specific Element**: The application-specific element of an AA is the node component that constructs, requests transmission of, accepts delivery of, and processes units of user application data.

**Convergence Layer Adapter**: A convergence layer adapter (CLA) is a node component that sends and receives bundles on behalf of the BPA, utilizing the services of some 'native' protocol stack that is supported in one of the networks within which the node is functionally located.

## 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. S. Burleigh, K. Fall, and E. Birrane. *Bundle Protocol Version 7*. RFC 9171. Reston, Virgina: ISOC, January 25, 2021.
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. *Information Technology—Open Systems Interconnection—Basic Reference Model: The Basic Model*. 2nd ed. International Standard, ISO/IEC 7498-1:1994. Geneva: ISO, 1994.
4. Space Assigned Numbers Authority (SANA). <http://sanaregistry.org/>.
5. L. Eggert, G. Fairhurst, and G. Shepard. *UDP Usage Guidelines*. RFC 8085. Reston, Virginia: ISOC, March 2017.
6. Sipos, B. et. al., Delay-Tolerant Networking TCP Convergence-Layer Protocol Version 4, RFC9174, Reston, Virginia, February 2022.
7. J. Postel, *User Datagram Protocol*, RFC768, ISOC, August 28, 1980.
8. 734.1-B-1 Licklider Transmission Protocol (LTP) for CCSDS
9. *Encapsulation Packet Protocol*. Issue 3. Recommendation for Space Data System Standards (Blue Book), CCSDS 133.1-B-3. Washington, D.C.: CCSDS, May 2020.
10. *Space Packet Protocol.* Issue 2. Recommendation for Space Data System Standards (Blue Book), CCSDS 133.0-B-2. Washington, D.C.: CCSDS, June 2020.

# **OVERVIEW**

## GENERAL

Delay Tolerant Networking is an end-to-end network service providing communications in and/or through environments characterized by one or more of the following:

* Intermittent connectivity;
	+ Link connectivity within an interplanetary environment can periodically experience Loss of Signal (LOS) due to a variety of factors, including solar conjunction, occultation, atmospheric signal dispersion, etc.
	+ Link connectivity in a near-Earth environment may periodically experience loss of signal due to obstructions, atmospheric signal dispersion, etc.
* Variable delays, which may be large and irregular;
	+ Delays in data transmission between nodes will occur in interplanetary (and larger) scale environments. This delay is caused mostly by the extreme distance data can be required to travel. Delay can also be caused by events like solar conjunction, where a planetary body may inhibit signal transmission
	+ Delays may also occur in smaller scale (e.g. near-Earth) environments, e.g. resulting from contention for scarce scheduled resources such as antenna transmission opportunities, power constraints on duty cycles, or transient loss of connectivity.
* Highly variable transmission error rates;
	+ Error characteristics may vary widely at different points along the end-to-end path and/or at different times due to external factors.
	+ For near-Earth missions error rates may be strongly affected by elevation angle.
* Asymmetric and simplex links.
	+ Deep space missions often carry constraints regarding the amount of equipment they can support on the satellite. The uplink bandwidth capacity (and the hardware required to support it) can often be minimized in favor of supporting other functions that require more of the satellite’s resources. The result of this constraint is an asymmetric, sometimes even simplex, link between the satellite and the receiver.
	+ Asymmetries may occur in near-Earth missions due to asymmetric hardware.
* Disparate Data Rates
	+ Data rates may vary greatly at different points along the end-to-end path. Thus a very high rate link may impinge on a node with a low-rate output, requiring the node to buffer traffic for a significant period of time.

One core element of DTN is the Bundle Protocol. BP provides end-to-end network services, operating above the data transport services provided by links or networks accessed via the CLAs, and forming a store-and-forward network. Key capabilities of the Bundle Protocol include:

* Ability to use physical motility for the movement of data
* Ability to move the responsibility for error control from one node to another
* Ability to cope with intermittent connectivity, including cases where the sender and receiver are not concurrently present in the network
* Ability to take advantage of scheduled, predicted, and opportunistic connectivity, whether bidirectional or unidirectional, in addition to continuous connectivity
* Ability to use available bandwidth for a wide variety of services and functions
* Late binding of bundle protocol network endpoint identifiers to underlying constituent network addresses

Reference [1] contains descriptions of these capabilities and rationale for the DTN architecture.

BP uses underlying “native” transport and/or network protocols for communications within a given constituent network. The layer at which those underlying protocols lie is known as the “convergence layer”. The interface between the BP layer and the convergence layer is known as the “convergence layer adapter”. This concept is illustrated in Figure 2-1. PDUs traveling from the application and bundle layer encounter a CLA, which is responsible for sending (and receiving) bundles according to the “native” protocol that the convergence layer uses underneath it (as interpreted in a standard OSI model with BP additions). Typically, a specific CLA is created for each unique “native” protocol. The CLA on the left, for example, could represent an adapter specific to a TCP network. The CLA on the right (CL B) could represent an interface to the Licklider Transmission Protocol (LTP), with “Link B1” representing LTP running over a CCSDS Data Link Layer protocol. Alternatively, BP can be used to support a connection between two separate internets e.g. an on-orbit internet and a ground internet, terrestrial or otherwise.



**Application Layer**

**Figure 2.1: Bundle Protocol End-to-End Delivery Service**

RFC 9171 describes the format of the messages (called bundles) passed between nodes participating in bundle transmission. In addition, it addresses endpoint naming and describes how the protocol may be extended to support new capabilities while maintaining compatibility with the base protocol. Neither RFC 9171 nor this document address bundle routing algorithms (e.g. schedule-aware bundle routing, SABR), mechanisms for populating the routing or forwarding information bases of bundle nodes, nor methods for scheduling bundle transmission (e.g. Contact Plan).

General refactoring of the bundle protocol has improved the protocol in terms of simplicity, power, and flexibility since the protocol was first released in CCSDS 734.2-B-1. These improvements make BPv7 incompatible with its previous iteration. Therefore, this document, upon publication, will obsolete CCSDS 734.2-B-1.

Bundle protocol supports end-to-end communications that may include austere environments where more commonly known communications protocols (e.g. TCP/IP) tend to break down and stop functioning. In scenarios like these, bundle protocol is an excellent technological innovation that allows multiple internetworking environments in previously unconnected locations to interact.

## SERVICES PROVIDED BY BP

BP provides a data transmission service to move “bundles” (contiguous groups of octets) of data from one BP node to another. The specific services provided at the service interface are:

1. Initiating a registration (registering a node in an endpoint);
2. Terminating a registration;
3. Switching a registration between Active and Passive states;
4. Transmitting a bundle to an identified bundle endpoint;
5. Canceling a transmission that has been requested;
6. Polling a registration that is in the Passive state;
7. Delivering a received bundle;
8. Reporting bundle status.

## QUALITIES OF SERVICE NOT PROVIDED BY BP

The Bundle Protocol as specified in this document does not provide the following services:

1. In-order delivery of bundles;
2. Guaranteed delivery of bundles;
3. Broadcast, multicast, or anycast bundle delivery.

Custody transfer is omitted from the Bundle Protocol version 7 specification and may be standardized later via additional mechanisms, possibly supported by extension blocks. In the context of this specification, the recommended way to improve reliability is to use a chain of reliable CLAs and/or an application level reliability mechanism.

