CoRE Working Group   A. Rahman, Ed.
Internet-Draft   InterDigital Communications, LLC
Intended status: Informational   E. Dijk, Ed.
Expires: August 9, 2013   Philips Research
                                                            February 5, 2013

Group Communication for CoAP
draft-ietf-core-groupcomm-05

Abstract

CoAP is a RESTful transfer protocol for constrained devices and networks. It is anticipated that constrained devices will often naturally operate in groups (e.g. in a building automation scenario all lights in a given room may need to be switched on/off as a group). This document defines how the CoAP protocol should be used in a group communication context. An approach for using CoAP on top of IP multicast is detailed for both constrained and un-constrained networks. Also, various use cases and corresponding protocol flows are provided to illustrate important concepts. Finally, guidance is provided for deployment in various network topologies.

Status of this Memo

This Internet-Draft will expire on August 9, 2013.

Copyright Notice

Table of Contents

1. Conventions and 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 [RFC2119].

These key words are used to establish a set of best practices for CoAP group communication. An implementation of CoAP group communication MAY implement these guidelines; an implementation claiming compliance to this document MUST implement the set.

This document assumes readers are familiar with the terms and concepts that are used in [I-D.ietf-core-coap]. In addition, this document defines the following terminology:

Group Communication
A source node sends a single message which is delivered to multiple destination nodes, where all destinations are identified to belong to a specific group. The source node itself may be part of the group. The underlying mechanism for group communication is assumed to be multicast based. The network involved may be a constrained network such as a low-power, lossy network.

Multicast
Sending a message to multiple destination nodes with one network invocation. There are various options to implement multicast including layer 2 (Media Access Control) and layer 3 (IP) mechanisms.

IP Multicast
A specific multicast solution based on the use of IP multicast addresses as defined in "IANA Guidelines for IPv4 Multicast Address Assignments" [RFC5771] and "IP Version 6 Addressing Architecture" [RFC4291].

Low power and Lossy Network (LLN)
A type of constrained IP network where devices are interconnected by a variety of low-power and lossy links (such as IEEE 802.15.4, Bluetooth LE, DECT, DECT ULE) or lossy links (such as IEEE P1901.2 power-line communication).

2. Introduction

2.1. Background

The Constrained Application Protocol (CoAP) is an application protocol (analogous to HTTP) for resource constrained devices operating in an IP network [I-D.ietf-core-coap]. Constrained devices can be large in number, but are often highly correlated to each other (e.g. by type or location). For example, all the light switches in a building may belong to one group and all the thermostats may belong to another group. Groups may be preconfigured before deployment or dynamically formed during operation. If information needs to be sent to or received from a group of devices, group communication mechanisms can improve efficiency and latency of communication and reduce bandwidth requirements for a given application. HTTP does not support any equivalent functionality to CoAP group communication.

2.2. Scope

This document describes how to use the CoAP protocol in a group communication context with IP Multicast running underneath CoAP. No changes to either CoAP or IP Multicast are required for this purpose. However, proper operation of group communication does require judicious use of these and a variety of other IETF protocols. The main contribution of this document lies in explaining how various IETF mechanisms may be used to fulfill CoAP group communication needs for specific use cases and deployments.

3. CoAP Group Communication Based on IP Multicast

3.1. IP Multicast Routing Background

IP Multicast routing protocols have been evolving for decades, resulting in proposed standards such as Protocol Independent Multicast - Sparse Mode (PIM-SM) [RFC4601]. Yet, due to various technical and marketing reasons, IP Multicast routing is not widely deployed on the general Internet. However, IP Multicast is very popular in specific deployments such as in enterprise networks (e.g. for video conferencing), smart home networks (e.g. UPnP) and carrier IPTV deployments. The packet economy and minimal host complexity of IP multicast make it attractive for group communication in constrained environments. Therefore IP multicast is the recommended underlying mechanism for CoAP group communication, and the approach assumed in this document.

To achieve IP multicast beyond a subnet, an IP multicast routing or forwarding protocol needs to be active on IP routers. An examples of a routing protocol specifically for LLNs is RPL (Section 12 of [RFC6550]) and an example of a forwarding protocol for LLNs is MPL

[I-D.ietf-roll-trickle-mcast]. PIM-SM [RFC4601] is often used for multicast routing in un-constrained networks.

IP multicast can also be run in a Link-Local (LL) scope. This means that there is no routing involved and an IP multicast message is only received over the link on which it was sent.

For a complete IP multicast solution, in addition to a routing/ forwarding protocol, a so-called "listener" protocol is needed for the devices to subscribe to groups (see Section 5.2).

3.2. Group Definition and Naming

A group is defined as a set of CoAP endpoints, where each endpoint is configured to receive a multicast CoAP request that is sent to the group's associated IP multicast address. An endpoint MAY be a member of multiple groups. Group membership of an endpoint MAY dynamically change over time.

For group communications, the Group URI will be the CoAP request URI. A Group URI has the scheme 'coap' and includes in the authority part either a group IP multicast address plus optional port number or a hostname plus optional port number that can be resolved to the group IP multicast address (e.g., a Group Name or Group FQDN). Group URIs follow the CoAP URI syntax [I-D.ietf-core-coap]. It is recommended for sending nodes to use the IP multicast address literal in the authority for the Group URI as the default.

If a Group FQDN is used, it can be uniquely mapped to a site-local or global multicast IP address via DNS resolution (if supported). Some examples of hierarchical Group FQDN naming (and scoping) for a building control application are shown below ([I-D.vanderstok-core-dna]):

URI authority	Targeted group
all.bldg6.example.com	"all nodes in building 6"
all.west.bldg6.example.com	"all nodes in west wing, building 6"
all.floor1.west.bldg6.examp...	"all nodes in floor 1, west wing, building 6"
all.bu036.floor1.west.bldg6...	"all nodes in office bu036, floor1, west wing, building 6"

Similarly, if supported, reverse mapping (from IP multicast address to Group FQDN) is possible using the reverse DNS resolution technique ([I-D.vanderstok-core-dna]).

