Internet Engineering Task Force (IETF)
Request for Comments: 6997
Category: Experimental
ISSN: 2070-1721

M. Goyal, Ed.
Univ. of Wisconsin Milwaukee
E. Baccelli
M. Philipp
INRIA
A. Brandt
Sigma Designs
J. Martocci
Johnson Controls

August 2013

Reactive Discovery of Point-to-Point Routes in Low-Power and Lossy Networks

Abstract

This document specifies a point-to-point route discovery mechanism, complementary to the Routing Protocol for Low-power and Lossy Networks (RPL) core functionality. This mechanism allows an IPv6 router to discover "on demand" routes to one or more IPv6 routers in a Low-power and Lossy Network (LLN) such that the discovered routes meet specified metrics constraints.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6997.

Table of Contents

1. Introduction

Targeting Low-power and Lossy Networks (LLNs), the IPv6 Routing Protocol for LLNs (RPL) [RFC6550] provides paths along a Directed Acyclic Graph (DAG) rooted at a single router in the network. Establishment and maintenance of a DAG are performed by routers in the LLN using Destination-Oriented DAG (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 automation [RFC5826] and building automation [RFC5867] applications, due to the following reasons:

- 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.

- 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 (i.e., the RPL functionality described in [RFC6550]) that enables an IPv6 router in the LLN to discover routes to one or more IPv6 routers in the LLN "on demand". The discovered routes may not be the best available but are guaranteed to meet the specified routing metric constraints. Thus, such routes are considered "good enough" from the application's perspective. This reactive P2P route discovery mechanism is henceforth referred to as P2P-RPL.

A mechanism to measure the end-to-end cost of an existing route is specified in [RFC6998]. As discussed in Section 4, measuring the end-to-end cost of an existing route may help in deciding 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 [RFC5826] and commercial building [RFC5867] environments, involves a device (say, a remote control) that suddenly needs to communicate with another device (say, a lamp) to which it does not already have a route (and whose network address it knows a priori). In this case, the remote control must be able to discover a route to the lamp "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. In this case, it is desirable to discover direct routes between various source-destination pairs that do not pass through the DAG's root.

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 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 [RFC6550] and [RFC6554]. Further terminology may be found in [ROLL-TERMS]. 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 direction: The direction from the Origin to the Target.

Reverse direction: The direction from the Target to the Origin.

Forward Route: A route in the Forward direction.

Reverse Route: A route in the Reverse direction.

Bidirectional Route: A route that can be used in both Forward and Reverse directions.

Ingress-only Interface: A network interface that can only receive packets.

Egress-only Interface: A network interface that can only send packets.

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.

RPL Security Configuration: The values for the Counter is Time, Security Algorithm, Key Identifier Mode, and Security Level fields, as defined in Section 6.1 of [RFC6550], inside the Security section of a secure RPL control message.

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 expected transmission count (ETX) along its current route to a Target to be 20 may use "ETX < x*20", where x is a fraction that the Origin chooses, as the constraint. A mechanism to measure the cost of an existing route between two IPv6 routers is specified in [RFC6998]. 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 those available along a global 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 "distance" between the Origin and the Target (in terms of the routing metrics in use), and the prevalent conditions in the network. In general, a P2P-RPL route may be better than the one along a global DAG if the Origin and the Target are nearby. Similarly, a P2P-RPL route may not be much better than the one along a global DAG if the Origin and the Target are far apart. Note that even when P2P-RPL routes are not much better than those along a global DAG, P2P-RPL routes may still be able to avoid

congestion that might occur near the root if the routing takes place only along a global DAG. In general, the cost associated with a P2P-RPL route discovery (in terms of the control messages -- mostly DIOs -- generated) increases with the distance between the Origin and the Target. However, it is possible to limit the cost of route discovery by carefully setting the routing constraints, the Trickle parameters (which govern DIO generation), and the time duration for which a router maintains its membership in the temporary DAG created for the route discovery. A network designer may take into consideration both the benefits (potentially better routes; no need to maintain routes proactively; avoid congestion near the global DAG's root) and costs when using P2P-RPL. The latency associated with a P2P-RPL route discovery again depends on the distance between the Origin and the Target and on the Trickle parameters.

Like core RPL [RFC6550], P2P-RPL operation requires that links have bidirectional reachability. For this reason, the routers participating in a P2P-RPL route discovery must ensure that

- Links that do not have bidirectional reachability do not become part of the route being discovered; and
- IPv6 addresses belonging to Ingress-only (or Egress-only) Interfaces do not become part of the route being discovered.

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. The routes are discovered and installed while the DAG is alive. Once the specified duration of their membership in the DAG is over, the routers leave the DAG, and hence the DAG ceases to exist. However, the installed routes are retained for their specified lifetime (which is different than the specified duration of a router's membership in the DAG) even though the DAG that caused their installation no longer exists. In P2P-RPL, 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-ranked (higher in numerical value) neighbors. Thus, the route discovery messages propagate away from the Origin rather than return to it. As in core RPL, DIO generation at a router is controlled by a Trickle timer [RFC6206], which allows a router to avoid generating unnecessary messages while providing protection against packet loss. P2P-RPL

also uses the routing metrics [RFC6551], Objective Functions, and packet-forwarding framework [RFC6554] [RFC6553] 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 up to four Source Routes per Target. The discovered routes are guaranteed to meet the specified routing metric constraints but may not be the best available. P2P-RPL may fail to discover any route if the specified routing constraints are overly strict.

The Origin initiates a P2P-RPL route discovery by forming a temporary DAG rooted at itself. 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 exactly one P2P Route Discovery Option (P2P-RDO, defined in Section 7) in which the Origin specifies the following information:

- The IPv6 address of a Target. This could be a unicast address or a multicast address. Any additional Targets may be specified by including one or more RPL Target options [RFC6550] inside the DIO.

- 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.

- The desired number of routes (if Source Routes are being discovered).

- Whether the Target(s) should send P2P Discovery Reply Object (P2P-DRO) messages (defined in Section 8) back to the Origin on receiving a DIO message. A P2P-DRO message carries a discovered Source Route back to the Origin or establishes a Hop-by-hop Route between the Origin and the Target.

A P2P-RDO also includes the best route from the Origin that the router, generating the P2P mode DIO, has seen so far.

A P2P mode DIO MAY also carry:

- 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 DIO messages may travel.
- One or more RPL Target options to specify additional unicast or multicast Targets.

