Internet Engineering Task Force (IETF)   P. Thubert, Ed.
Request for Comments: 9010   Cisco Systems
Updates: 6550, 6775, 8505   M. Richardson
Category: Standards Track   Sandelman
ISSN: 2070-1721   April 2021

                 Routing for RPL (Routing Protocol for Low-Power
                      and Lossy Networks) Leaves

Abstract

   This specification provides a mechanism for a host that implements a
   routing-agnostic interface based on IPv6 over Low-Power Wireless
   Personal Area Network (6LoWPAN) Neighbor Discovery to obtain
   reachability services across a network that leverages RFC 6550 for
   its routing operations. It updates RFCs 6550, 6775, and 8505.

Status of This Memo

   This is an Internet Standards Track document.

   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). Further information on
   Internet Standards is available in Section 2 of RFC 7841.

   Information about the current status of this document, any errata,
   and how to provide feedback on it may be obtained at
   https://www.rfc-editor.org/info/rfc9010.

Copyright Notice

Table of Contents

[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 "RPL: IPv6 Routing Protocol for Low-Power and Lossy
Networks" [RFC6550] to provide routing services for IPv6 [RFC8200]
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 two 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 data-plane 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 installs the routes proactively, but to adapt to fuzzy
connectivity -- whereby the physical topology cannot be expected to
reach a stable state -- it uses a lazy route maintenance operation
that 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 IPv6 over Low-Power Wireless Personal Area
Network (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 in the
forwarding operations, whereas others will only receive/originate
packets, acting as hosts in the data plane. Per the terminology of
[RFC6550], an IPv6 host [RFC8504] that is reachable over the RPL
network is called a "leaf".

Section 2 of [RFC9008] defines the terms "RPL leaf", "RPL-Aware Leaf"
(RAL), and "RPL-Unaware Leaf" (RUL). A RPL leaf is a host attached
to one or more RPL routers; as such, it relies on the RPL router(s)
to forward its traffic across the RPL domain but does not forward
traffic from another node. As opposed to the RAL, the RUL does not
participate in RPL and relies on its RPL router(s) to also inject the

routes to its IPv6 addresses in the RPL domain.

A RUL may be unable to participate because it is very energy
constrained or code-space constrained, or because it would be unsafe
to let it inject routes in RPL. Using 6LoWPAN ND as opposed to RPL
as the host-to-router interface limits the surface of the possible
attacks by the RUL against the RPL domain. If all RULs and RPL-Aware
Nodes (RANs) use 6LoWPAN ND for the neighbor discovery process, it is
also possible to protect the address ownership of all nodes,
including the RULs.

This document specifies how the router injects the host routes in the
RPL domain on behalf of the RUL. Section 5 details how the RUL can
leverage 6LoWPAN ND to obtain the routing services from the router.
In that model, the RUL is also a 6LoWPAN Node (6LN) and the RPL-aware
router is also a 6LoWPAN Router (6LR). Using the 6LoWPAN ND Address
Registration mechanism, the RUL signals that the router must inject a
host route for the Registered Address.

```
              ------+---------
                   |              Internet
                   |
             +-----+
             |     | <------------- 6LBR / RPL DODAG Root
             +-----+                 ^
                |                     |
          o      o   o  o            | RPL
       o o     o  o    o  o      o      o       |
       o  o o  o o    o    o  o   o  o    |   +
        o   o      o       o   o   o   o    |
       o  o   o  o   o  o     o    o  o   | 6LoWPAN ND
         o  o  o  o         o   o        |
        o        o           o    o       v
      o        o      o <------------ 6LR / RPL Border Router
                                       ^
                                       | 6LoWPAN ND only
                                       v
                 u <------------ 6LN / RPL-Unaware Leaf
```

                  Figure 1: Injecting Routes on Behalf of RULs

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 is described in Section 4.1.1 of [RFC9008].

Examples of possible RULs include severely energy-constrained sensors
such as window smash sensors (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 in the RPL protocol operated in the smart grid network
but can still interact with the smart grid for control and/or
metering.

This specification can be deployed incrementally in a network that
implements [RFC9008]. Only the root and the 6LRs that connect the
RULs need to be upgraded. The RPL routers on the path will only see
unicast IPv6 traffic between the root and the 6LR.

This document is organized as follows:

*   Sections 3 and 4 present in a non-normative fashion the salient
    aspects of RPL and 6LoWPAN ND, respectively, that are leveraged in
    this specification to provide connectivity to a 6LN acting as a
    RUL across a RPL network.

*   Section 5 lists the requirements that a RUL needs to match in
    order to be served by a RPL router that complies with this
    specification.

*   Section 6 presents the changes made to [RFC6550]; a new behavior
    is introduced whereby the 6LR advertises the 6LN's addresses in a
    RPL Destination Advertisement Object (DAO) message based on the ND
    registration by the 6LN, and the RPL DODAG root performs the
    Extended Duplicate Address Request / Extended Duplicate Address
    Confirmation (EDAR/EDAC) exchange with the 6LoWPAN Border Router
    (6LBR) on behalf of the 6LR; modifications are introduced to some
    RPL options and to the RPL Status to facilitate the integration of
    the protocols.

*   Section 7 presents the changes made to [RFC9009]; the use of the
    Destination Cleanup Object (DCO) message is extended to the Non-
    Storing RPL Mode of Operation (MOP) to report asynchronous issues
    from the root to the 6LR.

*   Section 8 presents the changes made to [RFC6775] and [RFC8505];
    the range of the Address Registration Option / Extended Address
    Registration Option (ARO/EARO) Status values is reduced to 64
    values, and the remaining bits in the original status field are
    now reserved.

*   Sections 9 and 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 uses the following abbreviations:

6BBR: 6LoWPAN Backbone Router
6CIO: 6LoWPAN Capability Indication Option
6LBR: 6LoWPAN Border Router
6LN: 6LoWPAN Node (a low-power host or router)
6LoRH: 6LoWPAN Routing Header
6LoWPAN: IPv6 over Low-Power Wireless Personal Area Network
6LR: 6LoWPAN Router
AP-ND: Address-Protected Neighbor Discovery
ARO: Address Registration Option
DAC: Duplicate Address Confirmation
DAD: Duplicate Address Detection
DAO: Destination Advertisement Object (a RPL message)
DAR: Duplicate Address Request
DCO: Destination Cleanup Object (a RPL message)
DIO: DODAG Information Object (a RPL message)
DODAG: Destination-Oriented Directed Acyclic Graph
EARO: Extended Address Registration Option
EDAC: Extended Duplicate Address Confirmation
EDAR: Extended Duplicate Address Request
EUI: Extended Unique Identifier
LLN: Low-Power and Lossy Network
MLD: Multicast Listener Discovery
MOP: RPL Mode of Operation
NA: Neighbor Advertisement
NBMA: Non-Broadcast Multi-Access
NCE: Neighbor Cache Entry
ND: Neighbor Discovery
NS: Neighbor Solicitation
PIO: Prefix Information Option
RA: Router Advertisement
RAL: RPL-Aware Leaf
RAN: RPL-Aware Node (either a RPL router or a RPL-Aware Leaf)
RH3: Routing Header for IPv6 (type 3)
ROVR: Registration Ownership Verifier
RPI: RPL Packet Information
RPL: Routing Protocol for Low-Power and Lossy Networks
RUL: RPL-Unaware Leaf
SAVI: Source Address Validation Improvement
SLAAC: Stateless Address Autoconfiguration
SRH: Source Routing Header
TID: Transaction ID (a sequence counter in the EARO)
TIO: Transit Information Option

. Related Documents

   The terminology used in this document is consistent with, and
   incorporates the terms provided in, "Terms Used in Routing for
   Low-Power and Lossy Networks" [RFC7102]. A glossary of classical
   6LoWPAN abbreviations 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", "RPI", "RPL Instance" (indexed by a RPLInstanceID), "up", and
   "down" 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 DAO and
   DIO messages are also specified in [RFC6550]. The DCO message is
   defined in [RFC9009].

   This document uses the terms "RUL", "RAN", and "RAL" consistently
   with [RFC9008]. A RAN is either a 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 (IPv6)"
      [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 IPv6 over Low-Power
      Wireless Personal Area Networks (6LoWPANs)" [RFC6775],
      "Registration Extensions for IPv6 over Low-Power Wireless Personal
      Area Network (6LoWPAN) Neighbor Discovery" [RFC8505],
      "Address-Protected Neighbor Discovery for Low-Power and Lossy
      Networks" [RFC8928], and "IPv6 Backbone Router" [RFC8929].

3. RPL External Routes and Data-Plane Artifacts

   RPL was initially designed to build stub networks whereby the only
   border router would be the RPL DODAG root (typically co-located with
   the 6LBR) and all the nodes in the stub would be RPL aware. But

[RFC6550] was also prepared to be extended for external routes
("targets" in RPL parlance), via the External ('E') flag in the
Transit Information Option (TIO). External targets provide the
ability to reach destinations that are outside the RPL domain and
connected to the RPL domain via RPL border routers that are not the
root. Section 4.1 of [RFC9008] provides a set of rules (summarized
below) that must be followed for routing packets to and from an
external destination. A RUL is a special case of an external target
that is also a host directly connected to the RPL domain.

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 DODAG root tunnels the data packets
directly to the 6LR that advertised the external route, which
decapsulates and forwards the original (inner) packets.

The RPL Non-Storing MOP signaling and the associated IPv6-in-IPv6
encapsulated packets appear as normal traffic to the intermediate
routers. 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 also be a host route.

