Workgroup: tcpm
Internet-Draft:
draft-boucadair-tcpm-rst-diagnostic-payload-02
Published: 4 April 2022
Intended Status: Standards Track
Expires: 6 October 2022
Authors: M. Boucadair
Orange

TCP RST Diagnostic Payload

Abstract

This document specifies a diagnostic payload format to be returned in TCP RST segments. Such payloads are used to share with the endpoints the reasons for which a TCP connection has been reset. This is meant to ease diagnostic and troubleshooting.

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 6 October 2022.

Copyright Notice

Copyright (c) 2022 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
2. Terminology
3. RST Diagnostic Payload
4. Some Examples
5. IANA Considerations
   5.1. RST Diagnostic Payload CBOR Key Values
   5.2. New Registry for TCP Failure Causes
6. Security Considerations
7. Acknowledgements
8. References
   8.1. Normative References
   8.2. Informative References

Author's Address

1. Introduction

A TCP connection [I-D.ietf-tcpm-rfc793bis] can be reset by a peer for various reasons, e.g., received data does not correspond to an active connection. Also, a TCP connection can be reset by an on-path service function (e.g., CGN [RFC6888], NAT64 [RFC6146], firewall) for several reasons. Typically, a NAT function can generate an RST segment to notify the peers upon the expiry of the lifetime of the corresponding mapping entry or because an RST segment was received from a peer (Section 2.2 of [RFC7857]). A TCP connection can also be closed by a user or an application at any time. However, the peer that receives an RST segment does not have any hint about the reason that led to terminating the connection. Likewise, the application that relies upon such a TCP connection may not easily identify the reason for a connection closure. Troubleshooting such events at the remote side of the connection that receives the RST segment may not be trivial.

This document fills this void by specifying a format of the diagnostic payload that is returned in an RST segment. Returning such data is consistent with the provision in Section 3.5.3 of [I-D.ietf-tcpm-rfc793bis] for RST segments.

This document does not change the conditions under which an RST segment is generated (Section 3.5.2 of [I-D.ietf-tcpm-rfc793bis]).

The generic procedure for processing an RST segment is specified in Section 3.5.3 of [I-D.ietf-tcpm-rfc793bis]. Only the deviations from that procedure to insert and validate an enclosed diagnostic payload is provided in Section 3. Section 4 provides a set of examples to illustrate the use of TCP RST diagnostic payloads.

This document specifies the format and the overall approach to ease maintaining the list of codes while allowing for adding new codes as needed in the future and accommodating any existing vendor-specific codes. An initial version of error codes is available in Table 1. However, the authoritative source to retrieve the full list of error codes is the IANA-maintained registry Section 5.2.

2. Terminology

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.

This document makes use of the terms defined in Section 4 of [I-D.ietf-tcpm-rfc793bis].

3. RST Diagnostic Payload

The RST diagnostic payload MUST be encoded using Concise Binary Object Representation (CBOR) Sequence [RFC8742]. The Concise Data Definition Language (CDDL) [RFC8610] for the diagnostic payload is as follows:

```
; This defines an array, the elements of which are to be used
; in a CBOR Sequence:
diagnostic-payload = [magic-word, reason]
; Magic word to identify a payload that follows this specification
magic-word = 12345
; Reset reason details:
reason= {
  ? reason-code: uint,
  ? pen:uint,
  ? reason-description: tstr,
}
```

Figure 1: Structure of the RST Diagnostic Payload

The RST diagnostic payload comprises a magic word that is used to unambiguously identify an RST payload that follows this specification. It MUST be set to the RFC number to be assigned to this document.

> Note to the RFC Editor: Please replace "12345" with the RFC number assigned to this document.

All parameters in the reason component of an RST diagnostic payload are mapped to their CBOR key values as specified in Section 5.1. The description of these parameters is as follows:

reason-code: This parameter takes a value from an available registry such as the "TCP Failure Causes" registry (Section 5.2).

pen: Includes a Private Enterprise Number [Private-Enterprise-Numbers]. This parameter is included when the reason code is not taken from the IANA-maintained registry (Section 5.2), but from a vendor-specific registry.

reason-description: It includes a brief description of the reset reason. This parameter SHOULD NOT be included if a reason code is supplied. This parameter is useful only for reset reasons that are not yet registered or for application-specific reasons.

