CoRE Working Group                                             K. Hartke
Internet-Draft                                   Universitaet Bremen TZI
Intended status: Standards Track                          Z. Shelby, Ed.
Expires: May 3, 2012                                           Sensinode
October 31, 2011

Observing Resources in CoAP
draft-ietf-core-observe-03

Abstract

CoAP is a RESTful application protocol for constrained nodes and networks. The state of a resource on a CoAP server can change over time. This document specifies a simple protocol extension for CoAP that gives clients the ability to observe such changes.

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 http://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 3, 2012.

Copyright Notice

Copyright (c) 2011 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 (http://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 the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
Table of Contents

1.  Introduction ................................................. 3
   1.1.  Background ........................................ 3
   1.2.  Protocol Overview .................................. 3
   1.3.  Design Philosophy ................................... 5
   1.4.  Conformance Requirements .............................. 6
2.  Options ...................................................... 6
   2.1.  Observe .............................................. 6
   2.2.  Max-OFE ............................................... 7
3.  Client-side Requirements ..................................... 7
   3.1.  Request ............................................... 7
   3.2.  Notifications ........................................ 8
   3.3.  Caching ............................................... 8
   3.4.  Reordering ........................................... 9
4.  Server-side Requirements ...................................... 10
   4.1.  Request ............................................... 10
   4.2.  Notifications ........................................ 11
   4.3.  Caching ............................................... 11
   4.4.  Reordering ........................................... 12
   4.5.  Retransmission ....................................... 13
5.  Intermediaries ................................................ 13
6.  Block-wise Transfers .......................................... 14
7.  Discovery ..................................................... 15
8.  Security Considerations ...................................... 15
9.  IANA Considerations .......................................... 15
10. Acknowledgements ............................................. 16
11. References ................................................... 16
    11.1. Normative References ................................ 16
    11.2. Informative References ............................... 16
Appendix A.  Examples ............................................. 18
    A.1. Proxying ............................................... 22
    A.2. Block-wise Transfer ................................... 24
Appendix B.  Modeling Resources to Tailor Notifications ......... 25
Appendix C.  Changelog ........................................... 25
Authors’ Addresses .............................................. 27
1. Introduction

1.1. Background

CoAP [I-D.ietf-core-coap] is an Application Protocol for Constrained Nodes/Networks. It is intended to provide RESTful services [REST] not unlike HTTP [RFC2616] while reducing the complexity of implementation as well as the size of packets exchanged in order to make these services useful in a highly constrained network of themselves highly constrained nodes.

The communication model of REST is that of a client exchanging resource representations with an origin server. The origin server is the definitive source for representations of the resources in its namespace. A client interested in a resource sends a request to the origin server that returns a response with a representation that is current at the time of the request.

This model does not work well when a client is interested in having a current representation of a resource over a period of time. Existing approaches from the HTTP world, such as repeated polling or long-polls [RFC6202], generate significant complexity and/or overhead and thus are less applicable in the constrained CoAP world.

The protocol specified in this document extends the CoAP core protocol with a mechanism to push resource representations from servers to interested clients, while still keeping the properties of REST.

Note that there is no intention for this mechanism to solve the full set of problems that the existing HTTP solutions solve, to replace publish/subscribe networks that solve a much more general problem [RFC5989], or to enable general two-way communication between clients and servers [I-D.ietf-hybi-thewebsocketprotocol].

1.2. Protocol Overview

The protocol is based on the well-known observer design pattern [GOF].

In this design pattern, components, called _observers_, register at a specific, known provider, called the _subject_, that they are interested in being notified whenever the subject undergoes a change in state. The subject is responsible for administering its list of registered observers. If multiple subjects are of interest, an observer must register separately for all of them. The pattern is typically used when a clean separation between related components is required, such as data storage and user interface.
The observer design pattern is realized in CoAP as follows:

Subject: In the context of CoAP, the subject is a resource in the namespace of a CoAP server. The state of the resource can change over time, ranging from infrequent updates to continuous state transformations.

Observer: An observer is a CoAP client that is interested in the current state of the resource at any given time.

Registration: A client registers its interest by sending an extended GET request to the server. In addition to returning a representation of the target resource, this request causes the server to add the client to the list of observers of the resource.

Notification: Whenever the state of a resource changes, the server notifies each client registered as observer for the resource. Each notification is an additional CoAP response sent by the server in reply to the GET request and includes a complete representation of the new resource state.

