Internet Engineering Task Force   M. Goyal, Ed.
Internet-Draft   University of Wisconsin
Intended status: Experimental   Milwaukee
Expires: September 7, 2012   E. Baccelli
                                                         M. Philipp
                                                              INRIA
                                                          A. Brandt
                                                       Sigma Designs
                                                        J. Martocci
                                                    Johnson Controls
                                                      March 6, 2012

**Reactive Discovery of Point-to-Point Routes in Low Power and Lossy
                            Networks**
                    draft-ietf-roll-p2p-rpl-09

Abstract

   This document specifies a point-to-point route discovery mechanism,
   complementary to the RPL core functionality. This mechanism allows
   an IPv6 router to discover "on demand" routes to one or more IPv6
   routers in the LLN such that the discovered routes meets specified
   metrics constraints.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

Targeting Low power and Lossy Networks (LLNs), the RPL routing
protocol [I-D.ietf-roll-rpl] provides paths along a Directed Acyclic
Graph (DAG) rooted at a single router in the network. Establishment
and maintenance of a DAG is performed by routers in the LLN using
DODAG Information Object (DIO) messages. When two arbitrary routers
(neither of which is the DAG's root) need to communicate, the data
packets are restricted to travel only along the links in the DAG.
Such point-to-point (P2P) routing functionality may not be sufficient
for several Home and Building Automation applications [RFC5826]
[RFC5867] due to the following reasons:

o The need to pre-establish routes: each potential destination in
   the network must declare itself as such ahead of the time a source
   needs to reach it.

o The need to route only along the links in the DAG: A DAG is built
   to optimize the routing cost to reach the root. Restricting P2P
   routes to use only the in-DAG links may result in significantly
   suboptimal routes and severe traffic congestion near the DAG root.

This document describes an extension to core RPL that enables an IPv6
router in the LLN to discover routes to one or more IPv6 routers in
the LLN "on demand", such that the discovered routes meet the
specified metrics constraints, without necessarily going along the
links in an existing DAG. This reactive P2P route discovery
mechanism is henceforth referred to as P2P-RPL. P2P-RPL does not
guarantee discovery of a route. Also, the discovered routes may not
be the best available. However, any discovered routes are guaranteed
to satisfy the desired constraints in terms of the routing metrics
and are thus considered "good enough" from the application's
perspective.

A mechanism to measure the end-to-end cost of an existing route has
been specified in [I-D.ietf-roll-p2p-measurement]. As discussed in
Section 4, measuring the end-to-end cost of an existing route may
help decide whether to initiate the discovery of a better route using
P2P-RPL and the metric constraints to be used for this purpose.

2. The Use Cases

One use case, common in home and commercial building environments,
involves a device (say a remote control or an airduct controller)
that suddenly needs to communicate with another device (say a lamp or
a humidity sensor) to which it does not already have a route. In
this case, the remote control (or the airduct controller) must be

able to discover a route to the lamp (or the humidity sensor) "on demand".

Another use case, common in a commercial building environment, involves a large LLN deployment where P2P communication along a particular DAG among hundreds (or thousands) of routers creates severe traffic congestion near that DAG's root, and thus routes across this DAG are desirable.

Other use cases involve scenarios where energy or latency constraints are not satisfied by the P2P routes along an existing DAG because they involve traversing many more intermediate routers than necessary to reach the destination.

[3](#). 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](#)].

Additionally, this document uses terminology from [[I-D.ietf-roll-terminology](#)] and [[I-D.ietf-roll-rpl](#)]. This document introduces the following terms:

Origin : The IPv6 router initiating the P2P-RPL route discovery.

Target : The IPv6 router at the other end point of the P2P route(s) to be discovered. A P2P-RPL route discovery can discover routes to multiple targets at the same time.

Intermediate Router: An IPv6 router that is neither the origin nor a target.

Forward Route: A route in the forward direction, i.e., from the origin to the target.

Backward Route: A route in the backward direction, i.e., from the target to the origin.

Bidirectional Route: A route that can be used in both forward and backward directions.

Source Route: A complete and ordered list of routers that can be used by a packet to travel from a source to a destination node.

Hop-by-hop Route: The route characterized by each router on the route

using its routing table to determine the next hop on the route.

4. Applicability

A route discovery using P2P-RPL may be performed by an origin when no
route exists between itself and the target(s) or when the existing
routes do not satisfy the application requirements. P2P-RPL is
designed to discover hop-by-hop or source routes to one or more
targets such that the discovered routes meet the specified
constraints. In some application contexts, the constraints that the
discovered routes must satisfy are intrinsically known or can be
specified by the application. For example, an origin that expects
its targets to be less than 5 hops away may use "hop-count < 5" as
the constraint. In other application contexts, the origin may need
to measure the cost of the existing route to a target to determine
the constraints. For example, an origin that measures the total ETX
along its current route to a target to be 20 may use "ETX < x*20",
where x is a fraction that the origin decides, as the constraint. A
mechanism to measure the cost of an existing route between two IPv6
routers is specified in [I-D.ietf-roll-p2p-measurement]. If there is
no existing route between the origin and the target(s) or the cost
measurement for the existing routes fails, the origin will have to
guess the constraints to be used in the initial route discovery.
Once, the initial route discovery succeeds or fails, the origin will
have a better estimate for the constraints to be used in the
subsequent route discovery.

P2P-RPL may result in discovery of better P2P routes than the ones
available along a DAG designed to optimize routing cost to the DAG's
root. The improvement in route quality depends on a number of
factors including the network topology, the routing metrics in use
and the prevalent conditions in the network. A network designer may
take into consideration both the benefits (potentially better routes;
no need to maintain routes proactively) and costs (control messages
generated during the route discovery process) when using P2P-RPL.

5. Functional Overview

This section contains a high level description of P2P-RPL.

A P2P-RPL route discovery takes place by forming a DAG rooted at the
origin. As is the case with core RPL, P2P-RPL uses IPv6 link-local
multicast DIO messages to establish a DAG. However, unlike core RPL,
this DAG is temporary in nature and routers in the DAG leave once the
DAG's life time is over. The sole purpose of DAG creation is to
discover routes to the target(s) and DIOs serve as the route

discovery messages. Each router joining the DAG determines a rank
for itself in the DAG and ignores the subsequent DIOs received from
lower (higher in numerical value) ranked neighbors. Thus, the route
discovery messages propagate away from the origin rather than return
back to it. As in core RPL, DIO generation at a router is controlled
by a Trickle timer [RFC6206] that allows a router to avoid generating
unnecessary messages while providing protection against unreliable
wireless communication. P2P-RPL also uses the routing metrics
[I-D.ietf-roll-routing-metrics], objective functions and packet
forwarding framework
[I-D.ietf-6man-rpl-routing-header][I-D.ietf-6man-rpl-option]
developed for core RPL.