At least one of "reason-code" and "reason-description" parameters MUST be included in an RST diagnostic payload. It is RECOMMENDED to omit "pen" if a reason code from the IANA-maintained registry (Section 5.2) fits the reset case.

Malformed RST diagnostic payload messages that include the magic number MUST be silently ignored by the receiver.

A peer that receives a valid diagnostic payload may pass the reset reason information to the local application in addition to the information (MUST-12) described in Section 3.6 of [I-D.ietf-tcpm-rfc793bis]. That information may also be logged locally, unless a local policy specifies otherwise. How the information is passed to an application and how it is stored locally is implementation specific.

4. Some Examples

To ease readability, the CBOR diagnostic notation (Section 8 of [RFC8949]) with the parameter names rather than their CBOR key values in Section 5.1 is used in Figures 3, 4, 5, and 6.

Figure 2 depicts an example of RST diagnostic payload that is generated to inform the peer that the TCP connection is reset because an ACK was received from that peer while the connection is still in the LISTEN state (Section 3.10.7.2 of [I-D.ietf-tcpm-rfc793bis]).

```
19 3039 # unsigned(12345)
A1      # map(1)
   01 # unsigned(1)
   02 # unsigned(2)
```

Figure 2: An RST Diagnostic Payload with Reason Code (CBOR Encoding)

Figure 3 depicts the same RST diagnostic payload as the one shown in Figure 2 but following the diagnostic notation.

```
[
  12345,
  {
    "reason-code": 2
  }
]
```

Figure 3: An RST Diagnostic Payload with Reason Code (Diagnostic Notation)

Figure 4 shows an example of RST diagnostic payload that includes a free description to report a case that is not covered yet by the IANA-maintained registry (Section 5.2).

```
[
  12345,
  {
    "reason-description": "brief human-readable description"
  }
]
```

Figure 4: An RST Diagnostic Payload with Reason Description (Diagnostic Notation)

An RST diagnostic payload may also be reset by an on-path service function. For example, the following diagnostic payload is returned by a NAT upon expiry of the mapping entry to which the TCP connection is bound (Figure 5).

```
[
  12345,
  {
    "reason-code": 8
  }
]
```

Figure 5: An RST Diagnostic Payload to Report Connection Timeout (Diagnostic Notation)

Figure 6 illustrates the RST diagnostic payload that is returned by a peer that resets a TCP connection for a reason code 1234 defined by a vendor with the private enterprise number 32473.

```
[
  12345,
  {
    "reason-code": 1234,
    "pen": 32473
  }
]
```

Figure 6: An RST Diagnostic Payload to Report Vendor-Specific Reason Code (Diagnostic Notation)

Figure 6 uses the Enterprise Number 32473 defined for documentation use [RFC5612].

5. IANA Considerations

5.1. RST Diagnostic Payload CBOR Key Values

IANA is requested to create a new subregistry titled "RST Diagnostic Payload CBOR Key Values" under the "Transmission Control Protocol (TCP) Parameters" registry [IANA-TCP].

The structure of this subregistry and the initial values are provided below:

Parameter Name	CBOR Key	CBOR Major Type & Information	Reference
reason-code	1	0 unsigned	[ThisDocument]
pen	2	0 unsigned	[ThisDocument]
reason-description	3	3 text string	[ThisDocument]

The key value MUST be an integer in the 1-255 range.

The assignment policy for this registry is "IETF Review" (Section 4.8 of [RFC8126]).

5.2. New Registry for TCP Failure Causes

This document requests IANA to create a new subregistry entitled "TCP Failure Causes" under the "Transmission Control Protocol (TCP) Parameters" registry [IANA-TCP].

Values are taken from the 1-65535 range.

The assignment policy for this registry is "Expert Review" (Section 4.5 of [RFC8126]).