As the routers join the temporary DAG, they keep track of the best route(s) (so far from the Origin) 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 contains inside the P2P-RDO a complete Source Route from the Origin to this Target. Since the links in the discovered route have bidirectional reachability (Section 7), the Target may use the discovered route to reach the Origin. Thus, a router that provides a particular service in the LLN (e.g., an outside temperature server) could initiate a P2P-RPL route discovery listing all its potential clients as Targets, thereby allowing the clients to discover a Source Route back to the server. In this case, the Origin (the server) might want to disable the generation of P2P-DRO messages by the Targets (the clients). If the Origin has requested that P2P-DRO messages be sent back, the Target may select the discovered route 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 Route(s) to the Origin via P2P-DRO messages, with one P2P-DRO message carrying one discovered route. On receiving a P2P-DRO message, the Origin stores the discovered route in its memory. This specification allows the Origin to discover up to four Source Routes per Target, thereby allowing the Origin to have sufficient ready-to-use alternatives should one or more of these

routes fail. If a Hop-by-hop Route is being discovered, the Target sends a P2P-DRO message containing the selected route to the Origin. The P2P-DRO message travels back to the Origin along the selected route, establishing state for the Forward Route in the routers on the path.

The Target may request that the Origin acknowledge the receipt of a P2P-DRO message by sending back a P2P-DRO Acknowledgement (P2P-DRO-ACK) message (defined in Section 10). The Origin unicasts a P2P-DRO-ACK message to the Target. If the Target does not receive the requested P2P-DRO-ACK within a certain time interval of sending a P2P-DRO, it resends the P2P-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 P2P-DRO message to let the nodes in the LLN know about the completion of the route discovery process. The routers receiving such a P2P-DRO should not generate any more DIOs for this temporary DAG, nor should they process any received DIOs for this temporary DAG in the future. However, such routers must still process the P2P-DROs received for this temporary DAG.

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. 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 exactly one P2P Route Discovery Option (P2P-RDO, specified in Section 7).

6.1. Setting a P2P Mode DIO

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

- RPLInstanceID: RPLInstanceID MUST be a local value as described in Section 5.1 of [RFC6550]. The Origin chooses the RPLInstanceID to be used for a particular route discovery in accordance with the following rules:
  - The Origin SHOULD NOT reuse a RPLInstanceID for a route discovery if some routers might still maintain membership in the DAG that the Origin had initiated for the previous route discovery using this RPLInstanceID. As described in Section 7,

a router's membership in a DAG created for a P2P-RPL route discovery lasts for the time duration (say, 't' seconds) indicated by the L field inside the P2P-RDO. In general, there is no upper bound on the time duration by when all the routers have left the DAG created for a P2P-RPL route discovery. In the specific case where the discovered route must be at most 'n' hops in length, all the routers must have left the DAG "(n+1)*t" seconds after its initiation by the Origin. In practice, all the routers should have joined the DAG within 't' seconds of its initiation (since the route discovery must complete while the Origin still belongs to the DAG), and hence all the routers should have left the DAG within "2*t" seconds of its initiation. Hence, it is usually sufficient that the Origin wait for twice the duration indicated by the L field inside the P2P-RDO used for the previous route discovery before reusing the RPLInstanceID for a new route discovery. Individual P2P-RPL deployments are encouraged to share their experience with various RPLInstanceID reuse policies to help guide the development of a Standards Track version of the protocol.

* When initiating a new route discovery to a particular Target, the Origin MUST NOT reuse the RPLInstanceID used in a previous route discovery to this Target if the state created during the previous route discovery might still exist in some routers. Note that it is possible that the previous route discovery did not succeed yet some routers still ended up creating state. The Default Lifetime and Lifetime Unit parameters in the DODAG Configuration Option specify the lifetime of the state that the routers, including the Origin and the Target, maintain for a Hop-by-hop or Source Route discovered using P2P-RPL. Suppose this lifetime is 'X' seconds. As discussed above, any state created during the previous route discovery was likely created within "2*t" seconds of its initiation. Hence, it is sufficient that the Origin lets a time duration equal to "X+2*t" seconds pass since the initiation of the previous route discovery before initiating a new route discovery to the same Target using the same RPLInstanceID.

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

- Grounded (G) Flag: This flag MUST be set to one. Unlike a global RPL instance, the concept of a floating DAG, used to provide connectivity within a sub-DAG detached from a grounded DAG, does not apply to a local RPL instance. Hence, an Origin MUST always set the G flag to one when initiating a P2P-RPL route discovery.

Further, item 3 of Section 8.2.2.2 in [RFC6550] does not apply, and a node MUST NOT initiate a new DAG if it does not have any parent left in a P2P-RPL DAG.

- Mode of Operation (MOP): This field MUST be set to four, corresponding to P2P Route Discovery mode.
- Destination Advertisement Trigger Sequence Number (DTSN): This field MUST be set to zero on transmission and ignored on reception.
- DODAGPreference (Prf): This field MUST be set to zero (least preferred).
- DODAGID: This field MUST be set to an IPv6 address of the Origin.
- The other fields in the DIO Base object can be set in the desired fashion as per the rules described in [RFC6550].

A received P2P mode DIO MUST be discarded if it does not follow the above-listed rules regarding the RPLInstanceID, Version Number, G flag, MOP, and Prf fields inside the Base object.

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

- The Origin MUST set the MaxRankIncrease parameter to zero to disable local repair of the temporary DAG. A received P2P mode DIO MUST be discarded if the MaxRankIncrease parameter inside the DODAG Configuration Option is not zero.
- The Origin SHOULD set the Trickle parameters (DIOIntervalDoublings, DIOIntervalMin, DIORedundancyConstant) as recommended in Section 9.2.
- The Origin sets the Default Lifetime and Lifetime Unit parameters to indicate the lifetime of the state that the routers, including the Origin and the Target(s), maintain for a Hop-by-hop or Source Route discovered using P2P-RPL.
- The Origin sets the other fields in the DODAG Configuration Option, including the Objective Code Point (OCP) identifying the Objective Function, in the desired fashion as per the rules described in [RFC6550].

- As discussed in Section 14, P2P-RPL does not distinguish between the "preinstalled" and "authenticated" security modes described in [RFC6550]. Consequently, the Origin MUST set the Authentication Enabled (A) flag to zero. A received P2P mode DIO MUST be discarded if the A flag inside the DODAG Configuration Option is not zero.

- An Intermediate Router (or a Target) MUST set various fields in the DODAG Configuration Option in the outgoing P2P mode DIOs to the values they had in the incoming P2P mode DIOs for this DAG.