# **CCSDS PROFILE OF RFC 9171**

## Bundle Protocol from RFC9171

This document adopts the Bundle Protocol as specified in Internet RFC 9171 (reference [1]), with the constraints and exceptions specified in section 3 of this document.

## NAMING SCHEMES

**3.2.1** Implementations of this specification shall support the ‘ipn’ URI scheme as defined in section 4.2.5.1.2 of RFC 9171, *Bundle Protocol Version 7* (reference [1]).

**3.2.2** Implementations of this specification shall support the null endpoint dtn:none from the dtn URI scheme in RFC 9171.

NOTE – This specification requires support for the ipn URI naming scheme and explicitly does not otherwise require support for the ‘dtn’ naming scheme defined in RFC 9171.

NOTE: The null endpoint dtn:none is encoded as the scheme number of the dtn URI scheme with a value zero scheme-specific part.

**3.2.3** Implementations shall use IPN node numbers assigned by SANA from the CCSDS CBHE Node Number Registry.

**3.2.4** Implementations shall use service numbers assigned by IANA / SANA from either the IANA CBHE Service Numbers registry or the SANA CBHE Service Numbers Registry.

NOTE: The IANA registry includes a private address space of CBHE Service Numbers that can be used for mission-specific purposes.

NOTE: The “CBHE” label was adopted before BPv7 was standardized; the name was enshrined in registries and is therefore used here.

## Bundle Creation

**3.3.1** Bundles shall be assigned source node ID and creation timestamps when ADUs are accepted for transmission by the bundle protocol agent. The combination of source node ID and creation timestamp is returned to the sending application in the bundle transmission request ID indication.

**3.3.2** The source node IDs of all non-anonymous bundles sourced by a given bundle protocol agent shall have the same node number.

NOTE: Users may use different service numbers in the source node IDs of bundles sent.

**3.3.3** Implementations are not required to be able to source bundles with sending EID dtn:none (anonymous bundles)

## Bundle Node Registration Constraints

**3.4.1** All endpoints in which a node is registered shall have that same node number.

## Minimum Supported Bundle Size

**3.5.1** Conformant CCSDS implementations shall be able to process bundles whose total size, including all extension blocks, is less than or equal to 10\*220 bytes (10 MB).

NOTE: Implementations may handle larger bundles.

# **SERVICE DESCRIPTION**

## SERVICES AT THE USER INTERFACE

**4.1.1** The services provided by the Bundle Protocol shall be made available to bundle protocol users and include the following:

a) initiate a registration (registering a node in an endpoint);

b) terminate a registration;

c) switch a registration between Active and Passive states as discussed in RFC 9171;

d) transmit an application data unit (ADU) to an identified bundle endpoint;

e) cancel a transmission;

f) poll a registration that is in the Passive state;

g) receive an ADU contained in a delivered bundle.

**4.1.2** The BP node shall be implemented such that virtually any number of transactions may be conducted concurrently in various stages of transmission or reception at a single BP node.

NOTE – To clarify: the implementation needs to be able to accept a primitive, and thereupon initiate a new transaction prior to the completion of previously initiated transactions. The requirement for concurrent transaction support therefore does not necessarily imply that the implementation needs to be able to begin initial transmission of data for one transaction while initial transmission of data for one or more other transactions is still in progress. (But neither is support for this functional model precluded.)

4.1.3 Error indications at the service interface are implementation matters not covered by this specification.

## SUMMARY OF PRIMITIVES

**4.2.1** The BP service shall consume the following request primitives:

– Register.request;

– Deregister.request;

– ChangeRegistrationState.request;

– Send.request;

– Cancel.request;

– Poll.request.

**4.2.2** The BP service shall deliver the following indication primitives:

– BundleSendRequest.indication;

– Bundle Delivery.indication.

## SUMMARY OF PARAMETERS

**4.3.1 DESTINATION COMMUNICATIONS ENDPOINT ID**

The destination communications endpoint ID parameter shall identify the communications endpoint to which the bundle is to be sent.

NOTE – One can think of a DTN communications endpoint as an application, but in general the definition is meant to be broader. For example, a single BPA (with a single endpoint ID) could service other local nodes such as elements of a sensor network using private protocols.

### SOURCE NODE ID

The source NODE ID parameter shall uniquely identify the communications endpoint from which the bundle was sent.

### REPORT-TO ENDPOINT ID

The report-to communications endpoint ID parameter shall identify the communications endpoint to which any bundle status reports pertaining to the bundle are sent.

**4.3.3 CREATION TIMESTAMP**

The creation timestamp comprises the bundle creation time and the creation timestamp sequence number.

**4.3.6 SEND REQUEST OPTIONS**

**4.3.6.1** The send request parameters shall indicate what optional procedures are additionally to be followed when transmitting the bundle and what optional services are requested.

**4.3.6.2** The value of the send request parameters shall include the following:

a) application data unit is an administrative record;

b) bundle must not be fragmented;

c) acknowledgement by application is requested;

d) request reporting of bundle reception;

e) request reporting of bundle forwarding;

f) request reporting of bundle delivery;

g) request reporting of bundle deletion;

h) status time is requested in all status reports.

NOTE – implementations may also allow inclusion of other information with the Send Request Parameters such as metadata and material to be included in particular extension blocks.

**4.3.7 BUNDLE DELIVERY INDICATION PARAMETERS**

**4.3.7.1** The delivery indication parameters shall be the ADU and the metadata from 4.3.7.2 below pertaining to the ADU.

**4.3.7.2** The value of the delivery indications parameters shall include the following:

a) application data unit is an administrative record;

b) acknowledgement by application is requested;

NOTE – implementations may also include other information with the Bundle Delivery Indication Parameters such as the source EID, creation time, and/or information from extension blocks.

**4.3.8 LIFETIME PARAMETER**

The lifetime parameter shall indicate the length of time, following initial creation time of a bundle, after which bundle protocol agents may discard the bundle.

**4.3.9 APPLICATION DATA UNIT PARAMETER**

The application data unit parameter shall indicate the location (in memory or non-volatile storage, a local implementation matter) of the application data conveyed by the bundle.

**4.3.10 BUNDLE SEND REQUEST ID**

The Bundle Send Request ID parameter shall identify a particular bundle. The Bundle Send Request ID comprises the source node ID and creation timestamp.

**4.3.11 DELIVERY FAILURE ACTION**

**4.3.11.1** The Delivery Failure Action parameter shall identify the response the node is to take on receipt of a bundle that is deliverable subject to the registration when the registration is in the Passive state (see 4.3.11).

**4.3.11.2** The Delivery Failure Action parameter shall signal one of the following possible responses:

– defer delivery of the bundle;

– abandon delivery of the bundle.

NOTE - RFC 9171 section 5.7 (Bundle Delivery) contains more on when deferred bundles may be delivered to receiving applications.

**4.3.12 REGISTRATION STATE**

The Registration State is the state machine characterization of a given node’s membership in a given endpoint. A registration state must at any time be in one of two states: Active or Passive.

NOTE – A registration always has an associated ‘delivery failure action’ which denotes the action to be taken upon receipt of a bundle that is deliverable subject to the registration when the registration is in the Passive state (refer to 4.3.10). Further definition of Registration can be found in section 5.7 of RFC9171.