An origin may use P2P-RPL to discover routes to one or more targets
identified by one or more unicast/multicast addresses. P2P-RPL
allows for the discovery of one hop-by-hop route or upto four source
routes per target. P2P-RPL allows an origin to piggyback time-
critical application data on the DIO messages for delivery to the
target(s). P2P-RPL does not guarantee discovery of a route to a
target. Also, the discovered routes may not be the best available.
However, any discovered routes are guaranteed to satisfy the desired
constraints in terms of the routing metrics and are thus considered
"good enough" from the application's perspective.

A P2P-RPL route discovery takes place by forming a temporary DAG
rooted at the origin. The DIOs, used to create the temporary DAG,
are identified by a new Mode of Operation (P2P Route Discovery mode
defined in Section 6). The DIOs, listing the P2P Route Discovery
mode as the Mode of Operation, are henceforth referred to as the P2P
mode DIOs. A P2P mode DIO always carries one P2P Route Discovery
Option (defined in Section 7.1) in which the origin specifies the
following information:

o The IPv6 address of a target. This could be a unicast address or
   a multicast one. Any additional targets may be specified by
   including one or more RPL Target Options [I-D.ietf-roll-rpl]
   inside the DIO.

o The nature of the route(s) to be discovered: hop-by-hop or source
   routes. This specification allows for the discovery of one hop-
   by-hop route or up to four source routes per target.

o The desired number of routes (if source routes are being
   discovered).

o Whether the target(s) should send Discovery Reply Object (DRO)
   messages (defined in Section 8) back to the origin on receiving a
   DIO message. A DRO message carries a discovered source route back

to the origin or establishes a hop-by-hop route between the origin and the target. By not allowing the generation of DRO messages, an origin can use P2P-RPL as purely a mechanism to deliver time-critical application data to the target(s).

A P2P Route Discovery Option also accumulates a route from the origin to a target as the routers join the temporary DAG.

A P2P mode DIO MAY also carry:

o One or more Metric Container Options to specify:

   * The relevant routing metrics.

   * The constraints that the discovered route must satisfy. These constraints also limit how far the DIOs message may travel.

o One or more RPL Target options to specify additional unicast or multicast targets.

o One or more Data Options (defined in Section 7.2) to carry time-critical application-level data to be delivered to the target(s).

As the routers join the temporary DAG, they keep track of the best (partial) route(s) they have seen and advertise these routes, along with the corresponding routing metrics, in their P2P mode DIOs. A router, including the target(s), discards a received P2P mode DIO if the aggregated routing metrics on the route advertised by the DIO do not satisfy the listed constraints. These constraints can be used to limit the propagation of P2P mode DIO messages. A router may also discard a received P2P mode DIO if it does not wish to be a part of the discovered route due to limited resources or due to policy reasons.

When a target receives a P2P mode DIO, it forwards the data in any Data Options to the higher layer. The target may remember the discovered route for use as a source route to reach the origin. If the origin has requested DRO messages to be sent back, the target may select the route contained in the received DIO for further processing as described next. This document does not specify a particular method for the target to use to select a route for further processing. Example methods include selecting any route that meets the constraints or selecting the best route(s) discovered over a certain time period.

If one or more source routes are being discovered, the target sends the selected source routes to the origin via DRO messages with one DRO message carrying one discovered route. On receiving a DRO

message, the origin stores the discovered route in its memory. If a
hop-by-hop route is being discovered, the target sends a DRO message
containing the selected route to the origin. The DRO message travels
back to the origin along the selected route, establishing state for
this route in the routers on the path. The target may include one or
more Data Options in a DRO message to deliver any time-critical
application data to the origin.

The target may request the origin to acknowledge the receipt of a DRO
message by sending back a DRO Acknowledgement (DRO-ACK) message
(defined in Section 10). The origin unicasts a DRO-ACK message to
the target. When the target does not receive the requested DRO-ACK
within a certain time interval of sending a DRO, it resends the DRO
message (up to a certain number of times) carrying the same route as
before.

The use of trickle timers to delay the propagation of DIO messages
may cause some nodes to generate these messages even when the desired
routes have already been discovered. In order to preempt the
generation of such unnecessary messages, the target may set a "stop"
flag in the DRO message to let the nodes in the LLN know about the
completion of the route discovery process. The routers receiving
such a DRO should not generate any more DIOs for this temporary DAG.
Neither should they process any received DIOs for this temporary DAG
in future. However, such routers must still process the DROs
received for this temporary DAG.

[6](6). **P2P Route Discovery Mode Of Operation**

This section specifies a new RPL Mode of Operation (MOP), P2P Route
Discovery mode (or P2P mode, for short), with value 4 (to be
confirmed by IANA). A DIO message, listing P2P mode as the MOP, is
identified as performing a P2P-RPL route discovery by creating a
temporary DAG. A P2P mode DIO MUST carry one and only one P2P Route
Discovery Option (specified in Section 7.1).

[6.1](6.1). **Setting a P2P Mode DIO**

The Base Object in a P2P mode DIO message MUST be set in the
following manner:

o RPLInstanceID: RPLInstanceID MUST be a local value as described in
   Section 5.1 of [I-D.ietf-roll-rpl]. The origin MUST NOT use the
   same RPLInstanceID in two or more concurrent route discoveries.

o Version Number: MUST be set to zero. The temporary DAG used for
   P2P-RPL route discovery does not exist long enough to have new

versions.

o Grounded (G) Flag: MUST be set to zero since this DAG is temporary
   in nature, is created solely for the purpose of P2P-RPL route
   discovery and MUST NOT be used for packet routing.

o Mode of Operation (MOP): MUST be set to 4, corresponding to P2P
   Route Discovery mode.

o DTSN: MUST be set to zero on transmission and ignored on
   reception.

o DODAGPreference (Prf): This field MUST be set to zero (least
   preferred).

o DODAGID: This field MUST be set to an IPv6 address of the origin.

o The other fields in the DIO Base Object can be set in the desired
   fashion as per the rules described in [I-D.ietf-roll-rpl].

The DODAG Configuration Option, inside a P2P mode DIO MUST be set in
the following manner:

o MaxRankIncrease: This field MUST be set to zero to disable local
   repair of the temporary DAG.

o Trickle parameters (DIOIntervalDoublings, DIOIntervalMin,
   DIORedundancyConstant) SHOULD be set as described in Section 9.2.

o The Default Lifetime and Lifetime Unit parameters in DODAG
   Configuration option indicate the life time of the state the
   routers maintain for a hop-by-hop route established using P2P-RPL
   and may be set as desired.

o The other fields in the DODAG Configuration Option, including the
   OCP identifying the Objective function, can be set in the desired
   fashion as per the rules described in [I-D.ietf-roll-rpl].

