Workgroup: ROLL
Updates: 6550, 6775, 8505 (if approved)
Published: 9 December 2020
Intended Status: Standards Track
Expires: 12 June 2021
Authors: P. Thubert, Ed. M. Richardson
Cisco Systems Sandelman

Routing for RPL Leaves

Abstract

This specification updates RFC6550, RFC6775, and RFC8505, to provide routing services to RPL Unaware Leaves that implement 6LoWPAN ND and the extensions therein.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

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

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

This Internet-Draft will expire on 12 June 2021.

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

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

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

RPL can be deployed in conjunction with IPv6 Neighbor Discovery (ND) [RFC4861] [RFC4862] and 6LoWPAN ND [RFC6775] [RFC8505] to maintain reachability within a Non-Broadcast Multiple-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 terminate packets, acting as Hosts in the data-plane. In [RFC6550] terms, an IPv6 Host [RFC8504] that is reachable over the RPL network is called a Leaf.

Section 2 of [USEofRPLinfo] 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 router(s); 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 to RPL, and relies on its RPL router(s) also to inject the routes to its IPv6 addresses in the RPL domain.

A RUL may be unable to participate because it is very energy-constrained, 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, and can protect RUL for its address ownership.

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.

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 of [USEofRPLinfo].

Examples of possible RULs include severely energy constrained sensors such as window smash sensor (alarm system), and kinetically powered light switches. Other applications of this specification may include a smart grid network that controls appliances - such as washing machines or the heating system - in the home. Appliances may not participate to the RPL protocol operated in the Smartgrid network but can still interact with the Smartgrid for control and/or metering.

This document is organized as follows:

* Section 3 and Section 4 present 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 expectations 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 DAO message based on the ND registration by the 6LN, and the RPL root performs the EDAR/EDAC exchange with the 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 [EFFICIENT-NPDAO]; the use of the DCO message is extended to the Non-Storing 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 ND status codes is reduced down to 64 values, and the remaining bits in the original status field are now reserved.

* Section 9 and Section 10 present the operation of this specification for unicast and multicast flows, respectively, and Section 11 presents associated security considerations.

2. Terminology

2.1. Requirements Language

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

2.2. Glossary

This document uses the following acronyms:

AR: Address Resolution (aka Address Lookup)
ARQ: Automatic Repeat reQuest
6CIO: 6LoWPAN Capability Indication Option
6LN: 6LoWPAN Node (a Low Power Host or Router)
6LR: 6LoWPAN Router
(E)ARO: (Extended) Address Registration Option
(E)DAR: (Extended) Duplicate Address Request
(E)DAC: (Extended) Duplicate Address Confirmation
DAD: Duplicate Address Detection
DAO: Destination Advertisement Object (a RPL message)
DCO: Destination Cleanup Object (a RPL message)
DIS: DODAG Information solicitation (a RPL message)
DIO: DODAG Information Object (a RPL message)
DODAG: Destination-Oriented Directed Acyclic Graph
LLN: Low-Power and Lossy Network
NA: Neighbor Advertisement
NCE: Neighbor Cache Entry
ND: Neighbor Discovery
NS: Neighbor solicitation
RA: Router Advertisement

ROVR: Registration Ownership Verifier
RPI: RPL Packet Information
RAL: RPL-Aware Leaf
RAN: RPL-Aware Node (either a RPL Router or a RPL-Aware Leaf)
RUL: RPL-Unaware Leaf
TID: Transaction ID (a sequence counter in the EARO)

2.3. References

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

"RPL", the "RPL Packet Information" (RPI), "RPL Instance" (indexed by a RPLInstanceID) are defined in "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks" [RFC6550]. The RPI is the abstract information that RPL defines to be placed in data packets, e.g., as the RPL Option [RFC6553] within the IPv6 Hop-By-Hop Header. By extension, the term "RPI" is often used to refer to the RPL Option itself. The DODAG Information solicitation (DIS), Destination Advertisement Object (DAO) and DODAG Information Object (DIO) messages are also specified in [RFC6550]. The Destination Cleanup Object (DCO) message is defined in [EFFICIENT-NPDAO].

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

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

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

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

6LoWPAN ND: Neighbor Discovery Optimization for Low-Power and Lossy Networks [RFC6775], "Registration Extensions for 6LoWPAN Neighbor

Discovery" [RFC8505], and "Address Protected Neighbor Discovery for Low-power and Lossy Networks" [RFC8928].

