

Comment

1.4.3.1

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).

Not sure how 0 CLA scenario works

PICS mandates at least one CLA

Comment

endpoint identifier, EID: A text string identifying the destination of a bundle (see RFC 9171, section 3.1). Each endpoint ID (EID) is a Uniform Resource Identifier (URI). As such, each endpoint ID can be characterized as having this general structure:

< scheme name > : < scheme-specific part, or ‘SSP’ >

Does it only identify the destination of a bundle? What about source EID and report to EID?

Comment

B2.1.4.3 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.

“LTP Block” instead of just “LTP” in the above title.

Comment

De-encapsulate or decapsulation

(I had seen decapsulation used somewhere. Although “decapsulation” is correct, networking parlance uses “De-encapsulate” and it corresponds to “encapsulate”, which has been used in the CCSDS document.)

Comment

Support for dtn:none	Supports sending bundles with source dtn:non	This document: 3.3.4	O	
----------------------	----------------------------------------------	----------------------	---	--

dtm:none instead of dtm:non in the second column

Comment

Comment

Do the service numbers have to be assigned by SANA? (just a question)

I think there was a recent discussion that some service number range will be available for the users to use as they please.

Comment

Page A-5. A-6

	Section 4			
LTP CLA	Implements bundle encapsulation in LTP blocks	This document: B2.1.4	O.1	
UDP CLA	Implements bundle encapsulation in UDP datagrams.	This document: B2.1.3	O.1	

DRAFT CCSDS RECOMMENDED STANDARD FOR CCSDS BUNDLE PROTOCOL SPECIFICATION

Item	Protocol Feature	Reference	Status	Support
Space Packets CLA	Implements encapsulation of bundles in Space Packets	This document B2.1.5	O.1	

Refer to 0.1 in the 2nd last column (Status)

Mandates that at least one of the CLA from the set {LTP CLA, UDP CLA, Space Pkt CLA} should be implemented.

Conflicts with zero CLA mentioned earlier in the document

- Should this set also include TCPCL, EEPCL? (They are there in Annex B)

Comment

Item	Protocol Feature	Reference	Status	Support
Bundle Deletion	Follows RFC 9171 procedures when deleting a bundle	RFC 9171 Section 5.10	M	
Discarding a Bundle	Follows RFC 9171 procedures when discarding a bundle.	RFC 9171 Section 5.11	M	
Administrative Records	Formats administrative records per RFC 9171	RFC 9171 section 6.1		

M missing the last row, Page A-7

Comment

Added PICS

Ability of the implementation to be able to process extension blocks headers in general. (At the minimum, implementations should be able to inform they are unable to process extension blocks for a given block type)

Comment

B2.1.1 General

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

Conflict with zero CLA statement earlier in the document

Comment

B2.1.3.1 UDP Maximum Bundle Transmission Size

The maximum size of a bundle that can be encapsulated in the UDP (reference [8]) CLA is 65,535 bytes.

Above statement is not correct

"This field (length field of UDP) specifies the length in bytes of the UDP header and UDP data. The minimum length is 8 bytes, the length of the header. The field size sets a theoretical limit of 65,535 bytes (8-byte header + 65,527 bytes of data) for a UDP datagram. However, the actual limit for the data length, which is imposed by the underlying IPv4 protocol, is **65,507** bytes (65,535 bytes - 8-byte UDP header - 20-byte IP header)." [from Wiki]

[Comment](#)

B2.1.6 Encapsulation Packet Protocol Convergence Layer (reference [6])

Use of EPP at the start of the title would be consistent with the other titles like , UDP, LTP, SPP etc.

[Comment](#)

B2.1.4.4 RELIABLE TRANSMISSION VIA LTP

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

B2.1.4.5 UNRELIABLE TRANSMISSION VIA LTP

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

Title case and not all caps

[Comment](#)

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.

"or deleted" - change to "and/or deleted" (They are not mutually exclusive. A bundle can be forwarded and deleted.)