A default DODAG Configuration Option comes in effect if a P2P mode
DIO does not carry an explicit one. The default DODAG Configuration
Option has the following parameter values:

o Authentication Enabled: 0

o DIOIntervalMin: 6, which translates to 64ms as the value for Imin
   parameter in Trickle operation.

o DIORedundancyConstant: 1

o MaxRankIncrease: 0

o Default Lifetime: 0xFF

o Lifetime Unit: 0xFFFF

o Objective Code Point: 0, i.e., OF0 [I-D.ietf-roll-of0] is the
   default objective function.

o The remaining parameters have default values as specified in
   [I-D.ietf-roll-rpl].

The routing metrics and constraints [I-D.ietf-roll-routing-metrics]
used in P2P-RPL route discovery are included in one or more Metric
Container Options [I-D.ietf-roll-rpl] inside the P2P mode DIO. Note
that a DIO need not include a Metric Container if OF0 is the
objective function in effect. In that case, a P2P mode DIO may still
specify an upper limit on the maximum rank, that a router may have in
the temporary DAG, inside the P2P Route Discovery Option (described
in Section 7.1).

A P2P mode DIO:

o MUST carry one (and only one) P2P Route Discovery Option
   (described in Section 7.1). The P2P Route Discovery Option allows
   for the specification of one unicast or multicast address for the
   target.

o MAY carry one or more RPL Target Options to specify additional
   unicast/multicast addresses for the target.

o MAY carry one or more Metric Container Options to specify routing
   metrics and constraints.

o MAY carry one or more Data Options (described in Section 7.2)
   containing time-critical application data to be delivered to the
   target(s).

o MAY carry one or more Route Information or Prefix Information
   Options (described in [I-D.ietf-roll-rpl]).

A router MUST discard a received P2P mode DIO if it violates any of
the rules listed above.

7. New RPL Control Message Options

   This document defines two new RPL control message options: the P2P
   Route Discovery Option and the Data Option.

7.1. P2P Route Discovery Option (P2P-RDO)

```
        -
     0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |   Type = 10   | Option Length |R|H| N | Compr | L |MaxRank/NH |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                                                               |
     |                          Target                               |
     |                                                               |
     |                                                               |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                                                               |
     |                       Address[1..n]                           |
     |                                                               |
     |                                                               |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
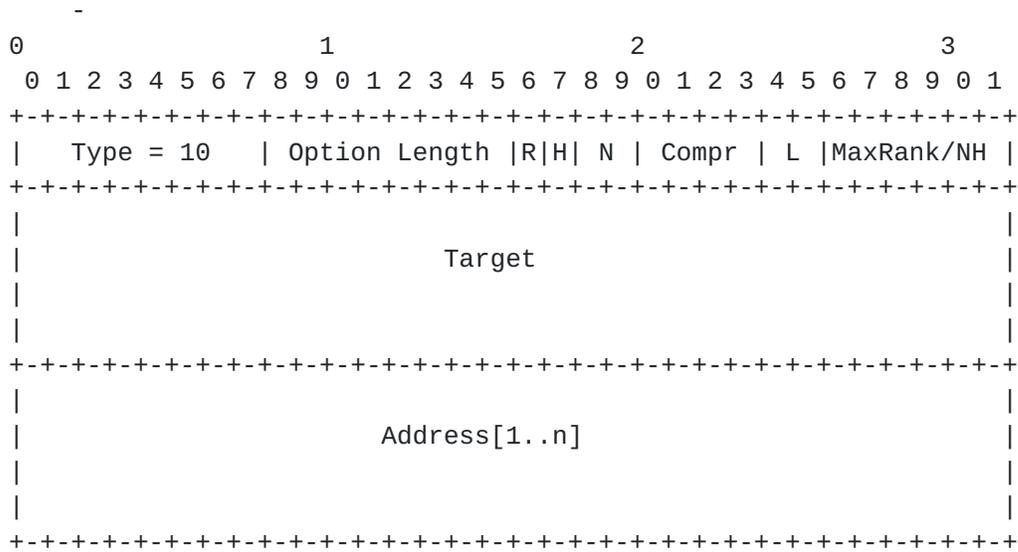
        Figure 1: Format of P2P Route Discovery Option (P2P-RDO)

   The format of a P2P Route Discovery Option (P2P-RDO) is illustrated
   in Figure 1. A P2P mode DIO and a DRO (defined in Section 8) message
   MUST carry one and at most one P2P-RDO. A P2P-RDO consists of the
   following fields:

   o Option Type: 0x0A (to be confirmed by IANA).

   o Option Length: 8-bit unsigned integer, representing the length in
      octets of the option, not including the Option Type and Option
      Length fields.

   o Reply (R): The origin sets this flag to one to allow the target(s)
      to send DRO messages back to the origin. If this flag is zero, a
      target MUST NOT generate any DRO message.

   o Hop-by-hop (H): This flag is valid only if the R flag is set to
      one. The origin sets this flag to one if it desires hop-by-hop
      routes. The origin sets this flag to zero if it desires source
      routes. This specification allows for the establishment of one
      hop-by-hop route or up to four source routes per target. The hop-
      by-hop route is established in the forward direction, i.e. from

the origin to the target. This specification does not allow for
the establishment of hop-by-hop routes in the backward direction.

o Number of Routes (N): This flag is valid only if the R flag is one
   and H flag is zero, i.e. the targets are allowed to generate DRO
   messages carrying discovered source routes back to the origin. In
   this case, the value in the N field plus one indicates the number
   of source routes that each target should convey to the origin.
   When hop-by-hop routes are being discovered, the N field MUST be
   set to zero on transmission and ignored on reception.

o Compr: 4-bit unsigned integer indicating the number of prefix
   octets that are elided from the Target field and the Address
   vector. For example, Compr value will be zero if full IPv6
   addresses are carried in the Target field and the Address vector.

o Life Time (L): A 2-bit field that indicates the suggested life
   time of the temporary DAG, i.e., the suggested duration a router
   joining the temporary DAG SHOULD maintain its membership in the
   DAG. The mapping between the values in this field and the life
   time of the temporary DAG is as follows:

   * 0x00: 1 second;

   * 0x01: 4 seconds;

   * 0x02: 16 seconds;

   * 0x03: 64 seconds;

   The origin sets this field based on its expectation regarding the
   time required for the DIOs to reach the target(s).

o MaxRank/NH:

   * When a P2P-RDO is included in a P2P mode DIO, this field
      indicates the upper limit on the integer portion of the rank
      (calculated using the DAGRank() macro defined in
      [I-D.ietf-roll-rpl]) that a router may have in the temporary
      DAG being created. An intermediate router MUST NOT join a
      temporary DAG being created by a P2P mode DIO if the integer
      portion of its rank would be equal to or higher (in numerical
      value) than the MaxRank limit. A target can join the temporary
      DAG at a rank whose integer portion is equal to the MaxRank. A
      router MUST discard a received P2P mode DIO if the integer part
      of the advertised rank equals or exceeds the MaxRank limit. A
      value 0 in this field indicates that the MaxRank is infinity.

   * When a P2P-RDO is included in a DRO message, this field
      indicates the index of the next hop address inside the Address
      vector.

o Target: An IPv6 address of the target after eliding Compr number
   of prefix octets. When the P2P-RDO is included in a P2P mode DIO,
   this field may contain a unicast address or a multicast one. Any
   additional target addresses can be specified by including one or
   more RPL Target Options [I-D.ietf-roll-rpl] in the DIO. When the
   P2P-RDO is included in a DRO, this field MUST contain a unicast
   IPv6 address of the target generating the DRO.

o Address[1..n]: A vector of IPv6 addresses representing a (partial)
   route in the forward direction:

   * Each element in the Address vector has size (16 - Compr) octets
      and MUST contain a valid IPv6 address with first Compr octets
      elided.

   * The total number of elements inside the Address vector is given
      by n = (Option Length - 2 - (16 - Compr))/(16 - Compr).

   * The IPv6 addresses in the Address vector MUST be reachable in
      both forward and backward directions. Reachability in the
      backward direction allows a DRO message to use the route
      accumulated in the Address vector to travel from the target to
      the origin.

   * The Address vector MUST carry the accumulated route in the
      forward direction, i.e., the first element in the Address
      vector must contain the IPv6 address of the router next to the
      origin and so on.

   * The origin and target addresses MUST NOT be included in the
      Address vector.

   * A router adding its address to the vector MUST ensure that its
      address does not already exist in the vector. A router
      specifying a complete route in the Address vector MUST ensure
      that the vector does not contain any address more than once.

   * The Address vector MUST NOT contain any multicast addresses.

7.2. Data Option

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Type = 11   | Option Length |    Data                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...                       |
```
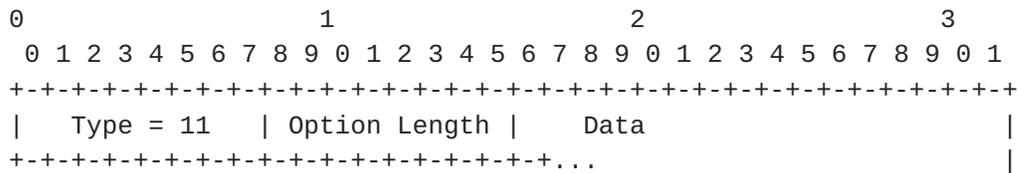
Figure 2: Format of Data Option