**4.3.13 BUNDLE DELIVERY METADATA**

The Bundle Delivery Metatadata parameter shall uniquely identify the delivered bundle and shall at minimum indicate the delivered bundle’s remaining time to live and the time the bundle was received.

**4.4 BP SERVICE PRIMITIVES**

**4.4.1 Register.request**

**4.4.1.1 Function**

The Register.request primitive shall be used to notify the BP agent of the node’s membership in a communications endpoint.

**4.4.1.2 Semantics**

Register.request shall provide parameters as follows:

Register.request (delivery failure action, destination communications endpoint ID)

**4.4.1.3 When Generated**

Register.request may be generated by any BP application at any time.

**4.4.1.4 Effect on Receipt**

**4.4.1.4.1** Receipt of Register.request shall cause the BP agent to declare the node’s registration in the indicated endpoint.

**4.4.1.4.2** The registration shall initially be in Passive state.

**4.4.1.4.3** The indicated failure action shall be taken upon arrival of any bundle destined for this endpoint, as long as the registration remains in Passive state.

**4.4.1.5 Discussion—Additional Comments**

Registration in particular endpoints (especially those associated with the node number of the node) may be implicit in the instantiation of the bundle protocol agent or could require explicit registration requests from applications.

**4.4.2 Deregister.request**

**4.4.2.1 Function**

The Deregister.request primitive shall be used to notify the BP agent of the end of the node’s membership in the indicated endpoint.

**4.4.2.2 Semantics**

Deregister.request shall provide parameters as follows:

Deregister.request (destination communications endpoint ID)

**4.4.2.3 When Generated**

Deregister.request may be generated by any BP application at any time when the node is registered in the indicated endpoint.

**4.4.2.4 Effect on Receipt**

Receipt of Deregister.request shall cause the node’s registration in the indicated endpoint to be rescinded.

**4.4.2.5 Discussion—Additional Comments**

None

**4.4.3 ChangeRegistrationState.request**

**4.4.3.1 Function**

The ChangeRegistrationState.request primitive shall be used to notify the BP agent of a desired change in the registration state.

**4.4.3.2 Semantics**

ChangeRegistrationState.request shall provide parameters as follows:

ChangeRegistrationState.request (destination communications endpoint ID, registrationState)

**4.4.3.3 When Generated**

ChangeRegistrationState.request may be generated by any BP application at any time when the node is registered in the indicated endpoint.

**4.4.3.4 Effect on Receipt**

**4.4.3.4.1** Receipt of ChangeRegistrationState.request shall cause the BP agent to change the state of the registration to the requested state.

**4.4.3.4.2** If the new state is Active, receipt of this request shall additionally cause the bundle protocol agent to deliver to the application all bundles, destined for the indicated endpoint, for which delivery was deferred.

**4.4.3.5 Discussion—Additional Comments**

Changing the state of the registration to ‘active’ implicitly associates with that end point the application that issued the request. The expected effect of this association is that all bundles destined for this endpoint will be delivered to that application, but the details of this association are an implementation matter.

**4.4.4 Send.request**

**4.4.4.1 Function**

The Send.request primitive shall be used by the application to request transmission of an application data unit from the source communications endpoint to a destination communications endpoint.

**4.4.4.2 Semantics**

Send.request shall provide parameters as follows:

Send.request (source node ID,

destination endpoint ID,

report-to endpoint ID,

send request options,

lifetime,

application data unit)

**4.4.4.3 When Generated**

Send.request may be generated by the source BP application at any time.

**4.4.4.4 Effect on Receipt**

Receipt of Send.request shall cause the BP agent to initiate bundle transmission procedures and shall cause a BundleRequestID.indication to be returned to the issuer of the send request.

**4.4.4.5 Discussion—Additional Comments**

None.

**4.4.5 Cancel.request**

**4.4.5.1 Function**

The Cancel.request primitive shall be used by the application to request termination of transmission of an application data unit for which the application previously requested transmission.

**4.4.5.2 Semantics**

Cancel.request shall provide parameters as follows:

Cancel.request (BundleRequestID)

**4.4.5.3 When Generated**

Cancel.request may be generated by the application at any time after requesting transmission of a bundle.

**4.4.5.4 Effect on Receipt**

Receipt of Cancel.request shall cause the BP agent to stop attempting to transmit and to discard the target bundle, if possible.

**4.4.5.5 Discussion—Additional Comments**

If the bundle has already been transmitted, there is no obligation on the sending BP agent to take any further action. It is an implementation matter whether a bundle that is in the process of being transmitted when a Cancel.request is received is terminated.

**4.4.6 Poll.request**

**4.4.6.1 Function**

The Poll.request primitive shall be used by the application to request immediate delivery of the least-recently received bundle that is currently deliverable subject to the node’s registration in the indicated endpoint.

**4.4.6.2 Semantics**

Poll.request shall provide parameters as follows:

Poll.request (destination communications endpoint ID)

**4.4.6.3 When Generated**

Poll.request may be generated by any BP application at any time when the node is registered in the indicated endpoint and that registration is in Passive state.

**4.4.6.4 Effect on Receipt**

Receipt of Poll.request shall cause the BP agent to deliver to the BP application the least-recently received bundle, destined for the destination communications endpoint ID, for which delivery was deferred.

NOTE – Prioritization applies only to forwarding of a bundle. Deferred bundles are delivered in the order in which they were received.

**4.4.6.5 Discussion—Additional Comments**

None.

**4.4.7 BundleRequestID.indication**

**4.4.7.1 Function**

The BundleRequestID.indication primitive shall be used to provide the application a reference to a particular bundle for which the application requested transmission.

**4.4.7.2 Semantics**

BundleRequestID.indication shall provide parameters as follows:

BundleRequestID.indication (SourceNodeID, CreationTimestamp)

**4.4.7.3 When Generated**

BundleRequestID.indication shall be generated by a BP agent after it has consumed a Send.request from the application.

**4.4.7.4 Effect on Receipt**

The effect on receipt of BundleRequestID.indication by a BP application is undefined.

**4.4.7.5 Discussion—Additional Comments**

On receiving this notice the sending application can, for example, release resources of its own that are allocated to the bundles being transmitted, or record the BundleRequestID so that transmission can be canceled in the future if necessary.

**4.4.8 BundleDelivery.indication**

**4.4.8.1 Function**

The BundleDelivery.indication primitive shall be used to deliver the application data unit and associated metadata to the service user.

**4.4.8.2 Semantics**

BundleDelivery.indication shall provide parameters as follows:

BundleDelivery.indication (bundle delivery metadata,

application data unit)

**4.4.8.3 When Generated**

BundleDelivery.indication shall be generated by a BP agent upon delivery of a bundle, either on reception of bundles destined for active registrations or in response to poll requests referencing passive registrations.

**4.4.8.4 Effect on Receipt**

The effect on receipt is defined by the application.

**4.4.8.5 Discussion—Additional Comments**

None.