3. RPL External Routes and Dataplane Artifacts

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

A 6LR that acts as a border Router for external routes advertises them using Non-Storing Mode DAO messages that are unicast directly to the Root, even if the DODAG is operated in Storing Mode. Non-Storing Mode routes are not visible inside the RPL domain and all packets are routed via the Root. The RPL Root tunnels the packets directly to the 6LR that advertised the external route, which decapsulates and forwards the original (inner) packet.

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

The RPL data packets always carry a Hop-by-Hop Header to transport a RPL Packet Information (RPI) [RFC6550]. So unless the RUL originates its packets with an RPI, the 6LR needs to tunnel them to the Root to add the RPI. As a rule of a thumb and except for the very special case above, the packets from and to a RUL are always encapsulated using an IP-in-IP tunnel between the Root and the 6LR that serves the RUL (see sections 7 and 8 of [USEofRPLinfo] for details). If the packet from the RUL has an RPI, the 6LR as a RPL border router SHOULD rewrite the RPI to indicate the selected Instance and set the flags, but it does not need to encapsulate the packet.

In Non-Storing Mode, packets going down carry a Source Routing Header (SRH). The IP-in-IP encapsulation, the RPI and the SRH are collectively called the "RPL artifacts" and can be compressed using [RFC8138]. 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. [USEofRPLinfo] expects the RUL to support the basic "IPv6 Node Requirements" [RFC8504]. In particular the RUL is expected to ignore the RPL artifacts that are either consumed or not applicable to a Host.

A RUL is not expected to support the compression method defined in [RFC8138]. For that reason, the border router uncompresses the

packet before forwarding over an external route to a RUL [USEofRPLinfo].

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. RFC 6775 Address Registration

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 Lookup) and Duplicate Address Detection (DAD).

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

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

4.2. RFC 8505 Extended Address Registration

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

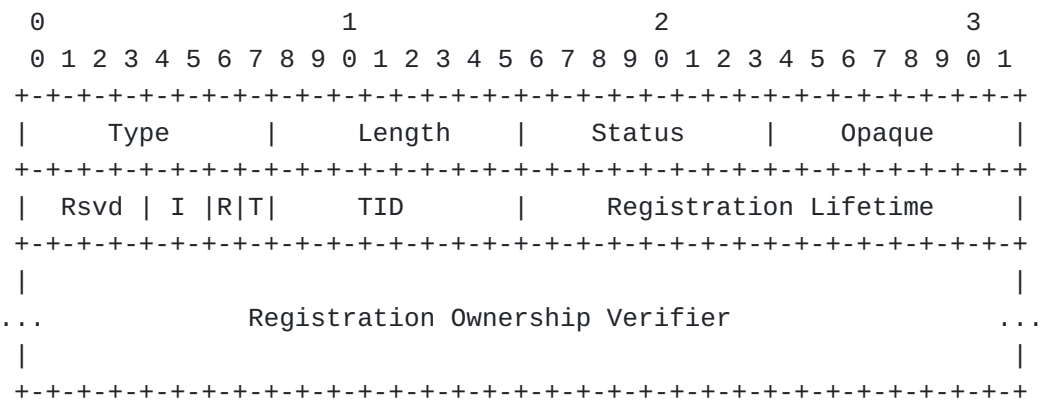

Figure 1: EARO Option Format

4.2.1. R Flag

[RFC8505] introduces the R Flag in the EARO. The Registering Node sets the R Flag to indicate whether the 6LR should ensure reachability for the Registered Address. If the R Flag is 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 that it uses another RPL Router for reachability services.

This document specifies how the R Flag is used in the context of RPL. A RPL Leaf that implements the 6LN functionality in [RFC8505] requires reachability services for an IPv6 address if and only if it sets the R Flag in the NS(EARO) used to register the address to a 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 R flag is set to 1 in an EARO that is placed either in an NS or an NA message.

4.2.2. TID, "I" Field and Opaque Fields

When the T Flag is set to 1, the EARO includes a sequence counter called Transaction ID (TID), that is needed to fill the Path Sequence Field in the RPL Transit Option. This is the reason why the support of [RFC8505] by the RUL, as opposed to only [RFC6775] is a prerequisite for this specification (more in Section 5.1). The EARO also transports an Opaque field and an associated "I" field that describes what the Opaque field transports and how to use it.

Section 9.2.1 specifies the use of the "I" field and the Opaque field by a RUL.

4.2.3. ROVR

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

"Address Protected Neighbor Discovery for Low-power and Lossy Networks" [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 ROVR field enable the 6LR to block traffic that is not sourced at an owned address.

