

ROLL  
Internet-Draft  
Updates: [6550](#), [8505](#) (if approved)  
Intended status: Standards Track  
Expires: 28 March 2021

P. Thubert, Ed.  
Cisco Systems  
M. Richardson  
Sandelman  
24 September 2020

Routing for RPL Leaves  
draft-ietf-roll-unaware-leaves-20

## Abstract

This specification extends [RFC6550](#) and [RFC8505](#) to provide routing services to Hosts called RPL Unaware Leaves that implement 6LoWPAN ND but do not participate in RPL. This specification also enables the RPL Root to proxy the 6LoWPAN keep-alive flows in its DODAG.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 28 March 2021.

## Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Simplified BSD License.

Internet-Draft

RPL Unaware Leaves

September 2020

## Table of Contents

<a href="#">1.</a>	<a href="#">Introduction</a>	<a href="#">3</a>
<a href="#">2.</a>	<a href="#">Terminology</a>	<a href="#">5</a>
<a href="#">2.1.</a>	<a href="#">Requirements Language</a>	<a href="#">5</a>
<a href="#">2.2.</a>	<a href="#">Glossary</a>	<a href="#">5</a>
<a href="#">2.3.</a>	<a href="#">References</a>	<a href="#">6</a>
<a href="#">3.</a>	<a href="#">RPL External Routes and Dataplane Artifacts</a>	<a href="#">7</a>
<a href="#">4.</a>	<a href="#">6LoWPAN Neighbor Discovery</a>	<a href="#">8</a>
<a href="#">4.1.</a>	<a href="#">RFC 6775</a> <a href="#">Address Registration</a>	<a href="#">8</a>
<a href="#">4.2.</a>	<a href="#">RFC 8505</a> <a href="#">Extended Address Registration</a>	<a href="#">8</a>
<a href="#">4.2.1.</a>	<a href="#">R Flag</a>	<a href="#">9</a>
<a href="#">4.2.2.</a>	<a href="#">TID, I Field and Opaque Fields</a>	<a href="#">9</a>
<a href="#">4.2.3.</a>	<a href="#">ROVR</a>	<a href="#">9</a>
<a href="#">4.3.</a>	<a href="#">RFC 8505</a> <a href="#">Extended DAR/DAC</a>	<a href="#">10</a>
<a href="#">4.3.1.</a>	<a href="#">RFC 7400</a> <a href="#">Capability Indication Option</a>	<a href="#">10</a>
<a href="#">5.</a>	<a href="#">Requirements on the RPL-Unaware Leaf</a>	<a href="#">11</a>
<a href="#">5.1.</a>	<a href="#">Support of 6LoWPAN ND</a>	<a href="#">11</a>
<a href="#">5.2.</a>	<a href="#">Support of IPv6 Encapsulation</a>	<a href="#">11</a>
<a href="#">5.3.</a>	<a href="#">Support of the HbH Header</a>	<a href="#">12</a>
<a href="#">5.4.</a>	<a href="#">Support of the Routing Header</a>	<a href="#">12</a>
<a href="#">6.</a>	<a href="#">Updating RFC 6550</a>	<a href="#">12</a>
<a href="#">6.1.</a>	<a href="#">Updated RPL Target Option</a>	<a href="#">13</a>
<a href="#">6.2.</a>	<a href="#">Updated DODAG Configuration Option</a>	<a href="#">14</a>
<a href="#">6.3.</a>	<a href="#">Updated RPL Status</a>	<a href="#">15</a>
<a href="#">7.</a>	<a href="#">Updating draft-ietf-roll-efficient-npdao</a>	<a href="#">16</a>
<a href="#">8.</a>	<a href="#">Updating RFC 8505</a>	<a href="#">16</a>
<a href="#">9.</a>	<a href="#">Protocol Operations for Unicast Addresses</a>	<a href="#">16</a>
<a href="#">9.1.</a>	<a href="#">General Flow</a>	<a href="#">17</a>
<a href="#">9.2.</a>	<a href="#">Detailed Operation</a>	<a href="#">19</a>
<a href="#">9.2.1.</a>	<a href="#">Perspective of the RUL Acting as 6LN</a>	<a href="#">19</a>
<a href="#">9.2.2.</a>	<a href="#">Perspective of the Border Router Acting as 6LR</a>	<a href="#">20</a>
<a href="#">9.2.3.</a>	<a href="#">Perspective of the RPL Root</a>	<a href="#">23</a>
<a href="#">9.2.4.</a>	<a href="#">Perspective of the 6LBR</a>	<a href="#">23</a>
<a href="#">10.</a>	<a href="#">Protocol Operations for Multicast Addresses</a>	<a href="#">24</a>
<a href="#">11.</a>	<a href="#">Security Considerations</a>	<a href="#">25</a>
<a href="#">12.</a>	<a href="#">IANA Considerations</a>	<a href="#">26</a>
<a href="#">12.1.</a>	<a href="#">Fixing the Address Registration Option Flags</a>	<a href="#">26</a>
<a href="#">12.2.</a>	<a href="#">Resizing the ARO Status values</a>	<a href="#">26</a>
<a href="#">12.3.</a>	<a href="#">New DODAG Configuration Option Flag</a>	<a href="#">27</a>
<a href="#">12.4.</a>	<a href="#">New RPL Target Option Flag</a>	<a href="#">27</a>
12.5.	<a href="#">New Subregistry for the RPL Non-Rejection Status values</a>	<a href="#">27</a>

<a href="#">12.6.</a>	New Subregistry for the RPL Rejection Status values . . .	<a href="#">28</a>
<a href="#">13.</a>	Acknowledgments . . . . .	<a href="#">28</a>
<a href="#">14.</a>	Normative References . . . . .	<a href="#">28</a>
<a href="#">15.</a>	Informative References . . . . .	<a href="#">31</a>
<a href="#">Appendix A.</a>	Example Compression . . . . .	<a href="#">32</a>

Authors' Addresses . . . . .	<a href="#">33</a>
------------------------------	--------------------

## [1.](#) Introduction

The design of Low Power and Lossy Networks (LLNs) is generally focused on saving energy, which is the most constrained resource of all. Other design constraints, such as a limited memory capacity, duty cycling of the LLN devices and low-power lossy transmissions, derive from that primary concern.

The IETF produced the "Routing Protocol for Low Power and Lossy Networks" [[RFC6550](#)] (RPL) to provide IPv6 [[RFC8200](#)] routing services within such constraints. RPL belongs to the class of Distance-Vector protocols, which, compared to link-state protocols, limit the amount of topological knowledge that needs to be installed and maintained in each node, and does not require convergence to avoid micro-loops.

To save signaling and routing state in constrained networks, RPL allows a path stretch (see [[RFC6687](#)]), whereby routing is only performed along a Destination-Oriented Directed Acyclic Graph (DODAG) that is optimized to reach a Root node, as opposed to along the shortest path between 2 peers, whatever that would mean in a given LLN. This trades the quality of peer-to-peer (P2P) paths for a vastly reduced amount of control traffic and routing state that would be required to operate an any-to-any shortest path protocol. Additionally, broken routes may be fixed lazily and on-demand, based on dataplane inconsistency discovery, which avoids wasting energy in the proactive repair of unused paths.

For many of the nodes, though not all, the DODAG provides multiple forwarding solutions towards the Root of the topology via so-called parents. RPL is designed to adapt to fuzzy connectivity, whereby the physical topology cannot be expected to reach a stable state, with a lazy control that creates the routes proactively, but may only fix them reactively, upon actual traffic. The result is that RPL provides reachability for most of the LLN nodes, most of the time,

but may not converge in the classical sense.

RPL can be deployed in conjunction with IPv6 Neighbor Discovery (ND) [[RFC4861](#)] [[RFC4862](#)] and 6LoWPAN ND [[RFC6775](#)] [[RFC8505](#)] to maintain reachability within a Non-Broadcast Multi-Access (NBMA) Multi-Link subnet.

In that mode, IPv6 addresses are advertised individually as Host routes. Some nodes may act as Routers and participate to the forwarding operations whereas others will only terminate packets, acting as Hosts in the data-plane. In [[RFC6550](#)] terms, an IPv6 Host [[RFC8504](#)] that is reachable over the RPL network is called a Leaf.

[[USEofRPLinfo](#)] introduces the terms RPL-Aware-Leaf (RAL) and RPL-Unaware Leaf (RUL). A RAL is a Leaf that injects Host routes in RPL to manage the reachability of its IPv6 addresses. Conversely, a RUL does not participate to RPL and cannot inject its Host routes in RPL. The RUL therefore needs a Host-to-Router interface to advertise its IPv6 addresses to its access Router so the Router can inject them the RPL network on its behalf. [Section 5](#) details the interface needed by a router that implements this specification.

This specification leverages the Address Registration mechanism defined in 6LoWPAN ND to enable a RUL acting as a 6LoWPAN Node (6LN) to interface with a RPL-Aware Router as a 6LoWPAN Router (6LR) and request that the 6LR injects a Host route for the Registered Address in the RPL routing on its behalf. A RUL may be unable to participate because it is very energy-constrained, or because it is unsafe to let it inject routes in RPL, in which case using 6LoWPAN ND as the interface for the RUL limits the surface of the possible attacks and optionally protects the address ownership.

The RPL Non-Storing Mode mechanism is used to extend the routing state with connectivity to the RULs even when the DODAG is operated in Storing Mode. The unicast packet forwarding operation by the 6LR serving a RUL, as described in section 4.1 of [[USEofRPLinfo](#)].

Examples of possible RULs include lightly powered sensors such as window smash sensor (alarm system), and kinetically powered light switches. Other applications of this specification may include a smart grid network that controls appliances - such as washing machines or the heating system - in the home. Appliances may not

participate to the RPL protocol operated in the Smartgrid network but can still interact with the Smartgrid for control and/or metering.