# **SERVICES BP REQUIRES OF THE SYSTEM**

## SYSTEM REQUIREMENTS

**5.1.1** BP nodes shall have access to a storage service.

NOTES

1. This storage mechanism may be in dynamic memory or via a persistent mechanism such as a solid-state recorder and may be organized by various means to include file systems.
2. The implementation of this storage can be shared among multiple elements of the communication stack so that reliability mechanisms at multiple layers do not have to maintain multiple copies of the data being transmitted.
3. Volume of storage required and duration of storage are mission- and implementation-dependent.
4. Storage reliability is subject to mission and service requirements.

**5.1.2** The following information shall be available to BP, either from the local operating environment or from the underlying communication service provider:

* forward advancing time that can be represented as ‘DTN time’ as defined by RFC 9171 (reference [1]);

- A counter conforming to the requirements of section 4.2.7 in RFC 9171 to provide sequence numbers for the creation timestamp fields of bundles.

NOTE – The means by which this information is accessed by BP is implementation-dependent.

## UNDERLYING COMMUNICATION SERVICE REQUIREMENTS

**5.2.1** Each convergence layer protocol adapter SHALL provide the following services to the bundle protocol agent:

* sending a bundle to a bundle node that is reachable via the convergence layer protocol;
* notifying the bundle protocol agent of the disposition of its data sending procedures with regard to a bundle, upon concluding those procedures;
* delivering to the bundle protocol agent a bundle that was sent by a bundle node via the convergence layer protocol.

NOTE - The convergence layer service interface specified here is neither exhaustive nor exclusive. That is, supplementary DTN protocol specifications (including, but not restricted to, the Bundle Protocol Security [BPSEC]) may expect convergence layer adapters that serve BP implementations conforming to those protocols to provide additional services such as reporting on the transmission and/or reception progress of individual bundles (at completion and/or incrementally), retransmitting data that were lost in transit, discarding bundle-conveying data units that the convergence layer protocol determines are corrupt or inauthentic, or reporting on the integrity and/or authenticity of delivered bundles.

In addition, bundle protocol relies on the capabilities of protocols at the convergence layer to minimize congestion. The potentially long round-trip times characterizing delay-tolerant networks are incompatible with end-to-end reactive congestion control mechanisms, so convergence-layer protocols are expected to provide rate limiting or congestion control.

**5.2.3** The service provided by the protocols beneath BP (not necessarily by the convergence layer protocol itself) shall deliver only complete bundles to the receiving BP Node.

**5.2.4** Delivery of duplicate bundles to a BPA by the underlying layer shall be acceptable.

# **ANNEX APROTOCOL IMPLEMENTATION CONFORMANCESTATEMENT PROFORMA(NORMATIVE)**

**OVERVIEW**

This annex provides the Protocol Implementation Conformance Statement (PICS) Requirements List (RL) for CCSDS-compliant implementations of BP. The PICS for an implementation is generated by completing the RL in accordance with the instructions below. An implementation shall satisfy the mandatory conformance requirements of the base standards referenced in the RL.

An implementation’s completed RL is called the PICS. The PICS states which capabilities and options of the protocol have been implemented. The following can use the PICS:

1. the protocol implementer, as a checklist to reduce the risk of failure to conform to the standard through oversight;
2. the supplier and acquirer or potential acquirer of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard PICS proforma;
3. the user or potential user of the implementation, as a basis for initially checking the possibility of interworking with another implementation (it should be noted that, while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PICSes);
4. a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

**INSTRUCTIONS FOR COMPLETING THE RL**

An implementer shows the extent of compliance to the protocol by completing the RL; that is, compliance to all mandatory requirements and the options that are not supported are shown. The resulting completed RL is called a PICS. In the Support column, each response shall be selected either from the indicated set of responses, or it shall comprise one or more parameter values as requested. If a conditional requirement is inapplicable, N/A should be used. If a mandatory requirement is not satisfied, exception information must be supplied by entering a reference Xi, where i is a unique identifier, to an accompanying rationale for the noncompliance.

## A1 NOTATION

**A3.1** The symbols in table A-1 are used in the RL to indicate the status of features.

**Table** **A-1: PICS Notation**

|  |  |
| --- | --- |
| **Symbol** | **Meaning** |
| M | Mandatory |
| O | Optional |
| O.<n> | Optional, but support of at least one of the group of options labeled by the same numeral <n> is required |

**A3.2** The symbols in table A-2 shall be used in the ‘Support’ column of the PICS.

**Table** **A-2: Symbols for PICS ‘Support’ Column**

|  |  |
| --- | --- |
| **Symbol** | **Meaning** |
| Y | Yes, the feature is supported by the implementation. |
| N | No, the feature is not supported by the implementation. |
| N/A | The item is not applicable. |

## A2 REFERENCED BASE STANDARDS

**A4.1** The base standards referenced in the RL shall be:

1. CCSDS BP (this document);
2. RFC 9171 (reference [1]);

**A4.2** In the tables below, the notation in the Reference column combines one of the short-form document identifiers above (e.g., RFC 9171) with applicable subsection numbers in the referenced document. RFC numbers are used to facilitate reference to subsections within the Internet specifications.

## A3 GENERAL INFORMATION

**IDENTIFICATION OF PICS**

|  |  |  |
| --- | --- | --- |
| **Ref** | **Question** | **Response** |
| 1 | Date of Statement (DD/MM/YYYY) |  |
| 2 | PICS serial number |  |
| 3 | System conformance statement cross-reference |  |

**IDENTIFICATION OF IMPLEMENTATION UNDER TEST (IUT)**

|  |  |  |
| --- | --- | --- |
| **Ref** | **Question** | **Response** |
| 1 | Implementation name |  |
| 2 | Implementation version |  |
| 3 | Name of hardware (machine) used in test |  |
| 4 | Version of hardware (machine) used in test |  |
| 5 | Name of operating system used during test |  |
| 6 | Version of operating system used during test |  |
| 7 | Additional configuration information pertinent to the test |  |
| 8 | Other information |  |

**IDENTIFICATION**

|  |  |  |
| --- | --- | --- |
| **Ref** | **Question** | **Response** |
| 1 | Supplier |  |
| 2 | Point of contact for queries |  |
| 3 | Implementation name(s) and version(s) |  |
| 4 | Other information necessary for full identification (e.g., name(s) and version(s) for machines and/or operating systems |  |

**PROTOCOL SUMMARY**

|  |  |  |
| --- | --- | --- |
| **Ref** | **Question** | **Response** |
| 1 | Protocol version |  |
| 2 | Addenda implemented |  |
| 3 | Amendments implemented |  |
| 4 | Have any exceptions been required?NOTE – A YES answer means that the implementation does not conform to the protocol. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming. | 1. Yes
2. No
 |
| 5 | Date of statement (DD/MM/YYYY) |  |