Figure 2 shows an example of a CoAP client registering and receiving three notifications: the first upon registration and then two when the state of the resource changes. Registration request and notifications are identified by the presence of the Observe Option defined in this document. Notifications also echo the token specified by the client in the request, so the client can easily correlate them to the request.
The client is removed from the list of observers when it is no longer interested in the observed resource. The server can determine the client’s continued interest from the client’s acknowledgement of confirmable notifications. If a client wants to receive notifications after it has been removed from the list of observers, it needs to register again. The client can determine that it’s still on the list of observers from the fact that it receives notifications. The protocol includes clear rules for what to do when a client does not receive a notification for some time, or a server does not receive acknowledgements.

### 1.3. Design Philosophy

The protocol builds on the architectural elements of REST: a server that is responsible for the state and representation of the resources in its namespace, a client that is responsible for keeping the application state, and the stateless exchange of resource representations. (A server needs to keep track of the observers though, similar to how HTTP servers need to keep track of the TCP connections from their clients.) The protocol enables high
scalability and efficiency through the support of caches and intermediaries that multiplex the interest of multiple clients in the same resource into a single association.

The server is the authority for determining under what conditions resources change their state and how often observers are notified. The protocol does not offer explicit means for setting up triggers, thresholds or other conditions; it is up to the server to expose observable resources that change their state in a way that is meaningful for the application. Resources can be parameterized to achieve similar effects though; see Appendix B for examples.

Since bandwidth is in short supply in constrained environments, servers must adapt the rate of notifications to each client. This implies that a client cannot rely on observing every single state a resource goes through. Instead, the protocol is designed on the principle of _eventual consistency_: it guarantees that if the resource does not undergo a new change in state, eventually all observers will have a current representation of the last resource state.

1.4. Conformance Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Options

<table>
<thead>
<tr>
<th>No.</th>
<th>C/E</th>
<th>Name</th>
<th>Format</th>
<th>Length</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Elective</td>
<td>Observe</td>
<td>uint</td>
<td>0-2 B</td>
<td>(none)</td>
</tr>
<tr>
<td>14</td>
<td>Elective</td>
<td>Max-OFE</td>
<td>uint</td>
<td>0-4 B</td>
<td>0</td>
</tr>
</tbody>
</table>

2.1. Observe

The Observe Option, when present, modifies the GET method so it does not only retrieve a representation of the current state of the resource identified by the request URI, but also requests the server to add the client to the list of observers of the resource. The exact semantics are defined in the sections below. The value of the option in a request MUST be zero on transmission and MUST be ignored on reception.

In a response, the Observe Option identifies the message as a
notification, which implies that the client has been added to the list of observers and that the server will notify the client of further changes to the resource state. The option’s value is a sequence number that can be used for reordering detection (see Section 3.4 and Section 4.4). It is encoded as a variable-length unsigned integer as defined in Appendix A of RFC XXXX [I-D.ietf-core-coap].

Since the Observe Option is elective, a GET request that includes the Observe Option will automatically fall back to a normal GET request if the server does not support the protocol specified in this document.

The Observe Option MUST NOT occur more than once in a request or response.

2.2. Max-OFE

The freshness of a notification for caching purposes is determined by the Max-Age Option. However, a server may want to enable a cache to continue to optimistically use a cached representation even when the freshness indicated by the Max-Age Option has expired (see Section 3.3 and Section 4.3).

The time span for which this optimism is justified is under control of the server: it can use the Max-OFE Option to indicate a desired "optimistic freshness extension". This is also a promise by the server that it intends to send another notification within this time period. The exact semantics are defined in the sections below. The value of this option is a time span in seconds, measured from the time of expiry of Max-Age. The option is elective and defaults to zero (which means that no optimistic freshness extension is granted).

The Max-OFE Option MUST NOT occur more than once in a response.

3. Client-side Requirements

3.1. Request

A client can register its interest in a resource by issuing a GET request that includes an empty Observe Option. If the server returns a 2.xx response that includes an Observe Option as well, the server has added the client successfully to the list of observers of the target resource and the client will be notified of changes to the resource state for as long as the server can assume the client’s interest.
3.2. Notifications

Notifications are additional responses sent by the server in reply to the GET request. Each notification includes an Observe Option with a sequence number (see Section 3.4), a Token Option that matches the token specified by the client in the GET request, and a payload in the same representation format as the initial response.