This specification does not address how the protection 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. RFC 8505 Extended DAR/DAC

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

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

This specification avoids the periodic EDAR/EDAC exchange across the LLN. The 6LR turns the periodic NS(EARO) from the RUL into a DAO message to the Root on every refresh, but it only generates the EDAR upon the first registration, for the purpose of DAD, which must be verified before the address is injected in RPL. Upon the DAO message, the Root proxies the EDAR exchange to refresh the state at the 6LBR on behalf of the 6LR, as illustrated in Figure 7.

4.3.1. RFC 7400 Capability Indication Option

"6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)" [RFC7400] defines the

6LoWPAN Capability Indication Option (6CIO) that enables a node to expose its capabilities in Router Advertisement (RA) messages.

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

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

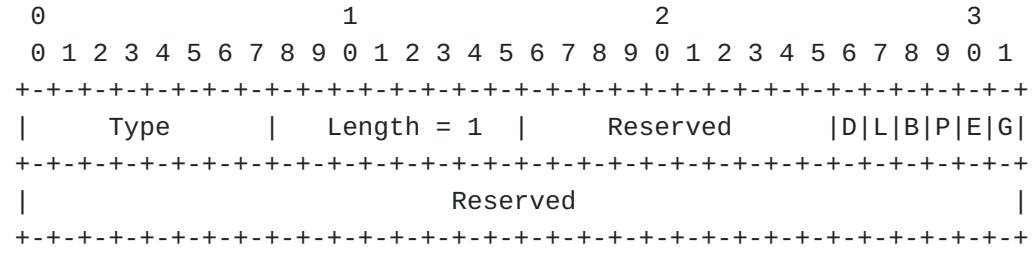

Figure 2: 6CIO flags

A 6LR that 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], more in Section 9.2.

5. Requirements on the RPL-Unware Leaf

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

5.1. Support of 6LoWPAN ND

To obtain routing services from a Router that implements this specification, a RUL needs to implement [RFC8505] and set the "R" and "T" flags in the EARO to 1 as discussed in Section 4.2.1 and Section 4.2.3, respectively. Section 9.2.1 specifies new behaviors for the RUL, e.g., when the R Flag set to 1 in a 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 CIO 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 implements [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 to 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 till the Address Registration finally shows on those routes.

[RFC8505] introduces error Status values in the NA(EARO) which can be received synchronously upon an NS(EARO) or asynchronously. The RUL 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 2.1 of [USEofRPLinfo] defines the rules for tunneling either to the final destination (e.g., a RUL) or to its attachment Router (designated as 6LR). In order to terminate the IP-in-IP 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 [USEofRPLinfo], this is not mandated by [RFC8504], so the Root typically terminates the IP-in-IP tunnel at the parent 6LR. It is thus not necessary for a RUL to support IP-in-IP decapsulation.

5.3. Support of the HbH Header

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

5.4. Support of the Routing Header

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

6. 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 [USEofRPLinfo], an IP-in-IP encapsulation between the 6LR and the RPL Root is used to carry the RPL artifacts and remove them when forwarding outside the RPL domain, e.g., to a RUL.

This document also synchronizes the liveness monitoring at the Root and the 6LBR. The same value of lifetime is used for both, and a single keep-alive message, the RPL DAO, traverses the RPL network. A new behavior is introduced whereby the RPL Root proxies the EDAR message to the 6LBR on behalf of the 6LR (more in Section 8), for any Leaf node that implements the 6LN functionality in [RFC8505].

Section 6.7.7 of [RFC6550] introduces the RPL Target Option, which can be used in RPL Control messages such as the DAO message to signal a destination prefix. This document adds the capabilities to transport 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 respectively by a new ROVR Size field being non-zero and a new "Advertiser address in Full" 'F' flag set to 1, more in Section 6.1.

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

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

Section 12 of [RFC6550] details the RPL support for multicast flows when the RPLInstance is operated in the MOP of 3 ("Storing Mode of Operation with multicast support"). This specification extends the RPL Root operation to proxy-relay the MLDv2 [RFC3810] operation between the RUL and the 6LR, more in 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 Root to generate the proxied EDAR message to the 6LBR.

The new 'F' flag is set to 1 to indicate that the Target Prefix field contains the IPv6 address of the advertising node, in which case the length of the Target Prefix field is 128 bits regardless of the value of the Prefix Length field. If the 'F' flag is set to 0, the Target Prefix field MUST be aligned to the next byte boundary after the size (expressed in bits) indicated by the Prefix Length field. Padding bits are reserved and set to 0 per 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 3. It is backward compatible with the Target Option 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.