**BASIC REQUIREMENTS**

| **Item** | **Protocol Feature** | **Reference** | **Status** | **Support** |
| --- | --- | --- | --- | --- |
| BP Formatting | Formats bundles as BPv7 per RFC9171. | Section 3.1. RFC9171 Section 4 except section 4.2.5.1 and section 4.4 | M |  |
| Previous Node | Recognizes, parses, and acts on the previous node extension block. | RFC9171 section 4.4.1 | M |  |
| Bundle Age | Recognizes, parses, and acts on the bundle age extension block. | RFC9171 section 4.4.2 | M |  |
| Hop Count | Recognizes, parses, and acts on the hop count extension block. | RFC9171 section 4.4.3 | M |  |
| BPv7 | Identifies bundles as version 7 in the primary block. | RFC9171 section 9.2 | M |  |
| IPN\_naming | Support for the ipn URI Naming Scheme | Section 3.2.1. RFC 9171 section 4.2.5.1.2 | M |  |
| dtn:none | Support for the dtn:none endpoint ID | Section 3.2.2. RFC9171 section 4.2.5.1.1 | M |  |
| IPN Node No | Use IPN node numbers assigned by SANA | This document: 3.2.3 | M |  |
| IPN Service No | Use IPN service numbers assigned by IANA / SANA | This document: 3.2.4 | M |  |
| Bundle Creation Metadata | Bundle creation timestamp and timestamp sequence number assigned when ADU is accepted for transmission. | Section 3.3.1 | M |  |
| Source Node ID | The source node IDs for all non-anonymous bundles sources shall have the same node number. | Section 3.3.2 | M |  |
| Support for dtn:none | Supports sending bundles with source dtn:non | Section 3.3.3 | O |  |
| Registration Constraints | All endpoints in which a node is registered shall have the same node number. | Section 3.4.1 | M |  |
| Minimum Bundle Size | Supports processing of bundles whose total size is less than or equal to 10\*220 bytes (10 MB) | Section 3.5.1 | M |  |
| Service Interface | Supports the service interface in section 4. | Section 4. | M |  |
| LTP CLA | Implements bundle encapsulation in LTP blocks. | This document: B2.1.3 | O.1 |  |
| UDP CLA | Implements bundle encapsulation in UDP datagrams. | This document: B2.1.2 | O.1 |  |
| Space Packets CLA | Implements encapsulation of bundles in Space Packets. | This document B2.1.4 | O.1 |  |
| BP Managed Information | Implements the BP managed information described in Annex C | This document, annex C | M |  |
| Generation of Administrative Records | Follows RFC9171 rules for generation of administrative records. | RFC9171 Section 5.1 | M |  |
| Bundle Transmission | Follows RFC9171 procedures for bundle transmission. | RFC9171 Section 5.2 | M |  |
| Forwarding Contraindicated | Follows RFC9171 procedures when forwarding is contraindicated. | RFC9171 Section 5.3 | M |  |
| Forwarding Failed | Follows RFC9171 procedures when forwarding a bundle fails. | RFC9171 Section 5.4 | M |  |
| Bundle Expiration | Follows RFC9171 procedures when a bundle expires. | RFC9171 Section 5.5 | M |  |
| Bundle Reception | Follows RFC9171 procedures when receiving a bundle. | RFC9171 Section 5.6 | M |  |
| Local Bundle Delivery | Follows RFC9171 procedures when delivering a bundle to the application agent. | RFC9171 Section 5.7 | M |  |
| Bundle Fragmentation | Follows RFC9171 procedures when fragmenting a bundle. | RFC9171 Section 5.8 | M |  |
| Application Data Unit Reassembly | Follows RFC9171 procedures when reassembling and ADU. | RFC9171 Section 5.9 | M |  |
| Bundle Deletion | Follows RFC9171 procedures when deleting a bundle. | RFC9171 Section 5.10 | M |  |
| Discarding a Bundle | Follows RFC9171 procedures when discarding a bundle. | RFC9171 Section 5.11 | M |  |
| Canceling a Transmission | Follows RFC9171 procedures when canceling a transmission. | RFC9171 Section 5.12 | M |  |
| Administrative Records | Formats administrative records per TFC9171 | RFC9171 section 6.1 |  |  |
| Bundle Status Reports | Formats status reports per RFC9171 | RFC9171 section 6.1.1 | M |  |
| MIB\_state | Bundle State Information | This document: table C-1 | M |  |
| MIB\_errors | Error and Reporting Information | This document: table C-2 | M |  |
| MIB\_registration | Registration Information | This document: table C-3 | M |  |
| MIB\_CL\_info | Convergence-Layer Information | This document: table C-4 | M |  |
| MIB\_Config | General Configuration Information | This document: annex C | M |  |

# **ANNEX BCONVERGENCE LAYER ADAPTERS (NORMATIVE)**

## B1 OVERVIEW

This annex describes various Convergence Layer Adapters (CLAs) to support mission operations both in space and on the ground. There are many possible convergence layer protocols to support the various communications interfaces with which the Bundle Protocol may interact. This annex is in no manner comprehensive or rigorous but contains CCSDS supported CLAs that have been demonstrated under various environments, have been requested to be included at the time of this writing, and appear applicable to CCSDS users.

## B2 CONVERGENCE LAYER ADAPTERS

**B2.1 AVAILABLE CL ADAPTERS**

Compliant implementations shall implement at least one of the CLAs in this section.

**B2.1.1 TCP Convergence Layer Adapter**

When sending/receiving bundles using TCP at the convergence layer, bundles shall be encapsulated in TCP packets according to the Delay-Tolerant Networking TCP Convergence-Layer Protocol [RFC 9174]

NOTE – IANA has allocated TCP port 4556 for the TCP CLA.

**B2.1.2 UDP convergence Layer adapter – Encapsulation of bundles in UDP datagrams**

**B2.1.2.3 UDP Maximum Bundle Transmission Size**

The maximum size of a bundle that can be encapsulated in the UDP CLA is 65,535 bytes.

**B2.1.2.4 Bundle Encapsulation in UDP**

Each bundle shall be encapsulated into one UDP datagram with no additional bytes.

NOTE – Bundle protocol agents should endeavor to send bundles of such a size as not to require fragmentation by the IP (Internet Protocol) layer. In practice this generally means keeping the size of the IP datagram (including the IP and UDP headers, plus the bundle) to no more than 1500 bytes.

**B2.1.2.5 UDP Port Number**

All implementations should use UDP port 4556/UDP.

**B2.1.2.6 Network Interactions**

All implementations should ensure that the traffic sent by the UDP convergence layer adaptor does not adversely affect other traffic on the network.

NOTE –Network characteristics can best be managed on a closed network or a network with reserved bandwidth; or the utilization of congestion control procedures as described in RFC 8085 (reference [5]) can be adopted.

NOTE – UDP does not provide any congestion control; UDP CLAs that may be used over large shared networks like the Internet should take measures to ensure that they do not adversely affect other traffic on the network. One such measure would be to control the rate at which UDP datagrams are emitted from the CLA; another would be to define a datagram congestion control protocol (DCCP)-based CLA. See RFC7122 for more information.

**B2.1.3 LTP convergence Layer adapter – Encapsulation of Bundles in LTP Blocks**

**B2.1.3.2 LTP Blocks Include Only Whole Bundles**

An LTP CLA shall only include an integral number of complete bundles in an LTP block.

**B2.X.X.X Length, Value Encoding of Bundles in LTP Blocks**

Each bundle in an LTP block shall be preceded by a CBOR unsigned integer whose value is the length of the bundle (including all blocks) in octets.

**B2.1.3.3 Decapsulation of bundles Encapsulated in LTP**

Bundles shall be extracted from LTP blocks at the receiver and shall be passed to the receiving BPA.