The RPL data packets typically carry a Hop-by-Hop Header with a RPL
Option [RFC6553] that contains the RPI (the RPL Packet Information,
as defined in Section 11.2 of [RFC6550]). Unless the RUL already
placed a RPL Option in the outer header chain, the packets from and
to the RUL are encapsulated using an IPv6-in-IPv6 tunnel between the
root and the 6LR that serves the RUL (see Sections 7 and 8 of
[RFC9008] for details). If the packet from the RUL has an RPI, the
6LR acting as a RPL border router rewrites the RPI to indicate the
selected RPL Instance and set the flags, but it does not need to
encapsulate the packet (see Section 9.2.2).

In Non-Storing mode, packets going down the DODAG carry a Source
Routing Header (SRH). The IPv6-in-IPv6 encapsulation, the RPI, and
the SRH are collectively called the "RPL artifacts" and can be
compressed using the method defined in [RFC8138]. Appendix A
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. [RFC9008] expects the RUL to
support the basic IPv6 node requirements per [RFC8504] and, in
particular, the mandates in Sections 4.2 and 4.4 of [RFC8200]. As
such, the RUL is expected to ignore the RPL artifacts that may be
left over -- either an SRH whose Segments Left is zero or a RPL

Option in the Hop-by-Hop Header (which can be skipped when not
recognized; see Section 5.3 for details).

A RUL is not expected to support the compression method defined in
[RFC8138]. For that reason, the border router (the 6LR here)
uncompresses the packet before forwarding it over an external route
to a RUL [RFC9008].

4. 6LoWPAN Neighbor Discovery

This section goes through the 6LoWPAN ND mechanisms that this
specification leverages, as a non-normative reference to the reader.
The full normative text is to be found in [RFC6775], [RFC8505], and
[RFC8928].

4.1. Address Registration per RFC 6775

The classical 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 address lookup) and Duplicate
Address Detection (DAD).

"Neighbor Discovery Optimization for IPv6 over Low-Power Wireless
Personal Area Networks (6LoWPANs)" [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 unicast Address Registration mechanism that
contributes to reducing the use of multicast messages compared to the
classical IPv6 ND protocol.

[RFC6775] also introduces the Address Registration Option (ARO),
which 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 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. Extended Address Registration per RFC 8505

"Registration Extensions for IPv6 over Low-Power Wireless Personal
Area Network (6LoWPAN) Neighbor Discovery" [RFC8505] updates RFC 6775
with a generic Address Registration mechanism that can be used to
access services such as routing and ND proxy functions. To that
effect, [RFC8505] defines the Extended Address Registration Option
(EARO), as shown in Figure 2:

    0   1   2   3

```
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |     Type      |    Length     |    Status     |    Opaque     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Rsvd | I |R|T|     TID       |      Registration Lifetime     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                                                               |
   ...         Registration Ownership Verifier (ROVR)           ...
   |                                                               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
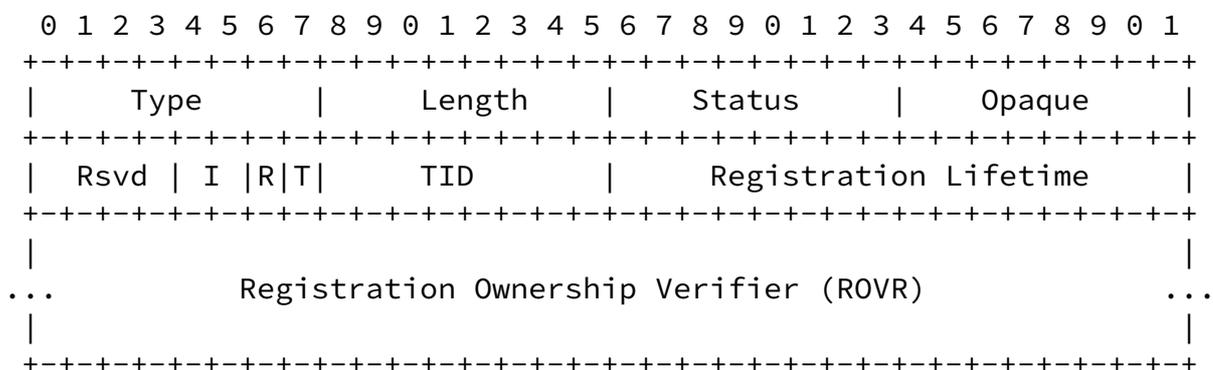
Figure 2: EARO Format

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 set to 0,
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 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 from [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 6LR
acting as a RPL border router. 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 to 1.

Section 9.2 specifies additional operations when the R flag is set to
1 in an EARO that is placed in either an NS message or an NA message.

4.2.2. TID, "I" Field, and Opaque Field

When the T flag is set to 1, the EARO includes a sequence counter
called the "Transaction ID" (TID), which is needed to fill the Path
Sequence field in the RPL Transit Information Option (TIO). For this
reason, support of [RFC8505] by the RUL, as opposed to only
[RFC6775], is a prerequisite for this specification; this requirement
is fully explained 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. Route Ownership Verifier

Section 5.3 of [RFC8505] introduces the Registration Ownership

Verifier (ROVR) field, which has a variable length of 64 to 256 bits.
The ROVR replaces the 64-bit Extended Unique Identifier (EUI-64) in
the ARO [RFC6775], which was used to uniquely identify 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" [RFC8928] leverages the ROVR field as a cryptographic proof
of ownership to prevent a rogue third party from registering an
address that is already owned. The use of the ROVR field enables the
6LR to block traffic that is not sourced at an owned address.

This specification does not address how the protection offered by
[RFC8928] could be extended for use in 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. EDAR/EDAC per RFC 8505

[RFC8505] updates the DAR/DAC messages to EDAR/EDAC messages 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 specified in
Section 8.2.6 of [RFC6775], though in an LLN, a duration longer than
the default value of the RetransTimer (RETRANS_TIMER) [RFC4861] of 1
second may be necessary to cover the round-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 in
Section 9.1.

4.3.1. Capability Indication Option per RFC 7400

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

[RFC8505] defines a number of bits in the 6CIO; in particular:

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length = 1   |      Reserved       |D|L|B|P|E|G|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Reserved                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
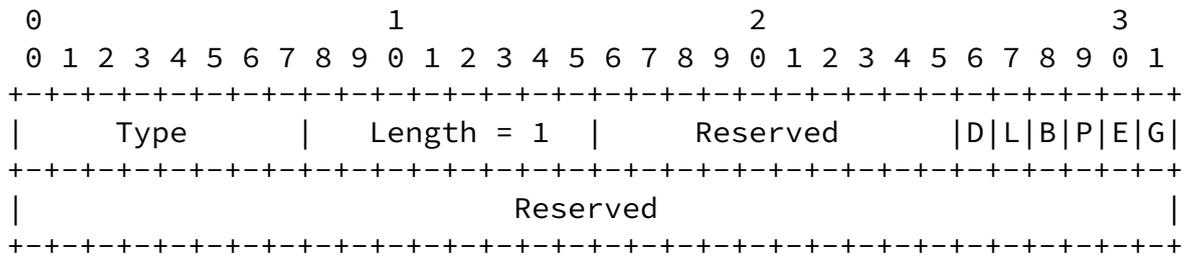
Figure 3: 6CIO Flags

A 6LR that provides reachability services for a RUL in a RPL network
as specified in this document includes a 6CIO in its RA messages and
set the L, P, and E flags to 1 as prescribed by [RFC8505]; this is
fully explained in Section 9.2.

5. Requirements for the RPL-Unaware Leaf

This document describes how RPL routing can be extended to reach a
RUL. This section specifies the minimal RPL-independent
functionality that the RUL needs to implement in order 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 sets the "R"
and "T" flags in the EARO to 1 as discussed in Sections 4.2.1 and
4.2.2, respectively. Section 9.2.1 specifies new behaviors for the
RUL, e.g., when the R flag set to 1 in an NS(EARO) is not echoed in
the NA(EARO), which indicates that the route injection failed.

The RUL is expected to request routing services from a router only if
that router originates RA messages with a 6CIO that has the L, P, and
E flags all set to 1 as discussed in Section 4.3.1, unless configured
to do so. It is suggested that the RUL also implement [RFC8928] 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 with all
the 6LRs from which it desires routing services.

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

[RFC8505] introduces error Status values in the NA(EARO) that can be received synchronously upon an NS(EARO) or asynchronously. The RUL needs to support both cases and refrain from using the address when the Status value indicates a rejection (see Section 6.3).

5.2. Support of IPv6 Encapsulation

Section 4.1.1 of [RFC9008] defines the rules for signaling an external destination (e.g., a RUL) and tunneling to its attachment router (designated as a 6LR). In order to terminate the IPv6-in-IPv6 tunnel, the RUL, as an IPv6 host, would have to be capable of decapsulating the tunneled packet and either drop the encapsulated packet if it is not the final destination or pass it to the upper layer for further processing. As indicated in Section 4.1 of [RFC9008], this is not mandated by [RFC8504], and the IPv6-in-IPv6 tunnel from the root is terminated at the parent 6LR. It is thus not necessary for a RUL to support IPv6-in-IPv6 decapsulation.

5.3. Support of the Hop-by-Hop 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 [RFC9008] 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 SRH, which has a Routing Type of 3 [RFC6554], is ignored when Segments Left is zero. When Segments Left is non-zero, the RUL discards the packet and sends an ICMP Parameter Problem message with Code 0 to the packet's source address, pointing to the unrecognized Routing Type.

6. Enhancements to 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 [RFC9008], IPv6-in-IPv6 encapsulation between the 6LR and the RPL DODAG 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 lifetime value is used for both, and a single keep-alive message, the RPL DAO, traverses the RPL network. Another

new behavior is introduced whereby the RPL DODAG root proxies the
EDAR message to the 6LBR on behalf of the 6LR (see Section 8), for
any leaf node that implements the 6LN functionality described 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. This document adds capabilities for
transporting the ROVR field (see Section 4.2.3) and the IPv6 address
of the prefix advertiser when the Target is a shorter prefix. Their
use is signaled by a new ROVR Size field being non-zero and a new
"Advertiser address in Full (F)" flag set to 1, respectively; see
Section 6.1.

This specification defines a new flag, "Root Proxies EDAR/EDAC (P)",
in the RPL DODAG Configuration option; see Section 6.2.

Furthermore, this specification provides the ability to carry the
EARO Status defined for 6LoWPAN ND in RPL DAO and DCO messages,
embedded in a RPL Status; see Section 6.3.

Section 12 of [RFC6550] details RPL support for multicast flows when
the RPL Instance is operated with a MOP setting of 3 ("Storing Mode
of Operation with multicast support"). This specification extends
the RPL DODAG root operation to proxy-relay the MLDv2 operation
[RFC3810] between the RUL and the 6LR; see Section 10.

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 DODAG root to generate the proxied EDAR message to the 6LBR.

   The Target Prefix of the RPL Target option is left (high bit)
   justified and contains the advertised prefix; its size may be smaller
   than 128 when it indicates a prefix route. The Prefix Length field
   signals the number of bits that correspond to the advertised prefix;
   it is 128 for a host route or less in the case of a prefix route.
   This remains unchanged.

   This specification defines the new 'F' flag. When it is set to 1,
   the size of the Target Prefix field MUST be 128 bits and it MUST
   contain an IPv6 address of the advertising node taken from the
   advertised prefix. In that case, the Target Prefix field carries two
   distinct pieces of information: a route that can be a host route or a
   prefix route, depending on the Prefix Length; and an IPv6 address
   that can be used to reach the advertising node and validate the
   route.

   If the 'F' flag is set to 0, the Target Prefix field can be shorter
   than 128 bits, and it MUST be aligned to the next byte boundary after

the end of the prefix. Any additional bits in the rightmost octet
are filled with padding bits. Padding bits are reserved and set to 0
as specified in 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 ROVR Size field is taken
from the Flags field, which is an update to the "RPL Target Option
Flags" IANA registry.

The updated format is illustrated in Figure 4. It is backward
compatible with the Target option defined in [RFC6550]. It is
recommended that the updated format be used as a replacement in new
implementations in all MOPs in preparation for upcoming route
ownership validation mechanisms based on the ROVR, unless the device
or the network is so constrained that this is not feasible.

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |   Type = 0x05 | Option Length |F|X|Flg|ROVRsz | Prefix Length |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 |               Target Prefix (Variable Length)                 |
 .                                                               .
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 ...            Registration Ownership Verifier (ROVR)        ...
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
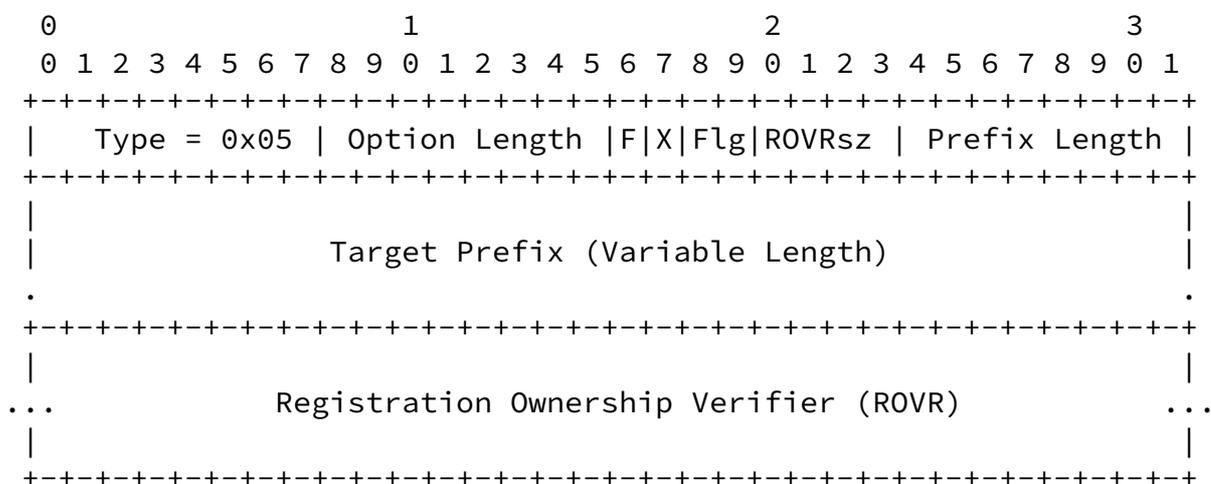
                    Figure 4: Updated Target Option

New fields:

F: 1-bit flag. Set to 1 to indicate that the Target Prefix field
    contains the complete (128-bit) IPv6 address of the advertising
    node.

X: 1-bit flag. Set to 1 to request that the root perform a proxy
    EDAR/EDAC exchange.

    The 'X' flag can only be set to 1 if the DODAG is operating in
    Non-Storing mode and if the root sets the "Root Proxies EDAR/EDAC
    (P)" flag to 1 in the DODAG Configuration option; see
    Section 6.2.

    The 'X' flag can be set for host routes to RULs and RANs; it can
    also be set for internal prefix routes if the 'F' flag is set,
    using the node's address in the Target Prefix field to form the

EDAR, but it cannot be used otherwise.

Flg (Flags): The 2 bits remaining unused in the Flags field are
     reserved for flags. The field MUST be initialized to 0 by the
     sender and MUST be ignored by the receiver.

ROVRsz (ROVR Size): Indicates the size of the ROVR. It MUST be set
     to 1, 2, 3, or 4, indicating a ROVR size of 64, 128, 192, or 256
     bits, respectively.

     If a legacy Target option is used, then the value must remain 0,
     as specified in [RFC6550].

     In the case of a value above 4, the size of the ROVR is
     undetermined and this node cannot validate the ROVR; an
     implementation SHOULD propagate the whole Target option upwards
     as received to enable the verification by an ancestor that would
     support the upgraded ROVR.

Registration Ownership Verifier (ROVR): This is the same field as in
     the EARO; see [RFC8505].

6.2. Additional Flag in the RPL 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. This option was originally designed with four bit positions
reserved for future use as flags.

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |   Type = 0x04 |Opt Length = 14| |P| | |A|      ...          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                +
                                   |4 bits |
```
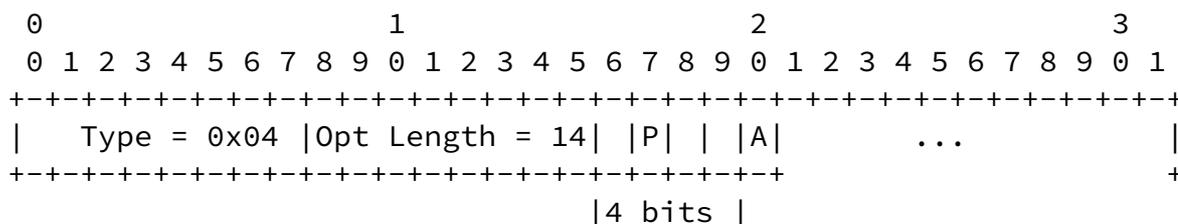
             Figure 5: DODAG Configuration Option (Partial View)

This specification defines a new flag, "Root Proxies EDAR/EDAC (P)".
The 'P' flag is encoded in bit position 1 of the reserved flags in
the DODAG Configuration option (counting from bit 0 as the most
significant bit), and it is set to 0 in legacy implementations as
specified in Sections 20.14 and 6.7.6 of [RFC6550], respectively.

The 'P' flag is set to 1 to indicate that the root performs the proxy
operation, which implies that it supports this specification and the
updated RPL Target option (see Section 6.1).

Section 4.1.3 of [RFC9008] updates [RFC6550] to indicate that the

definition of the flags applies to MOP values from zero (0) to six
(6) only. For a MOP value of 7, the implementation MUST assume that
the root performs the proxy operation.

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 'P' flag as set
by the root, and when the 'P' flag is set to 1, 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. 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 EARO; see
Section 4.1 of [RFC8505]. This specification adds the ability to
allow the carriage of 6LoWPAN ND Status values in RPL DAO and DCO
messages, embedded in the RPL Status field.

To achieve this, the range of the ARO/EARO Status values is reduced
to 0-63, which updates the IANA registry created for [RFC6775]. This
reduction ensures that the values fit within a RPL Status as shown in
Figure 6. See Sections 12.2, 12.5, and 12.6 for the respective IANA
declarations. These updates are reasonable because the associated
registry relies on the Standards Action policy [RFC8126] for
registration and only values up to 10 are currently allocated.

```
                     0 1 2 3 4 5 6 7
                    +-+-+-+-+-+-+-+-+
                    |U|A|StatusValue|
                    +-+-+-+-+-+-+-+-+
```
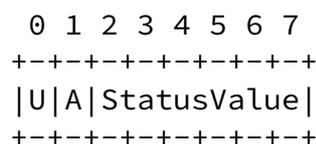
                   Figure 6: RPL Status Format

This specification updates the RPL Status with the following
subfields:

U: 1-bit flag. Set to 1 to indicate a rejection. When set to 0, a
    Status 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 RPL Status value.

Status Value: 6-bit unsigned integer.

    If the 'A' flag is set to 1, this field transports a value
    defined for the 6LoWPAN ND EARO Status.

    When the 'A' flag is set to 0, this field transports a Status
    value defined for RPL.