The designated experts may approve registration once they checked that the new requested code is not covered by an existing code and if the provided reasoning to register the new code is acceptable. A registration request may supply a pointer to a specification where that code is defined. However, a registration may be accepted even if no permanent and readily available public specification is available.

The registry is initially populated with the following values:

Value	Description	Specification (if available)
1	Data lost. New data is received after CLOSE is called	Sections 3.6.1 and 3.10.7.1 of [I-D.ietf-tcpm-rfc793bis]
2	Still in LISTEN. Received ACK while the connection still in the LISTEN state	Section 3.10.7.2 of [I-D.ietf-tcpm-rfc793bis]
3	Malformed Message	[ThisDocument]
4	Not Authorized	[ThisDocument]
5	Resource Exceeded	[ThisDocument]
6	Network Failure. This code can be used by service functions such as translators.	[ThisDocument]
7	Connection Reset received from the peer. This code can be used by service functions such as translators.	[ThisDocument]
8	Destination Unreachable. This code can be used by service functions such as translators.	[ThisDocument]
9	Connection Timeout. This code can be used by service functions such as translators.	[ThisDocument]

Table 1: Initial TCP Failure Causes

6. Security Considerations

[I-D.ietf-tcpm-rfc793bis] discusses TCP-related security considerations. RST-specific attacks and their mitigations are discussed in Section 3.10.7.3 of [I-D.ietf-tcpm-rfc793bis].

In addition to these considerations, it is RECOMMENDED to control the size of acceptable diagnostic payload and keep it as brief as possible. Also, it is RECOMMENDED to avoid leaking privacy-related

information as part of the diagnostic payload (e.g., including a description such as "user X resets explicitly the connection" is not recommended).

7. Acknowledgements

The "diagnostic payload" name is inspired by Section 5.5.2 of [RFC7252] that was cited by Carsten Bormann in the tcpm mailing list.

Thanks to Jon Jon Shallow for the comments.

8. References

8.1. Normative References

[I-D.ietf-tcpm-rfc793bis] Eddy, W. M., "Transmission Control Protocol (TCP) Specification", Work in Progress, Internet-Draft, draft-ietf-tcpm-rfc793bis-28, 7 March 2022, <https://www.ietf.org/archive/id/draft-ietf-tcpm-rfc793bis-28.txt>.

[Private-Enterprise-Numbers] "Private Enterprise Numbers", 4 May 2020, <https://www.iana.org/assignments/enterprise-numbers>.

[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>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[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>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/info/rfc8610>.

[RFC8742] Bormann, C., "Concise Binary Object Representation (CBOR) Sequences", RFC 8742, DOI 10.17487/RFC8742, February 2020, <https://www.rfc-editor.org/info/rfc8742>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/info/rfc8949>.

8.2. Informative References

[IANA-TCP] IANA YANG, "Transmission Control Protocol (TCP) Parameters", <https://www.iana.org/assignments/tcp-parameters/tcp- parameters.xhtml>.

[RFC5612] Eronen, P. and D. Harrington, "Enterprise Number for Documentation Use", RFC 5612, DOI 10.17487/RFC5612, August 2009, <https://www.rfc-editor.org/info/rfc5612>.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, DOI 10.17487/RFC6146, April 2011, <https://www.rfc-editor.org/info/rfc6146>.

[RFC6888] Perreault, S., Ed., Yamagata, I., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common Requirements for Carrier-Grade NATs (CGNs)", BCP 127, RFC 6888, DOI 10.17487/RFC6888, April 2013, <https://www.rfc-editor.org/info/rfc6888>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/info/rfc7252>.

[RFC7857] Penno, R., Perreault, S., Boucadair, M., Ed., Sivakumar, S., and K. Naito, "Updates to Network Address Translation (NAT) Behavioral Requirements", BCP 127, RFC 7857, DOI 10.17487/RFC7857, April 2016, <https://www.rfc-editor.org/info/rfc7857>.

Author's Address

Mohamed Boucadair
Orange
35000 Rennes
France

Email: mohamed.boucadair@orange.com