3.3. Port Configuration

A CoAP group member listens for CoAP messages on the group's IP multicast address, on a specified UDP port. Note that the default UDP port is the CoAP default port 5683 but a non-default UDP port MAY be specified for the group; in which case implementers MUST ensure that all group members are configured to use this same port.

Group communications will not work if there diversity in the authority port (i.e. a diversity of dynamic port addresses across the group) or if the resources are located at different paths on different end-points. Therefore, some measures must be present to ensure uniformity in port number and resource names/locations within a group. All CoAP multicast requests MUST be sent using the port number as follows:

1. A preconfigured port number, if available. The pre-configuration mechanism MUST ensure that the same port number is preconfigured across all endpoints in a group and across all CoAP clients performing the group requests.

2. If the client is configured to use service discovery including port discovery, it uses a port number obtained via a service discovery lookup operation as a valid CoAP port for the targeted CoAP multicast group.

3. Otherwise use the default CoAP UDP port.

3.4. Group Discovery and Member Discovery

CoAP defines a resource discovery capability [RFC6690], but does not specify how to discover groups (e.g. find a group to join or send a multicast message to) or how to discover members of a group (e.g. to address selected group members by unicast). A simple ad-hoc method to discover members of a CoAP group would be to send a multicast "CoAP ping" [I-D.ietf-core-coap]. The collected responses to the ping would then give an indication of the group members.

3.5. Group Resource Manipulation

Group communications SHALL only be used for idempotent methods (i.e. CoAP GET, PUT, and DELETE). The CoAP messages that are sent via multicast SHALL be Non-Confirmable.

A unicast response per server MAY be sent back to answer the group request (e.g. response "2.05 Content" to a group GET request) taking into account the congestion control rules defined in Section 3.8. The unicast responses received may be a mixture of success (e.g. 2.05

Content) and failure (e.g. 4.04 Not Found) codes depending on the individual server processing result.

Group communications SHALL NOT be used for non-idempotent methods (i.e. CoAP POST). This is because not all group members are guaranteed to receive the multicast request, and the sender can not readily find out which group members did not receive it.

All CoAP multicast requests SHOULD operate on URI paths ("links") as follows:

1. Preconfigured URI paths, if available. The pre-configuration mechanism MUST ensure that these URIs are preconfigured across all CoAP servers in a group and all CoAP clients performing the group requests.

2. If the client is configured to use default CoRE service discovery, it uses URI paths which were retrieved from a "/.well-known/core" lookup on at least one group member endpoint; where the selected URI paths are known from application knowledge to be available in all endpoints in the group. The URI path configuration mechanism on servers MUST ensure that these URIs (identified as being supported by the group) are configured on all group endpoints.

3. If the client is configured to use another form of service discovery, it uses URI paths from an equivalent service discovery lookup which returns the resources supported by all group members.

3.6. Multicast Request Acceptance and Response Suppression

CoAP [I-D.ietf-core-coap] and CoRE Link Format [RFC6690] define normative requirements for two aspects:

1. Multicast request acceptance; in what cases a request is accepted and executed, and when not.

2. Multicast response suppression; in what cases the response of an executed request is returned to the requesting endpoint, and when not.

This section aims to first summarize these normative requirements and then present guidelines, for a number of multicast example applications, in what way the request suppression and response suppression should be configured.

To apply any rules for request and/or response suppression, the IP

stack interface of a CoAP server must be able to indicate for an incoming request that the destination address of the request was multicast. The case that an IP stack interface cannot provide this indication, is the exception case for the RECOMMENDED behaviours listed below. In that case, only response suppression (aspect 2.) can be supported for selected resources which are known (through application knowledge) and configured to be used for multicast requests.

For aspect 1 (request acceptance), the requirements are:

- A server SHOULD NOT accept a multicast request that cannot be "authenticated" in some way (cryptographically or by some multicast boundary limiting the potential sources) [I-D.ietf-core-coap].
- A server SHOULD NOT accept a multicast discovery request with a query string (as defined in CoRE Link Format [RFC6690]) if filtering ([RFC6690]) is not supported by the server;
- A server SHOULD NOT accept a multicast request that acts on a specific resource for which multicast support is not required. (Note that for discovery resource "/.well-known/core" multicast support is always required. Implementers are advised to disable multicast support by default on any other resource, until explicitly enabled by an application.)

Regarding the first requirement see Section 6.3 for examples of multicast boundary limiting methods.

For aspect 2 (response suppression), the requirements are:

- A server SHOULD NOT respond to a multicast discovery request if the filter specified by the request's query string does not match;
- A server MAY choose not to respond to a multicast request, if there's nothing useful to respond (e.g. error or empty response). This optional response suppression will be illustrated by some use cases in the remainder of this section.

The above response suppression requirements are complemented by the following guidelines in this document. CoAP servers should preferably implement configurable response suppression, enabling at least the following configuration items per resource:

- Suppression of all 2.xx success responses;

- Suppression of all 4.xx client errors;

- Suppression of all 5.xx server errors;

- Suppression of all 2.05 responses with empty payload.

Below a number of group communication example applications are mentioned and in what way these could typically make use of response suppression as defined by the above four configuration items.

- CoAP resource discovery: suppression of 2.05 responses with empty payload and all 4.xx and 5.xx errors.