This document is organized as follows:

- \* [Section 3](#) and [Section 4](#) present salient aspects of RPL and 6LoWPAN ND, respectively, that are leveraged in this specification to provide connectivity to a RUL across a RPL network.
- \* [Section 5](#) lists the expectations that a RUL needs to match in order to be served by a RPL router that complies with this specification.
- \* [Section 6](#), [Section 7](#), and [Section 8](#) present the additions made to [\[RFC6550\]](#), [\[EFFICIENT-NPDAO\]](#), and [\[RFC8505\]](#).
- \* [Section 9](#) and [Section 10](#) present the operation of this specification for unicast and multicast flows, respectively, and [Section 11](#) presents associated security considerations.

## [2.](#) Terminology

### [2.1.](#) Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [BCP 14](#) [\[RFC2119\]](#) [\[RFC8174\]](#) when, and only when, they appear in all capitals, as shown here.

### [2.2.](#) Glossary

This document often uses the following acronyms:

AR: Address Resolution (aka Address Lookup)

ARQ: Automatic Repeat reQuest

6CIO: 6LoWPAN Capability Indication Option

6LN: 6LoWPAN Node (a Low Power Host or Router)

6LR: 6LoWPAN Router

(E)ARO: (Extended) Address Registration Option

(E)DAR: (Extended) Duplicate Address Request

(E)DAC: (Extended) Duplicate Address Confirmation

DAD: Duplicate Address Detection  
DAO: Destination Advertisement Object (a RPL message)  
DCO: Destination Cleanup Object (a RPL message)  
DIS: DODAG Information solicitation (a RPL message)  
DIO: DODAG Information Object (a RPL message)  
DODAG: Destination-Oriented Directed Acyclic Graph  
LLN: Low-Power and Lossy Network  
NA: Neighbor Advertisement  
NCE: Neighbor Cache Entry  
ND: Neighbor Discovery  
NS: Neighbor solicitation  
RA: Router Advertisement  
ROVR: Registration Ownership Verifier  
RPI: RPL Packet Information  
RAL: RPL-Aware Leaf  
RAN: RPL-Aware Node (either a RPL Router or a RPL-Aware Leaf)  
RUL: RPL-Unaware Leaf  
TID: Transaction ID (a sequence counter in the EARO)

### [2.3.](#) References

The Terminology used in this document is consistent with and incorporates that described in "Terms Used in Routing for Low-Power and Lossy Networks (LLNs)" [[RFC7102](#)]. A glossary of classical 6LoWPAN acronyms is given in [Section 2.2](#). Other terms in use in LLNs are found in "Terminology for Constrained-Node Networks" [[RFC7228](#)]. This specification uses the terms 6LN and 6LR to refer specifically to nodes that implement the 6LN and 6LR roles in 6LoWPAN ND and does not expect other functionality such as 6LoWPAN Header Compression [[RFC6282](#)] from those nodes.

"RPL", the "RPL Packet Information" (RPI), "RPL Instance" (indexed by a RPLInstanceID) are defined in "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks" [[RFC6550](#)]. The RPI is the abstract

information that RPL defines to be placed in data packets, e.g., as the RPL Option [[RFC6553](#)] within the IPv6 Hop-By-Hop Header. By extension, the term "RPI" is often used to refer to the RPL Option itself. The DODAG Information solicitation (DIS), Destination Advertisement Object (DAO) and DODAG Information Object (DIO) messages are also specified in [[RFC6550](#)]. The Destination Cleanup Object (DCO) message is defined in [[EFFICIENT-NPDAO](#)].

This document uses the terms RPL-Unaware Leaf (RUL) and RPL Aware Leaf (RAL) consistently with [[USEofRPLinfo](#)]. The term RPL-Aware Node (RAN) is introduced to refer to a node that is either an RAL or a RPL Router. As opposed to a RUL, a RAN manages the reachability of its addresses and prefixes by injecting them in RPL by itself.

In this document, readers will encounter terms and concepts that are discussed in the following documents:

Classical IPv6 ND: "Neighbor Discovery for IP version 6" [[RFC4861](#)] and "IPv6 Stateless Address Autoconfiguration" [[RFC4862](#)],

6LoWPAN: "Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing" [[RFC6606](#)] and "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [[RFC4919](#)], and

6LoWPAN ND: Neighbor Discovery Optimization for Low-Power and Lossy Networks [[RFC6775](#)], "Registration Extensions for 6LoWPAN Neighbor Discovery" [[RFC8505](#)], and "Address Protected Neighbor Discovery for Low-power and Lossy Networks" [[AP-ND](#)].

### [3.](#) RPL External Routes and Dataplane Artifacts

Section 4.1 of [[USEofRPLinfo](#)] provides a set of rules detailed below that MUST be followed for routing packets from and to a RUL.

A 6LR that acts as a border Router for external routes advertises them using Non-Storing Mode DAO messages that are unicast directly to the Root, even if the DODAG is operated in Storing Mode. Non-Storing

Mode routes are not visible inside the RPL domain and all packets are routed via the Root. The RPL Root tunnels the packets directly to the 6LR that advertised the external route, which decapsulates and forwards the original (inner) packet.

The RPL Non-Storing MOP signaling and the associated IP-in-IP encapsulated packets appear as normal traffic to the intermediate Routers. The support of external routes only impacts the Root and the 6LR. It can be operated with legacy intermediate Routers and does not add to the amount of state that must be maintained in those Routers. A RUL is an example of a destination that is reachable via an external route that happens to be also a Host route.

The RPL data packets always carry a Hop-by-Hop Header to transport a RPL Packet Information (RPI) [[RFC6550](#)]. So unless the RUL originates its packets with an RPI, the 6LR needs to tunnel them to the Root to add the RPI. As a rule of a thumb and except for the very special case above, the packets from and to a RUL are always encapsulated using an IP-in-IP tunnel between the Root and the 6LR that serves the RUL (see sections [7.1.4](#), [7.2.3](#), [7.2.4](#), [7.3.3](#), [7.3.4](#), [8.1.3](#), [8.1.4](#), [8.2.3](#), [8.2.4](#), [8.3.3](#) and [8.3.4](#) of [[USEofRPLinfo](#)] for details).

In Non-Storing Mode, packets going down carry a Source Routing Header (SRH). The IP-in-IP encapsulation, the RPI and the SRH are collectively called the "RPL artifacts" and can be compressed using [[RFC8138](#)]. Figure 11 presents an example compressed format for a packet forwarded by the Root to a RUL in a Storing Mode DODAG.

The inner packet that is forwarded to the RUL may carry some RPL artifacts, e.g., an RPI if the original packet was generated with it, and an SRH in a Non-Storing Mode DODAG. [[USEofRPLinfo](#)] expects the RUL to support the basic "IPv6 Node Requirements" [[RFC8504](#)]. In particular the RUL is expected to ignore the RPL artifacts that are either consumed or not applicable to a Host.

A RUL is not expected to support the compression method defined in [[RFC8138](#)]. Unless configured otherwise, the border Router MUST restore the outgoing packet before forwarding over an external route, even if it is not the destination of the incoming packet, and even when delivering to a RUL.



#### 4.1. [RFC 6775](#) Address Registration

The classic "IPv6 Neighbor Discovery (IPv6 ND) Protocol" [[RFC4861](#)] [[RFC4862](#)] was defined for serial links and transit media such as Ethernet. It is a reactive protocol that relies heavily on multicast operations for address discovery (aka lookup) and duplicate address detection (DAD).

"Neighbor Discovery Optimizations for 6LoWPAN networks" [[RFC6775](#)] adapts IPv6 ND for operations over energy-constrained LLNs. The main functions of [[RFC6775](#)] are to proactively establish the Neighbor Cache Entry (NCE) in the 6LR and to prevent address duplication. To that effect, [[RFC6775](#)] introduces a new unicast Address Registration mechanism that contributes to reducing the use of multicast messages compared to the classical IPv6 ND protocol.

[[RFC6775](#)] defines a new Address Registration Option (ARO) that is carried in the unicast Neighbor solicitation (NS) and Neighbor Advertisement (NA) messages between the 6LoWPAN Node (6LN) and the 6LoWPAN Router (6LR). It also defines the Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC) messages between the 6LR and the 6LoWPAN Border Router (6LBR). In an LLN, the 6LBR is the central repository of all the Registered Addresses in its domain and the source of truth for uniqueness and ownership.

#### 4.2. [RFC 8505](#) Extended Address Registration

"Registration Extensions for 6LoWPAN Neighbor Discovery" [[RFC8505](#)] updates the behavior of [RFC 6775](#) to enable a generic Address Registration to services such as routing and ND proxy, and defines the Extended Address Registration Option (EARO) as shown in Figure 1:

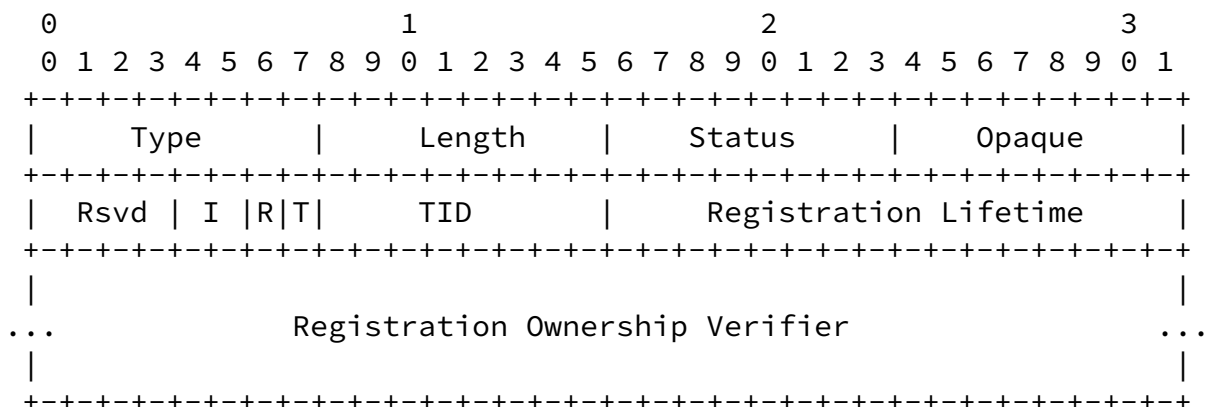


Figure 1: EARO Option Format

#### [4.2.1.](#) R Flag

[RFC8505] introduces the "R" flag in the EARO. The Registering Node sets the "R" flag to indicate whether the 6LR should ensure reachability for the Registered Address. If the "R" flag is not set, then the Registering Node handles the reachability of the Registered Address by other means. In a RPL network, this means that either it is a RAN that injects the route by itself or that it uses another RPL Router for reachability services.