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

- Authentication Enabled: 0

- DIOIntervalMin: 6, which translates to 64 ms as the value for the Imin parameter in a Trickle operation. This value is roughly one order of magnitude larger than the typical transmission delay on IEEE 802.15.4 links and corresponds to the recommendation in Section 9.2 for well-connected topologies.

- DIORedundancyConstant: 1. See the discussion in Section 9.2.

- MaxRankIncrease: 0 (to disable local repair of the temporary DAG).

- Default Lifetime: 0xFF, to correspond to infinity.

- Lifetime Unit: 0xFFFF, to correspond to infinity.

- Objective Code Point: 0, i.e., OF0 [RFC6552] is the default Objective Function (OF).

- The remaining parameters have default values as specified in [RFC6550].

Individual P2P-RPL deployments are encouraged to share their experience with these default values to help guide the development of a Standards Track version of the protocol.

The routing metrics and constraints [RFC6551] used in P2P-RPL route discovery are included in one or more Metric Container options [RFC6550] 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-RDO.

A P2P mode DIO:

- MUST carry one (and only one) P2P-RDO. The P2P-RDO allows for the specification of one unicast or multicast address for the Target. A received P2P mode DIO MUST be discarded if it does not contain exactly one P2P-RDO.

- MAY carry one or more RPL Target options to specify additional unicast/multicast addresses for the Target. If a unicast address is specified, it MUST be a global address or a unique-local address.

- MAY carry one or more Metric Container options to specify routing metrics and constraints.

- MAY carry one or more Route Information Options [RFC6550]. In the context of P2P-RPL, a Route Information Option advertises to the Target(s) the Origin's connectivity to the prefix specified in the option.

- MAY carry one DODAG Configuration Option. If a P2P mode DIO does not carry an explicit DODAG Configuration Option, the default DODAG Configuration Option defined in this section is considered to be in effect.

A RPL option other than those listed above MUST be ignored when found inside a received P2P mode DIO and MUST NOT be included in the P2P mode DIOs that the receiving router generates.

In accordance with core RPL, a P2P mode DIO MUST propagate via link-local multicast. The IPv6 source address in a P2P mode DIO MUST be a link-local address, and the IPv6 destination address MUST be the link-local multicast address all-RPL-nodes [RFC6550]. A P2P mode DIO MUST be transmitted on all interfaces the router has in this RPL routing domain [RFC6554].

7. P2P Route Discovery Option (P2P-RDO)

This section defines a new RPL control message option: the P2P Route Discovery Option (P2P-RDO).

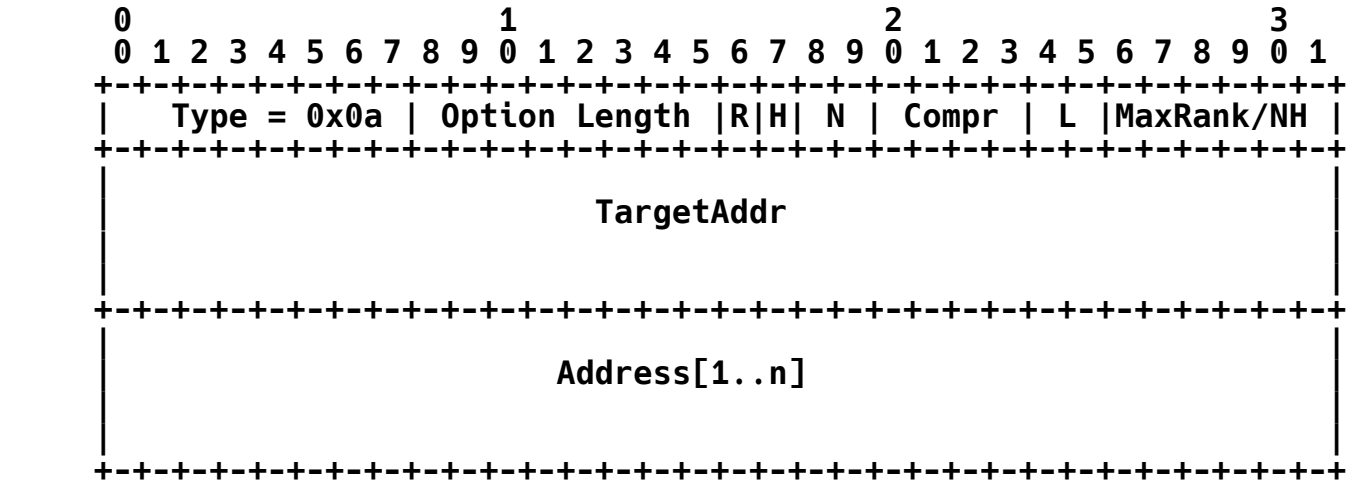

Figure 1: Format of the P2P Route Discovery Option (P2P-RDO)

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

- Option Type: 0x0a.
- Option Length: This field is an 8-bit unsigned integer representing the length in octets of the option, not including the Option Type and Option Length fields.
- Reply (R): The Origin sets this flag to one to allow the Target(s) to send P2P-DRO messages back to the Origin. If this flag is set to zero, a Target MUST NOT generate any P2P-DRO messages.
- 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 Reverse direction.

- Number of Routes (N): This field is valid only if the R flag is set to one and the H flag is set to zero, i.e., the Targets are allowed to generate P2P-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.

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

- Lifetime (L): This is a 2-bit field that indicates the exact duration that a router joining the temporary DAG, including the Origin and the Target(s), MUST maintain its membership in the DAG. A router MUST leave the temporary DAG once the time elapsed since it joined reaches the value indicated by this field. The mapping between the value in this field and the duration of the router's membership in 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 route discovery to complete, which includes the time required for the DIOs to reach the Target(s) and the P2P-DROs to travel back to the Origin. The time required for the DIOs to reach the Target(s) would in turn depend on the Trickle parameters (Imin and the redundancy constant) as well as the expected distance (in terms of hops and/or ETX) to the Target(s). While deciding on the value in this field, the Origin should also take into account the fact that all routers joining the temporary DAG would need to stay in the DAG for this much time.