- Lighting control: suppress all 2.xx responses after a lighting change command.

- Update group configuration data using multicast PUT: no suppression at all. Use collected responses to identify which group members did not receive the new configuration; then attempt using CoAP CON unicast to update those group members.

- Multicast firmware update by sending blocks of data: suppress all 2.xx and 5.xx responses. After having sent all multicast blocks, the client checks each endpoint by unicast to identify which blocks are still missing in each endpoint.

- Conditional reporting for a group (e.g. sensors) based on a URI query: suppress all 2.05 responses with empty payload (i.e. if a query produces no matching results).

3.7. Configuring Group Membership In Endpoints

The group membership of a CoAP server may be determined in one or more of the following ways. First, the group membership may be preconfigured before node deployment. Second, it may be configured during operation by another node e.g. a commissioning device. Third, a node may be programmed to discover (query) its group membership during operation using a specific service discovery means.

In the first case, the preconfigured group may be a multicast IP address or a hostname which is during operation resolved to a multicast IP address by the endpoint using DNS.

In the second case, typical in building control, a commissioning tool determines to which groups a sensor or actuator node belongs, and writes this information to the node, which can subsequently join the correct IP multicast group on its network interface. The information written may again be a multicast IP address or a hostname.

To achieve smoother interoperability between nodes/endpoints from different manufacturers, an OPTIONAL RESTful method of configuring CoAP endpoints with relevant group information is specified here. This approach MUST use unicast methods (GET/PUT/POST) only as it is a method of configuring group information in individual endpoints. Using multicast operations in this situation may lead to unexpected (possibly circular) behavior in the network.

CoAP endpoints implementing this mechanism MUST support at least one discoverable "Group Configuration" resource of resource type (rt) [RFC6690] "core.gp" where "gp" is shorthand for "group". This resource is used by an authorized endpoint to manage group membership of the CoAP endpoint.

The resource of type "core.gp" has a JSON content format. A (unicast) GET on this resource returns a JSON array of group objects, each group object formatted as shown below:

```
Req: GET /gp
Res: 2.05 Content (Content-Format: application/json)
[ { "n": "Room-A-Lights.floor1.west.bldg6.example.com",
    "ip": "ff15::4200:f7fe:ed37:14ca" }
]
```

where the OPTIONAL "n" key/value pair defines the Group name as FQDN and the OPTIONAL "ip" key/value pair defines the associated multicast IP address. A CoAP endpoint can be added to another group by a (unicast) POST on the resource with a single JSON group object, which updates the existing resource by adding the group object to the existing ones:

```
Req: POST /gp (Content-Format: application/json)
{ "n": "floor1.west.bldg6.example.com",
  "ip": "ff15::4200:f7fe:ed37:14cb" }
Res: 2.04 Changed
```

A (unicast) PUT with as payload an array of JSON group objects will replace all current group memberships with the new ones as defined in the payload. After a change effected on the "core.gp" type resource, the endpoint MUST effect registration/deregistration from corresponding IP multicast groups as soon as possible.

3.8. Congestion Control

Multicast CoAP requests may result in a multitude of replies from different nodes, potentially causing congestion. Therefore both the sending of multicast requests and sending unicast CoAP responses to multicast requests should be conservatively controlled.

The base CoAP draft [I-D.ietf-core-coap] reduces multicast-specific congestion risks through the following measures:

- A server MAY choose not to respond to a multicast request if there's nothing useful to respond (e.g. error or empty response). See Section 3.6 for more detailed guidelines on response suppression.

- A server SHOULD limit the support for multicast requests to specific resources where multicast operation is required.

- A multicast request MUST be Non-Confirmable.

- A response to a multicast request SHOULD be Non-Confirmable (Section 5.2.3).

- A server does not respond immediately to a multicast request, but SHOULD first wait for a time that is randomly picked within a predetermined time interval called the Leisure.

- A server SHOULD NOT accept multicast requests that can not be authenticated in some way. See Section 3.6 for more details on request suppression and multicast source authentication.

Additional guidelines to reduce congestion risks are:

- A server in an LLN should only support multicast GET for resources that are small, e.g. the payload of the response fits into a single link-layer frame.

- A server can minimize the payload length in response to a multicast GET on "/.well-known/core" by using hierarchy in arranging link descriptions for the response. An example of this is given in Section 5 of [RFC6690].

- Alternatively a server can also minimize the payload length of a response to a multicast GET (e.g. on "/.well-known/core") using CoAP blockwise transfers [I-D.ietf-core-block], returning only a first block of the link format description.

- A client should always aim to use IP multicast with link-local scope if possible. If this is not possible, then site-local scope IP multicast should be considered. If this is not possible, then global scope IP multicast should be considered as a last resort only.

3.9. Exceptions

Group communication using IP multicast offers improved network efficiency and latency amongst other benefits. However, group communications may not always be possible to implement in a given network. The primary reason for this will be if IP multicast is not supported in the network. For example, in a LLN, if the RPL protocol is used and set to "Non-storing mode" [RFC6550] there will be no IP multicast routing in that network beyond link-local scope. This means that any CoAP group communications above link-local scope will not be supported in that network.

4. Use Cases and Corresponding Protocol Flows

4.1. Introduction

The use of CoAP group communication is shown in the context of the following two use cases and corresponding protocol flows:

- Discovery of Resource Directory: discovering the local CoRE RD which contains links (URIs) to resources stored on other servers [RFC6690].

- Lighting Control: synchronous operation of a group of IPv6-connected lights (e.g., 6LoWPAN [RFC4944] lights).