When building a DCO or a DAO-ACK message upon an IPv6 ND NA or an
EDAC message, the RPL DODAG root MUST copy the 6LoWPAN ND status code
unchanged in the RPL Status Value field and set the 'A' flag to 1.
The RPL DODAG root MUST set the 'U' flag to 1 for all rejection and
unknown status codes. The status codes in the 1-10 range [RFC8505]
are all considered rejections.

Reciprocally, upon a DCO or a DAO-ACK message from the RPL DODAG root
with a RPL Status that has the 'A' flag 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. Enhancements to RFC 9009

   [RFC9009] defines the DCO message for RPL Storing mode only, with a
   link-local scope. All nodes in the RPL network are expected to
   support the specification, since the message is processed hop by hop
   along the path that is being cleaned up.

   This specification extends the use of the DCO message to the Non-
   Storing MOP, whereby the DCO is sent end to end by the root directly
   to the RAN that injected the DAO message for the considered target.
   In that case, intermediate nodes do not need to support [RFC9009];
   they forward the DCO message as a plain IPv6 packet between the root
   and the RAN.

   In the case of a RUL, the 6LR that serves the RUL acts as the RAN
   that receives the Non-Storing DCO. This specification leverages the
   Non-Storing DCO between the root and the 6LR that serves as the
   attachment router for a RUL. A 6LR and a root that support this
   specification MUST implement the Non-Storing DCO.

8. Enhancements to RFCs 6775 and 8505

This document updates [RFC6775] and [RFC8505] to reduce the range of
the ARO/EARO Status values to 64 values. The two most significant
(leftmost) bits of the original ND Status field are now reserved;
they MUST be set to 0 by the sender and ignored by the receiver.

This document also updates the behavior of a 6LR acting as a RPL
router and of a 6LN acting as a RUL in the 6LoWPAN ND Address
Registration as follows:

* If the RPL DODAG root advertises the ability to proxy the EDAR/
   EDAC exchange to the 6LBR, the 6LR refrains from sending the keep-
   alive EDAR message. If it is separated from the 6LBR, the root
   regenerates the EDAR message to the 6LBR periodically, upon a DAO
   message that signals the liveliness of the address.

* The use of the R flag is extended to the NA(EARO) to confirm
   whether the route was installed.

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
presented in Section 4.3.

If the 'P' flag is set to 0, 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.

Section 9.1 provides an overview of the route injection in RPL,
whereas Section 9.2 offers more details from the perspective of the
different nodes involved in the flow.

9.1. General Flow

This specification eliminates the need to exchange keep-alive EDAR
and EDAC messages 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 DODAG root upon the DAO message that refreshes the RPL
routing state. The first EDAR upon a new Address Registration cannot
be proxied, though, as it is generated 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 DODAG 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 7 illustrates that,
for the first Address Registration, both the DAD and the keep-alive

EDAR/EDAC exchanges happen in the same sequence.

```
        6LN/RUL              6LR    <6LR*>    Root              6LBR
          |<---Using ND--->|<--Using RPL->|<-----Using ND---->|
          |                |<----------Using ND------------->|
          |                |              |                   |
          |    NS(EARO)    |              |                   |
          |--------------->|              |                   |
          |                |      EDAR    |                   |
          |                |------------------------------->|
          |                |              |                   |
          |                |      EDAC    |                   |
          |                |<-------------------------------|
          |                |              |                   |
          |                |   DAO(X=0)   |                   |
          |                |------------->|                   |
          |                |              |                   |
          |                |   DAO-ACK    |                   |
          |                |<-------------|                   |
          |    NA(EARO)    |              |                   |
          |<---------------|              |                   |
          |                |              |                   |
```
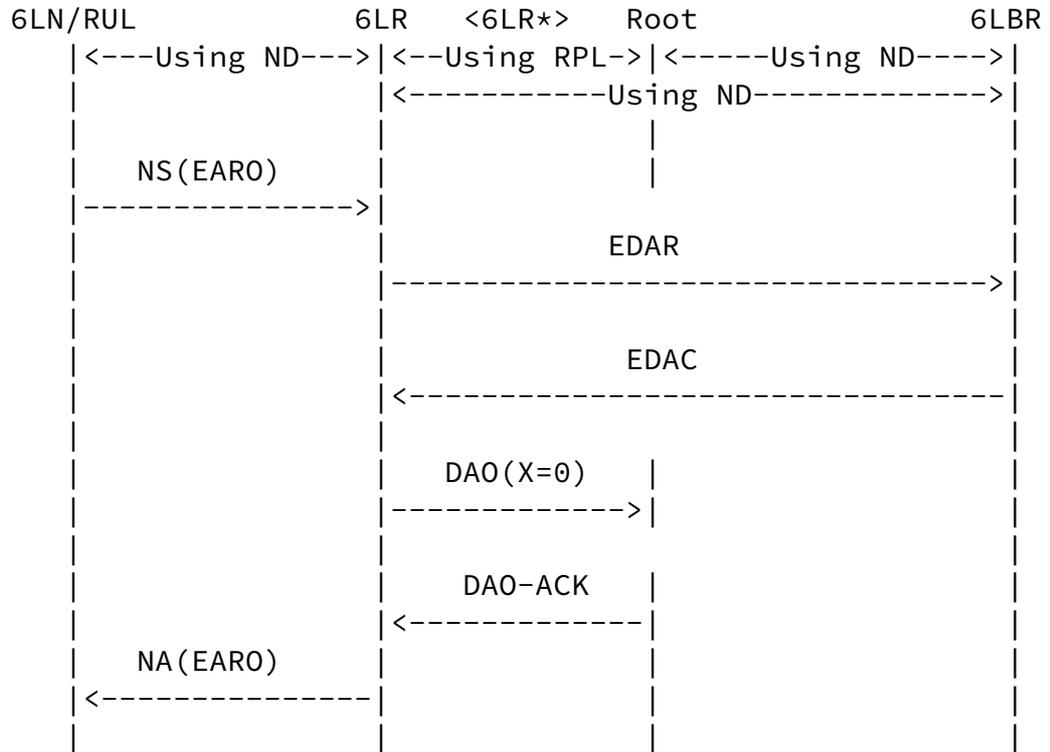
                 Figure 7: First RUL Registration Flow

This flow requires that the lifetimes and sequence counters in
6LoWPAN ND and RPL be aligned.

To achieve this, 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 7 for RPL
Non-Storing mode, the EDAR/EDAC exchange takes place as prescribed by
[RFC8505]. If the exchange fails, the 6LR returns an NA message with
a non-zero status to the 6LN, the NCE is not created, and the address
is not injected in RPL. Otherwise, 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 Address Registration refresh is performed by the 6LN to keep the
NCE in the 6LR alive before the lifetime expires. Upon the refresh
of a registration, the 6LR reinjects the corresponding route in RPL
before it expires, as illustrated in Figure 8.

```
        6LN/RUL    <-ND->    6LR    <-RPL-> Root    <-ND->    6LBR
          |                |              |                   |
          |    NS(EARO)    |              |                   |
          |--------------->|              |                   |
          |                |   DAO(X=1)   |                   |
          |                |------------->|                   |
```

```
          |               |               |    EDAR       |
          |               |               |-------------->|
          |               |               |    EDAC       |
          |               |               |<--------------|
          |               |    DAO-ACK    |               |
          |               |<------------- |               |
          |    NA(EARO)   |               |               |
          |<--------------|               |               |
```
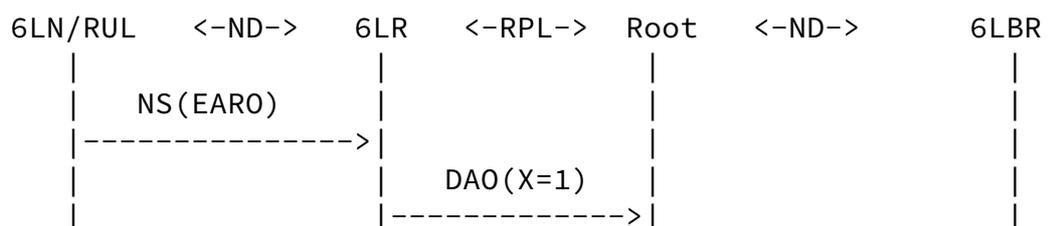
                 Figure 8: Next RUL Registration Flow

This is what causes the RPL DODAG root to refresh the state in the
6LBR, using an EDAC message. In the case of an error in the proxied
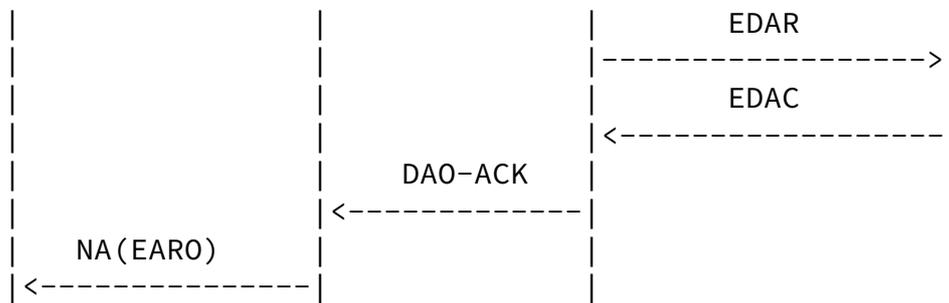EDAR flow, the error is returned in the DAO-ACK using a RPL Status
with the 'A' flag set to 1, which embeds a 6LoWPAN Status value as
discussed in Section 6.3.

The 6LR may receive a requested DAO-ACK after it received an
asynchronous Non-Storing DCO, but the non-zero 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).