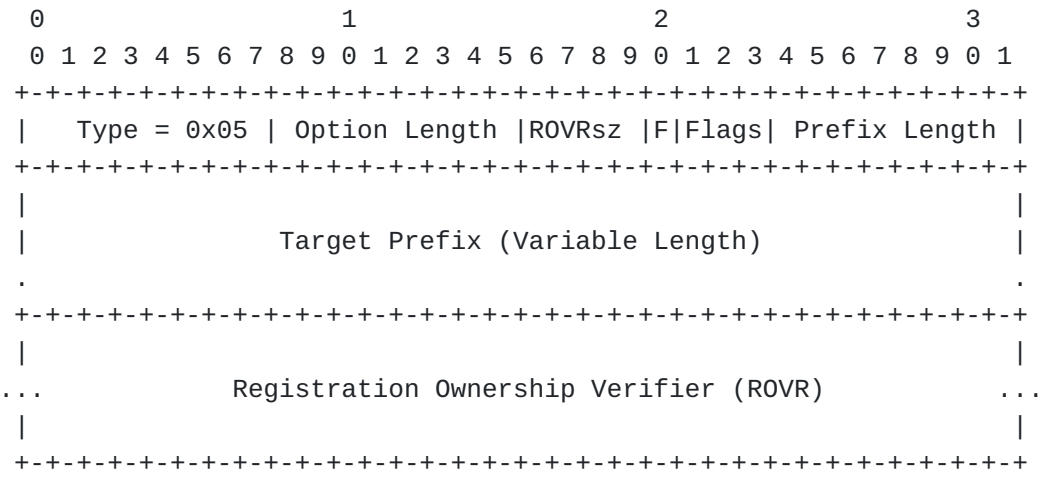

Figure 3: Updated Target Option

New fields:

ROVRsz (ROVR Size): Indicates the Size of the ROVR. It SHOULD be 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 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.

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

Flags: The 4 bits remaining unused in the Flags field are reserved for flags. The field MUST be initialized to zero by the sender and MUST be ignored by the receiver.

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

6.2. New 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 4 bit positions reserved for future use as Flags.

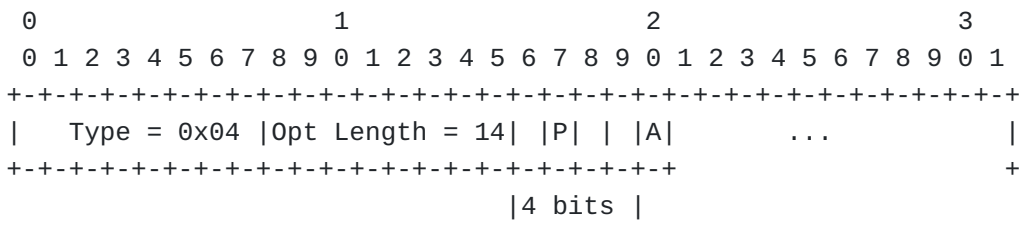

Figure 4: DODAG Configuration Option (Partial View)

This specification defines a new flag "Root Proxies EDAR/EDAC" (P). The 'P' flag is 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 respectively in Sections 20.14 and 6.7.6 of [RFC6550].

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 4.3 of [USEofRPLinfo] updates [RFC6550] to indicate that the definition of the Flags applies to Mode of Operation (MOP) values zero (0) to six (6) only. For a MOP value of 7, the implementation MUST consider 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 to 1 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 and values are assigned as follows:

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

Table 1: RPL Status per RFC 6550

The 6LoWPAN ND Status was defined for use in the EARO, see section 4.1 of [RFC8505]. This specification enables to carry the 6LoWPAN ND Status values in RPL DAO and DCO messages, embedded in the RPL Status field.

To achieve this, 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 5. See Section 12.2, Section 12.5, and Section 12.6 for the respective IANA declarations.

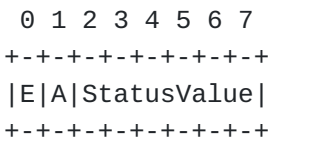

Figure 5: RPL Status Format

This specification updates the RPL Status with subfields as indicated below:

E: 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 Status value defined for IPv6 ND EARO. When the 'A' flag is set to 0, the Status value is defined for RPL.