A notification can be confirmable or non-confirmable (i.e. sent in a confirmable or non-confirmable message). If a client does not recognize the token in a confirmable notification, it MUST NOT acknowledge the message and SHOULD reject it with a RST message. Otherwise, the client MUST acknowledge the message with an ACK message as usual.

An acknowledgement signals to the server that the client is alive and interested in receiving further notifications; if the server does not receive an acknowledgement in reply to a confirmable notification, it will assume that the client is no longer interested and will eventually remove it from the list of observers.

Notifications will have a 2.05 (Content) response code in most cases. They may also have a 2.03 (Valid) response code, if the client includes an ETag Option in its request (see Section 3.3). In the event that the state of an observed resource is changed in a way that would cause a normal GET request to return an error (for example, when the resource is deleted), the server will send a notification with an error response code (4.xx/5.xx) and empty the list of observers of the resource.

3.3. Caching

As notifications are just additional responses, notifications partake in caching as defined by Section 5.6 of RFC XXXX [I-D.ietf-core-coap]. Both the freshness model and the validation model are supported. The freshness model also serves as the model for the client to determine if it’s still on the list of observers or if it needs to re-register its interest in the resource.

A client MAY store a notification like a response in its cache and use a stored response/notification that is fresh without contacting the origin server. A notification is considered fresh while its age is not greater than its Max-Age and if it has not been invalidated by a newer notification or as the result of a request.

Ideally, the server will provide a new notification exactly when the freshness of the latest notification expires. This may not always be possible though, due to network latency and/or resources that change
their state in unpredictable intervals. In this case, the client MAY optimistically use a stale (non-fresh) notification while the notification’s age is not greater than Max-Age plus Max-OFE and the notification has not been invalidated.

If the client does not receive a notification before Max-Age plus Max-OFE expires, the client can assume it has been removed from the list of observers (e.g., due to a loss of server state). In this case, it needs to re-register by issuing a new GET request with an Observe Option.

To make sure it has a fresh representation and/or it is on the list of observers, a client MAY issue another GET request with an Observe Option at any time. The new GET request SHOULD specify a new token to avoid ambiguity. It is RECOMMENDED that the client does not issue the request before the Max-Age of the latest notification expires (i.e. while it still has a fresh notification).

When a client has one or more notifications stored, it can use the ETag Option in its request to give the server an opportunity to select a stored response to be used. The client MAY include an ETag Option for each stored response that is applicable. It needs to keep those responses in the cache until it is no longer interested in receiving notifications for the target resource or it issues a new GET request with a new set of entity-tags. When the observed resource changes its state to a representation identified by one of the ETag Options, the server can send a 2.03 (Valid) notification instead of a 2.05 (Content) notification.

3.4. Reordering

Messages that carry notifications can arrive in a different order than they were sent. Since the goal is eventual consistency (see Section 1.3), a client can safely skip a notification that arrives later than a newer notification. For this purpose, the server sets the value of the Observe Option in each notification to a sequence number.

A client MAY treat a notification as outdated (not fresh) under the following condition:

\[(V_1 - V_2) \% (2^{16}) < (2^{15}) \quad \text{and} \quad T_2 < (T_1 + (2^{14}))\]

where \(V_1\) is the value of the Observe Option of the latest valid notification received, \(V_2\) the value of the Observe Option of the present notification, \(T_1\) a client-local timestamp of the latest valid notification received (in seconds), and \(T_2\) a client-local timestamp of the present notification.
Design Note: The first condition essentially verifies that $V_2 > V_1$ holds in 16-bit sequence number arithmetic [RFC1982]. The second condition checks that the time expired between the two incoming messages is not so large that the sequence number might have wrapped around and the first check is therefore invalid. (In other words, after about $2^{14}$ seconds elapse without any notification, the client does not need to check the sequence numbers in order to assume an incoming notification is new.) The constants of $2^{14}$ and $2^{15}$ are non-critical, as is the even speed or precision of the clock involved.

4. Server-side Requirements

4.1. Request

A GET request that includes an Observe Option requests the server not only to return a representation of the resource identified by the request URI, but also to add the client to the list of observers of the target resource. If no error occurs, the server MUST return a response with the representation of the current resource state and MUST notify the client of subsequent changes to the state as long as the client is on the list of observers.

A server that is unable or unwilling to add the client to the list of observers of the target resource MAY silently ignore the Observe Option and process the GET request as usual. The resulting response MUST NOT include an Observe Option, the absence of which signals to the client that it will not be notified of changes to the resource state and, e.g., needs to poll the resource instead.

