Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: 2 October 2025

M. Blanchet

31 March 2025

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

draft-blanchet-dtn-http-over-bp-03

Abstract

This document describes the encapsulation of HTTP requests and responses 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

Copyright Notice

Table of Contents

1. Introduction

An important use case of Delay-Tolerant Networks(DTN) using the Bundle Protocol[RFC9171](BP) is in space communications. Current scenarios by space agencies[ioag] involves the use of an Internet Protocol (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 http requests and responses 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 HTTP software and tools to use http-based applications, while the http requests and responses when transiting in space is 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. In theory, there should be no timeout at the HTTP layer, but timeouts are typical at the transport layer. Therefore, care should be taken on how to setup the whole path to avoid those potential issues. This document describes some possible solutions.

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. Encapsulation

Similar to [draft-blanchet-dtn-over-email], this document defines the encapsulation of HTTP requests and responses into bundles of the Bundle Protocol

Since HTTP is a query-response protocol, the client must keep a handle of its communication with the server to get the response. On regular IP networks, this is done together with the transport which accomplishes a direct connection between the two peers. That notion of direct //connection does not exist when using BP. Therefore, the encapsulation is prepended with a connection ID and a sequence number. The connection ID is generated by the client. The connection ID is a random number which should have similar characteristics to UUIDs. The actual details of the connection ID is left to the implementation, however, the connection ID appears as a string of ASCII characters, with the same restrictions as [RFC4122]. The sequence number is a positive integer and is set by the client and the server. It is zero if the query or response is complete in the single return. In case of long responses such as real-time media, the response is continuous and in this case, the server starts with the value 1 and increase the sequence number by one each time it sends a new packet for the same response and the same connection id. The client may also use the sequence number to tell the server that the query is still not finished in the first packet, for example, when a POST is used with an embedded large file. Similarly, the client increments the sequence number by one for each packet.

Herein, the client and server are in fact a small piece of software between the bundle protocol agent and the HTTP client or server.

In case the http request or response is too large for the bundle agent and that the client or server did not slice the request or response into smaller pieces as described in the previous paragraph, then the bundle agent uses bundle fragmentation as described in section 5.8 of RFC9171 to slice the http data in multiple bundles. It is the responsability of the receiving bundle agent to properly reassemble the http data into the source http content. Both sides may use their sequence numbers and they are independent and can be used at the same time. Both the client and the server keeps track of the connection ids and sequence numbers. When multiple packets are sent and therefore sequence numbers were incremented from 1, the last packet of the sending agent is indicated with sequence number zero. In other words, sequence number zero means no more packets.

The receiving bundle agent will receive the http-containing bundle(s) on the specific assigned IANA service number. It is expected that the agent will transfer the http data to a http listener that will deliver to the appropriate location as normal practice on (Earth) Internet.

3. Negotiation, Redirect and other Considerations

Given the nature of DTN networks, negotiations such as HTTP version negotiations, URL redirection, and other techniques are still possible and working in this proposal, but not recommended as they would trigger additional bundles over a long delay network, which may end up triggering timeouts at some level, such as the application. Therefore, careful configuration of both endpoints to avoid that extra trafic is advised. Initial key negotiation is however difficult to avoid, unless offpath or static key configuration is done. Given that http2 and http3 create possible long standing connections, then the extra initial key negotiation is not too costly compared to the possible duration of the connection between the two peers.

4. Encapsulation Format

The encapsulation is done as follows inside a bundle: First appears at the beginning of all bundles the connection idm which is a string of undefined length terminated with ASCII CR-LF. Then the sequence number follows for all bundles, as a string representing a positive integer of undefined length terminated with ASCII CR-LF. As described above, the sequence number can be zero when no other packet will come. Following the CR-LF of the sequence number is the actual HTTP content. For example, for an HTTP1.1 query, the HTTP content after the terminated sequence number could be: "GET /index.html HTTP/1.1". Various HTTP headers may be added as needed. After the terminated sequence number could be any HTTP content of any HTTP version, including binary frames. This specification is agnostic of the HTTP version.

TBD: artwork of bundle encapsulation

5. Considerations

Configuring and deploying an isolated IP network on a planetary body with local HTTP servers or clients, DNS servers or other infrastructure needs careful considerations. These operational considerations are not described here and are outside the scope of this document.

6. 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. However, this specification works as is, if that device is augmented by a local IP stack, with an HTTP listener, where the final source or destination of the HTTP packet is within the spacecraft.

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: "HTTP content". 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.

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>.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/info/rfc4122>.

[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>.

[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>.

9.2. Informative References

[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.

[draft-blanchet-dtn-over-email]
Blanchet, MB., "Encapsulation of Email over Delay-Tolerant Networks(DTN) using the Bundle Protocol", 17 January 2023, <draft-blanchet-dtn-over-email-00>.

Acknowledgements

The following people have reviewed and provided comments to improve this document (in no particular order): Stuart Card, Mark Nottingham, Ed Birrane.

Author’s Address

Marc Blanchet
Email: marc.blanchet@viagenie.ca