[Comment](#)

Table C-2: Error and Reporting Information

Managed Information Item	Description	Req?
	Bundle Deletions	

What is the meaning of "Req?"

Do we need the question mark - "Req?"

[Comment](#)

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 nonexistent 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.

Not sure what is meant by "merely physical"

E4 PAYLOAD BLOCK

Table E-3: Block Content for Previous Node Block

Term		Logical Data Type	Range
blockContentType	payload	byte string	NA

E5 PREVIOUS NODE BLOCK

Table E-4: Block Content for Previous Node Block

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

E2 table title should say "Payload" instead of "Previous Node"

Table E-8: 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)
<hr/>			
BSRStatusType	receivedEvent	eventDataPointType	(See below - eventDataPointType)
	forwardedEvent	eventDataPointType	(See below - eventDataPointType)
	deliveredEvent	eventDataPointType	(See below - eventDataPointType)
	deletedEvent	eventDataPointType	(See below - eventDataPointType)
<hr/>			
eventDataPointType	eventAssertion	Boolean	(0 .. 1)
	eventTimestamp (see note 5)	unsigned integer (see note 3)	(0..2 ⁶⁴ -1)

Range for subjectCreationTimestamp is not correct. (row 4, seeing from right hand side)

This is not just the time, but also the sequence number

Therefore simply stating the range as (0..2⁶⁴-1) is not correct.

[Comment](#)

ANNEX E

BP ELEMENT NOMENCLATURE

Annex is informative or normative? Doesn't say - not consistent with other annexes

[Comment](#)

ANNEX F

IPN URI SCHEME UPDATES

(INFORMATIVE)

This document references the ipn URI scheme per RFC9171 where endpoint identifiers are of the form <node number>.<service number> The IETF DTN WG is current working an

"Currently" instead of "current"

[Comment - Additions to Annex H](#)

AE
ASE
ION
SS&A - Service Sites and Apertures (SS&A)

5.3 UNDERLYING COMMUNICATION SERVICE REQUIREMENTS

5.3.1 Each convergence layer protocol adapter shall provide the following services to the bundle protocol agent:

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

In point "C" above, it might be better to use some other word instead of "delivering" to avoid confusing the casual reader into believing that this is Delivery of bundle as defined by bundle protocol.

NOTES

- 1 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 as specified in RFC 9172) 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.
- 2 Additionally, BP 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.

5.3.2 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.

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

Similarly, at the start of 5.3.3 and at the end of 1st point above.

Comment

Page 1-1
Section 1.2 , 3rd para
LTP is missing.

Comment

Page 1-2

- Annex F contains the Interplanetary Internet (ipn) URI scheme updates.
- Annex G contains informative references.
- Annex H contains abbreviations and acronyms used in this document.

Use consistent title case

Annex - F - * Scheme Updates

Annex - G - * Informative References

Annex - H - Abbreviations and Acronyms *

Comment

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).

Application Agent should be lowercase.

Comment

application data unit, ADU: The application-specific data being transferred via the Bundle Protocol. The data in an ADU is carried in the payload block(s) of a bundle, and may be split among the payloads of multiple bundles if the original bundle is fragmented.

“Payload block(s) of a bundle”

There is only one payload block in a bundle.

Comment

block: One of the Bundle Protocol data structures that together constitute a well-formed bundle.

There is no other data structure (at this level of abstraction). So, use of “One of the Bundle Protocol data structures” is questionable. There are many different kinds of blocks, but they are still all blocks. (see the last sentence below as well)

bundle: 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.

Comment

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. This concept is illustrated in figure 2-1, in which BP is used to provide an end-to-end data delivery service over an internetwork (on the left) and a link-layer hop (on the right). Wherever the data path transits the bundle layer in the diagram, data may be stored waiting for an outbound path to become available.

Since bundles may be held in storage at the destination (where the bundle is not waiting for an outbound path), the last sentence may be extended to account for this case as well.