4.2. Network Configuration

To illustrate the use cases we define two network configurations. Both are based on the topology as shown in Figure 1. The two configurations using this topology are:

1. Subnets are 6LoWPAN networks; the routers Rtr-1 and Rtr-2 are 6LoWPAN Border Routers (6LBRs, [RFC6775]).

2. Subnets are Ethernet links; the routers Rtr-1 and Rtr-2 are multicast-capable Ethernet routers.

Both configurations are further specified by the following:

- A large room (Room-A) with three lights (Light-1, Light-2, Light-3) controlled by a Light Switch. The devices are organized into two subnets. In reality, there could be more lights (up to several hundreds) but these are not shown for clarity.

- Light-1 and the Light Switch are connected to a router (Rtr-1) which is also a CoAP Resource Directory (RD).

- Light-2 and the Light-3 are connected to another router (Rtr-2) which is also a CoAP RD.

- The routers are connected to an IPv6 network backbone which is also multicast enabled. In the general case, this means the network backbone and Rtr-1/Rtr-2 support a PIM based multicast routing protocol, and MLD for forming groups. In a limited case, if the network backbone is one link, then the routers only have to support MLD-snooping (Appendix A) for the following use cases to work.

- The DNS server is optional. If the server is there then certain DNS based features are available (e.g. DNS resolution of URI to IP multicast address). If the DNS server is not there, then different manual provisioning of the network is required (e.g. IP multicast addresses are hardcoded into devices).

```
                                                                 Network
                                                                Backbone
                                                                       |
      ################################################                 |
      #                                       Room-A #                 |
      #         **********************               #                 |
      #       **  Subnet-1            **             #                 |
      #     *                            *           #                 |
      #    *     +----------+             *          #                 |
      #   *      |  Light   |-------+      *         #                 |
      #  *       |  Switch  |       |       *        #                 |
      #  *       +----------+  +---------+  *        #                 |
      #  *                     |  Rtr-1  |-----------------------------|
      #  *                     +---------+  *        #                 |
      #  *       +----------+        |      *        #                 |
      #   *      |  Light-1 |--------+     *         #                 |
      #    *     +----------+             *          #                 |
      #     *                            *           #                 |
      #       **                      **             #                 |
      #         **********************               #                 |
      #                                              #                 |
      #                                              #                 |
      #        **********************                #                 |
      #       **  Subnet-2            **             #                 |
      #     *                            *           #                 |
      #    *     +----------+             *          #                 |
      #   *      |  Light-2 |-------+      *         #                 |
      #  *       |          |       |       *        #                 |
      #  *       +----------+  +---------+  *        #                 |
      #  *                     |  Rtr-2  |-----------------------------|
      #  *                     +---------+  *        #                 |
      #  *       +----------+        |      *        #                 |
      #   *      |  Light-3 |--------+     *         #                 |
      #    *     +----------+             *          #                 |
      #     *                            *           #                 |
      #       **                      **             #                 |
      #         **********************               #                 |
      #                                              #                 |
     #################################################                 |
                                                                       |
                                        +------------+                 |
                                        |    DNS     |                 |
                                        |   Server   |-----------------+
                                        | (Optional) |
                                        +------------+
```

Figure 1: Network Topology of a Large Room (Room-A)

4.3. Discovery of Resource Directory

The protocol flow for discovery of a RD for the given network (of Figure 1) is shown in Figure 2:

- The fixture for Light-2 is installed and powered on for the first time.
- Light-2 will then search for the local RD (RD-2) by sending out a GET request (with the "/.well-known/core?rt=core.rd" request URI) to the site-local "All CoAP Nodes" address. In this case, the site is configured to include at least all nodes in the subnet.
- This multicast message will then go to each node in subnet-2. However, only Rtr-2 (RD-2) will respond because the GET is qualified by the query string "?rt=core.rd". Note that the router Rtr-2 is configured not to forward this multicast request further onto the backbone.
- Note that the flow is shown only for Light-2 for clarity. Similar flows will happen for Light-1, Light-3 and the Light Switch when they are first powered on.

The RD may also be discovered by other means such as by assuming a default location (e.g. on a 6LBR), using DHCP, anycast address, etc. However, these approaches do not invoke CoAP group communication so are not further discussed here.

For other discovery use cases such as discovering local CoAP servers, services or resources group communication can be used in a similar fashion as in the above use case. Both Link-Local (LL) and site-local discovery are possible this way.

```
                                    Light      Rtr-1      Rtr-2   Network
   Light-1   Light-2    Light-3     Switch    (RD-1)     (RD-2)  Backbone
    |          |          |          |          |          |          |
    |          |          |          |          |          |          |
    **********************************          |          |          |
    *   Light-2 is installed         *          |          |          |
    *   and powers on for first time *          |          |          |
    **********************************          |          |          |
    |          |          |          |          |          |          |
    |          |          |          |          |          |          |
    |          | COAP NON Mcast(GET                        |          |
    |          |           /.well-known/core?rt=core.rd)   |          |
    |          |--------->-------------------------------->|          |
    |          |          |          |          |          |          |
    |          |          |          |          |          |          |
    |          |          |          |          |          |          |
    |          | COAP NON (2.05 Content                    |          |
    |          |         </rd>;rt="core.rd";ins="Primary") |          |
    |          |<------------------------------------------|          |
    |          |          |          |          |          |          |
```

Figure 2: Resource Directory Discovery via Multicast Message

4.4. Lighting Control

The protocol flow for a building automation lighting control scenario for the network (Figure 1) in 6LoWPAN configuration is shown in sequence in Figure 3 for the case that the CoAP servers in each Light are configured to not generate a CoAP response to lighting control CoAP multicast requests. (See section Section 3.6 for more details on response suppression by a server.)