This document specifies how the "R" flag is used in the context of RPL. A RPL Leaf that implements the 6LN functionality in [RFC8505] requires reachability services for an IPv6 address if and only if it sets the "R" flag in the NS(EARO) used to register the address to a RPL border Router acting as 6LR. Upon receiving the NS(EARO), the RPL Router generates a DAO message for the Registered Address if and only if the "R" flag is set. More in [Section 9.2](#).

#### [4.2.2.](#) TID, I Field and Opaque Fields

When the "T" flag is set, the EARO includes a sequence counter called Transaction ID (TID), that is needed to fill the Path Sequence Field in the RPL Transit Option. This is the reason why the support of [RFC8505] by the RUL, as opposed to only [RFC6775] is a prerequisite for this specification (more in [Section 5.1](#)). The EARO also transports an Opaque field and an associated "I" field that describes what the Opaque field transports and how to use it. [Section 9.2.1](#) specifies the use of the "I" field and the Opaque field by a RUL.

#### [4.2.3.](#) ROVR

[Section 5.3 of \[RFC8505\]](#) introduces the Registration Ownership Verifier (ROVR) field of variable length from 64 to 256 bits. The ROVR is a replacement of the EUI-64 in the ARO [RFC6775] that was used to identify uniquely an Address Registration with the Link-Layer address of the owner but provided no protection against spoofing.

"Address Protected Neighbor Discovery for Low-power and Lossy Networks" [AP-ND] leverages the ROVR field as a cryptographic proof of ownership to prevent a rogue third party from misusing the address. [AP-ND] adds a challenge/response exchange to the [RFC8505] Address Registration and enables Source Address Validation by a 6LR.

This specification does not address how the protection by [AP-ND] could be extended for the use of RPL. On the other hand, it adds the ROVR to the DAO to build the proxied EDAR at the Root (see

[Section 6.1](#)), which means that nodes that are aware of the Host route are also aware of the ROVR associated to the Target Address.

### [4.3.](#) [RFC 8505](#) Extended DAR/DAC

[RFC8505] updates the DAR/DAC messages into the Extended DAR/DAC to carry the ROVR field. The EDAR/EDAC exchange takes place between the 6LR and the 6LBR. It is triggered by an NS(EARO) message from a 6LN to create, refresh, and delete the corresponding state in the 6LBR. The exchange is protected by the retry mechanism (ARQ) specified in 8.2.6 of [\[RFC6775\]](#), though in an LLN, a duration longer than the RETRANS\_TIMER [\[RFC4861\]](#) of 1 second may be necessary to cover the Turn Around Trip delay between the 6LR and the 6LBR.

RPL [\[RFC6550\]](#) specifies a periodic DAO from the 6LN all the way to the Root that maintains the routing state in the RPL network for the lifetime indicated by the source of the DAO. This means that for each address, there are two keep-alive messages that traverse the whole network, one to the Root and one to the 6LBR.

This specification avoids the periodic EDAR/EDAC exchange across the LLN. The 6LR turns the periodic NS(EARO) from the RUL into a DAO message to the Root on every refresh, but it only generates the EDAR upon the first registration, for the purpose of DAD, which must be verified before the address is injected in RPL. Upon the DAO message, the Root proxies the EDAR exchange to refresh the state at the 6LBR on behalf of the 6LR, as illustrated in Figure 8.

#### [4.3.1.](#) [RFC 7400](#) Capability Indication Option

"6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)" [\[RFC7400\]](#) defines the 6LoWPAN Capability Indication Option (6CIO) that enables a node to expose its capabilities in Router Advertisement (RA) messages. [\[RFC8505\]](#) defines a number of bits in the 6CIO, in particular:

- L: Node is a 6LR.
- E: Node is an IPv6 ND Registrar -- i.e., it supports registrations based on EARO.
- P: Node is a Routing Registrar, -- i.e., an IPv6 ND Registrar that also provides reachability services for the Registered Address.

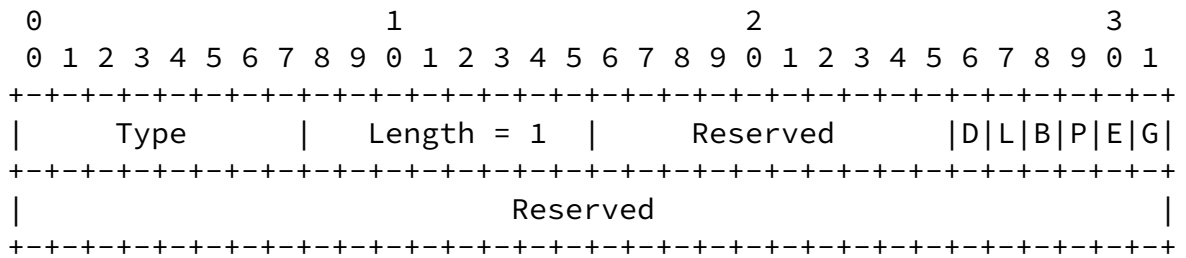


Figure 2: 6CIO flags

A 6LR that can provide reachability services for a RUL in a RPL network as specified in this document MUST include a 6CIO in its RA messages and set the L, P and E flags as prescribed by [\[RFC8505\]](#).

## 5. Requirements on the RPL-Unaware Leaf

This document provides RPL routing for a RUL. This section describes the minimal RPL-independent functionality that the RUL needs to implement to obtain routing services for its addresses.

### 5.1. Support of 6LoWPAN ND

To obtain routing services from a Router that implements this specification, a RUL needs to implement [\[RFC8505\]](#) and set the "R" and "T" flags in the EARO as discussed in [Section 4.2.1](#) and [Section 4.2.3](#), respectively. The RUL is expected not to request routing services from a Router that does not originate RA messages with a CIO that has the L, P, and E flags all set as discussed in [Section 4.3.1](#), unless configured to do so. It is suggested that the RUL also implements [\[AP-ND\]](#) to protect the ownership of its addresses.

A RUL that may attach to multiple 6LRs is expected to prefer those that provide routing services. The RUL needs to register to all the 6LRs from which it desires routing services.

Parallel Address Registrations to several 6LRs should be performed in an rapid sequence, using the exact same EARO for the same Address. Gaps between the Address Registrations will invalidate some of the routes till the Address Registration finally shows on those routes.

[\[RFC8505\]](#) introduces error Status values in the NA(EARO) which can be

received synchronously upon an NS(EARO) or asynchronously. The RUL MUST support both cases and MUST refrain from using the address when the Status Value indicates a rejection.

## [5.2.](#) Support of IPv6 Encapsulation

Section 2.1 of [[USEofRPLinfo](#)] defines the rules for tunneling either to the final destination (e.g., a RUL) or to its attachment Router (designated as 6LR). To terminate the IP-in-IP tunnel, the RUL, as an IPv6 Host, must be able to decapsulate the tunneled packet and either drop the inner packet if it is not the final destination, or pass it to the upper layer for further processing. Unless it is aware by other means that the RUL can handle IP-in-IP properly, which is not mandated by [[RFC8504](#)], the Root terminates the IP-in-IP tunnel at the parent 6LR. It is thus not necessary for a RUL to support IP-in-IP decapsulation.

## [5.3.](#) Support of the HbH Header

A RUL is expected to process an Option Type in a Hop-by-Hop Header as prescribed by [section 4.2 of \[RFC8200\]](#). An RPI with an Option Type of 0x23 [[USEofRPLinfo](#)] is thus skipped when not recognized.

## [5.4.](#) Support of the Routing Header

A RUL is expected to process an unknown Routing Header Type as prescribed by [section 4.4 of \[RFC8200\]](#). This implies that the Source Routing Header with a Routing Type of 3 [[RFC6554](#)] is ignored when the Segments Left is zero, and the packet is dropped otherwise.

## [6.](#) Updating [RFC 6550](#)

This document specifies a new behavior whereby a 6LR injects DAO messages for unicast addresses (see [Section 9](#)) and multicast addresses (see [Section 10](#)) on behalf of leaves that are not aware of RPL. The RUL addresses are exposed as external targets [[RFC6550](#)]. Conforming to [[USEofRPLinfo](#)], an IP-in-IP encapsulation between the 6LR and the RPL Root is used to carry the RPL artifacts and remove them when forwarding outside the RPL domain, e.g., to a RUL.

This document also synchronizes the liveness monitoring at the Root and the 6LBR. The same value of lifetime is used for both, and a

single keep-alive message, the RPL DAO, traverses the RPL network. A new behavior is introduced whereby the RPL Root proxies the EDAR message to the 6LBR on behalf of the 6LR (more in [Section 8](#)), for any Leaf node that implements the 6LN functionality in [\[RFC8505\]](#).