- 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 [RFC6550]) 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 of 0 in this field indicates that the MaxRank is infinity.
  - When a P2P-RDO is included in a P2P-DRO message, this field indicates the index of the next-hop (NH) address inside the Address vector.
- TargetAddr: This is 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 address. If a unicast address is specified, it MUST be a global address or a unique-local address. Any additional Target addresses can be specified by including one or more RPL Target options [RFC6550] in the DIO. When the P2P-RDO is included in a P2P-DRO, this field MUST contain a unicast global or unique-local IPv6 address of the Target generating the P2P-DRO.
- Address[1..n]: This is a vector of IPv6 addresses representing a complete route so far in the Forward direction:
  - Each element in the Address vector has size (16 - Compr) octets and MUST contain a valid global or unique-local IPv6 address with the 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 address that a router adds to the vector MUST belong to the interface on which the router received the DIO containing this P2P-RDO. Further, this interface MUST NOT be an Ingress-only Interface. This allows the route accumulated in the Address vector to be a Bidirectional Route that can be used by a Target to send a P2P-DRO message 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 none of its addresses already exist in the vector. A Target 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.

8. The P2P Discovery Reply Object (P2P-DRO)

This section defines two new RPL control message types: the P2P Discovery Reply Object (P2P-DRO), with code 0x04; and the Secure P2P-DRO, with code 0x84. A P2P-DRO serves one of the following functions:

- carries a discovered Source Route from a Target to the Origin;
- establishes a Hop-by-hop Route as it travels from a Target to the Origin.

A P2P-DRO message can also 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 P2P-DRO message MUST carry one (and only one) P2P-RDO whose TargetAddr field MUST contain a unicast IPv6 address of the Target that generates the P2P-DRO. A P2P-DRO message MUST travel from the Target to the Origin via link-local multicast along the route specified inside the Address vector in the P2P-RDO, as included in the P2P-DRO. The IPv6 source address in a P2P-DRO message MUST be a link-local address, and the IPv6 destination address MUST be the link-local multicast address all-RPL-nodes [RFC6550]. A P2P-DRO message MUST be transmitted on all interfaces the router has in this RPL routing domain [RFC6554].

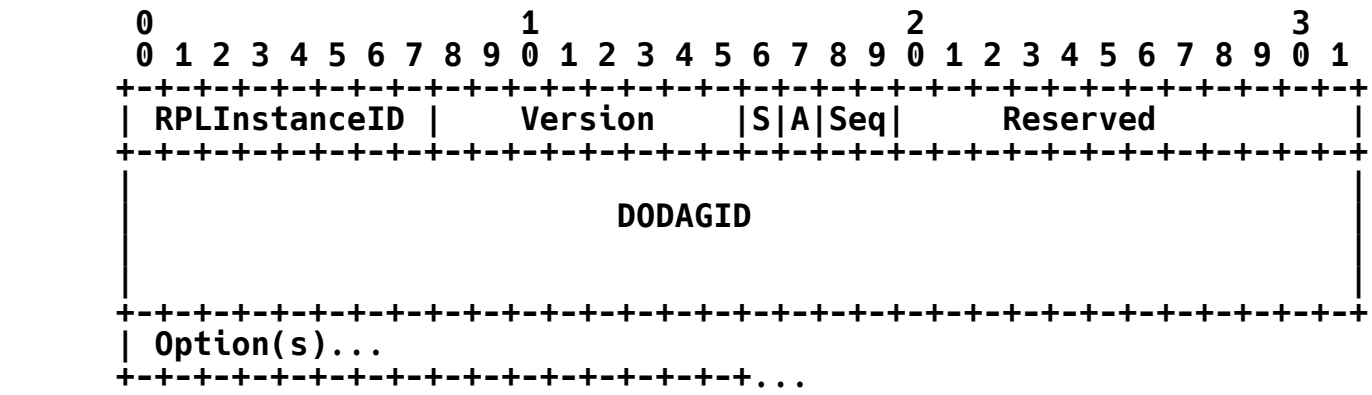

Figure 2: Format of the Base P2P Discovery Reply Object (P2P-DRO)

The format of the base P2P Discovery Reply Object (P2P-DRO) is shown in Figure 2. A base P2P-DRO consists of the following fields:

- RPLInstanceID: This field provides the RPLInstanceID of the temporary DAG used for route discovery.

- Version: This field provides 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.

- 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 P2P-DRO, including those not listed in the route carried inside a 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 transmissions for this temporary DAG.

  Note that the Stop flag serves to stop further DIO generation/processing for a P2P-RPL route discovery but does not affect the processing of P2P-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 P2P-DRO messages even if an earlier P2P-DRO message (with the same RPLInstanceID and DODAGID fields) had the Stop flag set to one. When set to zero, this flag does not imply anything and MUST be ignored on reception.

- Ack Required (A): This flag, when set to one by the Target, indicates that the Origin MUST unicast a P2P-DRO-ACK message (defined in Section 10) to the Target when it receives the P2P-DRO.

- Sequence Number (Seq): This 2-bit field indicates the sequence number for the P2P-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 P2P-DRO. The Origin includes the RPLInstanceID, the DODAGID, and the Sequence Number of the received P2P-DRO inside the P2P-DRO-ACK message it sends back to the Target.

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

- DODAGID: This field provides 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 advertising the temporary DAG.

- Options: The P2P-DRO message:

  * MUST carry one (and only one) P2P-RDO that MUST specify a complete route between the Target and the Origin. A received P2P-DRO message MUST be discarded if it does not contain exactly one P2P-RDO.

  * MAY carry one or more Metric Container options that contain the aggregated routing metrics values for the route specified in the P2P-RDO.

  A RPL option other than those listed above MUST be ignored when found inside a received P2P-DRO message.

8.1. Secure P2P-DRO

A Secure P2P-DRO message follows the format shown in Figure 7 of [RFC6550], where the base format is the base P2P-DRO shown in Figure 2.

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

A P2P Discovery Reply Object MUST carry one (and only one) P2P-RDO, which MUST be set as defined in Section 7. Specifically, the following fields MUST be set as follows:

- Reply (R): This flag MUST be set to zero on transmission and ignored on reception.
- Hop-by-Hop (H): The H flag in the P2P-RDO included in a P2P-DRO message MUST have the same value as the H flag in the P2P-RDO inside the corresponding DIO message.
- Number of Routes (N): This field MUST be set to zero on transmission and ignored on reception.
- Lifetime (L): This field MUST be set to zero on transmission and ignored on reception.
- MaxRank/NH: This field indicates the index of the next-hop address in the Address vector. When a Target generates a P2P-DRO message, the NH field is set to n = (Option Length - 2 - (16 - Compr))/(16 - Compr).
- TargetAddr: This field MUST contain a unicast global or unique-local IPv6 address of the Target generating the P2P-DRO.
- 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 that purpose. When a router joins a temporary DAG advertised by a P2P mode DIO, it MUST maintain its membership in the temporary DAG for the duration indicated by the L field inside 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 data packets. In other words, joining a temporary DAG does not allow a router to provision routing table

entries listing the router's parents in the temporary DAG as the next hops (i.e., the last bullet point in Section 3.2.8 of [RFC6550] is not applicable when the DAG is a temporary DAG created for the purpose of a P2P-RPL route discovery).