The format of a Data Option is illustrated in Figure 2. A P2P mode
DIO and a DRO (defined in Section 8) message MAY carry one or more
Data Options. A P2P-RDO consists of the following fields:

o Option Type: 0x0B (to be confirmed by IANA).

o Option Length: 8-bit unsigned integer, representing the length in
   octets of the option, not including the Option Type and Option
   Length fields.

o Data: If the Data Option is contained in a DIO, this field
   contains application data to be delivered to the target(s). If
   the Data Option is contained in a DRO, this field contains
   application data to be delivered to the origin.

8. The Discovery Reply Object (DRO)

This section defines two new RPL Control Message types, the Discovery
Reply Object (DRO), with code 0x04 (to be confirmed by IANA), and the
Secure DRO, with code 0x84 (to be confirmed by IANA). A DRO serves
one of the following functions:

o Carry a discovered source route from a target to the origin;

o Establish a hop-by-hop route as it travels from a target to the
   origin.

A DRO message MAY serve the function of letting the routers in the
LLN know that a P2P-RPL route discovery is complete and no more DIO
messages need to be generated for the corresponding temporary DAG. A
DRO message MAY also carry time-critical application data from the
target to the origin in one or more Data Options. A DRO message MUST
carry one P2P-RDO whose Target field MUST contain a unicast IPv6
address of the target that generated the DRO. A DRO message travels
from the target to the origin via link-local multicast along the
route specified inside the Address vector in the P2P-RDO.

```
     0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     | RPLInstanceID |    Version    |S|A|Seq|       Reserved        |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     |                                                               |
     |                           DODAGID                             |
     |                                                               |
     |                                                               |
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     | Option(s)...
     +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+...
```
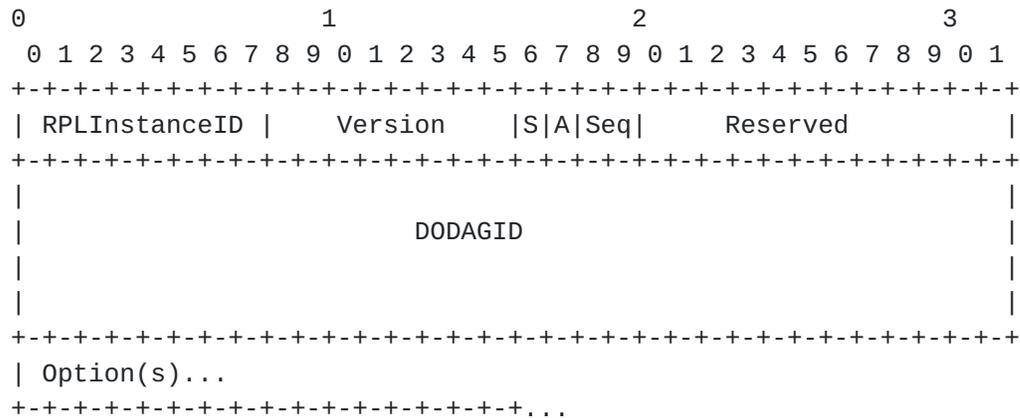
          Figure 3: Format of the base Discovery Reply Object (DRO)

   The format of the base Discovery Reply Object (DRO) is shown in
   Figure 3. A base DRO consists of the following fields:

   o RPLInstanceID: The RPLInstanceID of the temporary DAG used for
      route discovery.

   o Version: The Version of the temporary DAG used for route
      discovery. Since a temporary DAG always has value zero for the
      Version, this field MUST always be set to zero.

   o Stop (S): This flag, when set to one by a target, indicates that
      the P2P-RPL route discovery is over. All the routers receiving
      such a DRO, including the ones not listed in the route carried
      inside P2P-RDO,

      * SHOULD NOT process any more DIOs received for this temporary
         DAG;

      * SHOULD NOT generate any more DIOs for this temporary DAG;

      * SHOULD cancel any pending DIO transmission for this temporary
         DAG.