[Section 6.7.7 of \[RFC6550\]](#) introduces the RPL Target Option, which can be used in RPL Control messages such as the DAO message to signal a destination prefix. [Section 6.1](#) adds the capabilities to transport the ROVR field (see [Section 4.2.3](#)) and the full IPv6 Address of the prefix advertiser when the Target is a shorter prefix, signaled by a new "F" flag. The position of the "F" flag is indicated in [Section 12.4](#).

This specification defines the new "Root Proxies EDAR/EDAC" (P) flag and encodes it in one of these reserved flags of the the RPL DODAG Configuration option , more in [Section 6.2](#). The position of the "P" flag is indicated in [Section 12.3](#).

The RPL Status defined in [section 6.5.1 of \[RFC6550\]](#) for use in the DAO-ACK message is extended to be placed in DCO messages [\[EFFICIENT-NPDAO\]](#) as well. Furthermore, this specification enables to carry the EARO Status defined for 6LoWPAN ND in RPL DAO and DCO messages, embedded in a RPL Status, more in [Section 6.3](#).

## [6.1](#). Updated RPL Target Option

This specification updates the RPL Target Option to transport the ROVR that was also defined for 6LoWPAN ND messages. This enables the RPL Root to generate the proxied EDAR message to the 6LBR.

The new "F" flag is set to indicate that the Target Prefix field contains the address of the advertising node in full, in which case the length of the Target Prefix field is 16 bytes regardless of the value of the Prefix Length field. If the "F" flag is reset, the Target Prefix field MUST be aligned to the next byte boundary after the size (expressed in bits) indicated by the Prefix Length field. Padding bits are reserved and set to 0 as prescribed by [section 6.7.7 of \[RFC6550\]](#).

With this specification the ROVR is the remainder of the RPL Target Option. The size of the ROVR is indicated in a new ROVR Size field that is encoded to map one-to-one with the Code Suffix in the EDAR

message (see table 4 of [\[RFC8505\]](#)).

The modified format is illustrated in Figure 3. It is backward compatible with the Target Option in [\[RFC6550\]](#) and SHOULD be used as a replacement in new implementations even for Storing Mode operations in preparation for upcoming security mechanisms based in the ROVR.

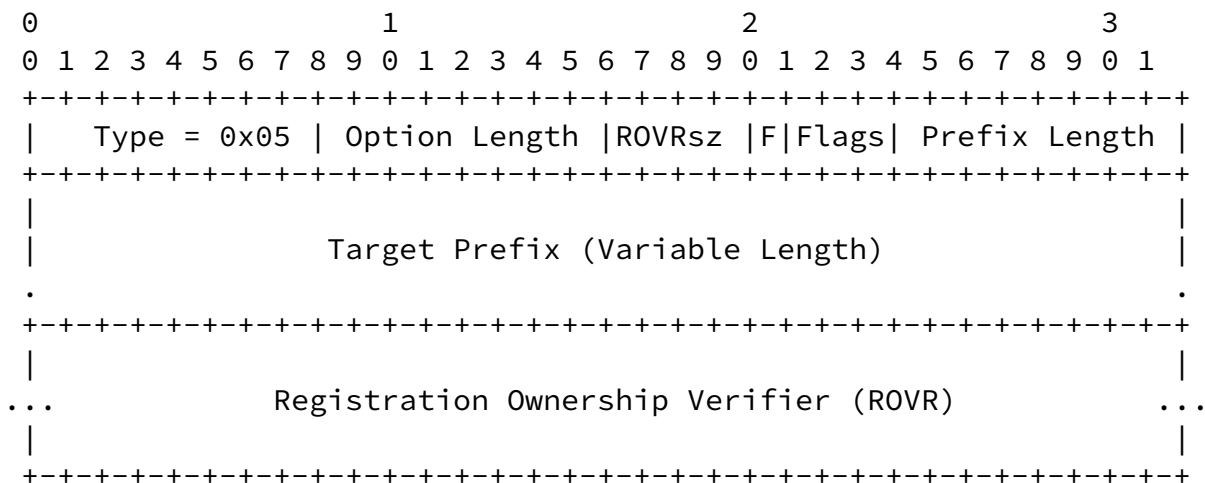


Figure 3: Updated Target Option

New fields:

ROVRsz: Indicates the Size of the ROVR. It MAY be 1, 2, 3, or 4, denoting a ROVR size of 64, 128, 192, or 256 bits, respectively.

F: 1-bit flag. Set to indicate that Target Prefix field contains an Address of prefix advertiser in full.

Registration Ownership Verifier (ROVR): This is the same field as in the EAR0, see [\[RFC8505\]](#)

## 6.2. Updated DODAG Configuration Option

The DODAG Configuration Option is defined in [Section 6.7.6 of \[RFC6550\]](#). Its purpose is extended to distribute configuration information affecting the construction and maintenance of the DODAG, as well as operational parameters for RPL on the DODAG, through the DODAG. As shown in Figure 4, the Option was originally designed with 4 bit positions reserved for future use as Flags.

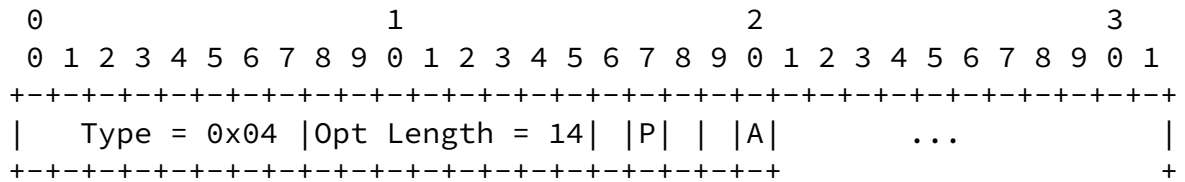


Figure 4: DODAG Configuration Option (Partial View)

This specification defines a new flag "Root Proxies EDAR/EDAC" (P). The "P" flag is set to indicate support for this specification at the Root within the DODAG. The "P" flag is encoded in position 1 of the reserved Flags in the DODAG Configuration Option (counting from bit 0 as the most significant bit) and set to 0 in legacy implementations as specified respectively in Sections [20.14](#) and [6.7.6](#) of [\[RFC6550\]](#).

The "P" flag is set to indicate that the Root performs the proxy operation, which implies that it supports the Updated RPL Target Option (see [Section 6.1](#)).

Section 4.3 of [\[USEofRPLinfo\]](#) updates [\[RFC6550\]](#) to indicate that the definition of the Flags applies to Mode of Operation (MOP) values zero (0) to six (6) only, leaving the flags reserved for MOP value seven (7). For a MOP value of 7, the bit in position 1 is considered unallocated and the Root is expected to perform the proxy operation by default.

The RPL DODAG Configuration Option is typically placed in a DODAG Information Object (DIO) message. The DIO message propagates down the DODAG to form and then maintain its structure. The DODAG Configuration Option is copied unmodified from parents to children. [\[RFC6550\]](#) states that "Nodes other than the DODAG Root MUST NOT modify this information when propagating the DODAG Configuration option". Therefore, a legacy parent propagates the "T" flag as set by the Root, and when the "T" flag is set, it is transparently flooded to all the nodes in the DODAG.

### [6.3.](#) Updated RPL Status

The RPL Status is defined in [section 6.5.1 of \[RFC6550\]](#) for use in the DAO-ACK message and values are assigned as follows:



Range	Meaning
0	Success/Unqualified acceptance
1-127	Not an outright rejection
128-255	Rejection

Table 1: RPL Status per [RFC 6550](#)

The 6LoWPAN ND Status was defined for use in the EAR0 and the currently defined values are listed in table 1 of [[RFC8505](#)]. This specification enables to carry the 6LoWPAN ND Status values in RPL DAO and DCO messages, embedded in the RPL Status field.

To achieve this, [Section 12.2](#) reduces the range of the EAR0 Status values to 0-63 to ensure that they fit within a RPL Status as shown in Figure 5.

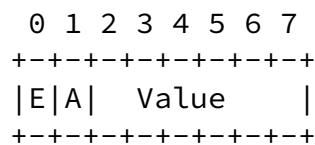


Figure 5: RPL Status Format

The following RPL Status subfields are defined:

E: 1-bit flag. Set to indicate a rejection. When not set, a value of 0 indicates Success/Unqualified acceptance and other values indicate "not an outright rejection" as per [RFC 6550](#).

A: 1-bit flag. Indicates the type of the Status Value.

Status Value: 6-bit unsigned integer. If the 'A' flag is set this field transports a Status Value defined for IPv6 ND EAR0. When the 'A' flag is not set, the Status Value is defined for RPL.

When building a DCO or a DAO-ACK message upon an IPv6 ND NA or a EDAC message, the RPL Root MUST copy the 6LoWPAN ND Status unchanged in the RPL Status and set the 'A' bit. The RPL Root MUST set the 'E' flag for Values in range 1-10 which are all considered rejections.

Reciprocally, upon a DCO or a DAO-ACK message from the RPL Root with a RPL Status that has the 'A' bit set, the 6LR MUST copy the RPL Status Value unchanged in the Status field of the EARO when generating an NA to the RUL.

#### 7. Updating [draft-ietf-roll-efficient-npdao](#)

[EFFICIENT-NPDAO] defines the DCO for RPL Storing Mode only, with a link-local scope. This specification extends its use to the Non-Storing MOP, whereby the DCO is sent unicast by the Root directly to the RAN that injected the DAO message for the considered target.

This specification leverages the DCO between the Root and the 6LR that serves as attachment Router for a RUL.