Given the nature of a temporary DAG created for a P2P-RPL route discovery, this document disallows the solicitation of P2P mode DIOs using DODAG Information Solicitation (DIS) messages as described in [RFC6550]. A router participating in a P2P-RPL route discovery MUST NOT reset its Trickle timer, which controls the transmission of P2P mode DIOs in response to a multicast DIS. Also, the router MUST NOT send a P2P mode DIO in response to a unicast DIS. In other words, the rules in Section 8.3 of [RFC6550] regarding a router's response to a multicast/unicast DIS are not applicable for P2P mode DIOs.

A router MUST detach from the temporary DAG created for a P2P-RPL route discovery once the duration of its membership in the DAG has reached the value indicated by the L field inside the P2P-RDO. After receiving a P2P-DRO with the Stop flag set to one, a router SHOULD NOT send or process any more DIOs for this temporary DAG and SHOULD also cancel any pending DIO transmissions.

9.2. Trickle Operation for P2P Mode DIOs

A 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 LLNs. When controlling the transmissions of a P2P mode DIO, a Trickle timer SHOULD follow the following rules:

- 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.

- 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.

- 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 the 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 transmissions yet.

- 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.

- The Imin parameter SHOULD be set taking into account the connectivity within the network. For highly connected networks, a small Imin value (on 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 the 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. Since the route discovery must complete while the Origin still belongs to the temporary DAG created for that purpose, the Origin should set the time duration for which a router maintains its membership in the temporary DAG (indicated by the L field inside the P2P-RDO) to a large enough value, taking into account the Imin value as well as the expected distance (in terms of hops and/or ETX) to the Target(s).

- 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 the resetting of the Trickle timer duration to the Imin value. Given the temporary nature of the DAGs used in P2P-RPL, the Trickle timer may not get a chance to increase much.

- 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. However, this setting may result in an increase in the time required for the route discovery process to complete. A higher value for the redundancy constant may be more suitable in

  * environments with high packet loss rates; or

  * deployments where the time required for the route discovery process to complete needs to be as small as possible; or

  * deployments where specific destinations are reachable only through specific Intermediate Routers (and hence these Intermediate Routers should not suppress their DIOs).

  A particular deployment should take into account the above-mentioned factors when deciding on the value of the redundancy constant.

Individual P2P-RPL deployments are encouraged to share their experience with these rules to help guide the development of a Standards Track version of the protocol. Applicability Statements that specify the use of P2P-RPL MUST provide guidance for setting Trickle parameters, particularly Imin and the redundancy constant.

9.3. Processing a P2P Mode DIO

The rules for DIO processing and transmission as described in Section 8 of RPL [RFC6550] apply to P2P mode DIOs as well, except as modified in this document. In particular, in accordance with Section 8.2.3 of RPL [RFC6550], a received P2P mode DIO MUST be discarded if it is malformed, according to the rules specified in this document and in [RFC6550].

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 into account the metric's value in both Forward and Reverse directions. Bidirectional reachability along a discovered route allows the Target to use this route to reach the Origin. In particular, the P2P-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:

- if the DIO advertises INFINITE_RANK as defined in Section 17 of [RFC6550]
- if the integer part of the rank advertised in the DIO equals or exceeds the MaxRank limit listed in the P2P Route Discovery Option
- if the routing metric values do not satisfy one or more of the mandatory route constraints listed in the DIO or if the router cannot evaluate the mandatory route constraints, e.g., if the router does not support the metrics used in the constraints
- if the router previously received a P2P-DRO message with the 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 DIO is received on an Ingress-only Interface; or
- if the receiving interface does not have a global or unique-local IPv6 address configured with the address prefix implied by the Compr field in the P2P-RDO inside the received DIO; or
- if the router cannot uniquely identify the address prefix implied by the Compr field in the P2P-RDO (this might happen if the receiving interface has multiple global/unique-local IPv6 addresses, each configured with a different address prefix); or
- if adding its IPv6 address to the route in the Address vector inside the P2P-RDO would result in the route containing multiple addresses belonging to this router.

On receiving a P2P mode DIO, an Intermediate Router MUST do the following. The 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 the 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 [RFC6550]. If the received DIO would allow the router to advertise a better route, the router MUST add a unicast IPv6 address of the receiving interface (after eliding Compr prefix octets) to the route in the Address vector inside the P2P-RDO and remember this route for inclusion in its future DIOs.

When an Intermediate Router adds an IPv6 address to a route, it MUST ensure that

- the IPv6 address is a unicast global or unique-local IPv6 address assigned to the interface on which the DIO containing the route was received;
- the IPv6 address was configured with the address prefix implied by the Compr field in the P2P-RDO inside the received DIO.

To improve the diversity of the routes being discovered, an Intermediate Router SHOULD keep track of multiple routes (as long as all these routes are the best seen so far), one of which SHOULD be selected in a uniform random manner for inclusion in the P2P-RDO

inside the router's next DIO. Note that the route accumulation in a P2P mode DIO MUST take place even if the Origin does not want any P2P-DRO messages to be generated (i.e., the R flag inside the P2P-RDO is set to zero). This is because the Target may still be able to use the accumulated route as a Source Route to reach the Origin.

9.5. Additional Processing of a P2P Mode DIO at the Target

The Target MAY remember the discovered route contained in the P2P-RDO in the received DIO for use as a Source Route to reach the Origin. The lifetime of this Source Route is specified by the Default Lifetime and Lifetime Unit parameters inside the DODAG Configuration Option currently in effect. This lifetime can be extended (or shortened) appropriately, following a hint from an upper-layer protocol.