If the client is already on the list of observers, the server MUST NOT add it a second time but MUST replace or update the existing entry. If the server receives a GET request that does not include an Observe Option, it MUST remove the client from the list of observers.

Two requests relate to the same list entry if both the request URI and the source of the requests match. The source of a request is determined by the security mode used (see Section 10 of RFC XXXX [I-D.ietf-core-coap]): With NoSec, it is determined by the source IP address and UDP port number. With other security modes, the source is also determined by the security context. Message IDs and Token Options MUST NOT be taken into account.

Any request with a method other than GET MUST NOT have a direct effect on a list of observers of a resource. However, such a request can have the indirect consequence of causing the server to send an error notification which affects the list of observers (e.g., when a
DELETE request is successful and an observed resource no longer exists).

4.2. Notifications

A client is notified of a resource state change by an additional response sent by the server in reply to the GET request. Each such notification response MUST include an Observe Option and MUST echo the token specified by the client in the GET request. If there are multiple clients, the order in which they are notified is not defined; the server is free to use any method to determine the order.

A notification SHOULD have a 2.05 (Content) or 2.03 (Valid) response code. However, in the event that the state of a resource changes in a way that would cause a normal GET request to return an error (for example, if the resource is deleted), the server SHOULD notify the client by sending a notification with an appropriate error response code (4.xx/5.xx) and MUST empty the list of observers of the resource.

The representation format/media type used in a notification MUST be the same format used in the initial response to the GET request. If the server is unable to continue sending notifications in this format, it SHOULD send a 5.00 (Internal Server Error) notification and MUST empty the list of observers of the resource.

A notification can be sent as a confirmable or a non-confirmable message. The message type used is typically application-dependent and MAY be determined by the server for each notification individually. For example, for resources that change in a somewhat predictable or regular fashion, notifications can be sent in non-confirmable messages; for resources that change infrequently, notifications can be sent in confirmable messages. The server can combine these two approaches depending on the frequency of state changes and the importance of individual notifications.

The acknowledgement of a confirmable notification implies the client’s continued interest in being notified. If the client rejects a confirmable notification with a RST message, the server MUST remove the client from the list of observers.

4.3. Caching

The Max-Age Option of a notification SHOULD be set to a value that indicates when the server will send the next notification. For example, if the server sends a notification every 30 seconds, a Max-Age Option with value 30 should be included. The server MAY send a new notification before Max-Age ends. The server SHOULD also include
a Max-OFE Option so the client can continue to use a notification in case the next notification arrives a bit later due to network latency. If the client does not receive a new notification before Max-Age plus Max-OFE ends, it will assume that it was removed from the list of observers (e.g., due to a loss of server state) and may issue a new GET request to re-register its interest.

It may not always be possible to predict when the server will send the next notification, for example, when a resource does not change its state in regular intervals. In this case, the server SHOULD set Max-Age to a good approximation and Max-OFE to a time span for which the server is willing to keep the client in the list of observers.

Setting the values for Max-Age and Max-OFE is a trade-off between increased usage of bandwidth and the risk of stale information. Smaller values lead to more notifications and more GET requests, while greater values result in network or device failures being detect later and data becoming stale.

When the observed resource changes its state and the origin server is about to send a 2.05 (Content) notification, then, whenever that notification has an entity-tag in the set of entity-tags specified by the client, it MAY send a 2.03 (Valid) response with an appropriate ETag Option instead. The server MUST NOT assume that the recipient has any response stored other than those identified by the entity-tags in the most recent GET request.

4.4. Reordering

Because messages can get reordered, the client needs a way to determine if a notification arrived later than a newer notification. For this purpose, the server MUST set the value of the Observe Option in each notification to the 16 least-significant bits of a strictly increasing sequence number. The sequence number MAY start at any value. The server MUST NOT reuse the same option value with the same client, token and resource within approximately 2**16 seconds (roughly 18.2 hours).

Implementation Note: A simple implementation that satisfies the requirements is to use a timestamp (in seconds) provided by the device’s clock, or a 16-bit unsigned integer variable that is incremented every second and wraps around every 2**16 seconds. It is not necessary that the clock reflects the correct local time or that it ticks exactly every second. Note that, on average, a server cannot send more than one notification per second per client, token and resource.
4.5. Retransmission

In CoAP, confirmable messages are retransmitted in exponentially increasing intervals for a certain number of attempts until they are acknowledged by the client. In the context of observing a resource, it is undesirable to continue transmitting the representation of a resource state when the state has changed in the meantime.