#### 8. Updating [RFC 8505](#)

This document updates [[RFC8505](#)] to change the behavior of a RPL Router acting as 6LR and of a RUL acting as 6LN in the 6LoWPAN ND Address Registration. If the RPL Root advertise the capability to proxy the EDAR/EDAC exchange to the 6LBR, the 6LR refrains from sending the keep-alive EDAR message. Instead, if it is separated from the 6LBR, the Root regenerates the EDAR message to the 6LBR periodically, upon a DAO message that signals the liveness of the Address.

#### 9. Protocol Operations for Unicast Addresses

The description below assumes that the Root sets the "P" flag in the DODAG Configuration Option and performs the EDAR proxy operation.

If the "P" flag is reset, the 6LR MUST generate the periodic EDAR messages and process the returned status as specified in [[RFC8505](#)]. If the EDAC indicates success, the rest of the flow takes place as presented but without the proxied EDAR/EDAC exchange.

### 9.1. General Flow

This specification eliminates the need to exchange keep-alive Extended Duplicate Address messages, EDAR and EDAC, all the way from a 6LN to the 6LBR across a RPL mesh. Instead, the EDAR/EDAC exchange with the 6LBR is proxied by the RPL Root upon the DAO message that refreshes the RPL routing state. The first EDAR upon a new Registration cannot be proxied, though, as it serves for the purpose of DAD, which must be verified before the address is injected in RPL.

In a RPL network where the function is enabled, refreshing the state in the 6LBR is the responsibility of the Root. Consequently, only addresses that are injected in RPL will be kept alive at the 6LBR by the RPL Root.

Since RULs are advertised using Non-Storing Mode, the DAO message flow and the keep alive EDAR/EDAC can be nested within the Address (re)Registration flow. Figure 6 illustrates that for the first Registration, both the DAD and the keep-alive EDAR/EDAC exchanges happen in the same sequence.

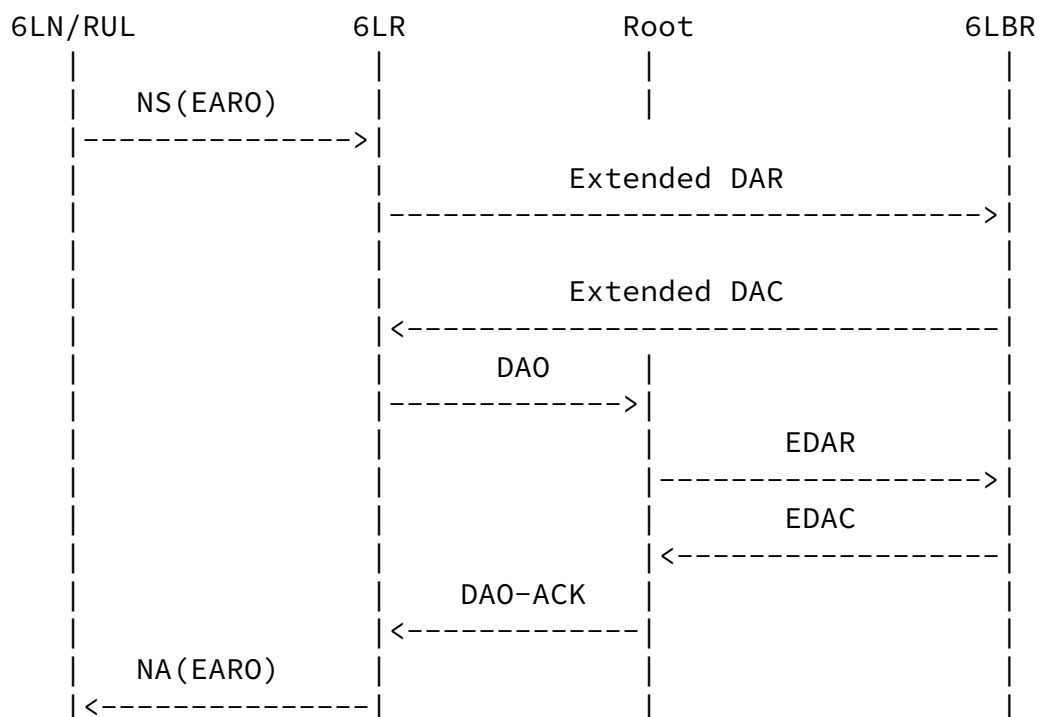


Figure 6: First RUL Registration Flow

To achieve this, the lifetimes and sequence counters in 6LoWPAN ND and RPL are aligned. In other words, the Path Sequence and the Path Lifetime in the DAO message are taken from the Transaction ID and the Address Registration lifetime in the NS(EARO) message from the 6LN.

On the first Address Registration, illustrated in Figure 6 for RPL Non-Storing Mode, the Extended Duplicate Address exchange takes place as prescribed by [RFC8505]. If the exchange fails, the 6LR returns an NA message with a negative status to the 6LN, the NCE is not created and the address is not injected in RPL. If it is successful, the 6LR creates an NCE and injects the Registered Address in the RPL routing using a DAO/DAO-ACK exchange with the RPL DODAG Root.

An issue may be detected later, e.g., the address moves within the LLN or to a different Root on a backbone [6BBR]. In that case the value of the status that indicates the issue can be passed from 6LoWPAN ND to RPL and back as illustrated in Figure 7.

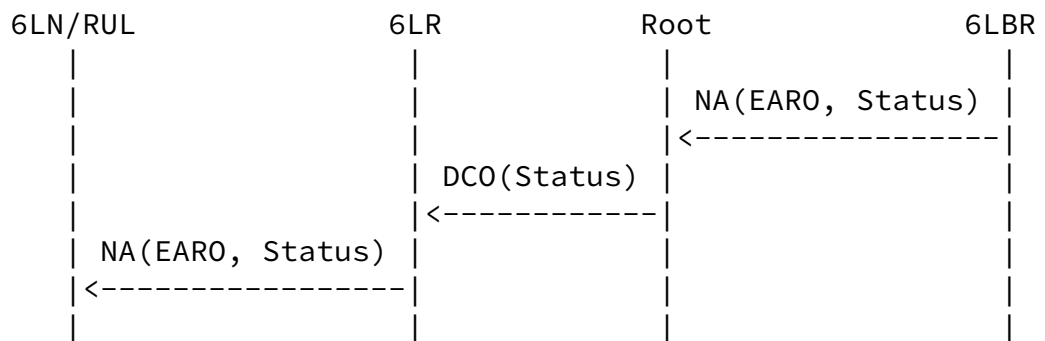


Figure 7: Asynchronous Issue

An Address re-Registration is performed by the 6LN to maintain the NCE in the 6LR alive before lifetime expires. Upon the refresh of an Address re-Registration, as illustrated in Figure 8, the 6LR injects the Registered Address in RPL.



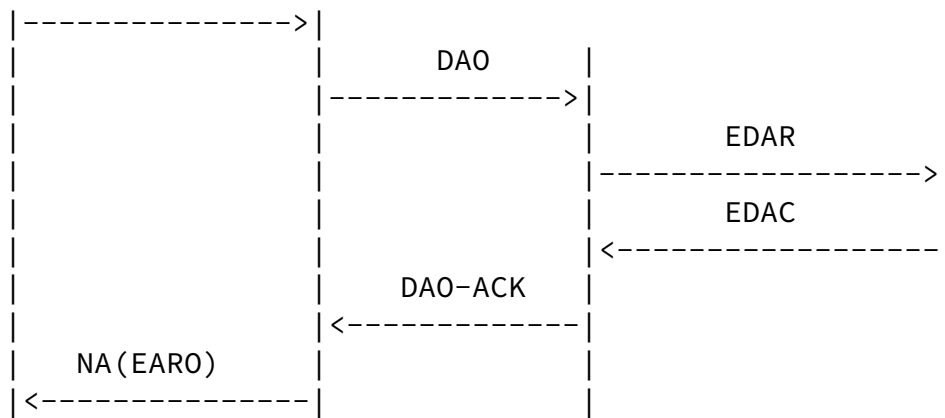


Figure 8: Next RUL Registration Flow

This is what causes the RPL Root to refresh the state in the 6LBR, using an EDAC message. In case of an error in the proxied EDAR flow, the error is returned in the DAO-ACK using a RPL Status with the 'A' flag set that imbeds a 6LoWPAN Status Value as discussed in [Section 6.3](#).

The 6LR may receive a requested DAO-ACK after it received an asynchronous DCO, but the negative Status in the DCO supersedes a positive Status in the DAO-ACK regardless of the order in which they are received. Upon the DAO-ACK - or the DCO if one arrives first - the 6LR responds to the RUL with an NA(EARO).

The RUL MAY terminate the registration at any time by using a Registration Lifetime of 0. This specification requires that the RPL Target Option transports the ROVR. This way, the same flow as the heartbeat flow is sufficient to inform the 6LBR using the Root as proxy as illustrated in Figure 8.

Any combination of the logical functions of 6LR, Root and 6LBR might be collapsed in a single node.

## [9.2](#). Detailed Operation

### [9.2.1](#). Perspective of the RUL Acting as 6LN

This specification does not alter the operation of a 6LoWPAN ND-

compliant 6LN, and a RUL is expected to operate as follows:

1. The 6LN obtains an IPv6 global address, either using Stateless Address Autoconfiguration (SLAAC) [[RFC4862](#)] based on a Prefix Information Option (PIO) [[RFC4861](#)] found in an RA message, or some other means such as DHCPv6 [[RFC3315](#)].
2. Once it has formed an address, the 6LN (re)registers its address periodically, within the Lifetime of the previous Address Registration, as prescribed by [[RFC6775](#)], to refresh the NCE before the lifetime indicated in the EARO expires. It MUST set the "T" flag and the TID is incremented each time and wraps in a lollipop fashion (see [section 5.2.1 of \[RFC8505\]](#) which is fully compatible with [section 7.2 of \[RFC6550\]](#)).
3. As stated in [section 5.2 of \[RFC8505\]](#), the 6LN can register to more than one 6LR at the same time. In that case, it uses the same EARO for all of the parallel Address Registrations. The 6LN SHOULD send the registration(s) that have a non-zero Registration Lifetime and ensure that one succeeds before it terminates other registrations, to maintain the state in the network and at the 6LBR and minimize the churn.