If the Reply flag inside the P2P-RDO in the received DIO is set to one, the Target MUST select one or more discovered routes and send one or more P2P-DRO messages, carrying one discovered route each, back to the Origin. If the H flag inside the P2P-RDO is set to one, the Target needs to select one route and send a P2P-DRO message along this route back to the Origin. As this P2P-DRO message travels back to the Origin, the routers on the path establish a hop-by-hop routing state, thereby establishing a Hop-by-hop Route in the Forward direction. If the H flag is set to zero, the number of Source Routes to be selected (and the number of P2P-DRO messages to be sent back) is given by one plus the value of the N field in the P2P-RDO. The Target may select the discovered route inside the received DIO as one or more of the routes that would be carried inside a P2P-DRO message back to the Origin. 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 of routes has 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 P2P-DRO message back to the Origin (identified by the DODAGID field in the DIO). The P2P-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 P2P-DRO message to one if it desires the Origin to send back a P2P-DRO-ACK message on receiving the P2P-DRO. In this case, the Target waits for the duration of P2P_DRO_ACK_WAIT_TIME for the P2P-DRO-ACK message to arrive. Failure to receive the P2P-DRO-ACK message within this time duration causes the Target to retransmit the

P2P-DRO message. The Target MAY retransmit the P2P-DRO message in this fashion up to MAX_P2P_DRO_RETRANSMISSIONS times. Both P2P_DRO_ACK_WAIT_TIME and MAX_P2P_DRO_RETRANSMISSIONS are configurable parameters to be chosen based on the characteristics of individual deployments. Note that all P2P-DRO transmissions and retransmissions MUST take place while the Target is still a part of the temporary DAG created for the route discovery. A Target MUST NOT transmit a P2P-DRO if it no longer belongs to this DAG.

The Target MAY set the Stop flag inside the P2P-DRO message to one if

- 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 TargetAddr inside the P2P-RDO with no additional Targets specified via RPL Target options; and

- the Target has already selected the desired number of routes.

The Target MAY include a Metric Container option in the P2P-DRO message. This Metric Container contains the end-to-end routing metric values for the route specified in the P2P-RDO. The Target MUST transmit the P2P-DRO message via a link-local multicast.

A Target MUST NOT forward a P2P mode DIO any further if no other Targets are to be discovered, i.e., if a unicast IPv6 address (of this Target) is specified as the TargetAddr inside the P2P-RDO and no additional Targets are specified via RPL Target options inside the DIOs for this route discovery. Otherwise, the Target MUST generate DIOs for this route discovery as an Intermediate Router would.

9.6. Processing a P2P-DRO at an Intermediate Router

If the DODAGID field in the received P2P-DRO does not list a router's own IPv6 address, the router considers itself an Intermediate Router and MUST process the received message in the following manner:

- The router MUST discard the received P2P-DRO with no further processing if it does not belong to the temporary DAG identified by the RPLInstanceID and the DODAGID fields in the P2P-DRO.

- If the Stop flag inside the received P2P-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 transmissions.

- The router MUST ignore any Metric Container options contained in the P2P-DRO message.

- If an Address[NH] element inside the P2P-RDO lists the router's own unicast IPv6 address, the router is a part of the route carried in the P2P-RDO. In this case, the router MUST do the following:
  - To prevent loops, the router MUST discard the P2P-DRO message with no further processing if the Address vector in the P2P-RDO includes multiple IPv6 addresses assigned to the router's interfaces.
  - If the H flag inside the P2P-RDO is set to 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 P2P-DRO
    - the route's destination, the Target (identified by the TargetAddr field inside the P2P-RDO)
    - the IPv6 address of the next hop, Address[NH+1] (unless the NH value equals the number of elements in the Address vector, in which case the Target itself is the next hop)

    This Hop-by-hop routing state MUST expire at the end of the lifetime specified by the Default Lifetime and Lifetime Unit parameters inside the DODAG Configuration Option used in P2P mode DIOs for this route discovery.
  - If the router already maintains a Hop-by-hop state listing the Target as the destination and carrying the same RPLInstanceID and DODAGID fields as the received P2P-DRO, and the next-hop information in the state does not match the next hop indicated in the received P2P-DRO, the router MUST discard the P2P-DRO message with no further processing. Note that this situation would occur in the following two cases:
    - When the route listed in the Address vector inside the P2P-RDO contains a previously undetected loop. In this case, this rule causes the P2P-DRO messages to be discarded.
    - When a Hop-by-hop Route between the Origin and the Target, previously established using the same RPLInstanceID and DODAGID as the route currently being established, still exists and at least partially overlaps the route currently being established.
  - The router MUST decrement the NH field inside the P2P-RDO and send the P2P-DRO message further via link-local multicast.

9.7. Processing a P2P-DRO at the Origin

When a router receives a P2P-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, notes the Target that originated this message (from the TargetAddr field inside the P2P-RDO), and processes the message in the following manner:

- The Origin MUST discard the received P2P-DRO with no further processing if it no longer belongs to the temporary DAG identified by the RPLInstanceID and the DODAGID fields in the P2P-DRO.

- If the Stop flag inside the received P2P-DRO is set to one, the Origin SHOULD NOT generate any more DIOs for this temporary DAG and SHOULD cancel any pending DIO transmissions.

- If the P2P-RDO inside the P2P-DRO has the H flag set to zero, the Address vector inside the P2P-RDO contains a Source Route to this Target. The Origin MUST set the lifetime of this Source Route to the value specified by the Default Lifetime and Lifetime Unit parameters inside the DODAG Configuration Option in the P2P mode DIOs used for this route discovery. This lifetime could be extended (or shortened) appropriately, following a hint from an upper-layer protocol.

- If the P2P-RDO inside the P2P-DRO has the H flag set to one, the P2P-DRO message is establishing a Hop-by-hop Route to this Target, and the Origin MUST store in its memory the state for this Hop-by-hop Route in the manner described in Section 9.6. This Hop-by-hop routing state MUST expire at the end of the lifetime specified by the Default Lifetime and Lifetime Unit parameters inside the DODAG Configuration Option used in P2P mode DIOs for this route discovery. A Standards Track version of P2P-RPL may consider specifying a signaling mechanism that will allow the Origin to extend (or shorten) the lifetime of a P2P-RPL Hop-by-hop Route, following a suitable hint from an upper-layer protocol.

- If the received P2P-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 this Target.

- If the A flag is set to one in the received P2P-DRO message, the Origin MUST generate a P2P-DRO-ACK message as described in Section 10 and unicast the message to the Target. The Origin MAY use the route just discovered to send the P2P-DRO-ACK message to the Target. Section 12 describes how a packet may be forwarded along a Source/Hop-by-hop Route discovered using P2P-RPL.

