CoAP: Non-traditional response forms
draft-bormann-core-responses-00

Abstract

In CoAP as defined by RFC 7252, responses are always unicast back to a client that posed a request. The present memo describes two forms of responses that go beyond that model. These descriptions are not intended as advocacy for adopting these approaches immediately, they are provided to point out potential avenues for development that would have to be carefully evaluated.

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 May 17, 2018.

Copyright Notice

Copyright (c) 2017 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 Simplified BSD License text as described in Section 4.e of
1. Introduction

In CoAP as defined by RFC 7252, responses are always unicast back to a client that posed a request. A server may want to send a response to a request that it did not receive, may want to multicast a response, or both.

The descriptions in this specification are not intended as advocacy for adopting these approaches immediately, they are provided to point out potential avenues for development that would have to be carefully evaluated.

1.1. 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.

The term "byte" is used in its now customary sense as a synonym for "octet".

Terms used in this draft:
Configured request: A request that reaches the server in another way than by transmitting a usual CoAP request on the same communication channel a response is expected on.

Embedded request: A request that is provided by the server to the recipient of its response by embedding it into the response.

2. Response with embedded request

A server can send a response to a request that it did not actually receive by embedding the request which the response answers in the response.

The option "Response-For" contains a request packaged as in Section 5.2 of [I-D.ietf-core-object-security]. The response is then intended to serve as a response to this request.

<table>
<thead>
<tr>
<th>No.</th>
<th>C</th>
<th>U</th>
<th>N</th>
<th>R</th>
<th>Name</th>
<th>Format</th>
<th>Length</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>C</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Response-For</td>
<td>opaque</td>
<td>0-1023</td>
<td>(none)</td>
</tr>
</tbody>
</table>

Table 1: The Response-For Option

The CoAP Token becomes meaningless for this form of response; responses with embedded requests are therefore sent with an zero-length Token. (In essence, the "Response-For" option takes the place of the request the Token usually stands for.)

The congestion control considerations for confirmable and non-confirmable messages apply unchanged.

3. Response for configured request

A request may reach the server using a different means than that used for the response. For instance, the request may be configured in the server. Without limiting generality, we speak about _configured requests_.

The client MUST be cognizant of that configuration as the request uses a token from the token name space it controls.

3.1. Examples for configured requests
3.2. Example: Periodic request

A server may be configured to act on a configured request every day at 12:00.

3.3. Example: Event driven request

A server may be configured to act on a configured request each time it reboots.

3.4. Example: Configured observe

A server may be configured with a GET request from a client that includes an Observe option with value 0. This means that the server will send updates to the state of the resource addressed by the GET request to the configured address of the client.

The considerations of Section 4.5 of [RFC7641] apply. How losing interest reflects back into to configuration and whether there is some form of error notification to the source of the configuration is out of scope of the present specification.

3.5. Multicast responses

A server MAY send a response to a multicast address. (This needs to be a response to a configured request as a normal request cannot be sent from a multicast address.)

Note that, as the originator of a multicast response is a unicast address, the relaxation of matching rules described in Section 8.2 of [RFC7252] does not apply.

The token space in CoAP is owned by the client, which is identified by a transport endpoint (address/port). Here, the address is a multicast address, so the token name space is shared by all nodes joined to that multicast address. The assumption for multicast responses is that, for each multicast group, there is some form of management for the token space (and the port number) that everyone can participate that needs to join that multicast group; the specific form of management is out of the scope of this specification. Note that this means that multicast responses MUST NOT be sent to unmanaged multicast addresses such as All Coap Nodes (Section 12.8 of [RFC7252]).

Multicast responses are always non-confirmable. The congestion control considerations for non-confirmable multicast messages apply unchanged.
3.6. Respond-To option

What has been called "configured request" here may also be triggered by a usual CoAP request that carries the Respond-To option. (The term "configured request" is still appropriate as the server ought to be configured to accept this option; see Section 5.)

If a single client wants to request a server to send the response to a specific multicast address, it can include the "Respond-To" option. This contains an opaque string with the port number as a 16-bit number (in network byte order), followed by the IP address (4-byte IPv4 or 16-byte IPv6).

<table>
<thead>
<tr>
<th>No.</th>
<th>C</th>
<th>U</th>
<th>N</th>
<th>R</th>
<th>Name</th>
<th>Format</th>
<th>Length</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>C</td>
<td>U</td>
<td>-</td>
<td>-</td>
<td>Respond-To</td>
<td>opaque</td>
<td>6-18</td>
<td>(none)</td>
</tr>
</tbody>
</table>

4. IANA Considerations

This draft adds the following option numbers to the CoAP Option Numbers registry of [RFC7252]:

<table>
<thead>
<tr>
<th>Number</th>
<th>Name</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>TBD</td>
<td>Response-For</td>
<td>RFCthis</td>
</tr>
<tr>
<td>TBD</td>
<td>Respond-To</td>
<td>RFCthis</td>
</tr>
</tbody>
</table>

Table 2: CoAP Option Numbers

5. Security Considerations

TBD

(Clearly, multicast responses pose a potential for amplification, in particular if unverified sources can cause them via Respond-To. Discuss how to mitigate.)

A Respond-To option can be used to incite a server to send data to a third party. This ought not be done blindly, i.e., only with considered application assent.

The CoAP request/response mechanism allows the client to ascertain a level of authentication (not resistant though to on-path attackers unless the communication is protected) and freshness of the response:
The Token echoed in the response shows that the responder had knowledge of the (fresh) request (Section 5.3.1 of [RFC7252]). Responses with embedded requests can not be authenticated or checked for freshness this way. Their content therefore is less trustworthy than normal responses unless authenticated in another way (e.g., via [I-D.ietf-core-object-security]).

6. References

6.1. Normative References


6.2. Informative References


Acknowledgements

TBD

Author’s Address