[Comment](#)

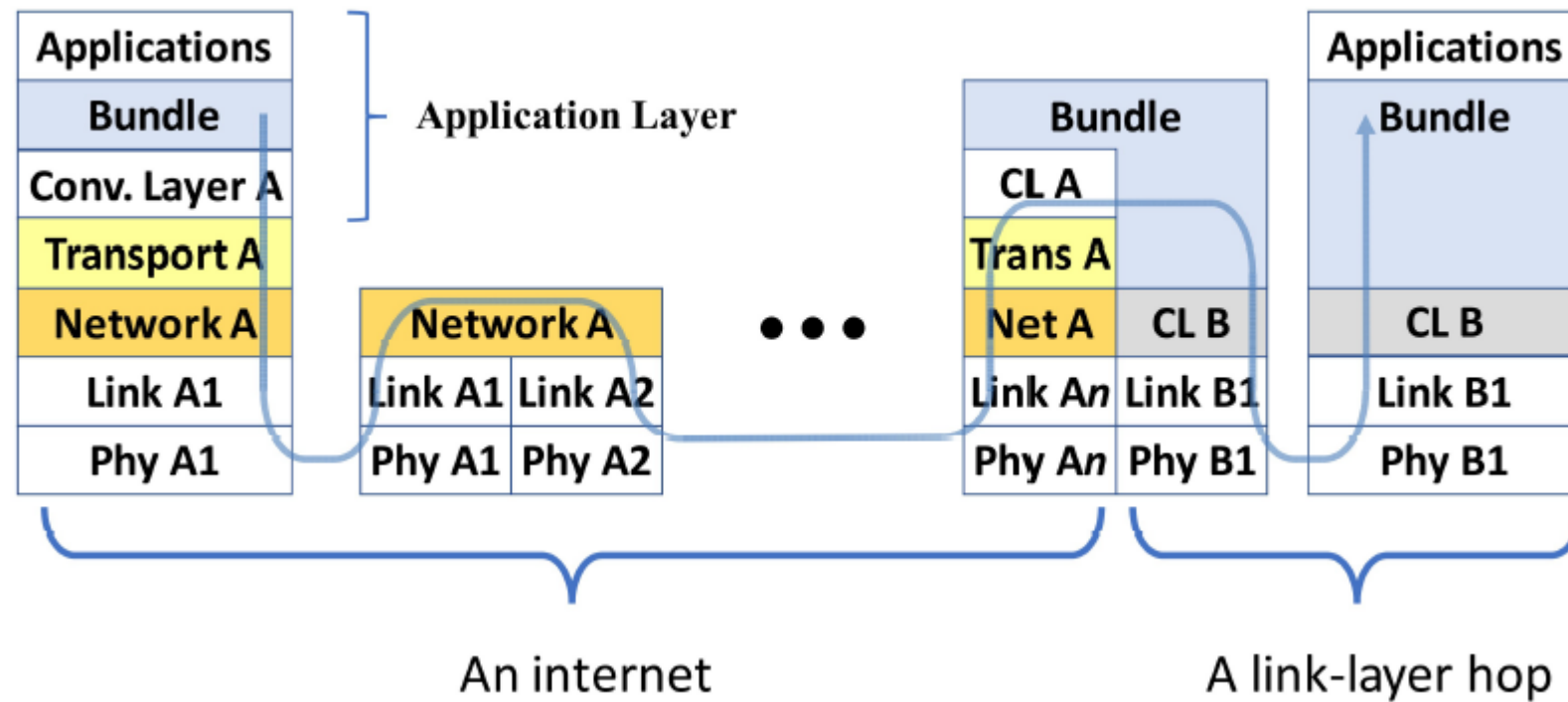
BP uses underlying ‘native’ Data Link Layer transport and/or network protocols for communications within a given constituent network. The layer at which those underlying protocols lie is known as the ‘convergence layer’. The interface between the BP layer and the convergence layer is known as the ‘convergence 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 (CL A) , 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) (reference [9]), 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, for example, an on-orbit internet and a ground internet, terrestrial or otherwise.