In addition, Figure 4 shows a protocol flow example for the case that servers do respond to a lighting control multicast request with CoAP NON responses. There are two success responses and one 5.00 error response. In this particular use case the Light Switch does not check, based on the responses, that all Lights in the group actually received the multicast request, because it is not configured with an exhaustive list of IP addresses of all Lights belonging to the group. However, based on received error responses it could take additional action such as logging a fault or alerting the user via its LCD display.

Reliability of CoAP multicast is not guaranteed. Therefore, one or more lights in the group may not have received the CoAP control request due to packet loss. In this use case there is no detection

nor correction of such situations: the application layer expects that the multicast forwarding/routing will be of sufficient quality to provide on average a very high probability of packet delivery to all CoAP endpoints in a multicast group. An example protocol to accomplish this is the MPL forwarding protocol for LLNs [I-D.ietf-roll-trickle-mcast].

We assume the following steps have already occurred before the illustrated flows:

1. Startup phase: 6LoWPANs are formed. IPv6 addresses assigned to all devices. The CoAP network is formed.

2. Network configuration (application-independent): 6LBRs are configured with multicast address blocks to filter out or to pass through to/from the 6LoWPAN.

3. Commissioning phase (application-related): The IP multicast address of the group (Room-A-Lights) has been configured in all the Lights and in the Light Switch.

4. As an alternative to the previous step, when a DNS server is available, the Light Switch and/or the Lights have been configured with a group hostname which each nodes resolves to the above IP multicast address of the group.

Note for the Commissioning phase: the switch's software supports sending unicast, multicast or proxied unicast/multicast CoAP requests, including processing of the multiple responses that may be generated by a multicast CoAP request.

```
                                    Light                        Network
   Light-1   Light-2    Light-3     Switch    Rtr-1      Rtr-2  Backbone
    |          |          |          |          |          |          |
    |          |          |          |          |          |          |
    |          |          ***********************          |          |
    |          |          *   User flips on     *          |          |
    |          |          *   light switch to   *          |          |
    |          |          *   turn on all the   *          |          |
    |          |          *   lights in Room A  *          |          |
    |          |          ***********************          |          |
    |          |          |          |          |          |          |
    |          |          |          |          |          |          |
    |          |          |    COAP NON Mcast(PUT,         |          |
    |          |          |    Payload=lights ON)          |          |
    |<-------------------------------+--------->|          |          |
    ON         |          |          |          |-------------------->|
    |          |          |          |          |          |<---------|
    |          |<---------|<-------------------------------|          |
    |          ON         ON         |          |          |          |
    ^          ^          ^          |          |          |          |
    ***********************          |          |          |          |
    *   Lights in Room-A  *          |          |          |          |
    *   turn on (nearly   *          |          |          |          |
    *   simultaneously)   *          |          |          |          |
    ***********************          |          |          |          |
    |          |          |          |          |          |          |
```

Figure 3: Light Switch Sends Multicast Control Message

```
                                    Light                        Network
   Light-1   Light-2    Light-3     Switch    Rtr-1      Rtr-2  Backbone
    |          |          |          |          |          |          |
    |     COAP NON (2.04 Changed)    |          |          |          |
    |------------------------------->|          |          |          |
    |          |          |          |          |          |          |
    |          |          |          |          |          |          |
    |          COAP NON (2.04 Changed)          |          |          |
    |          |------------------------------------------>|          |
    |          |          |          |          |          |--------->|
    |          |          |          |          |<--------------------|
    |          |          |          |<---------|          |          |
    |          |          |          |          |          |          |
    |          |        COAP NON (5.00 Internal Server Error)         |
    |          |          |------------------------------->|          |
    |          |          |          |          |          |--------->|
    |          |          |          |          |<--------------------|
    |          |          |          |<---------|          |          |
    |          |          |          |          |          |          |
```

Figure 4: Lights (Optionally) Respond to Multicast CoAP Request

4.5. Lighting Control in MLD Enabled Network

The use case of previous section can also apply in networks where nodes support the MLD protocol [RFC3810]. The Lights then take on the role of MLDv2 listener and the routers (Rtr-1, Rtr-2) are MLDv2 Routers. In the Ethernet based network configuration, MLD may be available on all involved network interfaces. Use of MLD in the 6LoWPAN based configuration is also possible, but requires MLD support in all nodes in the 6LoWPAN which is usually not implemented in many deployments.

The resulting protocol flow is shown in Figure 5. This flow is executed after the commissioning phase, as soon as Lights are configured with a group address to listen to. The MLD Reports may require periodic refresh activity as specified by the MLD protocol.

After the shown sequence of MLD Report messages has been executed, both Rtr-1 and Rtr-2 are automatically configured to forward multicast traffic destined to Room-A-Lights onto their connected subnet. Hence, no manual Network Configuration of routers, as previously indicated in Section 4.4, is needed anymore.

```
                                    Light                   Network
   Light-1   Light-2    Light-3     Switch    Rtr-1      Rtr-2  Backbone
    |          |          |          |          |          |          |
    |          |          |          |          |          |          |
    |          |          |          |          |          |          |
    | MLD Report: Join    |          |          |          |          |
    | Group (Room-A-Lights)          |          |          |          |
    |---LL------------------------------------->|          |          |
    |          |          |          |          |MLD Report: Join     |
    |          |          |          |          |Group (Room-A-Lights)|
    |          |          |          |          |---LL---->----LL---->|
    |          |          |          |          |          |          |
    |          | MLD Report: Join    |          |          |          |
    |          | Group (Room-A-Lights)          |          |          |
    |          |---LL------------------------------------->|          |
    |          |          |          |          |          |          |
    |          |          | MLD Report: Join    |          |          |
    |          |          | Group (Room-A-Lights)          |          |
    |          |          |---LL-------------------------->|          |
    |          |          |          |          |          |          |
    |          |          |          |          |MLD Report: Join     |
    |          |          |          |          |Group (Room-A-Lights)|
    |          |          |          |          |<--LL-----+---LL---->|
    |          |          |          |          |          |          |
    |          |          |          |          |          |          |
```

Figure 5: Joining Lighting Groups Using MLD

5. Deployment Guidelines

This section provides guidelines how an IP Multicast based solution for CoAP group communication can be deployed in various network configurations.