4. Following [section 5.1 of \[RFC8505\]](#), a 6LN acting as a RUL sets the "R" flag in the EARO of at least one registration, whereas acting as a RAN it never does. If the "R" flag is not echoed in the NA, the RUL SHOULD attempt to use another 6LR. The RUL SHOULD send the registration(s) with the "R" flag set and ensure that one succeeds before it sends the registrations with the flag reset. In case of a conflict with the preceding rule on lifetime, the rule on lifetime has precedence.
5. The 6LN may use any of the 6LRs to which it registered as default gateway. Using a 6LR to which the 6LN is not registered may result in packets dropped at the 6LR by a Source Address Validation function (SAVI) so it is NOT RECOMMENDED.

Even without support for RPL, a RUL may be aware of opaque values to be provided to the routing protocol. If the RUL has a knowledge of the RPL Instance the packet should be injected into, then it SHOULD set the Opaque field in the EARO to the RPLInstanceID, else it MUST leave the Opaque field to zero.

Regardless of the setting of the Opaque field, the 6LN MUST set the "I" field to zero to signal "topological information to be passed to a routing process" as specified in [section 5.1 of \[RFC8505\]](#).

A RUL is not expected to produce RPL artifacts in the data packets, but it MAY do so. For instance, if the RUL has a minimal awareness of the RPL Instance then it can build an RPI. A RUL that places an RPI in a data packet MUST indicate the RPLInstanceID of the RPL Instance where the packet should be forwarded. All the flags and the Rank field are set to zero as specified by [section 11.2 of \[RFC6550\]](#).

### [9.2.2](#). Perspective of the Border Router Acting as 6LR

Also as prescribed by [\[RFC8505\]](#), the 6LR generates an EDAR message upon reception of a valid NS(EARO) message for the registration of a new IPv6 Address by a 6LN. If the initial EDAR/EDAC exchange succeeds, then the 6LR installs an NCE for the Registration Lifetime. For the registration refreshes, if the RPL Root has indicated that it proxies the keep-alive EDAR/EDAC exchange with the 6LBR (see [Section 6](#)), the 6LR MUST refrain from sending the keep-alive EDAR.

If the "R" flag is set in the NS(EARO), the 6LR MUST inject the Host route in RPL, unless this is barred for other reasons, such as the saturation of the RPL parents. The 6LR MUST use a RPL Non-Storing Mode signaling and the updated Target Option (see [Section 6.1](#)). The 6LR MUST request a DAO-ACK by setting the 'K' flag in the DAO message. Success injecting the route to the RUL is indicated by the 'E' flag set to 0 in the RPL status of the DAO-ACK message.

The Opaque field in the EARO hints the 6LR on the RPL Instance that SHOULD be used for the DAO advertisements, and for the forwarding of packets sourced at the registered address when there is no RPI in the packet, in which case the 6LR MUST encapsulate the packet to the Root adding an RPI in the outer header. If the Opaque field is zero, the 6LR is free to use the default RPL Instance (zero) for the registered address or to select an Instance of its choice.

If the "I" field is not zero, then the 6LR MUST consider that the Opaque field is zero. If the Opaque field is not zero, then it is expected to carry a RPLInstanceID for the RPL Instance suggested by the 6LN. If the 6LR does not participate to the associated Instance,

then the 6LR MUST consider that the Opaque field is zero; else, that is if the 6LR participates to the suggested RPL Instance, then the 6LR SHOULD use that Instance for the Registered Address.

The DAO message advertising the Registered Address MUST be constructed as follows:

1. The Registered Address is signaled as Target Prefix in the updated Target Option in the DAO message; the Prefix Length is set to 128. The ROVR field is copied unchanged from the EARO (see [Section 6.1](#)).
2. The 6LR indicates one of its global or unique-local IPv6 unicast addresses as the Parent Address in the RPL Transit Information Option (TIO) associated with the Target Option
3. The 6LR sets the External 'E' flag in the TIO to indicate that it redistributes an external target into the RPL network
4. the Path Lifetime in the TIO is computed from the Lifetime in the EARO Option. This adapts it to the Lifetime Units used in the RPL operation; note that if the lifetime is 0, then the DAO message is a No-Path DAO that cleans up the the routes down to the RUL; this also causes the Root as a proxy to send an EDAR message to the 6LBR with a Lifetime of 0.
5. the Path Sequence in the TIO is set to the TID value found in the EARO option.

Upon receiving the DAO-ACK or an asynchronous DCO message, the 6LR MUST send the NA(EARO) to the RUL.

The 6LR MUST set "R" flag in the NA(EARO) back if and only if the 'E' flag is reset, indicating that the 6LR injected the Registered Address in the RPL routing successfully and that the EDAR proxy operation succeeded.

If the 'A' flag in the RPL Status is set, the embedded Status Value is passed back to the RUL in the EARO Status. If the 'E' flags is also set, the registration failed for 6LoWPAN ND related reasons, and the NCE is removed.



If the 'A' flag is not set in the RPL Status of the DAO-ACK, then the 6LoWPAN ND operation succeeded and an EARO Status of 0 (Success) MUST be returned to the RUL, even if the 'E' flag is set in the RPL Status. The EARO Status of 0 MUST also be used if the 6LR could not even try to inject the route.

This means that, in case of an error injecting the route that is not related to ND, the registration succeeds but the RPL route is not installed, which is signaled by the "R" flag reset. It is up to the 6LN to keep the binding with the 6LR or destroy it.

In a network where Address Protected Neighbor Discovery (AP-ND) is enabled, in case of a DAO-ACK or a DCO indicating transporting an EARO Status Value of 5 (Validation Requested), the 6LR MUST challenge the 6LN for ownership of the address, as described in section 6.1 of [\[AP-ND\]](#), before the Registration is complete. This ensures that the address is validated before it is injected in the RPL routing.

If the challenge succeeds then the operations continue as normal. In particular a DAO message is generated upon the NS(EARO) that proves the ownership of the address. If the challenge failed, the 6LR rejects the registration as prescribed by AP-ND and may take actions to protect itself against DoS attacks by a rogue 6LN, see [Section 11](#).

The 6LR may at any time send a unicast asynchronous NA(EARO) with the "R" flag reset to signal that it stops providing routing services, and/or with the EARO Status 2 "Neighbor Cache full" to signal that it removes the NCE. It may also send a final RA, unicast or multicast, with a Router Lifetime field of zero, to signal that it stops serving as Router, as specified in [section 6.2.5 of \[RFC4861\]](#).

If a 6LR receives a valid NS(EARO) message with the "R" flag reset and a Registration Lifetime that is not 0, and the 6LR was injecting the Registered Address due to previous NS(EARO) messages with the "R" flag set, then the 6LR MUST stop injecting the address. It is up to the Registering 6LN to maintain the corresponding route from then on, either keeping it active via a different 6LR or by acting as a RAN and managing its own reachability.

### [9.2.3.](#) Perspective of the RPL Root

A RPL Root SHOULD set the "P" flag in the RPL DODAG Configuration Option of the DIO messages that it generates (see [Section 6](#)) to signal that it proxies the EDAR/EDAC exchange and supports the Updated RPL Target option. The remainder of this section assumes that it does.

Upon reception of a DAO message, for each updated RPL Target Option (see [Section 6.1](#)) that creates or updates an existing RPL state, the Root MUST notify the 6LBR. This can be done using an internal API if they are integrated, or using a proxied EDAR/EDAC exchange if they are separate entities.

The EDAR message MUST be constructed as follows:

1. The Target IPv6 address from the RPL Target Option is placed in the Registered Address field of the EDAR message;
2. the Registration Lifetime is adapted from the Path Lifetime in the TIO by converting the Lifetime Units used in RPL into units of 60 seconds used in the 6LoWPAN ND messages;
3. the TID value is set to the Path Sequence in the TIO and indicated with an ICMP code of 1 in the EDAR message;
4. The ROVR in the RPL Target Option is copied as is in the EDAR and the ICMP Code Suffix is set to the appropriate value as shown in Table 4 of [[RFC8505](#)] depending on the size of the ROVR field.

Upon receiving an EDAC message from the 6LBR, if a DAO is pending, then the Root MUST send a DAO-ACK back to the 6LR. Else, if the Status in the EDAC message is not "Success", then it MUST send an asynchronous DCO to the 6LR.

In either case, the EDAC Status is embedded in the RPL Status with the 'A' flag set.

### [9.2.4.](#) Perspective of the 6LBR

The 6LBR is unaware that the RPL Root is not the new attachment 6LR of the RUL, so it is not impacted by this specification.

Upon reception of an EDAR message, the 6LBR acts as prescribed by [[RFC8505](#)] and returns an EDAC message to the sender.

## 10. Protocol Operations for Multicast Addresses

[Section 12 of \[RFC6550\]](#) details the RPL support for multicast flows. This support is not source-specific and only operates as an extension to the Storing Mode of Operation for unicast packets. Note that it is the RPL model that the multicast packet is passed as a Layer-2 unicast to each of the interested children. This remains true when forwarding between the 6LR and the listener 6LN.

"Multicast Listener Discovery (MLD) for IPv6" [\[RFC2710\]](#) and its updated version "Multicast Listener Discovery Version 2 (MLDv2) for IPv6" [\[RFC3810\]](#) provide an interface for a listener to register to multicast flows. MLDv2 is backwards compatible with MLD, and adds in particular the capability to filter the sources via black lists and white lists. In the MLD model, the Router is a "querier" and the Host is a multicast listener that registers to the querier to obtain copies of the particular flows it is interested in.