When building a DCO or a DAO-ACK message upon an IPv6 ND NA or a EDAC message, the RPL Root MUST copy the 6LoWPAN ND status code unchanged in the RPL Status value and set the 'A' flag to 1. The RPL Root MUST set the 'E' 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 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 draft-ietf-roll-efficient-npdao

[EFFICIENT-NPDAO] 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 [EFFICIENT-NPDAO]; 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 attachment Router for a RUL. A 6LR and a Root that support this specification MUST implement the Non-Storing DCO.

8. Enhancements to RFC 6775 and RFC8505

This document updates [RFC6775] and [RFC8505] to reduce the range of the ND status codes down to 64 values. The two most significant (leftmost) bits if the original ND status field are now reserved, they MUST be set to zero by the sender and ignored by the receiver.

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

* If the RPL Root advertises the capability 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.

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

In a RPL network where the function is enabled, refreshing the state in the 6LBR is the responsibility of the Root. Consequently, only addresses that are injected in RPL will be kept alive at the 6LBR by the RPL Root. Since RULs are advertised using Non-Storing Mode, the DAO message flow and the keep alive EDAR/EDAC can be nested within the Address (re)Registration flow. Figure 6 illustrates that, for the first Registration, both the DAD and the keep-alive EDAR/EDAC exchanges happen in the same sequence.

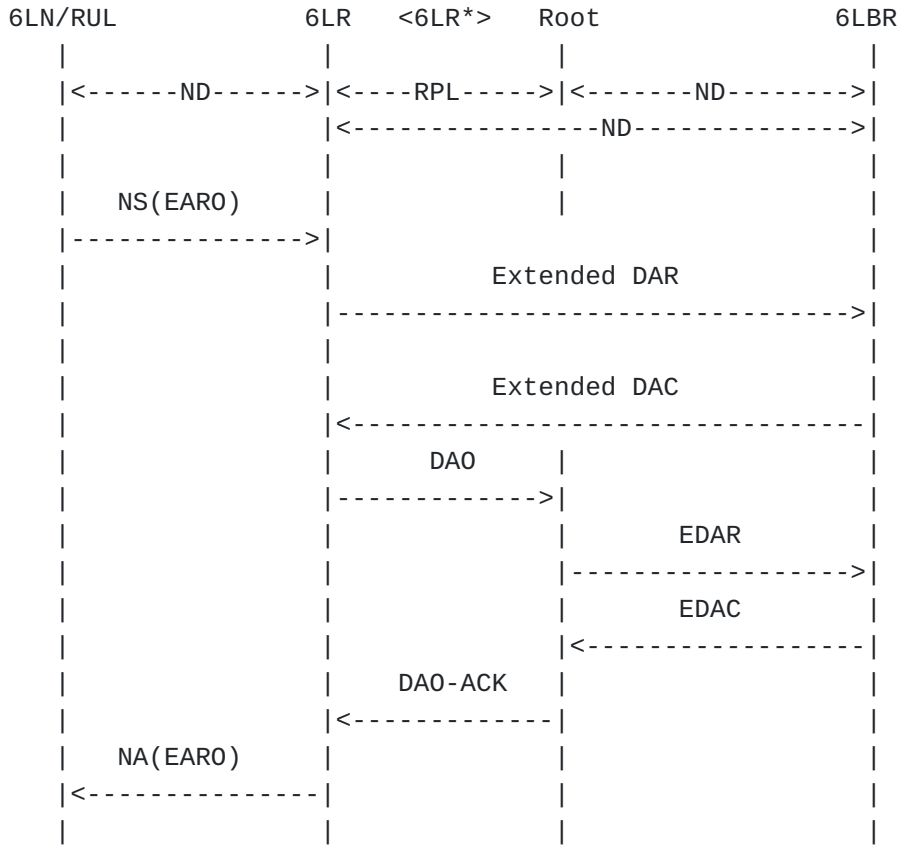

Figure 6: First RUL Registration Flow

This flow requires that the lifetimes and sequence counters in 6LoWPAN ND and RPL are 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 6 for RPL Non-Storing Mode, the Extended Duplicate Address exchange takes place as prescribed by [RFC8505]. If the exchange fails, the 6LR returns an NA message with a negative status to the 6LN, the NCE is not created, and the address is not injected in RPL. 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 maintain 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 7.