An issue may be detected later, e.g., the address moves to a
different DODAG with the 6LBR attached to a different 6LoWPAN
Backbone Router (6BBR); see Figure 5 in Section 3.3 of [RFC8929].
The 6BBR may send a negative ND Status, e.g., in an asynchronous
NA(EARO) to the 6LBR.

[RFC8929] expects that the 6LBR is co-located with the RPL DODAG
root, but if not, the 6LBR MUST forward the status code to the
originator of the EDAR -- either the 6LR or the RPL DODAG root that
proxies for it. The ND status code is mapped in a RPL Status value
by the RPL DODAG root, and then back to an ND Status by the 6LR to
the 6LN. Note that a legacy RAN that receives a Non-Storing DCO that
it does not support will ignore it silently, as specified in
Section 6 of [RFC6550]. The result is that it will remain unaware
that it is no longer reachable until its next RPL exchange happens.
This situation will be cleared upon the next Non-Storing DAO exchange
if the error is returned in a DAO-ACK.

Figure 9 illustrates this in the case where the 6LBR and the root are
not co-located, and the root proxies the EDAR/EDAC flow.

```
   6LN/RUL  <-ND->  6LR  <-RPL->  Root  <-ND->  6LBR  <-ND->  6BBR
      |               |               |               |        |
      |               |               |               |  NA(EARO)  |
      |               |               |               |<-----------|
      |               |               |    EDAC       |        |
      |               |               |<------------- |        |
      |               |     DCO       |               |        |
```

```
         |                 |<-----------|                 |                 |
         |    NA(EARO)     |            |                 |                 |
         |<------------|            |                 |                 |
         |                 |            |                 |                 |
```
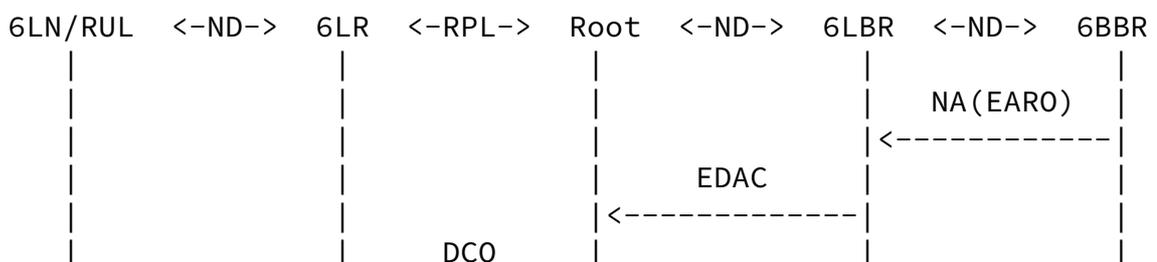
                     Figure 9: Asynchronous Issue

   If the root does not proxy, then the EDAC with a non-zero status
   reaches the 6LR directly. In that case, the 6LR MUST clean up the
   route using a DAO with a Lifetime of 0, and it MUST propagate the
   status back to the RUL in an NA(EARO) with the R flag set to 0.

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

   All or any combination of the 6LR, the root, and the 6LBR might be
   collapsed in a single node.

9.2. Detailed Operation

   The following sections specify the behavior of (1) the 6LN acting as
   a RUL, (2) the 6LR acting as a border router and serving the 6LN,
   (3) the RPL DODAG root, and (4) the 6LBR in the control flows that
   enable RPL routing back to the RUL, respectively.

9.2.1. Perspective of the 6LN Acting as a RUL

   This specification builds on the operation of a 6LoWPAN ND-compliant
   6LN/RUL, which is expected to operate as follows:

   1. The 6LN selects a 6LR that provides reachability services for a
       RUL. This is signaled by a 6CIO in the RA messages with the L,
       P, and E flags set to 1 as prescribed by [RFC8505].

   2. The 6LN obtains an IPv6 global address, via either (1) Stateless
       Address Autoconfiguration (SLAAC) [RFC4862] based on a Prefix
       Information Option (PIO) [RFC4861] found in an RA message or
       (2) some other means, such as DHCPv6 [RFC8415].

   3. Once it has formed an address, the 6LN registers its address and
       refreshes its registration periodically, early enough 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 sets the T flag to 1 as prescribed in
       [RFC8505]. 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]).

4. As stated in [Section 5.2 of [RFC8505]](), the 6LN can register with
    more than one 6LR at the same time. In that case, all the fields
    in the EARO are set to the same value for all of the parallel
    Address Registrations, with the exception of the Registration
    Lifetime field and the R flag, which may be set to different
    values. The 6LN may cancel a subset of its registrations or may
    transfer a registration from one or more old 6LRs to one or more
    new 6LRs. To do so, the 6LN sends a series of NS(EARO) messages,
    all with the same TID, with a zero Registration Lifetime to the
    old 6LR(s) and with a non-zero Registration Lifetime to the new
    6LR(s). In that process, the 6LN SHOULD send the NS(EARO) with a
    non-zero Registration Lifetime and ensure that at least one
    succeeds before it sends an NS(EARO) that terminates another
    registration. This avoids the churn related to transient route
    invalidation in the RPL network above the common parent of the
    involved 6LRs.

5. Following [Section 5.1 of [RFC8505]](), a 6LN acting as a RUL sets
    the R flag in the EARO of its registration(s) for which it
    requires routing services. If the R flag is not echoed in the
    NA, the RUL MUST assume that establishing the routing services
    via this 6LR failed, and it SHOULD attempt to use another 6LR.
    The RUL SHOULD ensure that one registration succeeds before
    setting the R flag to 0. In the case of a conflict with the
    preceding rule regarding the lifetime, the rule regarding the
    lifetime has precedence.

6. The 6LN may use any of the 6LRs to which it registered as the
    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 Improvement (SAVI) function [[RFC7039]()] and thus is not
    recommended.

Even without support for RPL, the RUL may be configured with an
opaque value to be provided to the routing protocol. If the RUL has
knowledge of the RPL Instance into which the packet should be
injected, then it SHOULD set the Opaque field in the EARO to the
RPLInstanceID; otherwise, it MUST leave the Opaque field as 0.

Regardless of the setting of the Opaque field, the 6LN MUST set the
"I" field to 0 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 minimal awareness of
the RPL Instance, then it can build an RPI. A RUL that places an RPI
in a data packet SHOULD indicate the RPLInstanceID of the RPL
Instance where the packet should be forwarded. It is up to the 6LR
(e.g., by policy) to use the RPLInstanceID information provided by
the RUL or rewrite it to the selected RPLInstanceID for forwarding
inside the RPL domain. All the flags and the SenderRank field are

set to 0 as specified by Section 11.2 of [RFC6550].

9.2.2. Perspective of the 6LR Acting as a Border Router

A 6LR that provides 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 to 1 as prescribed by [RFC8505].

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.

If the R flag is set to 1 in the NS(EARO), the 6LR SHOULD 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 RPL Non-Storing
mode signaling and the updated Target option (see Section 6.1). To
avoid a redundant EDAR/EDAC flow to the 6LBR, the 6LR SHOULD refrain
from setting the 'X' flag. The 6LR MUST request a DAO-ACK by setting
the 'K' flag in the DAO message. Successfully injecting the route to
the RUL's address will be indicated via the 'U' flag set to 0 in the
RPL Status of the DAO-ACK message.

For the registration refreshes, if the RPL DODAG root sets the 'P'
flag in the DODAG Configuration option to 1, then the 6LR MUST
refrain from sending the keep-alive EDAR; instead, it MUST set the
'X' flag to 1 in the Target option of the DAO messages, to request
that the root proxy the keep-alive EDAR/EDAC exchange with the 6LBR
(see Section 6); if the 'P' flag is set to 0, then the 6LR MUST set
the 'X' flag to 0 and handle the EDAR/EDAC flow itself.

The Opaque field in the EARO provides a means to signal which RPL
Instance is to be used for the DAO advertisements and the forwarding
of packets sourced at the Registered Address when there is no RPI in
the packet.

As described in [RFC8505], if the "I" field is 0, then the Opaque
field is expected to carry the RPLInstanceID suggested by the 6LN;
otherwise, there is no suggested RPL Instance. If the 6LR
participates in the suggested RPL Instance, then the 6LR MUST use
that RPL Instance for the Registered Address.

If there is no suggested RPL Instance or if the 6LR does not
participate in the suggested RPL Instance, it is expected that the
packets coming from the 6LN "can unambiguously be associated to at
least one RPL Instance" [RFC6550] by the 6LR, e.g., using a policy
that maps the 6-tuple to a RPL Instance.

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

1. The Registered Address is signaled as the Target Prefix in the
    updated Target option in the DAO message; the Prefix Length is
    set to 128 but the 'F' flag is set to 0, since the advertiser is
    not the RUL. 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 TIO associated with the
    Target option.

3. The 6LR sets the External ('E') flag in the TIO to indicate that
    it is redistributing an external target into the RPL network.

4. The Path Lifetime in the TIO is computed from the Registration
    Lifetime in the EARO. This operation converts seconds to the
    Lifetime Units used in the RPL operation. This creates the
    deployment constraint that the Lifetime Unit is reasonably
    compatible with the expression of the Registration Lifetime;
    e.g., a Lifetime Unit of 0x4000 maps the most significant byte of
    the Registration Lifetime to the Path Lifetime.

    In that operation, the Path Lifetime must be set to ensure that
    the path has a longer lifetime than the registration and also
    covers the round-trip time to the root.

    Note that if the Registration Lifetime is 0, then the Path
    Lifetime is also 0 and the DAO message becomes a No-Path DAO,
    which cleans up the routes down to the RUL's address; 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.