NOTE – Because senders may concatenate multiple bundles into an LTP block, all LTP CLA receivers need to be able to parse multiple bundles out of a received LTP block.

**B2.1.3.4 RELIABLE TRANSMISSION VIA LTP**

For reliable bundle transmission using LTP, bundles shall be encapsulated in LTP blocks containing only red-part (reliable) data.

**B2.1.3.5 UNRELIABLE TRANSMISSION VIA LTP**

For unreliable bundle transmission, bundles shall be encapsulated into LTP blocks containing only green-part (unreliable) data.

**B2.1.4 Space Packet Protocol (SPP) Convergence Layer8**

**B2.1.4.1 SPP Maximum Bundle Transmission Size**

The maximum size of a bundle that can be transferred using the SPP convergence layer adaptor shall be [2^16 - the size of any packet secondary header] Bytes.

**B2.1.4.2 Bundle Encapsulation in SPP**

Each bundle shall be encapsulated into one SPP packet with no additional bytes.

**B2.1.5 Encapsulation Packet Protocol (EPP) Convergence Layer7**

**B2.1.5.1 EPP Maximum Bundle Transmission Size**

Themaximum size of a bundle that can be transferred using the EPP convergence layer adaptor shall be 4,294,967,287 bytes.

**B2.1.5.2 Bundle Encapsulation in EPP**

Each bundle shall be encapsulated into one EPP packet with no additional bytes.

**B2.1.5.3 EPP Protocol Identifier (EPI)**

Implementations with EPP shall use EPI’s allocated by SANA.

# **ANNEX CBP MANAGED INFORMATION**

**(NORMATIVE)**

## C1 BASIC REQUIREMENTS

**C1.1** Each BP node shall support a set of managed information that represents the state of the node at a particular time. The minimal set of such information contains those data items identified by RFC 9171 and collected in this annex. This collection of managed information is shown as the MIB on the right of figure 1-1.

**C1.2** BP nodes shall support five types of managed information:

a) bundle state information;

b) error and reporting information;

c) registration information;

d) convergence layer information;

e) node state information.

**C1.3** In addition to required information, each BP node may choose to provide supplementary information. Each identified managed information item shall identify whether its collection and accurate reporting is required or recommended.

NOTES

1 Representation of, and mechanisms for access to, managed information items will be implementation matters.

2 Individual pieces of managed information may describe related events. Care must be taken when modifying these data to ensure that related data sets remain coherent. For example, when a cumulative counter ‘rolls over’ or is otherwise reset, related counters should also be reset.

## C2 BUNDLE STATE INFORMATION

**C2.1** **OVERVIEW**

Bundles do not have a natural end state within a node: they are forwarded, delivered, or deleted. As such, bundles at rest within a node exist pending a particular action. This set of managed information describes these bundle states and the transitions between them.

**C2.2 SUPPORTED TYPES OF BUNDLE STATE INFORMATION**

BP nodes shall support the bundle state information itemized in table C-1.

**Table** **C-1: Bundle State Information**

|  |  |  |
| --- | --- | --- |
| **Managed Information Item** | **Description** | **Req?** |
| **Retention Constraints** |
| Bundles Retained for Forwarding | The number of bundles/bytes associated with the retention constraint ***forward pending*** at this node. | Cumulative Bytes | No |
| Cumulative Bundles | Yes |
| Bundles Retained for Transmission | The number of bundles/bytes associated with the retention constraint ***dispatch pending*** at this node. | Cumulative Bytes | No |
| Cumulative Bundles | Yes |
| Bundles Retained for Reassembly | The number of bundles/bytes associated with the retention constraint ***reassembly pending*** at this node. | Cumulative Bytes | No |
| Cumulative Bundles | Yes |
| **Priority Counters** |
| Bulk Bundles Sourced | The number of bundles/bytes generated by this node with the ***bulk*** priority. | Cumulative Bytes | No |
| Cumulative Bundles | Yes |
| Normal Bundles Sourced | The number of bundles/bytes generated by this node with the ***normal*** priority. | Cumulative Bytes | No |
| Cumulative Bundles | Yes |
| Expedited Bundles Sourced | The number of bundles/bytes generated by this node with the ***expedited*** priority. | Cumulative Bytes | No |
| Cumulative Bundles | Yes |
| Bulk Bundles Queued | The number of bundles/bytes with the ***bulk*** priority currently resident on this node. | Cumulative Bytes | No |
| Cumulative Bundles | Yes |
| Normal Bundles Queued | The number of bundles/bytes with the ***normal*** priority currently resident on this node. | Cumulative Bytes | No |
| Cumulative Bundles | Yes |
| Expedited Bundles Queued | The number of bundles/bytes with the ***expedited*** priority currently resident on this node. | Cumulative Bytes | No |
| Cumulative Bundles | Yes |
| **Fragmentation** |
| Fragmentation | The number of bundles that have been fragmented by this node. | Cumulative Bundles | Yes |
| Number of Fragments | The number of fragments created by this bundle. | Cumulative Bundles | Yes |

## C3 NODE ERROR AND REPORTING INFORMATION

**C3.1 OVERVIEW**

Nodes generate reports in response to both anomalous and special events. This set of managed information reports on the number of errors and reports constructed at the node.

**C3.2 SUPPORTED TYPES OF ERROR AND REPORTING INFORMATION**

BP nodes shall support the error and reporting information itemized in table C-2.

**Table** **C-2: Error and Reporting Information**

| **Managed Information Item** | **Description** | **Req?** |
| --- | --- | --- |
| **Bundle Deletions** |
| No Info Deletions | The number of bundles deleted with the ***No additional information*** reason code. | Cumulative Bundles | No |
| Expired Deletions | The number of bundles deleted with the ***Lifetime expired*** reason code. | Cumulative Bundles | No |
| Uni-forwarded Deletions | The number of bundles deleted with the ***Forwarded over unidirectional link*** reason code. | Cumulative Bundles | No |
| Cancellation Deletions | The number of bundles deleted with the ***Transmission canceled*** reason code. | Cumulative Bundles | No |
| No Storage Deletions | The number of bundles deleted with the ***Depleted Storage*** reason code. | Cumulative Bundles | No |
| Bad EID Deletions | The number of bundles deleted with the ***Destination endpoint ID unintelligible*** reason code. | Cumulative Bundles | No |
| No Route Deletions | The number of bundles deleted with the ***No known route to destination from here*** reason code. | Cumulative Bundles | No |
| No Timely Contact Deletions | The number of bundles deleted with the ***No timely contact with next node on route*** reason code. | Cumulative Bundles | No |
| Bad Block Deletions | The number of bundles deleted with the ***Block unintelligible*** reason code. | Cumulative Bundles | No |
| Bytes deleted | The total number of bytes in all bundles deleted at this node. | Cumulative Bytes | No |
| **Bundle Processing Errors** |
| Failed Forwards | The number of bundles/bytes that have experienced a forwarding failure at this node. | Cumulative Bytes | No |
| Cumulative Bundles | Yes |
| Abandoned Delivery | The number of bundles/bytes whose delivery has been abandoned at this node. | Cumulative Bytes | No |
| Cumulative Bundles | Yes |
| Discarded Bundles | The number of bundles/bytes discarded at this node. | Cumulative Bytes | No |
| Cumulative Bundles | Yes |

## C4 REGISTRATION INFORMATION

**C4.1 OVERVIEW**

Each node registers in one or more endpoints. These registrations allow for the reception and processing of bundles in the context of the endpoints to which they are addressed.