Refer to 5th last line in the above screenshot

Suggest “CLA corresponding to CL A”

CLA (Convergence Layer Adapter) is not CL A (Convergence Layer A)

[Comment](#)



"User applications" instead of just "Applications" may provide more clarity.
Bundle Layer or BP Layer instead of just Bundle (which is a PDU corresponding to BP layer)

[Comment](#)

2.5.2 SECURITY

The CCSDS Delay Tolerant Networking Working Group (DTN WG) is currently standardizing a set of security services based on IETF RFC 9172 (BPsec) (reference [G3]). BPsec provides per-block (or per-group-of-blocks) security services, including cryptographic integrity and confidentiality. With the 'base' BPv7 protocol, there is no mechanism to prevent a node from 'spoofing' transmitted bundles by using the source EID of another node. While such attacks *might* be detectable by closely examining routing, there is no guarantee that such mechanisms would work or be sufficient.

Won't just EID suffice instead of "source EID."

[Comment](#)

2.5.3 NETWORK MANAGEMENT

There will be many configuration parameters that need to be managed for each bundle node. There is ongoing work in the SIS-DTN WG and in the IETF to standardize a network management protocol that provides a level of autonomy in resource-constrained environments. The Asynchronous Management Protocol, AMP [X - need informative reference, maybe need to talk about and include AMA as well?] is the current draft

[Refer to X in the above screenshot.](#)

[Comment](#)

2.5.3 NETWORK MANAGEMENT

There will be many configuration parameters that need to be managed for each bundle node. There is ongoing work in the SIS-DTN WG and in the IETF to standardize a network management protocol that provides a level of autonomy in resource-constrained environments. The Asynchronous Management Protocol, AMP [X - need informative reference, maybe need to talk about and include AMA as well?] is the current draft specification. AMP is structured to provide an overall management protocol and set of encoding rules for a set of Asynchronous Data Models (ADMs). The community (both SIS-DTN and IETF) envisions a set of ADMs that includes both basic specification-level ADMs (e.g. an ADM that describes the configuration and monitoring of a ‘stock’ BPv7 bundle node) together with implementation-specific ADMs (e.g. an ADM that includes information specific to a particular BPv7 implementation).

The benefits of standardizing a network management protocol are (probably) largely more relevant to monitoring than they are to configuration. That is, while an agency might allow some other agency to monitor various configuration parameters of a bundle node, it seems unlikely that an agency would allow another agency to configure that node. That said, we do expect to include capabilities such as control / configuration of contact plan information (in either an ION-specific ADM or potentially in a ‘BP Nodes that use contact plans’ ADM).

[Last sentence. Maybe make more formal](#)

Comment

3.2.2 Implementations of this specification are not required to deliver or forward bundles whose source, destination, or report-to endpoint identifiers use the dtn URI scheme in RFC 9171.

Except that dtn:none is needed for source EID

4.3 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, an application agent registered in a single endpoint could service other local nodes such as elements of a sensor network using private protocols.

4.3.2 SOURCE NODE ID

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

NOTE – Source node IDs are singleton endpoint IDs in which the node is registered as defined in RFC9171. In particular, when using the ipn URI scheme, the source node ID includes both a node number and a service number as described in 2.4.

4.3.3 DESTINATION ENDPOINT ID

The destination endpoint ID parameter shall uniquely identify the communications endpoint to which bundles should be delivered.

4.3.4 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.

Are 4.3.1 and 4.3.4 different? Or there should be only one of these two.

Refer to 4.3.2

[Comment](#)

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.

RFC 9171 doesn't mandate Delivery Failure Action (DFA). DFA may not be defined. (See RFC 9171 Section 5.7, step 2, 2nd bullet)
Does CCSDS mandate that all CCSDS compliant BP nodes will have a well defined DFA?

[Comment](#)

Reference G1 mentioned on page 12 is not actually Annex G1

[Comment](#)

bundle: 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.

This "bundling of metadata" and the concept of "immediate usability" of the data at the delivery seems to be out of sync with how we are using the bundle. (This is just a comment/observation and is not intended for anything more than that.)