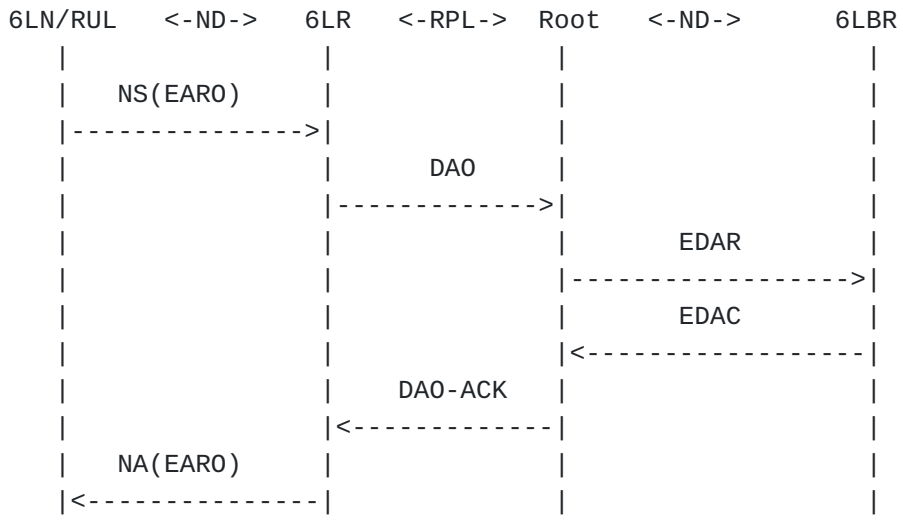

Figure 7: Next RUL Registration Flow

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

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

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 collocated with the RPL Root, but if not, the 6LBR MUST forward the status code to the originator of the EDAR, either the 6LR or the RPL Root that proxies for it. The ND status code is mapped in a RPL Status value by the RPL Root, and then back by the 6LR.

Figure 8 illustrates this in the case where the 6LBR and the Root are not collocated, and the Root proxies the EDAR messages.

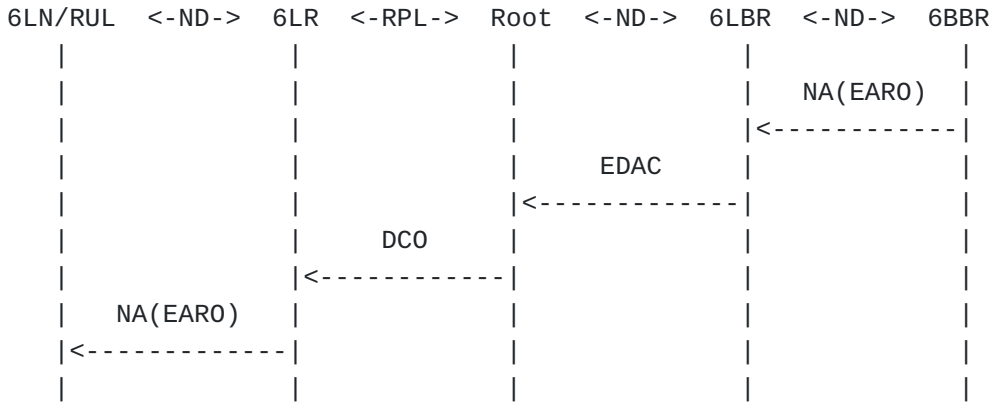

Figure 8: Asynchronous Issue

If the Root does not proxy, then the EDAC with a negative status reaches the 6LR directly. In that case, the 6LR MUST clean up the route using a DAO with a Lifetime of zero, and it MUST propagate the status back to the RUL in a 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 transports the ROVR. This way, the same flow as the heartbeat flow is sufficient to inform the 6LBR using the Root as proxy, as illustrated in Figure 7.

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

9.2. Detailed Operation

9.2.1. Perspective of the 6LN Acting as RUL

This specification does not alter 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 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, either using Stateless Address Autoconfiguration (SLAAC) [RFC4862] based on a Prefix Information Option (PIO) [RFC4861] found in an RA message, or some other means, such as DHCPv6 [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 to more than one 6LR at the same time. In that case, it uses the same EARO for all of the parallel Address Registrations, with the exception of the Registration Lifetime field and the setting of the R flag that may differ. The 6LN may cancel a subset of its registrations, or transfer a registration from one or more old 6LR(s) to one or more new 6LR(s). 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 SHOULD attempt to use another 6LR. The RUL SHOULD ensure that one registration succeeds before setting the R Flag to 0. In case of a conflict with the preceding rule on lifetime, the rule on 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 function (SAVI) [RFC7039] so it 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 the packet should be injected into, then it SHOULD set the Opaque field in the EARO to the RPLInstanceID, else it MUST leave the Opaque field to zero.