   Note that the stop flag serves to stop further DIO generation/
   processing for a P2P-RPL route discovery but it does not affect
   the processing of DRO messages at either the origin or the
   intermediate routers. In other words, a router (the origin or an
   intermediate router) MUST continue to process the DRO messages
   even if an earlier DRO message (with same RPLInstanceID and
   DODAGID fields) had the stop flag set to one.

o Ack Required (A): This flag, when set to one by the target,
   indicates that the origin MUST unicast a DRO-ACK message (defined
   in Section 10) to the target when it receives the DRO.

o Sequence Number (Seq): This 2-bit field indicates the sequence
   number for the DRO. This field is relevant when the A flag is set
   to one, i.e., the target requests an acknowledgement from the
   origin for a received DRO. The origin includes the RPLInstanceID,
   the DODAGID and the Sequence Number of the received DRO inside the
   DRO-ACK message it sends back to the target.

o Reserved: These bits are reserved for future use. These bits MUST
   be set to zero on transmission and MUST be ignored on reception.

o DODAGID: The DODAGID of the temporary DAG used for route
   discovery. The DODAGID also identifies the origin. The
   RPLInstanceID, the Version and the DODAGID together uniquely
   identify the temporary DAG used for route discovery and can be
   copied from the DIO message advertizing the temporary DAG.

o Options: The DRO message:

   * MUST carry one P2P-RDO that MUST specify a complete route
      between the target and the origin;

   * MAY carry one or more Metric Container Options that contains
      the aggregated routing metrics values for the route specified
      in P2P-RDO;

   * MAY carry one or more Data Options to carry any time-critical
      application data to the origin.

8.1. Secure DRO

A Secure DRO message follows the format in Figure 7 of
[I-D.ietf-roll-rpl], where the base format is the base DRO shown in
Figure 3.

8.2. Setting a P2P-RDO Carried in a Discovery Reply Object

A Discovery Reply Object MUST carry one P2P-RDO, which MUST be set as
defined in Section 7.1. Specifically, the following fields MUST be
set as specified next:

o Reply (R): This flag MUST be set to zero on transmission and
   ignored on reception.

o Hop-by-Hop (H): The H flag in the P2P-RDO included in a DRO
   message MUST have the same value as the H flag in the P2P-RDO
   inside the corresponding DIO message.

o Number of Routes (N): This field MUST be set to zero on
   transmission and ignored on reception.

o Life Time (L): This field MUST be set to zero on transmission and
   ignored on reception.

o MaxRank/NH: This field indicates the index of the next hop address
   in the Address vector. When a target generates a DRO message, the
   NH field is set to n = (Option Length - 2 - (16 - Compr))/(16 -
   Compr).

o Target: This field MUST contain a unicast IPv6 address of the
   target generating the DRO.

o Address[1..n]: The Address vector MUST contain a complete route
   between the origin and the target such that the first element in
   the vector contains the IPv6 address of the router next to the
   origin and the last element contains the IPv6 address of the
   router next to the target.

9. P2P-RPL Route Discovery By Creating a Temporary DAG

This section details the P2P-RPL route discovery operation.

9.1. Joining a Temporary DAG

All the routers participating in a P2P-RPL route discovery, including
the origin and the target(s), MUST join the temporary DAG being
created for the purpose. When a router joins a temporary DAG
advertized by a P2P mode DIO, it SHOULD maintain its membership in
the temporary DAG for the suggested Life Time duration listed in the
P2P-RDO. The only purpose of a temporary DAG's existence is to
facilitate the P2P-RPL route discovery process. The temporary DAG
MUST NOT be used to route packets. A router SHOULD detach from the
temporary DAG once the duration of its membership in the DAG has
exceeded the DAG's suggested life time. After receiving a DRO with
the stop flag set to one, a router SHOULD NOT send or receive any
more DIOs for this temporary DAG and SHOULD also cancel any pending
DIO transmission.

9.2. Trickle Operation For P2P Mode DIOs

   An RPL router uses a Trickle timer [RFC6206] to control DIO
   transmissions. The Trickle control of DIO transmissions provides
   quick resolution of any "inconsistency" while avoiding redundant DIO
   transmissions. The Trickle algorithm also imparts protection against
   loss of DIOs due to inherent lack of reliability in wireless
   communication. When controlling the transmissions of a P2P mode DIO,
   a Trickle timer SHOULD follow the following rules:

   o The receipt of a P2P mode DIO, that allows the router to advertise
      a better route (in terms of the routing metrics and the OF in use)
      than before, is considered "inconsistent" and hence resets the
      Trickle timer. Note that the first receipt of a P2P mode DIO
      advertising a particular temporary DAG is always considered an
      "inconsistent" event.

   o The receipt of a P2P mode DIO from a parent in the temporary DAG
      is considered neither "consistent" nor "inconsistent" if it does
      not allow the router to advertise a better route than before.
      Thus, the receipt of such DIOs has no impact on the Trickle
      operation. Note that this document does not impose any
      requirements on how a router might choose its parents in the
      temporary DAG.

   o The receipt of a P2P mode DIO is considered "consistent" if the
      source of the DIO is not a parent in the temporary DAG and either
      of the following conditions is true:

      * The DIO advertises a better route than the router but does not
         allow the router to advertise a better route itself; or

      * The DIO advertises a route as good as the route (to be)
         advertised by the router.

      Note that Trickle algorithm's DIO suppression rules are in effect
      at all times. Hence, a P2P-RPL router may suppress a DIO
      transmission even if it has not made any DIO transmission yet.

   o The receipt of a P2P mode DIO, that advertises a worse route than
      what the router advertises (or would advertise when it gets a
      chance to generate its DIO), is considered neither "consistent"
      nor "inconsistent", i.e., the receipt of such a DIO has no impact
      on the Trickle operation.

   o The Imin parameter SHOULD be set taking in account the
      connectivity within the network. For highly connected networks, a
      small Imin value (of the order of the typical transmission delay

for a DIO) may lead to congestion in the network as a large number
of routers reset their Trickle timers in response to the first
receipt of a DIO from the origin. These routers would generate
their DIOs within Imin interval and cause additional routers to
reset their trickle timers and generate more DIOs. Thus, for
highly connected networks, the Imin parameter SHOULD be set to a
value at least one order of magnitude larger than the typical
transmission delay for a DIO. For sparsely connected networks,
the Imin parameter can be set to a value that is a small multiple
of the typical transmission delay for a DIO. Note that the Imin
value has a direct impact on the time required for a P2P-RPL route
discovery to complete. In general, the time required for a P2P-
RPL route discovery would increase approximately linearly with the
value of the Imin parameter.

o The Imax parameter SHOULD be set to a large value (several orders
   of magnitude higher than the Imin value) and is unlikely to be
   critical for P2P-RPL operation. This is because the first receipt
   of a P2P mode DIO for a particular temporary DAG is considered an
   inconsistent event and would lead to resetting of Trickle timer
   duration to the Imin value. Given the temporary nature of the
   DAGs used in P2P-RPL, Trickle timer may not get a chance to
   increase much.

o The recommended value of redundancy constant "k" is 1. With this
   value of "k", a DIO transmission will be suppressed if the router
   receives even a single "consistent" DIO during a timer interval.
   This setting for the redundancy constant is designed to reduce the
   number of messages generated during a route discovery process and
   is suitable for environments with low or moderate packet loss
   rates. In environments with high packet loss rates, a higher
   value for the redundancy constant may be more suitable.

9.3. Processing a P2P Mode DIO

The rules for DIO processing and transmission, described in Section 8
of RPL [I-D.ietf-roll-rpl], apply to P2P mode DIOs as well except as
modified in this document.

