

Workgroup: Internet Engineering Task Force

Internet-Draft:

draft-blanchet-dtn-email-over-bp

Published: 4 March 2024

Intended Status: Standards Track

Expires: 5 September 2024

Authors: M. Blanchet

Encapsulation of Email over Delay-Tolerant Networks(DTN) using the Bundle Protocol

Abstract

This document describes the encapsulation of emails using RFC2442 format in the payload of bundles of the Bundle Protocol for the use case of Delay-Tolerant Networks(DTN) such as in space communications.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 5 September 2024.

Copyright Notice

Copyright (c) 2024 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

- [1. Introduction](#)
 - [1.1. Requirements Language](#)
 - [1.2. Vocabulary](#)
- [2. Description](#)
- [3. Encapsulation](#)
- [4. Considerations](#)
- [5. Use case where the endpoint is only a BP agent](#)
- [6. Alternatives](#)
- [7. IANA Considerations](#)
- [8. Security Considerations](#)
- [9. References](#)
 - [9.1. Normative References](#)
 - [9.2. Informative References](#)
- [Acknowledgements](#)
- [Author's Address](#)

1. Introduction

An important use case of Delay-Tolerant Networks(DTN) using the Bundle Protocol[[RFC9171](#)] is in space communications. Current scenarios by space agencies[[ioag](#)] involves the use of an IP network on the planetary body and the use of the Bundle Protocol between planetary bodies, including Earth. Therefore, there are IP endpoints at both ends, and then bundles could be used as a transport of Internet related application payload. This document describes the encapsulation of emails over bundles so that end-users on the remote end (aka on a planetary body such as Moon or Mars) or processes can use typical Internet Email software and tools to read/write emails, while the emails when transiting in space are encapsulated into bundles of the Bundle Protocol.

It should be noted that in DTNs, delays may be very large compared to normal delays on (Earth) Internet. Therefore, the SMTP [[RFC5321](#)] "conversation" between the two SMTP peers should be avoided since it will take many round-trips over long delays networks to achieve the delivery. Therefore, this document proposes to encapsulate the whole Email, including the envelope, using the Batch SMTP media-type [[RFC2442](#)] as a single file into bundles of the Bundle Protocol.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [[RFC2119](#)] [[RFC8174](#)] when, and only when, they appear in all capitals, as shown here.

1.2. Vocabulary

*Internet: identifies the global IP network on Earth as we know it

*Planetary body: describes Moon, Mars and others. In this document, we only care about ones that would have some IP networking installed

2. Description

In a typical scenario, the email would be created on (Earth) Internet, sent using regular delivery (DNS MX records, SMTP, ...) to a destination address that points to a location on a planetary body. That email would arrive to an SMTP server which is connected to the Bundle agent [[RFC9171](#)] capable of routing bundles to the final Bundle agent on the other planetary body, who has also a connection to an SMTP server. That SMTP server on the other planetary body is responsible for final delivery on that planetary body network. The target bundle protocol service number contained in the bundle is the one allocated by IANA per this document.

TBD: artwork representation

This document assumes that there is a close interaction between a Mail Transfer Agent(MTA) and a Bundle protocol agent, in, for example, the form of interprocess communication. However, the specific interaction is outside the scope of this document and is left to the implementation.

3. Encapsulation

The payload of the bundle [[RFC9171](#)] is a Batch SMTP media-type content [[RFC2442](#)] that includes both the email itself and the envelope. A bundle can only contain a single email.

If the email is too large to fit in a single bundle, then the bundle agent uses bundle fragmentation as described in section 5.8 of [[RFC9171](#)] to slice the email into multiple bundles. It is the responsibility of the receiving bundle agent to properly reassemble the multiple bundle payloads into the source email.

The receiving bundle agent will receive the email-containing bundle(s) on this document specifically assigned IANA service number. The agent transfers the email to a Mail Transfer Agent(MTA) that will deliver to the appropriate location as normal practice on Internet.

4. Considerations

Configuring and deploying an isolated IP network on a planetary body with local mail servers, DNS servers and email client needs careful consideration. For example, emails sent between two end-users on the same planetary body should not go through space links down to Earth and back to the planetary body. This operational consideration is not described here and is outside the scope of this document.

By using the encapsulation of emails using the [\[RFC2442\]](#) format, there is no negotiation and no declaration of capabilities as it is done in normal SMTP [\[RFC5321\]](#). Therefore, the source endpoint has no way by this solution to know the capabilities of the other endpoint. Therefore, on the target planetary bodies MTAs should be properly configured to receive the appropriate kind of emails sent from another planetary body.