When a server is in the process of delivering a confirmable notification and is waiting for an acknowledgement, and it wants to notify the client of a state change using a new confirmable message, it MUST stop retransmitting the old notification and SHOULD attempt to deliver the new notification with the number of attempts remaining from the old notification. When the last attempt to retransmit a confirmable message with a notification for a resource times out, the server SHOULD remove the client from the list of observers and MAY additionally remove the client from the lists of observers of all resources in its namespace.

The server SHOULD use a number of retransmit attempts (MAX_RETRANSMIT) such that removing a client from the list of observers before Max-Age plus Max-OFE ends is avoided.

A server MAY choose to skip a notification if it knows that it will send another notification soon (e.g., when the state is changing frequently). Similarly, it MAY choose to send a notification more than once. For example, when state changes occur in bursts, the server can skip some notifications, send notifications in non-confirmable messages, and make sure that the client observes the latest state change after the burst by repeating the last notification in a confirmable message.

5. Intermediaries

A client may be interested in a resource in the namespace of an origin server that is reached through one or more CoAP-to-CoAP intermediaries. In this case, the client registers its interest with the first intermediary towards the origin server, acting as if it was communicating with the origin server itself as specified in Section 3. It is the task of this intermediary to provide the client with a current representation of the target resource and send notifications upon changes to the target resource state, much like an origin server as specified in Section 4.

To perform this task, the intermediary SHOULD make use of the protocol specified in this document, taking the role of the client and registering its own interest in the target resource with the next
hop. If the next hop does not return a response with an Observe Option, the intermediary MAY resort to polling the next hop, or MAY itself return a response without an Observe Option. Note that the communication between each pair of hops is independent, i.e. each hop in the server role MUST determine individually how many notifications to send, of which type, and so on, MUST generate its own values for the Observe Option, and MUST set the values of the Max-Age Option and Max-OFE Option according to the age of the local current representation.

Because a client (or an intermediary in the client role) can only be once in the list of observers of a resource at a server (or an intermediary in the server role) -- as it makes no sense to observe the same resource multiple times -- an intermediary MUST observe a resource only once, even if there are multiple clients for which it observes the resource.

Note that an intermediary is not required to have a client to observe a resource; an intermediary MAY observe a resource, for instance, just to keep its own cache up to date.

See Appendix A.1 for examples.

6. Block-wise Transfers

Resources observed by clients may be larger than can be comfortably processed or transferred in one CoAP message. CoAP provides a block-wise transfer mechanism to address this problem [I-D.ietf-core-block]. The following rules apply to the combination of block-wise transfers with notifications.

As with basic GET transfers, the client can indicate its desired block size in a Block2 Option in the GET request. If the server supports block-wise transfers, it SHOULD take note of the block size for all notifications/responses resulting from the GET request (until the client is removed from the list of observers or the server receives a new GET request from the client).

When sending a 2.05 (Content) notification, the server always sends all blocks of the representation, suitably sequenced by its congestion control mechanism, even if only some of the blocks have changed with respect to a previous value. The server performs the block-wise transfer by making use of the Block2 Option in each block. When reassembling representations that are transmitted in multiple blocks, the client MUST NOT combine blocks carrying different Observe Option values, or blocks that have been received more than approximately 2**14 seconds apart.
See Appendix A.2 for an example.

7. Discovery

A web link [RFC5988] to a resource accessible by the CoAP protocol MAY indicate that the server encourages the observation of this resource by including the target attribute "obs". This is particularly useful in link-format documents [I-D.ietf-core-link-format].

This target attribute is used as a flag, and thus it has no value component -- a value given for the attribute MUST NOT be given for this version of the specification and MUST be ignored if present. The target attribute "obs" MUST NOT be given more than once for this version of the specification.

8. Security Considerations

The security considerations of RFC XXXX [I-D.ietf-core-coap] apply.

Note that the considerations about amplification attacks are somewhat amplified when observing resources. In NoSec mode, a server MUST therefore strictly limit the number of notifications that it sends between receiving acknowledgements that confirm the actual interest of the client in the data; i.e., any notifications sent in non-confirmable messages MUST be interspersed with confirmable messages. (An attacker may still spoof the acknowledgements if the confirmable messages are sufficiently predictable.)

As with any protocol that creates state, attackers may attempt to exhaust the resources that the server has available for maintaining the list of observers for each resource. Servers MAY want to access-control this creation of state. As degraded behavior, the server can always fall back to processing the request as a normal GET request (without an Observe Option) if it is unwilling or unable to add a client to the list of observers of a resource, including if system resources are exhausted or nearing exhaustion.