The following rules for processing a received P2P mode DIO apply to
both intermediate routers and the target.

A router SHOULD discard a received P2P mode DIO with no further
processing if it does not have bidirectional reachability with the
neighbor that generated the received DIO. Note that bidirectional
reachability does not mean that the link must have the same values
for a routing metric in both directions. A router SHOULD calculate
the values of the link-level routing metrics included in the received

DIO taking in account the metric's value in both forward and backward
directions. Bidirectional reachability along a discovered route
allows the target to use this route to reach the origin. In
particular, the DRO messages travel from the target to the origin
along a discovered route.

A router MUST discard a received P2P mode DIO with no further
processing:

o If the DIO advertises INFINITE_RANK as defined in
   [I-D.ietf-roll-rpl].

o If the integer part of the rank advertised in the DIO equals or
   exceeds the MaxRank limit listed in the P2P Route Discovery
   Option.

o If the router cannot evaluate the mandatory route constraints
   listed in the DIO or if the routing metric values do not satisfy
   one or more of the mandatory constraints.

o If the router previously received a DRO message with same
   RPLInstanceID and DODAGID as the received DIO and with the stop
   flag set to one.

The router MUST check the target addresses listed in the P2P-RDO and
any RPL Target Options included in the received DIO. If one of its
IPv6 addresses is listed as a target address or if it belongs to the
multicast group specified as one of the target addresses, the router
considers itself a target and processes the received DIO as specified
in Section 9.5. Otherwise, the router considers itself an
intermediate router and processes the received DIO as specified in
Section 9.4.

9.4. Additional Processing of a P2P Mode DIO At An Intermediate Router

An intermediate router MUST discard a received P2P mode DIO with no
further processing if the router cannot elide Compr (as specified in
the P2P-RDO) prefix octets from its IPv6 address.

On receiving a P2P mode DIO, an intermediate router MUST determine
whether this DIO advertises a better route than the router itself and
whether the receipt of the DIO would allow the router to advertise a
better route than before. Accordingly, the router SHOULD consider
this DIO as consistent/inconsistent from Trickle perspective as
described in Section 9.2. Note that the route comparison in a P2P-
RPL route discovery is performed using the parent selection rules of
the OF in use as specified in Section 14 of RPL [I-D.ietf-roll-rpl].
If the received DIO would allow the router to advertise a better

route, the router MUST remember the route advertised (inside the P2P-
RDO) in the DIO (after adding its own IPv6 address to the route) as
well as any Data Options for inclusion in its future DIOs. When an
intermediate router adds itself to a route, it MUST ensure that the
IPv6 address added to the route is reachable in both forward and
backward directions. To improve the diversity of the routes being
discovered, an intermediate router SHOULD keep track of multiple
partial routes to be advertised in the P2P-RDO inside its DIO. When
the router generates its DIO, it SHOULD randomly select the partial
route to be included in the P2P-RDO.

[9.5](9.5). Additional Processing of a P2P Mode DIO At The Target

The target MUST deliver the data contained in any Data Options in the
received DIO to the application layer. The target MAY store the
route contained in the P2P-RDO in the received DIO for use as a
source route to reach the origin. If the Reply flag inside the P2P-
RDO is zero, the target MUST discard the received DIO with no further
processing. Otherwise, the target MAY select the route contained in
the P2P-RDO to send a DRO message back to the origin. If the H flag
inside the P2P-RDO is one, the target needs to select one route and
send a DRO message along this route back to the origin. If the H
flag is zero, the number of routes to be selected (and the number of
DRO messages to be sent back) is given by one plus the value of the N
field in the P2P-RDO. This document does not prescribe a particular
method for the target to select the routes. Example methods include
selecting each route that meets the specified routing constraints
until the desired number have been selected or selecting the best
routes discovered over a certain time period. If multiple routes are
to be selected, the target SHOULD avoid selecting routes that have
large segments in common.

If the target selects the route contained in the P2P-RDO in the
received DIO, it sends a DRO message back to the origin (identified
by the DODAGID field in the DIO). The DRO message MUST include a
P2P-RDO that contains the selected route inside the Address vector.
Various fields inside the P2P-RDO MUST be set as specified in
Section 8.2. The target MAY set the A flag inside the DRO message to
one if it desires the origin to send back a DRO-ACK message on
receiving the DRO. In this case, the target waits for
DRO_ACK_WAIT_TIME duration for the DRO-ACK message to arrive.
Failure to receive the DRO-ACK message within this time duration
causes the target to retransmit the DRO message. The target MAY
retransmit the DRO message in this fashion up to
MAX_DRO_RETRANSMISSIONS times. The values of DRO_ACK_WAIT_TIME and
MAX_DRO_RETRANSMISSIONS are defined in Section 12.

The target MAY set the stop flag inside the DRO message to one if

o this router is the only target specified in the corresponding DIO,
   i.e., the corresponding DIO specified a unicast address of the
   router as the Target inside the P2P-RDO with no additional targets
   specified via RPL Target Options; and

o the target has already selected the desired number of routes.

The target MAY include a Metric Container Option in the DRO message.
This Metric Container contains the end-to-end routing metric values
for the route specified in the P2P-RDO. The target MAY include one
or more Data Options in the DRO message to carry time-critical
application data for the origin. The target MUST transmit the DRO
message via a link-local multicast.

A target MUST NOT forward a P2P mode DIO any further.

9.6. Processing a DRO At An Intermediate Router

When a router receives a DRO message that does not list its IPv6
address in the DODAGID field, the router MUST process the received
message in the following manner:

o If the stop flag inside the received DRO is set to one, the router
   SHOULD NOT send or receive any more DIOs for this temporary DAG
   and SHOULD cancel any pending DIO transmission.

o An intermediate router MUST ignore any Metric Container and Data
   Options contained in the DRO message.

o If Address[NH] element inside the Route Discovery Option lists the
   router's own IPv6 address, the router is a part of the route
   carried in the P2P-RDO. In this case, the router MUST do the
   following:

   * If the H flag inside the P2P-RDO is one, the router MUST store
      the state for the forward hop-by-hop route carried inside the
      P2P-RDO. This state consists of:

      + The RPLInstanceID and the DODAGID fields of the DRO.

      + The route's destination, the target (identified by Target
         field inside P2P-RDO).

      + The IPv6 address of the next hop, Address[NH+1] (unless NH
         value equals the number of elements in the Address vector,
         in which case the target itself is the next hop).

* If the router already maintains a hop-by-hop state listing the
  target as the destination and carrying same RPLInstanceID and
  DODAGID fields as the received DRO and the next hop information
  in the state does not match the next hop indicated in the
  received DRO, the router MUST drop the DRO message with no
  further processing.

* The router MUST decrement the NH field inside the P2P-RDO and
  send the DRO further via link-local multicast.