10. The P2P Discovery Reply Object Acknowledgement (P2P-DRO-ACK)

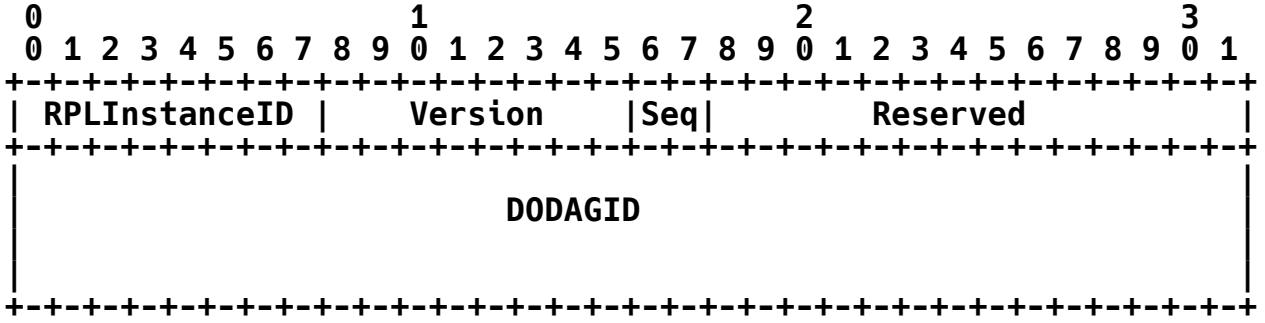

Figure 3: Format of the Base P2P Discovery Reply Object Acknowledgement (P2P-DRO-ACK)

A P2P-DRO message may fail to reach the Origin due to a number of reasons. Unlike the DIO messages, which benefit from Trickle-controlled retransmissions, the P2P-DRO messages are prone to loss due to unreliable packet transmission in LLNs. Since a P2P-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 P2P-DRO message (e.g., because of its inability to store the state for the Hop-by-hop Route that the P2P-DRO is establishing). To protect against the potential failure of a P2P-DRO message to reach the Origin, the Target MAY request that the Origin send back a P2P-DRO Acknowledgement (P2P-DRO-ACK) message on receiving a P2P-DRO message. Failure to receive such an acknowledgement within the P2P_DRO_ACK_WAIT_TIME interval of sending the P2P-DRO message forces the Target to resend the message (as described in Section 9.5).

This section defines two new RPL control message types: the P2P-DRO Acknowledgement (P2P-DRO-ACK), with code 0x05; and the Secure P2P-DRO-ACK, with code 0x85. A P2P-DRO-ACK message MUST travel as a unicast message from the Origin to the Target. The IPv6 source and destination addresses used in a P2P-DRO-ACK message MUST be global or unique-local. The format of a base P2P-DRO-ACK message is shown in Figure 3. Various fields in a P2P-DRO-ACK message MUST have the same values as the corresponding fields in the P2P-DRO message. The field marked as "Reserved" MUST be set to zero on transmission and MUST be

ignored on reception. A Secure P2P-DRO-ACK message follows the format shown in Figure 7 of [RFC6550], where the base format is the same as the base P2P-DRO-ACK shown in Figure 3.

11. Secure P2P-RPL Operation

Each RPL control message type, including those defined in this document, has a secure version. A secure RPL control message is identified by the value 1 in the most significant bit of the Code field. Each secure RPL control message contains a Security section (see Figures 7 and 8 of [RFC6550]) whose contents are described in Section 6.1 of [RFC6550]. Sections 6.1, 10, and 19 of [RFC6550] describe core RPL's security apparatus. These sections are applicable to P2P-RPL's secure operation as well, except as constrained in this section.

Core RPL allows a router to decide locally on a per-packet basis whether to use security and, if yes, what Security Configuration (see definition in Section 3) to use (the only exception being the requirement to send a Secure DIO in response to a Secure DIS; see Section 10.2 of [RFC6550]). In contrast, this document requires that routers participating in a P2P-RPL route discovery follow the Origin's lead regarding security. The Origin decides whether to use security, and the particular Security Configuration to be used for this purpose. All the routers participating in this route discovery MUST generate only secure control messages if the Origin so decides and MUST use for this purpose the Security Configuration that the Origin chose. The Origin MUST NOT set the "Key Identifier Mode" field inside the chosen Security Configuration to value 1, since this setting indicates the use of a per-pair key, which is not suitable for securing messages that travel by (link-local) multicast (e.g., DIOs) or that travel over multiple hops (e.g., P2P-DROs). The Origin MUST use the chosen Security Configuration to secure all the control messages (DIOs and P2P-DRO-ACKs) it generates.

A router MUST NOT join the temporary DAG being created for a P2P-RPL route discovery if:

- it receives both secure and unsecure DIOs or Secure DIOs with different Security Configurations pertaining to this route discovery (i.e., referring to the same RPLInstanceID and DODAGID combination) prior to joining; or
- it cannot use the Security Configuration found in the Secure DIOs pertaining to this route discovery.

When a router (an Intermediate Router or a Target) joins a temporary DAG being created using Secure DIOs, it MUST remember the common Security Configuration used in the received Secure DIOs and MUST use this configuration to secure all the control messages (DIOs and P2P-DROs) it generates.

If an Intermediate Router (or a Target) encounters a control message (a DIO or a P2P-DRO or a P2P-DRO-ACK) pertaining to this route discovery that is either not secure or does not follow the Security Configuration the router remembers for this route discovery, the router MUST enter the "lock down" mode for the remainder of its stay in this temporary DAG. An Intermediate Router (or a Target) in the "lock down" mode MUST NOT generate or process any control messages (irrespective of the Security Configuration used) pertaining to this route discovery. If the Origin receives a control message (a P2P-DRO) that does not follow the Security Configuration the Origin has chosen for this route discovery, it MUST discard the received message with no further processing.

12. Packet Forwarding along a Route Discovered Using P2P-RPL

An Origin uses the Source Routing Header (SRH) [RFC6554] 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 includes a RPL option [RFC6553] 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 infers 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.

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, a 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 that a router 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

In general, the security considerations for the operation of P2P-RPL are similar to those for the operation of RPL (as described in Section 19 of the RPL specification [RFC6550]). Sections 6.1 and 10 of [RFC6550] describe RPL's security framework, which provides data confidentiality, authentication, replay protection, and delay protection services. This security framework can also be used in P2P-RPL after taking into account the constraints specified in Section 11. P2P-RPL requires that all routers participating in a secure route discovery use the Security Configuration chosen by the Origin. The intention is to avoid compromising the overall security of a route discovery due to some routers using a weaker Security Configuration. With the "lock down" mechanism as described in Section 11 in effect, it is unlikely that an Origin would accept a route discovered under a Security Configuration other than the one it intended. Any attempt to use a different Security Configuration (than the one the Origin intended) is likely to result, in the worst case, in the failure of the route discovery process. In the best-case scenario, any such attempt by a rogue router would result in its neighbors entering the "lock down" mode and acting as firewalls to allow the route discovery to proceed in the remaining network.