On the first Address Registration, as illustrated in Figure 9, the 6LN, as an MLD listener, sends an unsolicited Report to the 6LR in order to start receiving the flow immediately.

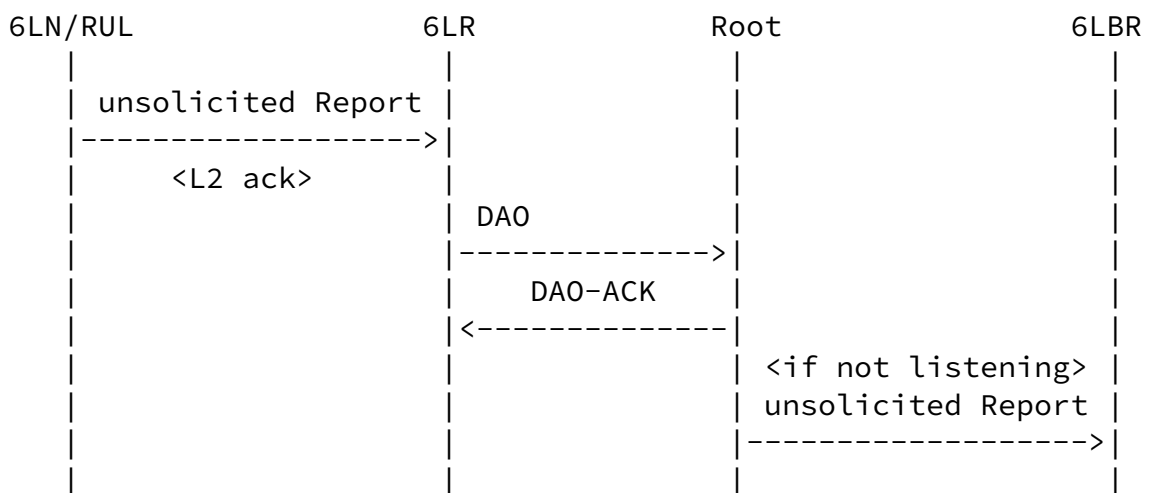


Figure 9: First Multicast Registration Flow

Since multicast Layer-2 messages are avoided, it is important that the asynchronous messages for unsolicited Report and Done are sent reliably, for instance using a Layer-2 acknowledgment, or attempted multiple times.

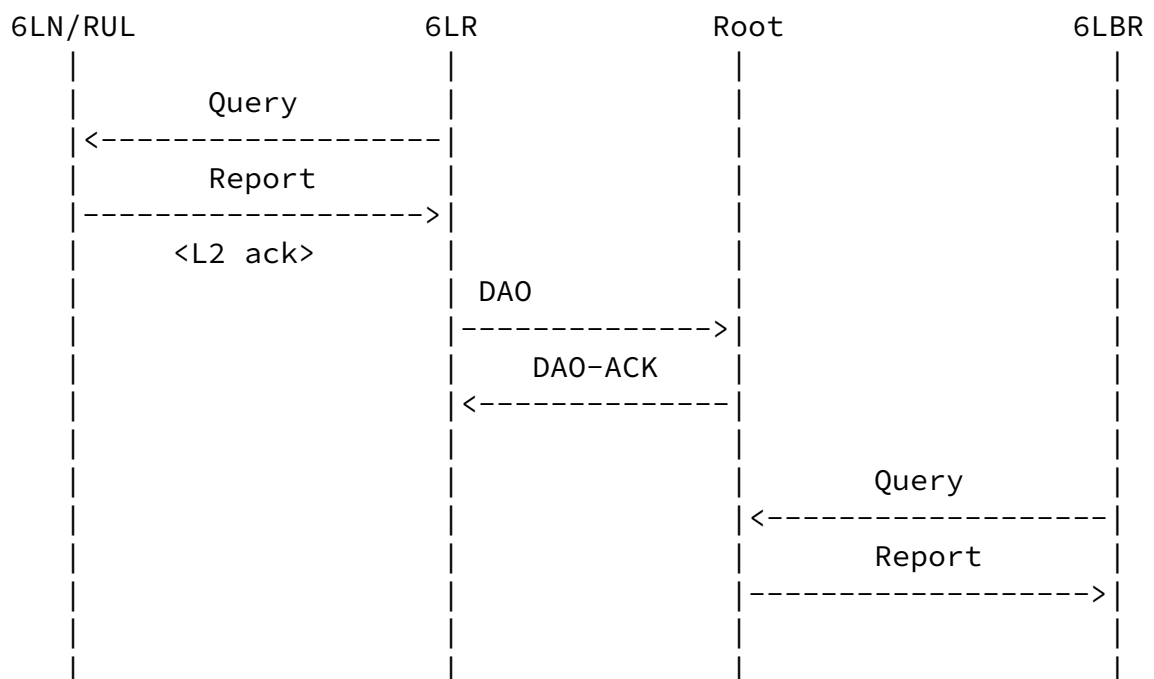
The 6LR acts as a generic MLD querier and generates a DAO for the multicast target. The lifetime of the DAO is set to be in the order of the Query Interval, yet larger to account for variable propagation delays.

The Root proxies the MLD exchange as a listener with the 6LBR acting as the querier, so as to get packets from a source external to the RPL domain.

Upon a DAO with a multicast target, the RPL Root checks if it is already registered as a listener for that address, and if not, it performs its own unsolicited Report for the multicast target.

An Address re-Registration is pulled periodically by 6LR acting as querier. Note that the message may be sent unicast to all the known individual listeners.

Upon the timing out of the Query Interval, the 6LR sends a Query to each of its listeners, and gets a Report back that is mapped into a DAO, as illustrated in Figure 10:



## Figure 10: Next Registration Flow

Note that any of the functions 6LR, Root and 6LBR might be collapsed in a single node, in which case the flow above happens internally, and possibly through internal API calls as opposed to messaging.

### 11. Security Considerations

First of all, it is worth noting that with [[RFC6550](#)], every node in the LLN is RPL-aware and can inject any RPL-based attack in the network. This specification isolates edge nodes that can only interact with the RPL Routers using 6LoWPAN ND, meaning that they cannot perform RPL insider attacks.

6LoWPAN ND can optionally provide SAVI features with [[AP-ND](#)], which reduces even more the attack perimeter that is available to the edge nodes.

The LLN nodes depend on the 6LBR and the RPL participants for their operation. A trust model must be put in place to ensure that the right devices are acting in these roles, so as to avoid threats such as black-holing, (see [[RFC7416](#) section 7]), Denial-Of-Service attacks whereby a rogue 6LR creates a high churn in the RPL network by advertising and removing many forged addresses, or bombing attack whereby an impersonated 6LBR would destroy state in the network by using the "Removed" Status code.

This trust model could be at a minimum based on a Layer-2 Secure joining and the Link-Layer security. This is a generic 6LoWPAN requirement, see Req5.1 in Appendix of [[RFC8505](#)]. It is needed in particular to prevent Denial-Of-Service attacks whereby a rogue 6LN creates a high churn in the RPL network by constantly registering and deregistering addresses with the "R" flag set in the EARO.

Additionally, the trust model could include a role validation to ensure that the node that claims to be a 6LBR or a RPL Root is entitled to do so.

At the time of this writing RPL does not have a zerotrust model whereby it is possible to validate the origin of an address that is injected in a DAO. This specification makes a first step in that direction by allowing the Root to challenge the RUL via the 6LR that

serves it.

## [12.](#) IANA Considerations

### [12.1.](#) Fixing the Address Registration Option Flags

[Section 9.1 of \[RFC8505\]](#) creates a Registry for the 8-bit Address Registration Option Flags field. IANA is requested to rename the first column of the table from "ARO Status" to "Bit number".

### [12.2.](#) Resizing the ARO Status values

[Section 12 of \[RFC6775\]](#) creates the Address Registration Option Status Values Registry with a range 0-255.

This specification reduces that range to 0-63.

IANA is requested to reduce the upper bound of the unassigned values in the Address Registration Option Status Values Registry from -255 to -63.

### [12.3.](#) New DODAG Configuration Option Flag

This specification updates the Registry that was created for [\[RFC6550\]](#) as the registry for "DODAG Configuration Option Flags" and updated as the registry for "DODAG Configuration Option Flags for MOP 0..6" by [\[USEofRPLinfo\]](#), by allocating one new Flag as follows:

Bit Number	Capability Description	Reference
1	Root Proxies EDAR/EDAC (P)	THIS RFC

Table 2: New DODAG Configuration Option Flag

### [12.4.](#) New RPL Target Option Flag

[Section 20.15 of \[RFC6550\]](#) creates a Registry for the 8-bit "RPL Target Option Flags" field. IANA is requested to reduce the size of the field in the Registry to 4 bits. This specification also defines a new entry in the Registry as follows:

Bit Number	Capability Description	Reference
1	Advertiser Address in Full (F)	THIS RFC

Table 3: New RPL Target Option Flag

### 12.5. New Subregistry for the RPL Non-Rejection Status values

This specification creates a new Subregistry for the RPL Non-Rejection Status values for use in RPL DAO-ACK and DCO messages with the 'A' flag reset, under the ICMPv6 parameters registry.

- \* Possible values are 6-bit unsigned integers (0..63).
- \* Registration procedure is "Standards Action" [[RFC8126](#)].
- \* Initial allocation is as indicated in Table 4:

Value	Meaning	Reference
0	Unqualified acceptance	<a href="#">RFC 6550</a>

Table 4: Acceptance values of the RPL Status

### 12.6. New Subregistry for the RPL Rejection Status values

This specification creates a new Subregistry for the RPL Rejection Status values for use in RPL DAO-ACK and RCO messages with the 'A' flag reset, under the ICMPv6 parameters registry.