**C4.2 SUPPORTED TYPES OF REGISTRATION INFORMATION**

BP nodes shall support the registration information itemized in table C-3.

**Table** **C-3: Registration Information**

| **Managed Information Item** | **Description** | **Req?** |
| --- | --- | --- |
| **Identity Information** |
| Endpoint Identifier | The Endpoint ID of this registered endpoint. | Yes |
| Activity State | The current state of the EID, at the time the managed information was queried.One of: ACTIVE or PASSIVE.  | Yes |
| Singleton State | Whether this EID is a singleton EID.One of: YES or NO. | Yes |
| Default Failure Action | The default action to be taken when delivery is not possible.One of: ABANDON or DEFER. | Yes |

## C5 NODE STATE INFORMATION

**C5.1 OVERVIEW**

Global node state information provides the context for using other managed information items.

**C5.2 SUPPORTED TYPES OF NODE STATE INFORMATION**

BP nodes shall support the node state information itemized in table C-4.

**Table** **C-4: Node State Information**

| **Managed Information Item** | **Description** | **Req?** |
| --- | --- | --- |
| **Identity Information** |
| Node Identifier | The Endpoint ID that uniquely and permanently identifies this node. | Yes |
| Bundle Protocol version numbers | The number(s) of the version(s) of the Bundle Protocol that is supported at this node.  | Yes |
| Available storage | The number of kilobytes of storage allocated to bundle retention at this node and not currently occupied by bundles. | Yes |
| Last up time | The most recent time at which the operation of this node was started or restarted.  | Yes |
| Registration count | The number of different endpoints in which this node has been registered since it was last started or restarted. | No |
| **Extension Information (one occurrence per extension)** |
| Extension name | The name identifying one of the BP extensions supported at this node. | Yes |

# **ANNEX DSECURITY, SANA, AND PATENT CONSIDERATIONS**

**(INFORMATIVE)**

## D1 SECURITY

**D1.1 OVERVIEW**

The Bundle Protocol as defined by RFC 9171 has factored in security from the outset of its design. The necessary security architecture and services have been developed in an accompanying RFC, the Bundle Protocol Security specification. Because BP was designed for a resource-constrained environment, it is essential to ensure that only those entities authorized to utilize those resources be allowed to do so.

Also, because of the long latencies and delays in the constrained environments which utilize BP, integrity and confidentiality are essential. Without adequate protections in place to ensure that data integrity and confidentiality are maintained, the difficulty in identifying compromised data will be compounded as a result of the unique environment of CCSDS missions.

**D1.2 SECURITY CONCERNS WITH RESPECT TO THE CCSDS DOCUMENT**

The BP specification (reference [1]) contains a security section (9), which addresses necessary measures to protect bundle protocol data and recommends the use of the Bundle Security Protocol (BPSec) of RFC9172. Two types of security blocks are defined in RFC9172:

1. Bundle Integrity Block (BIB) - Used to ensure the integrity of its plain text security target(s). The integrity information in the BIB MAY be verified by any node along the bundle path from the BIB security source to the bundle destination. Waypoints add or remove BIBs from bundles in accordance with their security policy. BIBs are never used for integrity protection of the cipher text provided by a BCB. Because security policy at BPSec nodes may differ regarding integrity verification, BIBs do not guarantee hop-by-hop authentication, as discussed in RFC9172 Section 1.1.
2. Block Confidentiality Block (BCB) - Indicates that the security target(s) have been encrypted at the BCB security source in order to protect their content while in transit. The BCB is decrypted by security acceptor nodes in the network, up to and including the bundle destination, as a matter of security policy. BCBs additionally provide integrity protection mechanisms for the cipher text they generate.

**D1.3 AUDITING OF RESOURCE USAGE**

No mechanisms are defined in this specification to audit or assist with the auditing of resource usage by the protocol.

**D1.4 POTENTIAL THREATS AND ATTACK SCENARIOS**

No potential threat or attack scenarios are discussed.

**D1.5 CONSEQUENCES OF NOT APPLYING SECURITY TO THE TECHNOLOGY**

By not applying the native security of the BP protocol and the extended security of BPSec allowed by BP, the system must rely on security measures provided at the CLA interfaces and below. For space applications these may be non-existent or merely physical because of the lack of integration between payload and ground systems interfaces. If no security is applied at the BP or lower layers, then applications may be open to man-in-the middle attacks, replay attacks, or a general loss of integrity of transported bundles.

## D2 SANA CONSIDERATIONS

The recommendations of this document do not require any action from SANA. We are not requesting that SANA instantiate any registries at this time. All registries referenced by this specification already exist in IANA / SANA.

## D3 PATENT CONSIDERATIONS

There are no known patents covering the Bundle Protocol as described in this document and its normative references.

# **ANNEX FBP ELEMENT NOMENCLATURE**

## F1 BP Block Tables

This annex specifies the canonical nomenclature for DTN BPv7 block field definitions. In the terms column, the non-canonical terms are given. The full canonical name is formed by prepending “BPv7.” and the table name transformed into camelcase followed by a dot. So for example the full canonical name of the ‘isFragment’ field in the primary block is:

BPv7.primaryBlock.controlFlags.isFragment

This section does not imply anything about implementation, encoding of values, or range limitations set by the encoding or implementation. For encoding and limits set by the encoding methods, see RFC9171.

Value limits imposed by implementations will be documented by forthcoming network management specifications.

**F2 Primary Block Elements**

**Table F-1: Primary Block**

|  |  |  |
| --- | --- | --- |
| **Term** | **Logical****Data Type** | **Range** |
| **bundleVersion** | unsigned integer | (0 .. ) |
| **bundleControlFlags** | **isFragment** | boolean | (0 .. 1) |
| **isAdmin** | boolean | (0 .. 1) |
| **doNotFragment** | boolean | (0 .. 1) |
| **E2EAckRequested** | boolean | (0 .. 1) |
| **stausReportTimeRequested** | boolean | (0 .. 1) |
| **receivedStatusRequested** | boolean | (0 .. 1) |
| **forwardedStatusRequested** | boolean | (0 .. 1) |
| **deliveredStatusRequested** | boolean | (0 .. 1) |
| **deletedStatusRequested** | boolean | (0 .. 1) |
| **crcType** | unsigned integer | (0 .. 2) |
| **destinationEID** | EID | (Dependent on addressing scheme) |
| **sourceEID** | EID | (Dependent on addressing scheme) |
| **reportToEID** | EID | (Dependent on addressing scheme) |
| **creationTimestamp** | **bundleCreationTime** | unsigned integer | (0 .. ) |
| **sequenceNumber** | unsigned integer | (0 .. ) |
| **bundleLifetime** | unsigned integer | (0 .. ) |
| **fragmentOffset** | unsigned integer | (0 .. ) |
| **totalADULength** | unsigned integer | (1 .. ) |
| **crcValue** | byte string | (0 .. ) |

**NOTE –** The value of the primaryBlock.BundleVersion field for the version of the bundle protocol specified in this document is 7.