5.1. Target Network Topologies

CoAP group communication can be deployed in various network topologies. First, the target network may be a regular IP network, or a LLN such as a 6LoWPAN network, or consist of mixed constrained/unconstrained network segments. Second, it may be a single subnet only or multi-subnet; e.g. multiple 6LoWPAN networks joined by a single backbone LAN. Third, a wireless network segment may have all nodes reachable in a single IP hop, or it may require multiple IP hops for some pairs of nodes to reach each other.

Each topology may pose different requirements on the configuration of

routers and protocol(s), in order to enable efficient CoAP group communication.

5.2. Advertising Membership of Multicast Groups

If a multicast routing/forwarding protocol is used in a network, server nodes that intend to receive CoAP multicast requests generally require a method to advertise the specific IP multicast address(es) they want to receive, i.e. a method to join specific IP multicast groups. This section identifies the ways in which this can be accomplished.

5.2.1. Using the Multicast Listener Discovery (MLD) Protocol

CoAP nodes that are IP hosts (i.e. not IP routers) are generally unaware of the specific multicast routing/forwarding protocol being used. When such a host needs to join a specific (CoAP) multicast group, it usually requires a way to signal to multicast routers which multicast traffic it wants to receive. For efficient multicast routing (i.e. avoid always flooding multicast IP packets), routers must know which hosts need to receive packets addressed to specific IP multicast destinations.

The Multicast Listener Discovery (MLD) protocol ([RFC3810], Appendix A) is the standard IPv6 method to achieve this. [RFC6636] discusses tuning of MLD for mobile and wireless networks. These guidelines may be useful when implementing MLD in LLNs.

Alternatively, to avoid the use of MLD in LLN deployments, either all nodes can be configured as multicast routers in an LLN, or a multicast forwarding/flooding protocol can be used that forwards any IP multicast packet to all forwarders (routers) in the subnet (LLN).

5.2.2. Using the RPL Routing Protocol

The RPL routing protocol [RFC6550] defines in Section 12 the advertisement of IP multicast destinations using DAO messages. This mechanism can be used by CoAP nodes (which are also RPL routers) to advertise IP multicast group membership to other RPL routers. Then, the RPL protocol can route multicast CoAP requests over multiple hops to the correct CoAP servers.

This mechanism can be used as a means to convey IP multicast group membership information to an edge router (e.g. 6LBR), in case the edge router is also the root of the RPL DODAG. This could be useful in LLN segments where MLD is not available and the edge router needs to know what IP multicast traffic to pass through from the backbone network into the LLN subnet.

5.2.3. Using the MPL Forwarding Protocol

The MPL forwarding protocol [I-D.ietf-roll-trickle-mcast] can be used in a predefined network domain for propagation of IP multicast packets to all MPL routers, over multiple hops. MPL is designed to work in LLN deployments. Due to its property of propagating all (non-link-local) IP multicast packets to all MPL routers, there is in principle no need for CoAP server nodes to advertise IP multicast group membership assuming that any IP multicast source is also part of the MPL domain.

5.3. 6LoWPAN-Specific Guidelines

To support multi-LoWPAN scenarios for CoAP group communication, it is RECOMMENDED that a 6LoWPAN Border Router (6LBR) will act in an MLD Router role on the backbone link. If this is not possible then the 6LBR SHOULD be configured to act as an MLD Multicast Address Listener and/or MLD Snooper (Appendix A) on the backbone link.

To avoid that backbone IP multicast traffic needlessly congests 6LoWPAN network segments, it is RECOMMENDED that a filtering means is implemented to block IP multicast traffic from 6LoWPAN segments where none of the 6LoWPAN nodes listen to this traffic. Possible means are:

- Filtering in 6LBRs based on information from the routing protocol. This allows a 6LBR to only forward multicast traffic onto the LoWPAN, for which it is known that there exists at least one listener on the LoWPAN.

- Filtering in 6LBRs based on MLD reports. Similar as previous but based directly on MLD reports from 6LoWPAN nodes. This only works in a single-IP-hop 6LoWPAN network, such as a mesh-under routing network or a star topology network, because MLD relies on link-local communication.

- Filtering in 6LBRs based on settings. Filtering tables with blacklists/whitelists can be configured in the 6LBR by system administration for all 6LBRs or configured on a per-6LBR basis.

- Filtering in router(s) or firewalls that provide access to constrained network segments. For example, in an access router/bridge that connects a regular intranet LAN to a building control IPv6 backbone. This backbone connects multiple 6LoWPAN segments, each segment connected via a 6LBR.

6. Security Considerations

This section describes the relevant security configuration for CoAP group communications using IP multicast. The threats to CoAP group communications are also identified and various approaches to mitigate these threats are summarized.

6.1. Security Configuration

As defined in [I-D.ietf-core-coap], CoAP group communications based on IP multicast must use the following security modes:

- Group communications MUST operate in CoAP NoSec (No Security) mode.
- Group communications MUST NOT use "coaps" scheme. That is, all group communications MUST use only "coap" scheme.
- Group communications MUST NOT use IPSec.