Upon receiving or timing out the DAO-ACK after an implementation-
specific number of retries, the 6LR MUST send the corresponding
NA(EARO) to the RUL. Upon receiving an asynchronous DCO message, it
MUST send an asynchronous NA(EARO) to the RUL immediately but still
be capable of processing the DAO-ACK if one is pending.

The 6LR MUST set the R flag to 1 in the NA(EARO) that it sends back
to the 6LN if and only if the 'U' flag in the RPL Status is set to 0,
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 to 1, the embedded Status
value is passed back to the RUL in the EARO Status. If the 'U' flag
is also set to 1, the registration failed for 6LoWPAN-ND-related
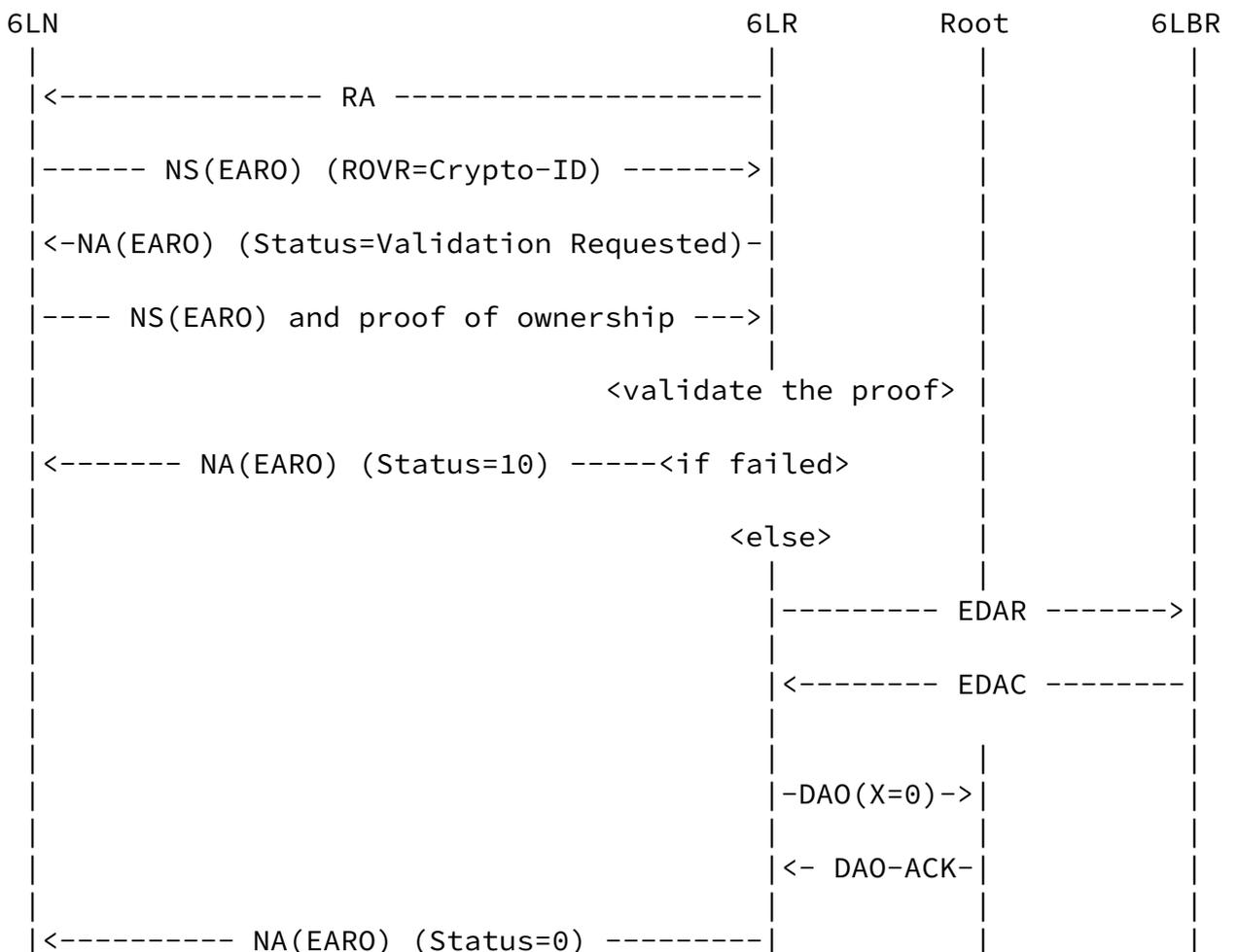reasons, and the NCE is removed.

An error injecting the route causes the 'U' flag to be set to 1. If

the error is not related to ND, the 'A' flag is set to 0. In that
case, the registration succeeds, but the RPL route is not installed.
So, the NA(EARO) is returned with a status indicating success but the
R flag set to 0, which means that the 6LN obtained a binding but no
route.

If the 'A' flag is set to 0 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 6LN. The EARO Status of 0 MUST also be used
if the 6LR did not attempt to inject the route but could create the
binding after a successful EDAR/EDAC exchange or refresh it.

If the 'U' flag is set to 1 in the RPL Status of the DAO-ACK, then
the route was not installed, and the R flag MUST be set to 0 in the
NA(EARO). The R flag MUST be set to 0 if the 6LR did not attempt to
inject the route.

In a network where Address-Protected Neighbor Discovery (AP-ND) is
enabled, in the case of a DAO-ACK or a DCO 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
[RFC8928], before the registration is complete. This flow,
illustrated in Figure 10, ensures that the address is validated
before it is injected in the RPL routing.

```
6LN                                           6LR       Root        6LBR
 |                                             |         |           |
 |<-------------- RA --------------------|     |         |           |
 |                                             |         |           |
 |------ NS(EARO) (ROVR=Crypto-ID) ------>|    |         |           |
 |                                             |         |           |
 |<-NA(EARO) (Status=Validation Requested)-|   |         |           |
 |                                             |         |           |
 |---- NS(EARO) and proof of ownership --->|   |         |           |
 |                                             |         |           |
 |                            <validate the proof> |     |           |
 |                                             |         |           |
 |<------- NA(EARO) (Status=10) -----<if failed>   |     |           |
 |                                             |         |           |
 |                                <else>       |         |           |
 |                                             |         |           |
 |                                             |--------- EDAR ------->|
 |                                             |         |           |
 |                                             |<------- EDAC --------|
 |                                             |         |           |
 |                                             |         |           |
 |                                             |-DAO(X=0)->|          |
 |                                             |         |           |
 |                                             |<- DAO-ACK-|          |
 |                                             |         |           |
 |<---------- NA(EARO) (Status=0) ---------|   |         |           |
```

```
|                                        |        |           |
|                                       ...       |           |
|                                        |        |           |
|------- NS(EARO) (ROVR=Crypto-ID) ------>|        |           |
|                                        |-DAO(X=1)->|         |
|                                        |        |-- EDAR -->|
|                                        |        |           |
|                                        |        |<-- EDAC --|
|                                        |<- DAO-ACK-|         |
|<---------- NA(EARO) (Status=0) ---------|        |           |
|                                        |        |           |
                                        ...
```
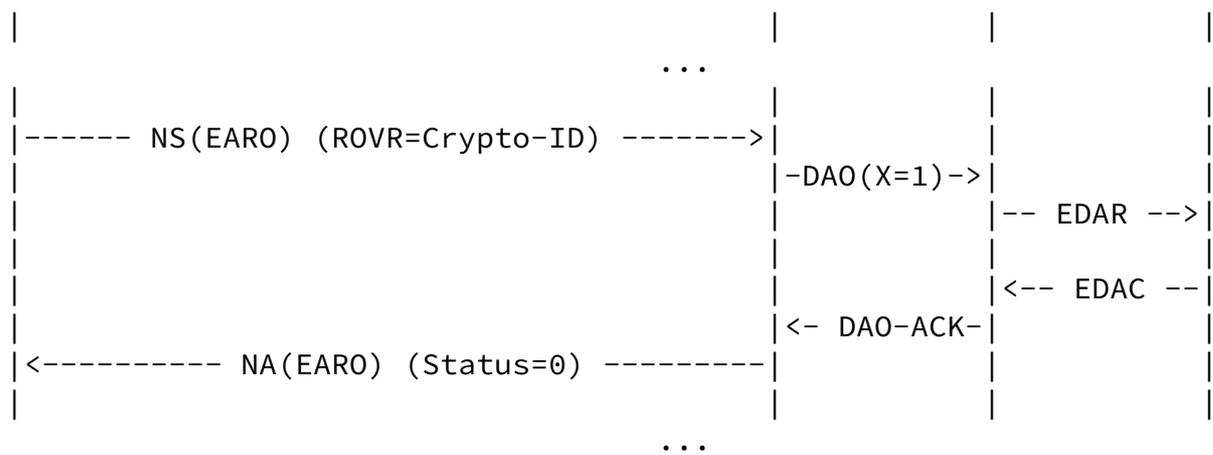
                Figure 10: Address Protection

If the challenge succeeded, 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 Denial-Of-Service (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 set to 0 to signal that it has stopped providing routing
services, and/or with an EARO Status of 2 (Neighbor Cache Full) to
signal that it removed the NCE. It may also send a final RA --
unicast or multicast -- with a router Lifetime field of 0, to signal
that it will cease to serve as the router, as specified in
Section 6.2.5 of [RFC4861]. This may happen upon a DCO or a DAO-ACK
message indicating that the path is already removed; otherwise, the
6LR MUST remove the host route to the 6LN using a DAO message with a
Path Lifetime of 0.