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

A RUL is not expected to produce RPL artifacts in the data packets, but it may do so. For instance, if the RUL has 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 Rank field are set to 0 as specified by section 11.2 of [RFC6550].

9.2.2. Perspective of the 6LR Acting as 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. For the registration refreshes, if the RPL Root has indicated that it proxies the keep-alive EDAR/EDAC exchange with the 6LBR (see Section 6), the 6LR MUST refrain from sending the keep-alive EDAR.

If the R Flag is set 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 a RPL Non-Storing Mode signaling and the updated Target Option (see Section 6.1). The 6LR MUST request a DAO-ACK by setting the 'K' flag in the DAO message. Success injecting the route to the RUL's address is indicated by the 'E' flag set to 0 in the RPL status of the DAO-ACK message.

The Opaque field in the EARO provides a mean 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 zero, then the Opaque field is expected to carry the RPLInstanceID suggested by the 6LN; otherwise, there is no suggested 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 else if the 6LR does not participate to the suggested 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 into an 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 RPL Transit Information Option (TIO) associated with the Target Option

3. The 6LR sets the External 'E' flag in the TIO to indicate that it 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 rounded, if needed, to the upper value to ensure that the path has a longer lifetime than the registration.

   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 option.

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, if a DAO-ACK is pending then the 6LR MUST wait for the DAO-ACK to send the NA(EARO) and deliver the status found in the DCO, else it MUST send an asynchronous NA(EARO) to the RUL immediately.

The 6LR MUST set the R Flag to 1 in the NA(EARO) back if and only if the 'E' flag 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 'E' 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 'E' 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 positive status 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 'E' 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 case of a DAO-ACK or a DCO indicating transporting an EARO Status value of 5 (Validation Requested), the 6LR MUST challenge the 6LN for ownership of the address, as described in section 6.1 of [RFC8928], before the Registration is complete. This flow, illustrated in Figure 9, ensures that the address is validated before it is injected in the RPL routing.