6.2. Threats

Essentially the above configuration means that there is no security at the CoAP layer for group communications. This is due to the fact that the current DTLS based approach for CoAP is exclusively unicast oriented and does not support group security features such as group key exchange and group authentication. As a direct consequence of this, CoAP group communications is vulnerable to all attacks mentioned in [I-D.ietf-core-coap] for IP multicast.

6.3. Threat Mitigation

[I-D.ietf-core-coap] identifies various threat mitigation techniques for CoAP IP multicast. In addition to those guidelines, it is recommended that for sensitive data or safety-critical control, a combination of appropriate link-layer security and administrative control of IP multicast boundaries should be used. Some examples are given below.

6.3.1. WiFi Scenario

In a home automation scenario (using WiFi), the WiFi encryption should be enabled to prevent rogue nodes from joining. Also, if MAC address filtering at the WiFi Access Point is supported that should also be enabled. The IP router should have the fire wall enabled to isolate the home network from the rest of the Internet. In addition, the domain of the IP multicast should be set to be either link-local scope or site-local scope. Finally, if possible, devices should be

configured to accept only Source Specific Multicast (SSM) packets (see [RFC4607]) from within the trusted home network. For example, all lights in a particular room should only accept IP multicast traffic originating from the master light switch in that room. In this case, the Spoofed Source Address considerations of Section 7.4 of [RFC4607] should be heeded.

6.3.2. 6LoWPAN Scenario

In a building automation scenario, a particular room may have a single 6LoWPAN topology with a single Edge Router (6LBR). Nodes on the subnet can use link-layer encryption to prevent rogue nodes from joining. The 6LBR can be configured so that it blocks any incoming IP multicast traffic. Another example topology could be a multi-subnet 6LoWPAN in a large conference room. In this case, the backbone can implement port authentication (IEEE 802.1X) to ensure only authorized devices can join the Ethernet backbone. The access router to this secured segment can also be configured to block incoming IP multicast traffic.

6.3.3. Future Evolution

In the future, to further mitigate the threats, the developing approach for DTLS-based IP multicast security for CoAP networks (see [I-D.keoh-tls-multicast-security]) or similiar approaches should be considered once they mature.

7. IANA Considerations

No request is made to IANA. (Note to RFC Editor: The required multicast address request to IANA is made in [I-D.ietf-core-coap]).

8. Acknowledgements

Thanks to Peter Bigot, Carsten Bormann, Anders Brandt, Angelo Castellani, Guang Lu, Salvatore Loreto, Kerry Lynn, Dale Seed, Zach Shelby, Peter van der Stok, and Juan Carlos Zuniga for their helpful comments and discussions that have helped shape this document.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4601] Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.

[RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[RFC5771] Cotton, M., Vegoda, L., and D. Meyer, "IANA Guidelines for IPv4 Multicast Address Assignments", BCP 51, RFC 5771, March 2010.

[RFC6550] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, March 2012.

[RFC6636] Asaeda, H., Liu, H., and Q. Wu, "Tuning the Behavior of the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) for Routers in Mobile and Wireless Networks", RFC 6636, May 2012.

[RFC6690] Shelby, Z., "Constrained RESTful Environments (CoRE) Link Format", RFC 6690, August 2012.

[RFC6775] Shelby, Z., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, November 2012.

[I-D.ietf-core-coap]
Shelby, Z., Hartke, K., Bormann, C., and B. Frank, "Constrained Application Protocol (CoAP)", draft-ietf-core-coap-13 (work in progress), December 2012.

9.2. Informative References

[I-D.ietf-core-block]
Bormann, C. and Z. Shelby, "Blockwise transfers in CoAP", draft-ietf-core-block-10 (work in progress), October 2012.

[I-D.vanderstok-core-dna]
Stok, P., Lynn, K., and A. Brandt, "CoRE Discovery, Naming, and Addressing", draft-vanderstok-core-dna-02 (work in progress), July 2012.

[I-D.ietf-roll-trickle-mcast]
Hui, J. and R. Kelsey, "Multicast Protocol for Low power and Lossy Networks (MPL)", draft-ietf-roll-trickle-mcast-03 (work in progress), January 2013.

[I-D.keoh-tls-multicast-security]
Keoh, S., Kumar, S., and E. Dijk, "DTLS-based Multicast Security for Low-Power and Lossy Networks (LLNs)", draft-keoh-tls-multicast-security-00 (work in progress), October 2012.

Appendix A. Multicast Listener Discovery (MLD)

In order to extend the scope of IP multicast beyond link-local scope, an IP multicast routing or forwarding protocol has to be active in routers on an LLN. To achieve efficient multicast routing (i.e. avoid always flooding multicast IP packets), routers have to learn which hosts need to receive packets addressed to specific IP multicast destinations.

The Multicast Listener Discovery (MLD) protocol [RFC3810] (or its IPv4 pendant IGMP) is today the method of choice used by an (IP multicast enabled) router to discover the presence of multicast listeners on directly attached links, and to discover which multicast addresses are of interest to those listening nodes. MLD was specifically designed to cope with fairly dynamic situations in which multicast listeners may join and leave at any time.

IGMP/MLD Snooping is a technique implemented in some corporate LAN routing/switching devices. An MLD snooping switch listens to MLD State Change Report messages from MLD listeners on attached links. Based on this, the switch learns on what LAN segments there is interest for what IP multicast traffic. If the switch receives at some point an IP multicast packet, it uses the stored information to decide onto which LAN segment(s) to send the packet. This improves

network efficiency compared to the regular behavior of forwarding every incoming multicast packet onto all LAN segments. An MLD snooping switch may also send out MLD Query messages (which is normally done by a device in MLD Router role) if no MLD Router is present.