Intermediaries MUST be careful to ensure that notifications cannot be employed to create a loop. A simple way to break any loops is to employ caches for forwarding notifications in intermediaries.

9. IANA Considerations

The following entries are added to the CoAP Option Numbers registry:
10. Acknowledgements

Carsten Bormann was an original author of this draft and is acknowledged for significant contribution to this document.

Thanks to Daniele Alessandrelli, Jari Arkko, Peter Bigot, Angelo Castellani, Gilbert Clark, Esko Dijk, Brian Frank, Salvatore Loreto and Charles Palmer for helpful comments and discussions that have shaped the document.

Klaus Hartke was funded by the Klaus Tschira Foundation.

11. References

11.1. Normative References

[I-D.ietf-core-block]

[I-D.ietf-core-coap]


11.2. Informative References


[I-D.ietf-core-link-format]
Shelby, Z., "CoRE Link Format",
draft-ietf-core-link-format-07 (work in progress),
July 2011.

[I-D.ietf-hybi-thewebsocketprotocol]
Fette, I. and A. Melnikov, "The WebSocket protocol",
draft-ietf-hybi-thewebsocketprotocol-17 (work in
progress), September 2011.

[REST] Fielding, R., "Architectural Styles and the Design of

August 1996.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H.,
Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext

to an HTTP Resource", RFC 5989, October 2010.

[RFC6202] Loreto, S., Saint-Andre, P., Salsano, S., and G. Wilkins,
"Known Issues and Best Practices for the Use of Long
Polling and Streaming in Bidirectional HTTP", RFC 6202,
April 2011.
### Appendix A. Examples