9.7. Processing a DRO At The Origin

When a router receives a DRO message that lists its IPv6 address in
the DODAGID field, the router recognizes itself as the origin for the
corresponding P2P-RPL route discovery and processes the message in
the following manner.

The origin MUST deliver data in any Data Options in the received DRO
to the application layer.

If the stop flag inside the received DRO is set to one, the origin
SHOULD NOT generate any more DIOs for this temporary DAG and SHOULD
cancel any pending DIO transmission.

If the P2P-RDO inside the DRO identifies the discovered route as a
source route (H=0), the origin MUST store in its memory the
discovered route contained in the Address vector.

If the P2P-RDO inside the DRO identifies the discovered route as a
hop-by-hop route (H=1), the origin MUST store in its memory the state
for the discovered route in the manner described in Section 9.6.

If the received DRO message contains one or more Metric Container
Options, the origin MAY store the values of the routing metrics
associated with the discovered route in its memory. This information
may be useful in formulating the constraints for any future P2P-RPL
route discovery to the target.

If the A flag is set to one in the received DRO message, the origin
MUST generate a DRO-ACK message as described in Section 10 and
unicast the message to the target (identified by the Target field
inside the P2P-RDO). The origin MAY use the route just discovered to
send the DRO-ACK message to the target. Section 11 describes how a
packet may be forwarded along a source/hop-by-hop route discovered
using P2P-RPL.

10. The Discovery Reply Object Acknowledgement (DRO-ACK)

```
  0                   1                   2                   3
   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  | RPLInstanceID |    Version    |Seq|         Reserved         |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |                                                               |
  |                           DODAGID                             |
  |                                                               |
  |                                                               |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
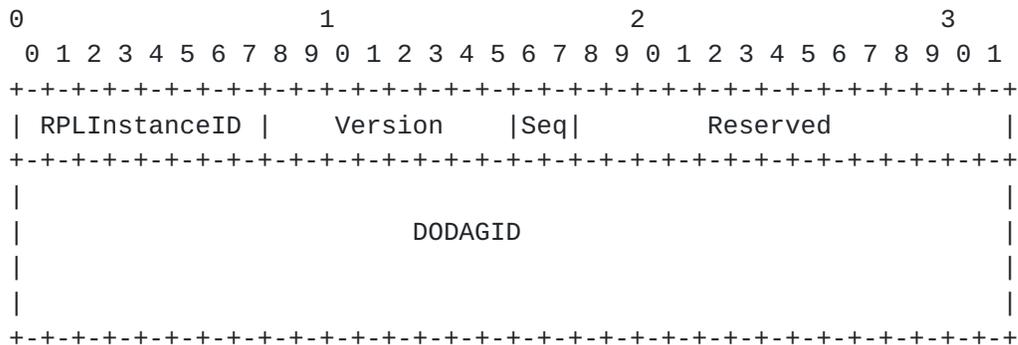
        Figure 4: Format of the base Discovery Reply Object Acknowledgement
                               (DRO-ACK)

   A DRO message may fail to reach the origin due to a number of
   reasons. Unlike the DIO messages that benefit from Trickle-
   controlled retransmissions, the DRO messages are prone to loss due to
   unreliable wireless communication. Since a DRO message travels via
   link-local multicast, it cannot use link-level acknowledgements to
   improve the reliability of its transmission. Also, an intermediate
   router may drop the DRO message (e.g., because of its inability to
   store the state for the hop-by-hop route the DRO is establishing).
   To protect against the potential failure of a DRO message to reach
   the origin, the target MAY request the origin to send back a DRO
   Acknowledgement (DRO-ACK) message on receiving a DRO message.
   Failure to receive such an acknowledgement within the
   DRO_ACK_WAIT_TIME interval of sending the DRO message forces the
   target to resend the message.

   This section defines two new RPL Control Message types: DRO
   Acknowledgement (DRO-ACK; with code 0x05; to be confirmed by IANA)
   and Secure DRO-ACK (with code 0x85; to be confirmed by IANA). A DRO-
   ACK message MUST travel as a unicast message from the origin to the
   target. The format of a base DRO-ACK message is shown in Figure 4.
   Various fields in a DRO-ACK message MUST have the same values as the
   corresponding fields in the DRO message. The field marked as
   "Reserved" MUST be set to zero on transmission and MUST be ignored on
   reception. A Secure DRO-ACK message follows the format in Figure 7
   of [I-D.ietf-roll-rpl], where the base format is same as the base
   DRO-ACK shown in Figure 4.

11. Packet Forwarding Along a Route Discovered Using P2P-RPL

   An origin MAY use a Source Routing Header (SRH)

[I-D.ietf-6man-rpl-routing-header] to send a packet along a source
route discovered using P2P-RPL.

Travel along a hop-by-hop route, established using P2P-RPL, requires
specifying the RPLInstanceID and the DODAGID (of the temporary DAG
used for the route discovery) to identify the route. This is because
a P2P-RPL route discovery does not use globally unique RPLInstanceID
values and hence both the RPLInstanceID (a local value assigned by
the origin) and the DODAGID (an IPv6 address of the origin) are
required to uniquely identify a P2P-RPL hop-by-hop route to a
particular destination.

An origin MAY include an RPL option [I-D.ietf-6man-rpl-option] inside
the IPv6 hop-by-hop options header of a packet to send it along a
hop-by-hop route established using P2P-RPL. For this purpose, the
origin MUST set the DODAGID of the temporary DAG used for the route
discovery as the source IPv6 address of the packet. Further, the
origin MUST specify inside the RPL option the RPLInstanceID of the
temporary DAG used for the route discovery and set the O flag inside
the RPL option to one. On receiving this packet, an intermediate
router checks the O flag and correctly infer the source IPv6 address
of the packet as the DODAGID of the hop-by-hop route. The router
then uses the DODAGID, the RPLInstanceID and the destination address
to identify the routing state to be used to forward the packet
further.

12. Constants

This document defines the following constants:

o DRO_ACK_WAIT_TIME: The time duration a target waits for the DRO-
   ACK before retransmitting a DRO message. DRO_ACK_WAIT_TIME has a
   value of 1 second.

o MAX_DRO_RETRANSMISSIONS: The maximum number of times a DRO message
   may be retransmitted if the target does not receive a DRO-ACK in
   response. MAX_DRO_RETRANSMISSIONS has a value 2.

13. Interoperability with Core RPL

This section describes how RPL routers that implement P2P-RPL
interact with RPL routers that do not. In general, P2P-RPL operation
does not affect core RPL operation and vice versa. However, core RPL
does allow a router to join a DAG as a leaf node even if it does not
understand the Mode of Operation (MOP) used in the DAG. Thus, an RPL
router that does not implement P2P-RPL may conceivably join a

temporary DAG being created for a P2P-RPL route discovery as a leaf
node and maintain its membership even though the DAG no longer
exists. This may impose a drain on the router's memory. However,
such RPL-only leaf nodes do not interfere with P2P-RPL route
discovery since a leaf node may only generate a DIO advertising an
INFINITE_RANK and all routers implementing P2P-RPL are required to
discard such DIOs. Note that core RPL does not require a router to
join a DAG whose MOP it does not understand. Moreover, RPL routers
in a particular deployment may have strict restrictions on the DAGs
they may join, thereby mitigating the problem.

The P2P-RPL mechanism described in this document works best when all
the RPL routers in the LLN implement P2P-RPL. In general, the
ability to discover routes as well as the quality of discovered
routes would deteriorate with the fraction of RPL routers that
implement P2P-RPL.

14. Security Considerations

The security considerations for the operation of P2P-RPL are similar
to the ones for the operation of RPL (as described in Section 19 of
[I-D.ietf-roll-rpl]). Section 10 of RPL specification
[I-D.ietf-roll-rpl] describes a variety of security mechanisms that
provide data confidentiality, authentication, replay protection and
delay protection services. Each RPL control message has a secure
version that allows the specification of the level of security and
the algorithms used to secure the message. The mechanism defined in
this document is based on the use of DIOs to form a temporary DAG and
discover P2P routes. These DIOs can be used in their secure versions
if desired. New RPL control messages defined in this document (DRO
and DRO-ACK) have secure versions as well. Thus, a particular P2P-
RPL deployment can analyze its security requirements and use the
appropriate set of RPL security mechanisms that meet those
requirements.

15. IANA Considerations

15.1. Additions to DIO Mode of Operation

IANA is requested to allocate a new value in the "DIO Mode of
Operation" registry for the "P2P Route Discovery Mode" described in
this document.