[RFC6636] discusses optimal tuning of the parameters of MLD for routers for mobile and wireless networks. These guidelines may be useful when implementing MLD in LLNs.

Appendix B. Change Log

Changes from ietf-04 to ietf-05:

- Added a new section 3.9 (Exceptions) that highlights that IP multicast (and hence group communications) is not always available (#187).
- Updated text on the use of [RFC2119] language (#271) in Section 1.
- Included guidelines on when (not) to use CoAP responses to multicast requests and when (not) to accept multicast requests (#273).
- Added guideline on use of core-block for minimizing response size (#275).
- Restructured section 6 (Security Considerations) to more fully describe threats and threat mitigation (#277).
- Clearly indicated that DNS resolution and reverse DNS lookup are optional.
- Removed confusing text about a single group having multiple IP addresses. If multiple IP addresses are required then multiple groups (with the same members) should be created.
- Removed repetitive text about the fact that group communications is not guaranteed.
- Merged previous section 5.2 (Multicast Routing) into 3.1 (IP Multicast Routing Background) and added link to section 5.2 (Advertising Membership of Multicast Groups).
- Clarified text in section 3.8 (Congestion Control) regarding precedence of use of IP multicast domains (i.e. first try to use link-local scope, then site-local scope, and only use global IP

multicast as a last resort).

- Extended group resource manipulation guidelines with use of preconfigured ports/paths for the multicast group.
- Consolidated all text relating to ports in a new section 3.3 (Port Configuration).
- Clarified that all methods (GET/PUT/POST) for configuring group membership in endpoints should be unicast (and not multicast) in section 3.7 (Configuring Group Membership In Endpoints).
- Various editorial updates for improved readability, including editorial comments by Peter van der Stok to WG list of December 18th, 2012.

Changes from ietf-03 to ietf-04:

- Removed section 2.3 (Potential Solutions for Group Communications) as it is purely background information and moved section to draft-dijk-core-groupcomm-misc (#266).
- Added reference to draft-keoh-tls-multicast-security to section 6 (Security Considerations).
- Removed Appendix B (CoAP-Observe Alternative to Group Communications) as it is as an alternative to IP Multicast that the WG has not adopted and moved section to draft-dijk-core-groupcomm-misc (#267).
- Deleted section 8 (Conclusions) as it is redundant (#268).
- Simplified light switch use case (#269) by splitting into basic operations and additional functions (#269).
- Moved section 3.7 (CoAP Multicast and HTTP Unicast Interworking) to draft-dijk-core-groupcomm-misc (#270).
- Moved section 3.3.1 (DNS-SD) and 3.3.2 (CoRE Resource Directory) to draft-dijk-core-groupcomm-misc as these sections essentially just repeated text from other drafts regarding DNS based features. Clarified remaining text in this draft relating to DNS based features to clearly indicate that these features are optional (#272).
- Focus section 3.5 (Configuring Group Membership) on a single proposed solution.

- Scope of section 5.3 (Use of MLD) widened to multicast destination advertisement methods in general.

- Rewrote section 2.2 (Scope) for improved readability.

- Moved use cases that are not addressed to draft-dijk-core-groupcomm-misc.

- Various editorial updates for improved readability.

Changes from ietf-02 to ietf-03:

- Clarified that a group resource manipulation may return back a mixture of successful and unsuccessful responses (section 3.4 and Figure 6) (#251).

- Clarified that security option for group communication must be NoSec mode (section 6) (#250).

- Added mechanism for group membership configuration (#249).

- Removed IANA request for multicast addresses (section 7) and replaced with a note indicating that the request is being made in [I-D.ietf-core-coap] (#248).

- Made the definition of 'group' more specific to group of CoAP endpoints and included text on UDP port selection (#186).

- Added explanatory text in section 3.4 regarding why not to use group communication for non-idempotent messages (i.e. CoAP POST) (#186).

- Changed link-local RD discovery to site-local in RD discovery use case to make it more realistic.

- Fixed lighting control use case CoAP proxying; now returns individual CoAP responses as in coap-12.

- Replaced link format I-D with RFC6690 reference.

- Various editorial updates for improved readability

Changes from ietf-01 to ietf-02:

- Rewrote congestion control section based on latest CoAP text including Leisure concept (#188)

- Updated the CoAP/HTTP interworking section and example use case with more details and use of MLD for multicast group joining

- Key use cases added (#185)

- References to [I-D.vanderstok-core-dna] and draft-castellani-core-advanced-http-mapping added

- Moved background sections on "MLD" and "CoAP-Observe" to Appendices

- Removed requirements section (and moved it to draft-dijk-core-groupcomm-misc)

- Added details for IANA request for group communication multicast addresses

- Clarified text to distinguish between "link local" and general multicast cases

- Moved lengthy background section 5 to draft-dijk-core-groupcomm-misc and replaced with a summary

- Various editorial updates for improved readability

- Change log added

Changes from ietf-00 to ietf-01:

- Moved CoAP-observe solution section to section 2

- Editorial changes

- Moved security requirements into requirements section

- Changed multicast POST to PUT in example use case

- Added CoAP responses in example use case

Changes from rahman-07 to ietf-00:

- Editorial changes

- Use cases section added

- CoRE Resource Directory section added

- Removed section 3.3.5. IP Multicast Transmission Methods
- Removed section 3.4 Overlay Multicast
- Removed section 3.5 CoAP Application Layer Group Management
- Clarified section 4.3.1.3 RPL Routers with Non-RPL Hosts case
- References added and some normative/informative status changes

Authors' Addresses

Akbar Rahman (editor)
InterDigital Communications, LLC

Email: Akbar.Rahman@InterDigital.com

Esko Dijk (editor)
Philips Research

Email: esko.dijk@philips.com