**NOTE –** The fragmentOffset and totalADULength fields are only present if the bundle is a fragment.

**F3 Block Shared Elements**

All blocks other than the primary block all share a common structure that includes information about the block, CRC information, and a block content field. Those shared elements are represented in the Table F-2.

NOTE: At the time of this specification, the following block types are defined.

* Payload Block: blockType Range (1)
* Previous Node Block: blockType Range (6)
* Age Block: blockType Range (7)
* Hop Count Block: blockType Range (10)

**Table F-1.1 Block Metadata**

|  |  |  |
| --- | --- | --- |
| **Term** | **Logical****Data Type** | **Range** |
| **blockType** | unsigned integer | (0 ..) |
| **blockNum** | unsigned integer | (1 .. ) |
| **processingControlFlags** | **replicateInAllBlocks** | boolean | (0 .. 1) |
| **reportStatusIfUnprocessed** | boolean | (0 .. 1) |
| **deleteIfUnprocessed** | boolean | (0 .. 1) |
| **removeIfUnprocessed** | boolean | (0 .. 1) |
| **crcType** | unsigned integer | (0 .. 2) |
| **blockContent** | blockContentType | (Dependent on value of blockType) |
| **crcValue** | byte string | (0 .. ) |

**F5 Payload Block**

**Table F-1.1 Block Content for Previous Node Block**

|  |  |  |
| --- | --- | --- |
| **Term** | **Logical****Data Type** | **Range** |
| **blockContentType** | payload | byte string | NA |

**F5 Previous Node Block**

**Table F-1.1 Block Content for Previous Node Block**

|  |  |  |
| --- | --- | --- |
| **Term** | **Logical****Data Type** | **Range** |
| **blockContentType** | eidForwarded | EID | (Dependent on addressing scheme) |

**F6 Bundle Age Block**

**Table F-1.1 Block Content for Bundle Age Block**

|  |  |  |
| --- | --- | --- |
| **Term** | **Logical****Data Type** | **Range** |
| **blockContentType** | bundleAge | unsigned integer | (0..2^64-1) |

**F7 Hop Count Block**

**Table F-1.1 Block Content for Hop Count Block**

|  |  |  |
| --- | --- | --- |
| **Term** | **Logical****Data Type** | **Range** |
| **blockContentType** | bundleHopLimit | unsigned integer | (1 .. 255) |
| bundleHopCount | unsigned integer | (1 .. 255) |

**F4 Administrative Record**

**Table F-1.1 Administrative Record**

|  |  |  |
| --- | --- | --- |
| **Term** | **Logical****Data Type** | **Range** |
| **adminRecordStructure** | recordType | unsigned integer | (0..2^64-1) |
| recordContent | Variant type (see note 1) | (Dependent on recordTypeCode) |

NOTE: At the time of this specification, the following record types are defined.

* Bundle Status Report: RecordType Range (1)

1 Variant type dependent on the value of recordTypeCode. RFC 9171 defines a recordContent for Bundle Status Record (BSR.)

**F4 Bundle Status Report Administrative Record Content**

**Table F-1.1 Record Content for Bundle Status Report**

|  |  |  |
| --- | --- | --- |
| **Term** | **Logical****Data Type** | **Range** |
| BSRRecordContentType | BSRStatus | BSRStatusType | See below - BSRStatusType |
| BSRReasonCode  | unsigned integer  (see note 2) | (0..2^64-1) |
| subjectSourceEID | EID | (Dependent on addressing scheme) |
| subjectCreationTimestamp | unsigned integer | (0..2^64-1) |
| subjectFragmentOffset (see note 4) | unsigned integer | (0..2^64-1) |
| subjectTotalADULength (see note 4) | unsigned integer | (0..2^64-1) |
|  |  |  |  |
| BSRStatusType | receivedEvent | eventDataPointType | See below - eventDataPointType |
| forwardedEvent | eventDataPointType | See below - eventDataPointType |
| deliveredEvent | eventDataPointType | See below - eventDataPointType |
| deletedEvent | eventDataPointType | See below - eventDataPointType |
|  |  |  |  |
| eventDataPointType | eventAssertion | boolean | (0 .. 1) |
| eventTimestamp (see note 5) | unsigned integer (see note 3) | (0..2^64-1) |

NOTES:

1. Administrative records are carried as payloads of bundles and are signaled by the BPv7.primaryBlock.bundleControlFlags.isAdmin field.
2. Enumerated value form the set of Valid status report reason codes that are registered in the IANA "Bundle Status Report Reason Codes" subregistry in the "Bundle Protocol" registry
3. Unsigned integer representing the DTN Time.
4. This is optional and is present if and only if the bundle whose status is being reported was a fragment.
5. This is optional and is present if the eventAssertion is 1 AND the "Report status time" flag was set to 1 in the bundle processing control flags of the bundle whose status is being reported

# **ANNEX GINFORMATIVE REFERENCES(INFORMATIVE)**

[G1] *Rationale, Scenarios, and Requirements for DTN in Space.* Issue 1. Report Concerning Space Data System Standards (Green Book), CCSDS 734.0-G-1. Washington, D.C.: CCSDS, August 2010.

[G2] J.H. Saltzer, D.P. Reed, and D.D. Clark. “End-to-End Arguments in System Design.” In *Proceedings of the 2nd International Conference on Distributed Computing Systems (April 8-10, 1981, Paris, France),* 509-512. Los Alamitos, CA, USA: IEEE Computer Society, 1981.

[G3] *Orga*nization 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.

[G4] L. Eggert, G. Fairhurst, and G. Shepard. UDP Usage Guidelines. RFC 8085. Reston, Virginia: ISOC, March 2017.

[G5] H. Kruse, S. Jero, and S. Ostermann. *Datagram Convergence Layers for the Delay- and Disruption-Tolerant Networking (DTN) Bundle Protocol and Licklider Transmission Protocol (LTP)*. RFC 7122. Reston, Virgina: ISOC, January 25, 2021.

# **ANNEX HABBREVIATIONS AND ACRONYMS(INFORMATIVE)**

Term Meaning

AA application agent

ADU Application Data Unit

AOS Advanced Orbiting Systems

AR Administrative Record

BP Bundle Protocol

BPA bundle protocol agent

BSR Bundle Status Report

CBOR Concise Binary Object Representation

CCSDS Consultative Committee for Space Data Systems

CRC cyclic redundancy check

CL convergence layer

CLA convergence layer adapter

DTN delay tolerant network

EID endpoint identifier

EPP Encapsulation Packet Protocol

IANA Internet Assigned Numbers Authority

IEC International Electrotechnical Commission

IP Internet Protocol

IPN Interplanetary Network

ISO International Organization for Standardization

ISOC Information Security Operations Center

LTP Licklider Transmission Protocol

OSI Open Systems Interconnection

PICS protocol implementation conformance statement

PDU protocol data unit

RL requirements list

RFC Request For Comment

SABR Schedule Aware Bundle Routing

SANA Space Assigned Numbers Authority

SDU service data unit

SPP Space Packet Protocol

TC Telecommand

TCP Transmission Control Protocol

TM Telemetry

UDP User Datagram Protocol

URI Uniform Resource Identifier

USLP Unified Space Link Protocol