As with typical SMTP on Internet, it is very possible that either improper configuration or other reasons cause the destination MTA to reject the email. In this case, it should send an error using the same technique on the reverse path, if at least the From address is parsable. If the email is not parsable on the destination MTA, then normal operational logging shall be used. Similarly to the previous paragraph, this consideration of non-negotiation of capabilities is not described here and is outside the scope of this document. It is however expected that this environment will be highly configured and managed, so that such issues shall not happen often.

It should be noted that attachments to emails will be part of this encapsulation mechanism by default.

5. Use case where the endpoint is only a BP agent

There are cases such as a spacecraft currently moving in space where there might be no IP network attached to it and has only a BP agent. This specification works also as is in this use case, if that device is augmented by a local IP stack, with an SMTP listener, where the final source or destination of the SMTP packet is within the spacecraft.

6. Alternatives

There are other ways to send email for this use case.

- *JMAP (RFC8620) could be used but would require http encapsulation over bundle protocol.

- *JMAP (RFC8620) JSON encoding of its data model could be encapsulated with a media-type similarly to Batch SMTP.

*Batch SMTP could be also encapsulated into a file transfer protocol such as CFDP and then MTA on both sides would have to watch the directory for new uploaded files and act upon those new files.

*A file synchronization mechanism such as rsync over some transport could also be used to synchronize user's mail stores. This method could work for some use cases, but have some issues. First, if the delay between two synchronisation events is sufficiently long, the origin mail store may contain a large amount of emails and be very big in size, therefore the synchronisation over the DTN network will be not only a big burden, but might contain non useful data, such as big files that are not relevant to read on the other side of the DTN network. Moreover, it does not create a way to exchange emails between the two end of the DTN network. It assumes that the same users are on both sides of the DTN network, which may well not be the case in many use cases.

*Inventing a new mail protocol native over bundle protocol

There are probably other ways to achieve the same goal. However, we believe this specification is the most simple and effective way. An implementation is pretty straightforward and could leverage all software and experience of Internet mail. For example, with this solution, it would be possible for an astronaut to use his mobile phone mail application to read his email while not knowing it has been carried over bundle protocol for some portions of the path.

7. IANA Considerations

This document requests IANA to allocate a new Bundle Protocol service number under the current CBHE Service Numbers and assign it to this document. Description should be: "RFC5322 content (aka Email)". If the registry is updated to indicate the Bundle Protocol version, this specification do apply for both BPv6 and BPv7, as it is agnostic of the BP version.

Note to IANA (to be removed by the RFC editor): prefer 25 to relate to the Internet email service, but not a big deal if not.

8. Security Considerations

Sending any payload with bad data over a space link is a somewhat DOS attack. It is expected that this environment will be highly managed and controlled, therefore, before a bundle is sent, the payload is properly verified and access control to the space network will be tightly controlled.

BPSEC[\[RFC9172\]](#) can be used to provide authentication and encryption at the Bundle layer.

9. References

9.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC2442] Freed, N., Newman, D., Belissent, J., and M. Hoy, "The Batch SMTP Media Type", RFC 2442, DOI 10.17487/RFC2442, November 1998, <<https://www.rfc-editor.org/info/rfc2442>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

9.2. Informative References

- [RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <<https://www.rfc-editor.org/info/rfc5321>>.
- [RFC9171] Burleigh, S., Fall, K., and E. Birrane, III, "Bundle Protocol Version 7", RFC 9171, DOI 10.17487/RFC9171, January 2022, <<https://www.rfc-editor.org/info/rfc9171>>.
- [RFC9172] Birrane, III, E. and K. McKeever, "Bundle Protocol Security (BPsec)", RFC 9172, DOI 10.17487/RFC9172, January 2022, <<https://www.rfc-editor.org/info/rfc9172>>.
- [ioag] Lunar Communications Architecture Working Group, Interagency Operations Advisory Group, "The Future Lunar Communications Architecture, Report of the Interagency Operations Advisory Group", January 2022.

Acknowledgements

The following people have reviewed and provided comments to improve this document (in no particular order): John Levine, Stephen Farrell, Stuart Card, Jorge Amodio, Ed Birrane, Pete Resnick.

Author's Address

Marc Blanchet

Email: marc.blanchet@viagenie.ca