A valid NS(EARO) message with the R flag set to 0 and a Registration
Lifetime that is not zero signals that the 6LN wishes to maintain the
binding but does not require (i.e., no longer requires) the routing
services from the 6LR. Upon this message, if, due to a previous
NS(EARO) with the R flag set to 1 the 6LR was injecting the host
route to the Registered Address in RPL using DAO messages, then the
6LR MUST invalidate the host route in RPL using a DAO with a Path
Lifetime of 0. It is up to the registering 6LN to maintain the
corresponding route from then on, by either (1) keeping it active via
a different 6LR or (2) acting as a RAN and managing its own
reachability.

When forwarding a packet from the RUL into the RPL domain, if the
packet does not have an RPI, the 6LR MUST encapsulate the packet to
the root and add an RPI. If there is an RPI in the packet, the 6LR
MUST rewrite the RPI, but it does not need to encapsulate.

9.2.3. Perspective of the RPL DODAG Root

A RPL DODAG root MUST set the 'P' flag to 1 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.

Upon reception of a DAO message, for each updated RPL Target option
(see Section 6.1) with the 'X' flag set to 1, the root MUST notify
the 6LBR by using a proxied EDAR/EDAC exchange; if the RPL DODAG root
and the 6LBR are integrated, an internal API can be used instead.

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. Otherwise, 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 to 1.

The proxied EDAR/EDAC exchange MUST be protected with a timer whose
appropriate duration and number of retries (1) are implementation
dependent and (2) SHOULD be configurable, since the root and the 6LBR
are typically nodes with a higher capacity and manageability than
6LRs. Upon timing out, the root MUST send an error back to the 6LR
as above, using either a DAO-ACK or a DCO, as appropriate, with the
'A' and 'U' flags set to 1 in the RPL Status, and a RPL Status value
of "6LBR Registry Saturated" [RFC8505].

9.2.4. Perspective of the 6LBR

The 6LBR is unaware that the RPL DODAG 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 behaves as prescribed by
[RFC8505] and returns an EDAC message to the sender.

10. Protocol Operations for Multicast Addresses

   Section 12 of [RFC6550] details RPL support for multicast flows.
   This support is activated by setting the MOP value to 3 ("Storing
   Mode of Operation with multicast support") in the DIO messages that
   form the DODAG. This section also applies if and only if the MOP of
   the RPL Instance is 3.

   RPL support for multicast 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 copied and
   transmitted 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 Version 2 (MLDv2) for IPv6" [RFC3810]
   provides an interface for a listener to register with multicast
   flows. In the MLD model, the router is a "querier", and the host is
   a multicast listener that registers with the querier to obtain copies
   of the particular flows it is interested in.

   The equivalent of the first Address Registration happens as
   illustrated in Figure 11. The 6LN, as an MLD listener, sends an
   unsolicited Report to the 6LR. This enables it to start receiving
   the flow immediately and causes the 6LR to inject the multicast route
   in RPL.

```
     6LN/RUL                6LR              Root               6LBR
        |                    |                |                    |
        | unsolicited Report |                |                    |
        |------------------->|                |                    |
        |                    | DAO            |                    |
        |                    |-------------->|                    |
        |                    |    DAO-ACK     |                    |
        |                    |<-------------|                    |
        |                    |                | <if not done already> |
        |                    |                |   unsolicited Report   |
        |                    |                |-------------------->|
        |                    |                |                    |
```
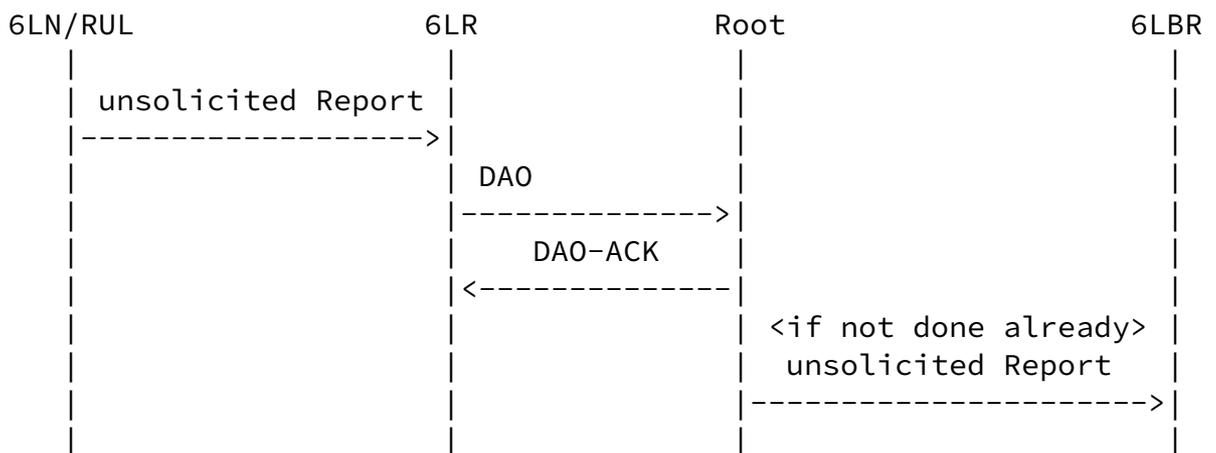
            Figure 11: First Multicast Registration Flow

   This specification does not change MLD but will operate more
   efficiently if the asynchronous messages for unsolicited Report and
   Done are sent by the 6LN as Layer 2 unicast to the 6LR, particularly
   on wireless.

   The 6LR acts as a generic MLD querier and generates a DAO with the
   multicast address as the Target Prefix as described in Section 12 of
   [RFC6550]. As for the unicast host routes, the Path Lifetime

associated to the Target is mapped from the Query Interval and is set
to be larger, to account for variable propagation delays to the root.
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 Target option for a multicast address, the RPL
DODAG root checks to see if it is already registered as a listener
for that address, and if not, it performs its own unsolicited Report
for the multicast address as described in Section 6.1 of [RFC3810].
The Report is source independent, so there is no source address
listed.

The equivalent of the registration refresh is pulled periodically by
the 6LR acting as the querier. Upon the timing out of the Query
Interval, the 6LR sends a Multicast Address Specific Query to each of
its listeners, for each multicast address. The listeners respond
with a Report. Based on the Reports, the 6LR maintains the
aggregated list of all the multicast addresses for which there is a
listener and advertises them using DAO messages as specified in
Section 12 of [RFC6550]. Optionally, the 6LR MAY send a General
Query, where the Multicast Address field is set to 0. In that case,
the multicast packet is passed as a Layer 2 unicast to each of the
interested children.

Upon a Report, the 6LR generates a DAO with as many Target options as
there are Multicast Address Records in the Report message, copying
the Multicast Address field in the Target Prefix of the RPL Target
option. The DAO message is a Storing mode DAO, passed to a selection
of the 6LR's parents.

Asynchronously to this, a similar procedure happens between the root
and a router, such as the 6LBR, that serves multicast flows on the
link where the root is located. Again, the Query and Report messages
are source independent. The root lists exactly once each multicast
address for which it has at least one active multicast DAO state,
copying the multicast address in the DAO state in the Multicast
Address field of the Multicast Address Records in the Report message.

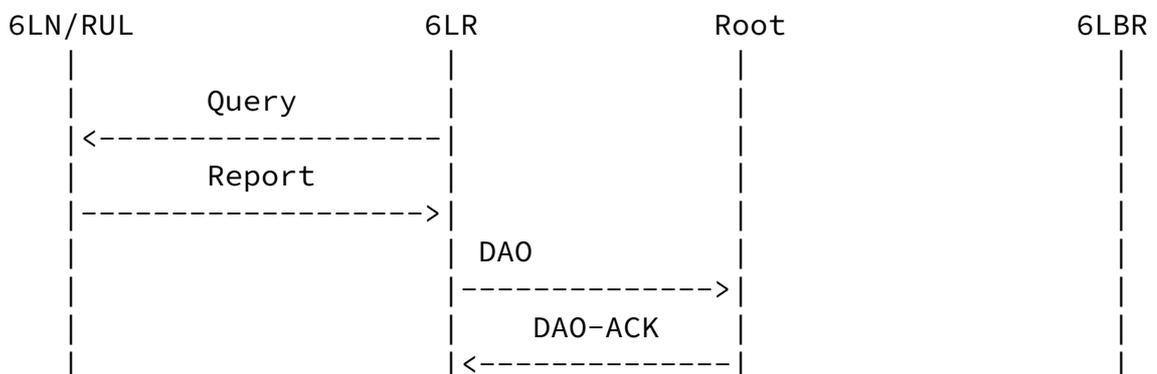This is illustrated in Figure 12:

```
    6LN/RUL                  6LR                 Root                6LBR
       |                      |                   |                   |
       |        Query         |                   |                   |
       |<-------------------- |                   |                   |
       |        Report        |                   |                   |
       |-------------------->|                    |                   |
       |                      | DAO               |                   |
       |                      |------------------->|                  |
       |                      |     DAO-ACK       |                   |
       |                      |<--------------    |                   |
```

```
            |                   |                   |        Query        |
            |                   |                   |<--------------------|
            |                   |                   |        Report       |
            |                   |                   |-------------------->|
            |                   |                   |                     |
```

                   Figure 12: Next Registration Flow

   Note that all or any combination of the 6LR, the root, and the 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

   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 improves this situation by isolating edge nodes that
   can only interact with the RPL routers using 6LoWPAN ND, meaning that
   they cannot perform RPL insider attacks.

   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 such threats
   as black-holing (see Section 7 of [RFC7416]), DoS attacks whereby a
   rogue 6LR creates a high churn in the RPL network by advertising and
   removing many forged addresses, or a bombing attack whereby an
   impersonated 6LBR would destroy state in the network by using a
   status code of 4 ("Removed") [RFC8505].