<table>
<thead>
<tr>
<th>Observed t</th>
<th>State</th>
<th>CLIENT</th>
<th>SERVER</th>
<th>Actual State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>unknown</td>
<td></td>
<td></td>
<td>18.5 C</td>
</tr>
<tr>
<td>3</td>
<td>-------&gt;</td>
<td></td>
<td></td>
<td>Header: GET 0x43011633</td>
</tr>
<tr>
<td>4</td>
<td>GET</td>
<td></td>
<td></td>
<td>Token: 0x4a</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td>Uri-Path: temperature</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td>Observe: 0</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>------&lt;</td>
<td></td>
<td></td>
<td>Header: 2.05 0x64451633</td>
</tr>
<tr>
<td>10</td>
<td>2.05</td>
<td></td>
<td></td>
<td>Token: 0x4a</td>
</tr>
<tr>
<td>11</td>
<td>18.5 C</td>
<td></td>
<td></td>
<td>Observe: 9</td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td>Max-Age: 15</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td>Max-OFE: 60</td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td></td>
<td>Payload: &quot;18.5 C&quot;</td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>------&lt;</td>
<td></td>
<td></td>
<td>Header: 2.05 0x54457b50</td>
</tr>
<tr>
<td>17</td>
<td>2.05</td>
<td></td>
<td></td>
<td>Token: 0x4a</td>
</tr>
<tr>
<td>18</td>
<td>19.2 C</td>
<td></td>
<td></td>
<td>Observe: 17</td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td>Max-Age: 15</td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td>Max-OFE: 60</td>
</tr>
<tr>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td>Payload: &quot;19.2 C&quot;</td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3:** A client registers and receives a notification of the current state and upon a state change.
<table>
<thead>
<tr>
<th>t</th>
<th>Observed State</th>
<th>CLIENT</th>
<th>SERVER</th>
<th>Actual State</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>____________</td>
<td>^</td>
<td>^</td>
<td>____________</td>
</tr>
<tr>
<td>25</td>
<td>19.2 C</td>
<td>19.2 C</td>
<td></td>
<td>____________</td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>X----+</td>
<td></td>
<td></td>
<td>Header: 2.05 0x54457b51</td>
</tr>
<tr>
<td>30</td>
<td>2.05</td>
<td>19.7 C</td>
<td></td>
<td>Token: 0x4a</td>
</tr>
<tr>
<td>31</td>
<td></td>
<td>Observe: 29</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td></td>
<td>Max-Age: 15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td></td>
<td>Max-OFE: 60</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>19.2 C</td>
<td></td>
<td></td>
<td>Payload: &quot;19.7 C&quot;</td>
</tr>
<tr>
<td>35</td>
<td>(optimistic)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>____________</td>
<td>&lt;------</td>
<td></td>
<td>Header: 2.05 0x55457b52</td>
</tr>
<tr>
<td>38</td>
<td>2.05</td>
<td>18.9 C</td>
<td></td>
<td>Token: 0x4a</td>
</tr>
<tr>
<td>39</td>
<td></td>
<td>Observe: 37</td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td></td>
<td>ETag: 0x78797a7a79</td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td></td>
<td>Max-Age: 15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42</td>
<td></td>
<td>Max-OFE: 60</td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td></td>
<td>Payload: &quot;18.9 C&quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>44</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4: The client optimistically assumes that the state did not change after Max-Age ended
<table>
<thead>
<tr>
<th>t</th>
<th>Observed State</th>
<th>CLIENT State</th>
<th>SERVER State</th>
<th>Actual State</th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>18.9 C</td>
<td></td>
<td>18.9 C</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>48</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>49</td>
<td></td>
<td></td>
<td>CRASH</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>51</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>53</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>18.9 C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>(optimistic)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>56</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5: The server crashes and leaves the client with stale information
<table>
<thead>
<tr>
<th>Observed t</th>
<th>CLIENT</th>
<th>SERVER</th>
<th>Actual State</th>
</tr>
</thead>
<tbody>
<tr>
<td>117</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>118</td>
<td>18.9 C</td>
<td></td>
<td>18.0 C</td>
</tr>
<tr>
<td>119</td>
<td>(invalid)</td>
<td>+-------+</td>
<td>Header: GET 0x44011634</td>
</tr>
<tr>
<td>120</td>
<td>GET</td>
<td></td>
<td>Token: 0xf9</td>
</tr>
<tr>
<td>121</td>
<td>Uri-Path: temperature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>122</td>
<td>Observe: 0</td>
<td></td>
<td>ETag: 0x78797a7a7a</td>
</tr>
<tr>
<td>123</td>
<td>Max-Age: 15</td>
<td></td>
<td>Max-OFE: 60</td>
</tr>
<tr>
<td>124</td>
<td>Max-OFE: 60</td>
<td></td>
<td>Payload: &quot;18.0 C&quot;</td>
</tr>
<tr>
<td>125</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>126</td>
<td></td>
<td>&lt;-------+</td>
<td>Header: 2.05 0x64451634</td>
</tr>
<tr>
<td>127</td>
<td>2.05</td>
<td></td>
<td>Token: 0xf9</td>
</tr>
<tr>
<td>128</td>
<td>18.0 C</td>
<td></td>
<td>Observe: 126</td>
</tr>
<tr>
<td>129</td>
<td>Max-Age: 15</td>
<td></td>
<td>Max-OFE: 60</td>
</tr>
<tr>
<td>130</td>
<td>Max-OFE: 60</td>
<td></td>
<td>Payload: &quot;18.0 C&quot;</td>
</tr>
<tr>
<td>131</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>132</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>133</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>134</td>
<td></td>
<td>&lt;-------+</td>
<td>Header: 2.03 0x5543aa0c</td>
</tr>
<tr>
<td>135</td>
<td>2.03</td>
<td>18.9 C</td>
<td>Token: 0xf9</td>
</tr>
<tr>
<td>136</td>
<td>18.9 C</td>
<td></td>
<td>Observe: 134</td>
</tr>
<tr>
<td>137</td>
<td>ETag: 0x78797a7a79</td>
<td></td>
<td></td>
</tr>
<tr>
<td>138</td>
<td>Max-Age: 15</td>
<td></td>
<td>Max-OFE: 60</td>
</tr>
<tr>
<td>139</td>
<td>Max-OFE: 60</td>
<td></td>
<td></td>
</tr>
<tr>
<td>140</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 6: The client re-registers and gives the server the opportunity to select a stored response.
A.1. Proxying

Figure 7: A proxy observes a resource to keep its cache up to date
Figure 8: A client observes a resource through a proxy
A.2. Block-wise Transfer

CLIENT          SERVER

+----->  Header: GET 0x43011636
        Token: 0xfb
        Uri-Path: status-icon
        Observe: 0

<-------  Header: 2.05 0x65451636
2.05      Token: 0xfb
        Block2: 0/1/128
        Observe: 62354
        Max-Age: 60
        Max-OFE: 60
        Payload: [128 bytes]

<-------  Header: 2.05 0x5545af9c
2.05      Token: 0xfb
        Block2: 1/0/128
        Observe: 62354
        Max-Age: 60
        Max-OFE: 60
        Payload: [27 bytes]