```
+----------+------------------------------------------+--------------+
|   MOP    |              Description                 |  Reference   |
|  Value   |                                          |              |
+----------+------------------------------------------+--------------+
|    4     |   Reactive P2P route discovery mode of   |    This      |
|          |                operation                 |   document   |
+----------+------------------------------------------+--------------+
```

                         DIO Mode of Operation

15.2. Additions to RPL Control Message Options

   IANA is requested to allocate new values in the "RPL Control Message
   Options" registry for the "P2P Route Discovery Option" and the "Data
   Option" described in this document.

```
+-------+---------------------+---------------+
| Value |       Meaning       |   Reference   |
+-------+---------------------+---------------+
|   10  | P2P Route Discovery | This document |
|   11  |        Data         | This document |
+-------+---------------------+---------------+
```

                     RPL Control Message Options

15.3. Additions to RPL Control Codes

   IANA is requested to allocate new code points in the "RPL Control
   Codes" registry for the "Discovery Reply Object" and "Discovery Reply
   Object Acknowledgement" (and their secure versions) described in this
   document.

```
+------+------------------------------------------------+---------------+
| Code |                 Description                    |   Reference   |
+------+------------------------------------------------+---------------+
| 0x04 |           Discovery Reply Object               | This document |
| 0x05 |   Discovery Reply Object Acknowledgement       | This document |
| 0x84 |       Secure Discovery Reply Object            | This document |
| 0x85 |       Secure Discovery Reply Object            | This document |
|      |               Acknowledgement                  |               |
+------+------------------------------------------------+---------------+
```

                           RPL Control Codes

16. Acknowledgements

   Authors gratefully acknowledge the contributions of the following

individuals (in alphabetical order) in the development of this
document: Dominique Barthel, Jakob Buron, Thomas Clausen, Richard
Kelsey, Phil Levis, Zach Shelby, Pascal Thubert, Hristo Valev and JP
Vasseur.

17. References

17.1. Normative References

[I-D.ietf-roll-routing-metrics]
          Barthel, D., Vasseur, J., Pister, K., Kim, M., and N.
          Dejean, "Routing Metrics used for Path Calculation in Low
          Power and Lossy Networks",
          draft-ietf-roll-routing-metrics-19 (work in progress),
          March 2011.

[I-D.ietf-roll-rpl]
          Brandt, A., Vasseur, J., Hui, J., Pister, K., Thubert, P.,
          Levis, P., Struik, R., Kelsey, R., Clausen, T., and T.
          Winter, "RPL: IPv6 Routing Protocol for Low power and
          Lossy Networks", draft-ietf-roll-rpl-19 (work in
          progress), March 2011.

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

[RFC6206] Levis, P., Clausen, T., Hui, J., Gnawali, O., and J. Ko,
          "The Trickle Algorithm", RFC 6206, March 2011.

17.2. Informative References

[I-D.ietf-6man-rpl-option]
          Hui, J. and J. Vasseur, "RPL Option for Carrying RPL
          Information in Data-Plane Datagrams",
          draft-ietf-6man-rpl-option-06 (work in progress),
          December 2011.

[I-D.ietf-6man-rpl-routing-header]
          Culler, D., Hui, J., Vasseur, J., and V. Manral, "An IPv6
          Routing Header for Source Routes with RPL",
          draft-ietf-6man-rpl-routing-header-07 (work in progress),
          December 2011.

[I-D.ietf-roll-of0]
          Thubert, P., "RPL Objective Function Zero",
          draft-ietf-roll-of0-20 (work in progress), September 2011.

   [I-D.ietf-roll-p2p-measurement]
              Goyal, M., Baccelli, E., Brandt, A., and J. Martocci, "A
              Mechanism to Measure the Quality of a Point-to-point Route
              in a Low Power and Lossy Network",
              draft-ietf-roll-p2p-measurement-03 (work in progress),
              March 2012.

   [I-D.ietf-roll-terminology]
              Vasseur, J., "Terminology in Low power And Lossy
              Networks", draft-ietf-roll-terminology-06 (work in
              progress), September 2011.

   [RFC5826] Brandt, A., Buron, J., and G. Porcu, "Home Automation
              Routing Requirements in Low-Power and Lossy Networks",
              RFC 5826, April 2010.

   [RFC5867] Martocci, J., De Mil, P., Riou, N., and W. Vermeylen,
              "Building Automation Routing Requirements in Low-Power and
              Lossy Networks", RFC 5867, June 2010.

Authors' Addresses

   Mukul Goyal (editor)
   University of Wisconsin Milwaukee
   3200 N Cramer St
   Milwaukee, WI 53201
   USA

   Phone: +1 414 2295001
   Email: mukul@uwm.edu

   Emmanuel Baccelli
   INRIA

   Phone: +33-169-335-511
   Email: Emmanuel.Baccelli@inria.fr
   URI: http://www.emmanuelbaccelli.org/

   Matthias Philipp
   INRIA

   Phone: +33-169-335-511
   Email: Matthias.Philipp@inria.fr

Anders Brandt
Sigma Designs
Emdrupvej 26A, 1.
Copenhagen, Dk-2100
Denmark

Phone: +45-29609501
Email: abr@sdesigns.dk

Jerald Martocci
Johnson Controls
507 E Michigan St
Milwaukee, WI 53202
USA

Phone: +1 414-524-4010
Email: jerald.p.martocci@jci.com