   This trust model could be, at a minimum, based on Layer 2 secure
   joining and link-layer security. This is a generic 6LoWPAN
   requirement; see Req-5.1 in Appendix B.5 of [RFC8505].

   In a general manner, the Security Considerations sections of
   [RFC6550], [RFC7416], [RFC6775], and [RFC8505] apply to this
   specification as well.

   In particular, link-layer security is needed to prevent DoS attacks
   whereby a rogue 6LN creates a high churn in the RPL network by
   constantly registering and deregistering addresses with the R flag
   set to 1 in the EARO.

   [RFC8928] updated 6LoWPAN ND with AP-ND. AP-ND protects the owner of
   an address against address theft and impersonation attacks in an LLN.
   Nodes supporting the extension compute a cryptographic identifier
   (Crypto-ID) and use it with one or more of their Registered
   Addresses. The Crypto-ID identifies the owner of the Registered
   Address and can be used to provide proof of ownership of the
   Registered Addresses. Once an address is registered with the
   Crypto-ID and proof of ownership is provided, only the owner of that

address can modify the registration information, thereby enforcing
SAVI. [RFC8928] reduces even further the attack perimeter that is
available to the edge nodes, and its use is suggested in this
specification.

Additionally, the trust model could include role validation (e.g.,
using role-based authorization) to ensure that the node that claims
to be a 6LBR or a RPL DODAG root is entitled to do so.

The Opaque field in the EARO enables the RUL to suggest a
RPLInstanceID where its traffic is placed. It is also possible for
an attacker RUL to include an RPI in the packet. This opens the door
to attacks where a RPL Instance would be reserved for critical
traffic, e.g., with a specific bandwidth reservation, that the
additional traffic generated by a rogue may disrupt. The attack may
be alleviated by traditional access control and traffic-shaping
mechanisms where the 6LR controls the incoming traffic from the 6LN.
More importantly, the 6LR is the node that injects the traffic in the
RPL domain, so it has the final word on which RPL Instance is to be
used for the traffic coming from the RUL, per its own policy. In
particular, a policy can override the formal language that forces the
use of the Opaque field or the rewriting of the RPI provided by the
RUL, in a situation where the network administrator finds it
relevant.

At the time of this writing, RPL does not have a route ownership
validation 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.

Section 6.1 indicates that when the length of the ROVR field is
unknown, the RPL Target option must be passed on as received in RPL
Storing mode. This creates a possible opening for using DAO messages
as a covert channel. Note that DAO messages are rare, and overusing
that channel could be detected. An implementation SHOULD notify the
network management system when a RPL Target option is received with
an unknown ROVR field size, to ensure that the network administrator
is aware of the situation.

[RFC9009] introduces the ability for a rogue common ancestor node to
invalidate a route on behalf of the target node. In this case, the
RPL Status in the DCO has the 'A' flag set to 0, and an NA(EARO) is
returned to the 6LN with the R flag set to 0. This encourages the
6LN to try another 6LR. If a 6LR exists that does not use the rogue
common ancestor, then the 6LN will eventually succeed gaining
reachability over the RPL network in spite of the rogue node.

12. IANA Considerations

12.1. Fixing the Address Registration Option Flags

Section 9.1 of [RFC8505] created a registry for the 8-bit Address
Registration Option Flags field. IANA has renamed the first column
of the table from "ARO Status" to "Bit Number".

12.2. Resizing the ARO Status Values

Section 12 of [RFC6775] created the "Address Registration Option
Status Values" registry with a range of 0-255.

This specification reduces that range to 0-63; see Section 6.3.

IANA has modified the "Address Registration Option Status Values"
registry so that the upper bound of the unassigned values is 63.
This document has been added as a reference. The registration
procedure has not changed.

12.3. New RPL DODAG Configuration Option Flag

IANA has assigned the following flag in the "DODAG Configuration
Option Flags for MOP 0..6" registry [RFC9008]:

```
    +------------+--------------------------+-----------+
    | Bit Number | Capability Description    | Reference |
    +------------+--------------------------+-----------+
    | 1          | Root Proxies EDAR/EDAC (P) | RFC 9010  |
    +------------+--------------------------+-----------+
```

            Table 2: New DODAG Configuration Option Flag

IANA has added this document as a reference for MOP 7 in the RPL
"Mode of Operation" registry.

12.4. RPL Target Option Flags Registry

This document modifies the "RPL Target Option Flags" registry
initially created per Section 20.15 of [RFC6550]. The registry now
includes only 4 bits (Section 6.1) and lists this document as an
additional reference. The registration procedure has not changed.

Section 6.1 also defines two new entries in the registry, as follows:

```
    +------------+------------------------------+-----------+
    | Bit Number | Capability Description        | Reference |
    +------------+------------------------------+-----------+
    | 0          | Advertiser address in Full (F) | RFC 9010  |
    +------------+------------------------------+-----------+
    | 1          | Proxy EDAR Requested (X)       | RFC 9010  |
    +------------+------------------------------+-----------+
```

            Table 3: RPL Target Option Flags Registry

12.5. New Subregistry for RPL Non-Rejection Status Values

   IANA has created a new subregistry for the RPL Non-Rejection Status
   values for use in the RPL DAO-ACK, DCO, and DCO-ACK messages with the
   'A' flag set to 0 and the 'U' flag set to 1, under the "Routing
   Protocol for Low Power and Lossy Networks (RPL)" registry.

   * Possible values are 6-bit unsigned integers (0..63).

   * The registration procedure is IETF Review [RFC8126].

   * The initial allocation is as indicated in Table 4:

   +-------+-------------------------------+--------------------+
   | Value | Meaning | Reference |
   +-------+-------------------------------+--------------------+
   | 0 | Success / Unqualified acceptance | RFC 6550 / RFC 9010 |
   +-------+-------------------------------+--------------------+
   | 1..63 | Unassigned | |
   +-------+-------------------------------+--------------------+

                Table 4: Acceptance Values of the RPL Status

12.6. New Subregistry for RPL Rejection Status Values

   IANA has created a new subregistry for the RPL Rejection Status
   values for use in the RPL DAO-ACK and DCO messages with the 'A' flag
   set to 0 and the 'U' flag set to 1, under the "Routing Protocol for
   Low Power and Lossy Networks (RPL)" registry.

   * Possible values are 6-bit unsigned integers (0..63).

   * The registration procedure is IETF Review [RFC8126].

   * The initial allocation is as indicated in Table 5:

           +-------+----------------------+-----------+
           | Value | Meaning | Reference |
           +-------+----------------------+-----------+
           | 0 | Unqualified rejection | RFC 9010 |
           +-------+----------------------+-----------+
           | 1 | No routing entry | RFC 9009 |
           +-------+----------------------+-----------+
           | 2..63 | Unassigned | |
           +-------+----------------------+-----------+

                Table 5: Rejection Values of the RPL Status

13. References

13.1. 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>.

   [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>.

   [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>.

   [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>.

   [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>.

   [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>.

   [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>.

   [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>.

   [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>.

   [RFC8928] Thubert, P., Ed., Sarikaya, B., Sethi, M., and R. Struik,
              "Address-Protected Neighbor Discovery for Low-Power and
              Lossy Networks", RFC 8928, DOI 10.17487/RFC8928, November
              2020, <https://www.rfc-editor.org/info/rfc8928>.

   [RFC9008] Robles, M.I., Richardson, M., and P. Thubert, "Using RPI
              Option Type, Routing Header for Source Routes, and IPv6-
              in-IPv6 Encapsulation in the RPL Data Plane", RFC 9008,
              DOI 10.17487/RFC9008, April 2021,
              <https://www.rfc-editor.org/info/rfc9008>.

   [RFC9009] Jadhav, R.A., Ed., Thubert, P., Sahoo, R.N., and Z. Cao,
              "Efficient Route Invalidation", RFC 9009,
              DOI 10.17487/RFC9009, April 2021,
              <https://www.rfc-editor.org/info/rfc9009>.

13.2. Informative References

   [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>.

   [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>.

   [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>.

   [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>.

[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>.

[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>.

[RFC7039] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, Ed.,
           "Source Address Validation Improvement (SAVI) Framework",
           RFC 7039, DOI 10.17487/RFC7039, October 2013,
           <https://www.rfc-editor.org/info/rfc7039>.

[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>.

[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>.

[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>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A.,
           Richardson, M., Jiang, S., Lemon, T., and T. Winters,
           "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)",
           RFC 8415, DOI 10.17487/RFC8415, November 2018,
           <https://www.rfc-editor.org/info/rfc8415>.

   [RFC8929] Thubert, P., Ed., Perkins, C.E., and E. Levy-Abegnoli,
              "IPv6 Backbone Router", RFC 8929, DOI 10.17487/RFC8929,
              November 2020, <https://www.rfc-editor.org/info/rfc8929>.

Appendix A. Example Compression

   Figure 13 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 it 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 13: Encapsulation to Parent 6LR in Storing Mode

   The difference from the example presented in Figure 19 of [RFC8138]
   is the addition of an SRH-6LoRH before the RPI-6LoRH to transport the
   compressed address of the 6LR as the destination address of the outer
   IPv6 header. In Figure 19 of [RFC8138], 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 13, the source of the IPv6-in-IPv6 encapsulation is the
   root, so it is elided in the IPv6-in-IPv6 6LoRH. The destination is
   the parent 6LR of the destination of the encapsulated 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. The result is 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 13 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 the RPI-6LoRH and then the IPv6-in-
   IPv6 6LoRH. When the IPv6-in-IPv6 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 encapsulated packet compressed per
[RFC6282].

Acknowledgments

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
URI: https://www.sandelman.ca/