<-------  Header: 2.05 0x5545af9d
2.05      Token: 0xfb
        Block2: 0/1/128
        Observe: 62444
        Max-Age: 60
        Max-OFE: 60
        Payload: [128 bytes]

<-------  Header: 2.05 0x5545af9e
2.05      Token: 0xfb
        Block2: 1/0/128
        Observe: 62444
        Max-Age: 60
        Max-OFE: 60
        Payload: [27 bytes]

Figure 9: A server sends two notifications of two blocks each
Appendix B. Modeling Resources to Tailor Notifications

A server may want to provide notifications that respond to very specific conditions on some state. This is best done by modeling the resources that the server exposes according to these needs.

For example, for a CoAP server with an attached temperature sensor,

- the server could, in the simplest form, expose a resource \(<\text{http://server/temperature}\>\) that changes its state every second to the current temperature measured by the sensor;

- the server could, however, also expose a resource \(<\text{http://server/temperature/felt}\>\) that changes its state to "cold" when the temperature drops below a preconfigured threshold, and to "warm" when the temperature exceeds a second, higher threshold;

- the server could expose a parameterized resource \(<\text{http://server/temperature/critical?above=45}\>\) that changes its state to the current temperature if the temperature exceeds the specified value, and changes its state to "OK" when the temperature drops below; or

- the server could expose a parameterized resource \(<\text{http://server/temperature?query=select+avg(temperature)+from+Sensor.window:time(30sec)}\>\) that accepts expressions of arbitrary complexity and changes its state accordingly.

In any case, the client is notified about the current state of the resource whenever the state of the appropriately modeled resource changes. By designing resources that change their state on certain conditions, it is possible to notify the client only when these conditions occur instead of continuously supplying it with information it doesn’t need. With parametrized resources, this is not limited to conditions defined by the server, but can be extended to arbitrarily complex conditions defined by the client. Thus, the server designer can choose exactly the right level of complexity for the application envisioned and devices used, and is not constrained to a "one size fits all" mechanism built into the protocol.

Appendix C. Changelog

Changes from ietf-02 to ietf-03:

- Separated client-side and server-side requirements.
o Fixed uncertainty if client is still in the list of observers by introducing a liveliness model based on Max-Age and a new option called Max-OFE (#174).

o Simplified the text on message reordering (#129).

o Clarified requirements for intermediaries.

o Clarified the combination of block-wise transfers with notifications (#172).

o Updated examples to show how the state observed by the client becomes eventually consistent with the actual state on the server.

o Added examples for parameterization of observable resource.

Changes from ietf-01 to ietf-02:

o Removed the requirement of periodic refreshing (#126).

o The new "Observe" Option replaces the "Lifetime" Option.

o Introduced a new mechanism to detect message reordering.

o Changed 2.00 (OK) notifications to 2.05 (Content) notifications.

Changes from ietf-00 to ietf-01:

o Changed terminology from "subscriptions" to "observation relationships" (#33).

o Changed the name of the option to "Lifetime".

o Clarified establishment of observation relationships.

o Clarified that an observation is only identified by the URI of the observed resource and the identity of the client (#66).

o Clarified rules for establishing observation relationships (#68).

o Clarified conditions under which an observation relationship is terminated.

o Added explanation on how clients can terminate an observation relationship before the lifetime ends (#34).

o Clarified that the overriding objective for notifications is eventual consistency of the actual and the observed state (#67).
o Specified how a server needs to deal with clients not
   acknowledging confirmable messages carrying notifications (#69).

o Added a mechanism to detect message reordering (#35).

o Added an explanation of how notifications can be cached,
   supporting both the freshness and the validation model (#39, #64).

o Clarified that non-GET requests do not affect observation
   relationships, and that GET requests without "Lifetime" Option
   affecting relationships is by design (#65).

o Described interaction with block-wise transfers (#36).

o Added Resource Discovery section (#99).

o Added IANA Considerations.

o Added Security Considerations (#40).

o Added examples (#38).

Authors’ Addresses

Klaus Hartke
Universitaet Bremen Tzi
Postfach 330440
Bremen  D-28359
Germany

Phone:  +49-421-218-63905
Fax:    +49-421-218-7000
Email:  hartke@tzi.org

Zach Shelby (editor)
Sensinode
Kidekuja 2
Vuokatti  88600
Finland

Phone:  +358407796297
Email:  zach@sensinode.com