- \* Possible values are 6-bit unsigned integers (0..63).
- \* Registration procedure is "Standards Action" [[RFC8126](#)].
- \* Initial allocation is as indicated in Table 5:

Value	Meaning	Reference
0	Unqualified rejection	This document

Table 5: Rejection values of the RPL Status

### [13.](#) Acknowledgments

The authors wish to thank Ines Robles, Georgios Papadopoulos and especially Rahul Jadhav and Alvaro Retana for their reviews and contributions to this document.

### [14.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", [RFC 2710](#), DOI 10.17487/RFC2710, October 1999, <<https://www.rfc-editor.org/info/rfc2710>>.

- [RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", [RFC 3810](#), DOI 10.17487/RFC3810, June 2004, <<https://www.rfc-editor.org/info/rfc3810>>.
- [RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs):



Overview, Assumptions, Problem Statement, and Goals",  
[RFC 4919](#), DOI 10.17487/RFC4919, August 2007,  
<<https://www.rfc-editor.org/info/rfc4919>>.

- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), DOI 10.17487/RFC4861, September 2007, <<https://www.rfc-editor.org/info/rfc4861>>.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", [RFC 4862](#), DOI 10.17487/RFC4862, September 2007, <<https://www.rfc-editor.org/info/rfc4862>>.
- [RFC6550] Winter, T., Ed., Thubert, P., Ed., 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](#), DOI 10.17487/RFC6550, March 2012, <<https://www.rfc-editor.org/info/rfc6550>>.
- [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](#), DOI 10.17487/RFC6553, March 2012, <<https://www.rfc-editor.org/info/rfc6553>>.
- [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](#), DOI 10.17487/RFC6554, March 2012, <<https://www.rfc-editor.org/info/rfc6554>>.
- [RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", [RFC 6775](#), DOI 10.17487/RFC6775, November 2012, <<https://www.rfc-editor.org/info/rfc6775>>.

- [RFC7102] Vasseur, JP., "Terms Used in Routing for Low-Power and Lossy Networks", [RFC 7102](#), DOI 10.17487/RFC7102, January 2014, <<https://www.rfc-editor.org/info/rfc7102>>.
- [RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", [RFC 7228](#), DOI 10.17487/RFC7228, May 2014, <<https://www.rfc-editor.org/info/rfc7228>>.
- [RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", [RFC 7400](#), DOI 10.17487/RFC7400, November 2014, <<https://www.rfc-editor.org/info/rfc7400>>.
- [RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 8126](#), DOI 10.17487/RFC8126, June 2017, <<https://www.rfc-editor.org/info/rfc8126>>.
- [RFC8138] Thubert, P., Ed., Bormann, C., Toutain, L., and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header", [RFC 8138](#), DOI 10.17487/RFC8138, April 2017, <<https://www.rfc-editor.org/info/rfc8138>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [BCP 14](#), [RFC 8174](#), DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.
- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, [RFC 8200](#), DOI 10.17487/RFC8200, July 2017, <<https://www.rfc-editor.org/info/rfc8200>>.
- [RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", [RFC 8505](#), DOI 10.17487/RFC8505, November 2018, <<https://www.rfc-editor.org/info/rfc8505>>.
- [AP-ND] Thubert, P., Sarikaya, B., Sethi, M., and R. Struik, "Address Protected Neighbor Discovery for Low-power and Lossy Networks", Work in Progress, Internet-Draft, [draft-ietf-6lo-ap-nd-23](#), 30 April 2020, <<https://tools.ietf.org/html/draft-ietf-6lo-ap-nd-23>>.
- [USEofRPLinfo] Robles, I., Richardson, M., and P. Thubert, "Using RPL Option Type, Routing Header for Source Routes and IPv6-in-

Internet-Draft

RPL Unaware Leaves

September 2020

IPv6 encapsulation in the RPL Data Plane", Work in Progress, Internet-Draft, [draft-ietf-roll-useofrplinfo-40](#), 25 June 2020, <<https://tools.ietf.org/html/draft-ietf-roll-useofrplinfo-40>>.

#### [EFFICIENT-NPDAO]

Jadhav, R., Thubert, P., Sahoo, R., and Z. Cao, "Efficient Route Invalidation", Work in Progress, Internet-Draft, [draft-ietf-roll-efficient-npdao-18](#), 15 April 2020, <<https://tools.ietf.org/html/draft-ietf-roll-efficient-npdao-18>>.

## 15. Informative References

- [RFC6606] Kim, E., Kaspar, D., Gomez, C., and C. Bormann, "Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing", [RFC 6606](#), DOI 10.17487/RFC6606, May 2012, <<https://www.rfc-editor.org/info/rfc6606>>.
- [RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), DOI 10.17487/RFC3315, July 2003, <<https://www.rfc-editor.org/info/rfc3315>>.
- [RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", [RFC 6282](#), DOI 10.17487/RFC6282, September 2011, <<https://www.rfc-editor.org/info/rfc6282>>.
- [RFC6687] Tripathi, J., Ed., de Oliveira, J., Ed., and JP. Vasseur, Ed., "Performance Evaluation of the Routing Protocol for Low-Power and Lossy Networks (RPL)", [RFC 6687](#), DOI 10.17487/RFC6687, October 2012, <<https://www.rfc-editor.org/info/rfc6687>>.
- [RFC7416] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., and M. Richardson, Ed., "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)", [RFC 7416](#), DOI 10.17487/RFC7416, January 2015, <<https://www.rfc-editor.org/info/rfc7416>>.
- [RFC8025] Thubert, P., Ed. and R. Cragie, "IPv6 over Low-Power

Wireless Personal Area Network (6LoWPAN) Paging Dispatch",  
[RFC 8025](#), DOI 10.17487/RFC8025, November 2016,  
<<https://www.rfc-editor.org/info/rfc8025>>.

Thubert & Richardson

Expires 28 March 2021

[Page 31]

Internet-Draft

RPL Unaware Leaves

September 2020

[RFC8504] Chown, T., Loughney, J., and T. Winters, "IPv6 Node Requirements", [BCP 220](#), [RFC 8504](#), DOI 10.17487/RFC8504, January 2019, <<https://www.rfc-editor.org/info/rfc8504>>.

[6BBR] Thubert, P., Perkins, C., and E. Levy-Abegnoli, "IPv6 Backbone Router", Work in Progress, Internet-Draft, [draft-ietf-6lo-backbone-router-20](#), 23 March 2020, <<https://tools.ietf.org/html/draft-ietf-6lo-backbone-router-20>>.

## [Appendix A](#). Example Compression

Figure 11 illustrates the case in Storing Mode where the packet is received from the Internet, then the Root encapsulates the packet to insert the RPI and deliver to the 6LR that is the parent and last hop to the final destination, which is not known to support [[RFC8138](#)].

```
+--+ ... -+-+- ... +-+- ... -+-+- ... -+-+-+ ... +-+-+ ... -+ ... +-...
|11110001|SRH-6LoRH| RPI- |IP-in-IP| NH=1      |11110CPP| UDP | UDP
|Page 1  |Type1 S=0| 6LoRH | 6LoRH  |LOWPAN_IPHC| UDP   | hdr |Payld
+-+- ... -+-+- ... +-+- ... -+-+- ... -+-+-+ ... +-+-+ ... -+ ... +-...
      <-4 bytes->                <-          RFC 6282          ->
                                   <-          No RPL artifact ...
```

Figure 11: Encapsulation to Parent 6LR in Storing Mode

The difference with the example presented in Figure 19 of [[RFC8138](#)] is the addition of a SRH-6LoRH before the RPI-6LoRH to transport the compressed address of the 6LR as the destination address of the outer IPv6 header. In the original example the destination IP of the outer header was elided and was implicitly the same address as the destination of the inner header. Type 1 was arbitrarily chosen, and the size of 0 denotes a single address in the SRH.

In Figure 11, the source of the IP-in-IP encapsulation is the Root, so it is elided in the IP-in-IP 6LoRH. The destination is the parent

6LR of the destination of the inner packet so it cannot be elided. If the DODAG is operated in Storing Mode, it is the single entry in the SRH-6LoRH and the SRH-6LoRH Size is encoded as 0. The SRH-6LoRH is the first 6LoRH in the chain. In this particular example, the 6LR address can be compressed to 2 bytes so a Type of 1 is used. It results that the total length of the SRH-6LoRH is 4 bytes.

In Non-Storing Mode, the encapsulation from the Root would be similar to that represented in Figure 11 with possibly more hops in the SRH-6LoRH and possibly multiple SRH-6LoRHs if the various addresses in the routing header are not compressed to the same format. Note that on the last hop to the parent 6LR, the RH3 is consumed and removed from the compressed form, so the use of Non-Storing Mode vs. Storing Mode is indistinguishable from the packet format.

The SRH-6LoRHs are followed by RPI-6LoRH and then the IP-in-IP 6LoRH. When the IP-in-IP 6LoRH is removed, all the 6LoRH Headers that precede it are also removed. The Paging Dispatch [[RFC8025](#)] may also be removed if there was no previous Page change to a Page other than 0 or 1, since the LOWPAN\_IPHC is encoded in the same fashion in the default Page 0 and in Page 1. The resulting packet to the destination is the inner packet compressed with [[RFC6282](#)].

#### Authors' Addresses

Pascal Thubert (editor)  
Cisco Systems, Inc  
Building D  
45 Allee des Ormes - BP1200  
06254 Mougins - Sophia Antipolis  
France

Phone: +33 497 23 26 34  
Email: pthubert@cisco.com

Michael C. Richardson  
Sandelman Software Works

Email: [mcr+ietf@sandelman.ca](mailto:mcr+ietf@sandelman.ca)  
URI: <http://www.sandelman.ca/>