The RPL specification [RFC6550] describes three modes of security: unsecured, preinstalled, and authenticated. In the unsecured mode, secure control messages are not used, and the only available security is the security provided by the link-layer protocols. In the preinstalled mode, all the nodes use a preinstalled group key to join a secure DAG as the "routers" or "hosts", where the term "router" means a node that is capable of forwarding packets received from its parents or children in the DAG, and the term "host" refers to nodes that cannot function as "routers". In the authenticated mode, the nodes can join a secure DAG as "hosts" using the preinstalled key but then need to authenticate themselves to a key server to obtain the key that will allow them to work as "routers". The temporary DAG created for a P2P-RPL discovery cannot be used for routing packets. Hence, it is not meaningful to say that a node joins this DAG as a "router" or a "host" in the sense defined above. Hence, in P2P-RPL, there is no distinction between the preinstalled and authenticated modes. A router can join a temporary DAG created for a secure P2P-RPL route discovery only if it can support the Security Configuration in use, which also specifies the key in use. It does not matter whether the key is preinstalled or dynamically acquired. The router must have the key in use before it can join the DAG being created for a secure P2P-RPL route discovery.

If a rogue router can support the Security Configuration in use (in particular, if it knows the key in use), it can join the secure P2P-RPL route discovery and cause various types of damage. Such a rogue router could advertise false information in its DIOs in order to include itself in the discovered route(s). It could generate bogus P2P-DRO messages carrying bad routes or maliciously modify genuine P2P-DRO messages it receives. A rogue router acting as the Origin could launch denial-of-service attacks against the LLN deployment by initiating fake P2P-RPL route discoveries; in this type of scenario, RPL's authenticated mode of operation, where a node can obtain the key to use for a P2P-RPL route discovery only after proper authentication, would be useful.

Since a P2P-DRO message travels along a Source Route specified inside the message, some of the security concerns that led to the deprecation of Type 0 routing headers [RFC5095] may apply. To avoid the possibility of a P2P-DRO message traveling in a routing loop, this document requires that each Intermediate Router confirm that the Source Route listed inside the message does not contain any routing loop involving itself before the router could forward the message further. As specified in Section 9.6, this check involves the router making sure that its IPv6 addresses do not appear multiple times inside the Source Route with one or more other IPv6 addresses in between.

15. IANA Considerations

15.1. Additions to Mode of Operation

This document defines a new Mode of Operation, entitled "P2P Route Discovery Mode of Operation" (see Section 6), assigned a value of 4 from the "Mode of Operation" space [RFC6550].

Value	Description	Reference
4	P2P Route Discovery Mode of Operation	This document

Mode of Operation

15.2. Additions to RPL Control Message Options

This document defines a new RPL option: "P2P Route Discovery" (see Section 7), assigned a value of 0x0a from the "RPL Control Message Options" space [RFC6550].

Value	Meaning	Reference
0x0a	P2P Route Discovery	This document

RPL Control Message Options

15.3. Additions to RPL Control Codes

This document defines the following new RPL messages:

- "P2P Discovery Reply Object" (see Section 8), assigned a value of 0x04 from the "RPL Control Codes" space [RFC6550].
- "Secure P2P Discovery Reply Object" (see Section 8.1), assigned a value of 0x84 from the "RPL Control Codes" space [RFC6550].
- "P2P Discovery Reply Object Acknowledgement" (see Section 10), assigned a value of 0x05 from the "RPL Control Codes" space [RFC6550].
- "Secure P2P Discovery Reply Object Acknowledgement" (see Section 10), assigned a value of 0x85 from the "RPL Control Codes" space [RFC6550].

Code	Description	Reference
0x04	P2P Discovery Reply Object	This document
0x84	Secure P2P Discovery Reply Object	This document
0x05	P2P Discovery Reply Object Acknowledgement	This document
0x85	Secure P2P Discovery Reply Object Acknowledgement	This document

RPL Control Codes

16. Known Issues and Future Work

This document is presented as an Experimental specification to facilitate P2P-RPL's deployment in LLN scenarios where reactive P2P route discovery is considered useful or necessary. It is anticipated that, once sufficient operational experience has been gained, this specification will be revised to progress it on to the Standards Track. Experience reports regarding P2P-RPL implementation and deployment are encouraged, particularly with respect to:

- Secure P2P-RPL operation (Section 11);
- Rules governing Trickle operation (Section 9.2);
- Values in the default DODAG Configuration Option (Section 6.1);
- The RPLInstanceID reuse policy (Section 6.1);
- Utility and implementation complexity of allowing multiple Target addresses in a P2P-RPL route discovery.

17. Acknowledgements

The authors gratefully acknowledge the contributions of the following individuals (in alphabetical order) in the development of this document: Dominique Barthel, Jakob Buron, Cedric Chauvenet, Thomas Clausen, Robert Cragie, Ralph Droms, Adrian Farrel, Stephen Farrell, Brian Haberman, Ted Humpal, Richard Kelsey, Phil Levis, Charles Perkins, Joseph Reddy, Michael Richardson, Zach Shelby, Martin Stiemerling, Pascal Thubert, Hristo Valev, and JP Vasseur.

18. References

18.1. Normative References

[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.

[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.

[RFC6551] Vasseur, JP., Kim, M., Pister, K., Dejean, N., and D. Barthel, "Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks", RFC 6551, March 2012.

[RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6554, March 2012.

18.2. Informative References

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, December 2007.

[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.

[RFC6552] Thubert, P., "Objective Function Zero for the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6552, March 2012.

[RFC6553] Hui, J. and JP. Vasseur, "The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams", RFC 6553, March 2012.

[RFC6998] Goyal, M., Ed., Baccelli, E., Brandt, A., and J. Martocci, "A Mechanism to Measure the Routing Metrics along a Point-to-Point Route in a Low-Power and Lossy Network", RFC 6998, August 2013.

[ROLL-TERMS] Vasseur, JP., "Terminology in Low power And Lossy Networks", Work in Progress, March 2013.

Authors' Addresses

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

Phone: +1-414-229-5001
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@gmx.de

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 Street
Milwaukee, WI 53202
USA

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