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

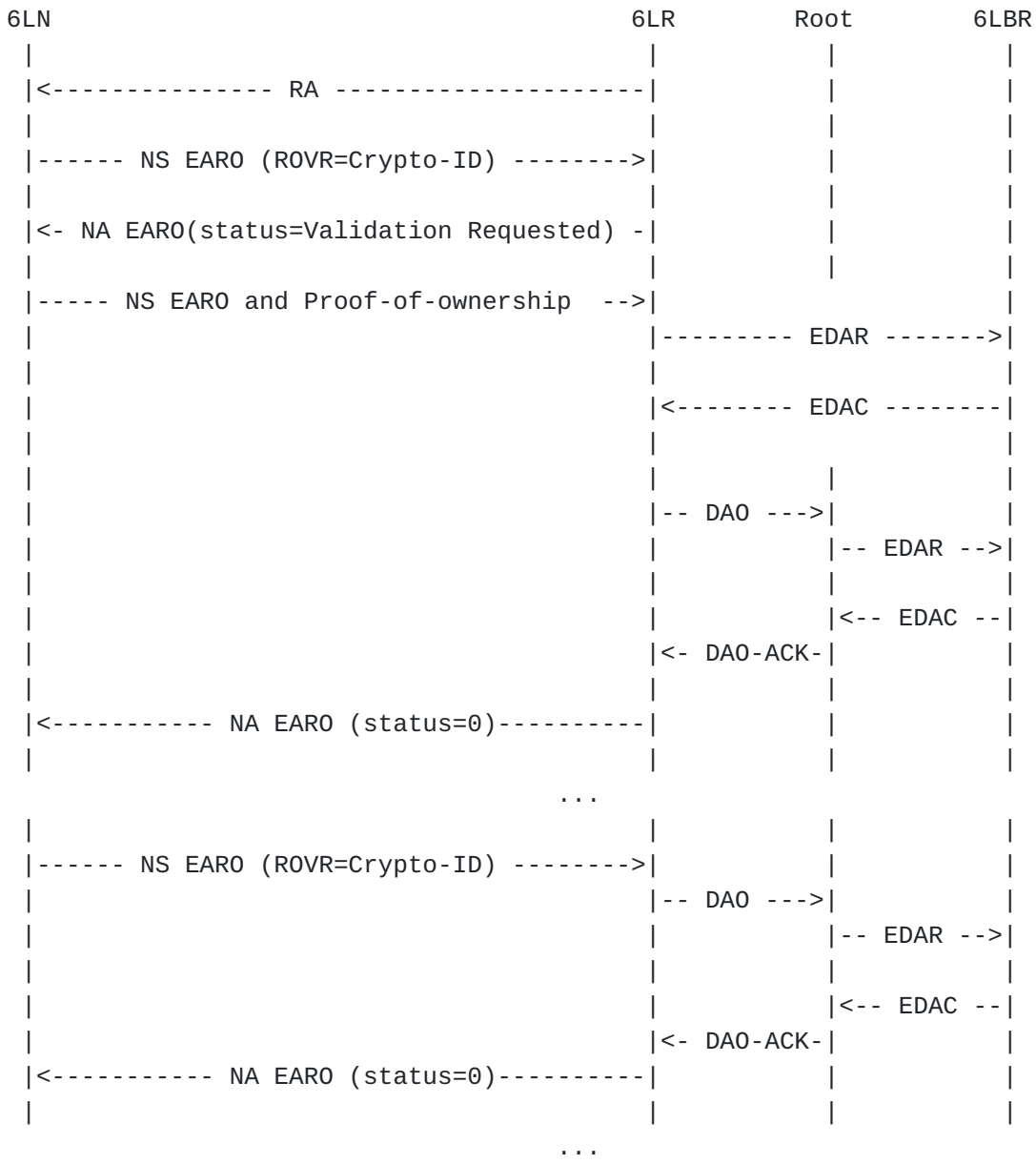

Figure 9: Address Protection

The 6LR may at any time send a unicast asynchronous NA(EARO) with the R Flag set to 0 to signal that it stops providing routing services, and/or with the EARO Status 2 "Neighbor Cache full" to signal that it removes the NCE. It may also send a final RA, unicast or multicast, with a Router Lifetime field of zero, to signal that it stops serving as Router, as specified in section 6.2.5 of [RFC4861]. This may happen upon a DCO or a DAO-ACK message indicating the path is already removed; else the 6LR MUST remove the Host route to the 6LN using a DAO message with a Path Lifetime of zero.

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 the routing services from the 6LR (any more). Upon this message, if, due to 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 zero. It is up to the Registering 6LN to maintain the corresponding route from then on, either keeping it active via a different 6LR or by acting as a RAN and managing its own reachability.

9.2.3. Perspective of the RPL Root

A RPL Root 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) that creates or updates an existing RPL state, the Root MUST notify the 6LBR by using a proxied EDAR/EDAC exchange. If if the RPL Root and the 6LBR are integrated, an internal API can be used.

The EDAR message MUST be constructed as follows:

1. The Target IPv6 address from the RPL Target Option is placed in the Registered Address field of the EDAR message;

2. the Registration Lifetime is adapted from the Path Lifetime in the TIO by converting the Lifetime Units used in RPL into units of 60 seconds used in the 6LoWPAN ND messages;

3. the TID value is set to the Path Sequence in the TIO and indicated with an ICMP code of 1 in the EDAR message;

4. The ROVR in the RPL Target Option is copied as is in the EDAR and the ICMP Code Suffix is set to the appropriate value as shown in Table 4 of [RFC8505] depending on the size of the ROVR field.

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

In either case, the EDAC Status is embedded in the RPL Status with the 'A' flag set to 1.

The proxied EDAR/EDAC exchange MUST be protected with a timer of an appropriate duration and a number of retries, that are implementation-dependent, and 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, either using a DAO-ACK or a DCO, as appropriate, with the 'A' and 'E' flags set to 1 in the RPL status, and a RPL Status value of of "6LBR Registry Saturated" [RFC8505].

9.2.4. Perspective of the 6LBR

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

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

10. Protocol Operations for Multicast Addresses

Section 12 of [RFC6550] details the RPL support for multicast flows. This support is activated by the MOP of 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 RPLInstance is 3.

The RPL support of 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 passed as a Layer-2 unicast to each of the interested children. This remains true when forwarding between the 6LR and the listener 6LN.

"Multicast Listener Discovery Version 2 (MLDv2) for IPv6" [RFC3810] provides an interface for a listener to register to multicast flows. In the MLD model, the Router is a "querier", and the Host is a multicast listener that registers to the querier to obtain copies of the particular flows it is interested in.

The equivalent of the first Address Registration happens as illustrated in Figure 10. 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.

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, in particular 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 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 Root checks if it is already registered as a listener for that address, and if not, it performs its own unsolicited Report for the multicast address as described in section 5.1 of [RFC3810]. The report is source independent, so there is no Source Address listed.

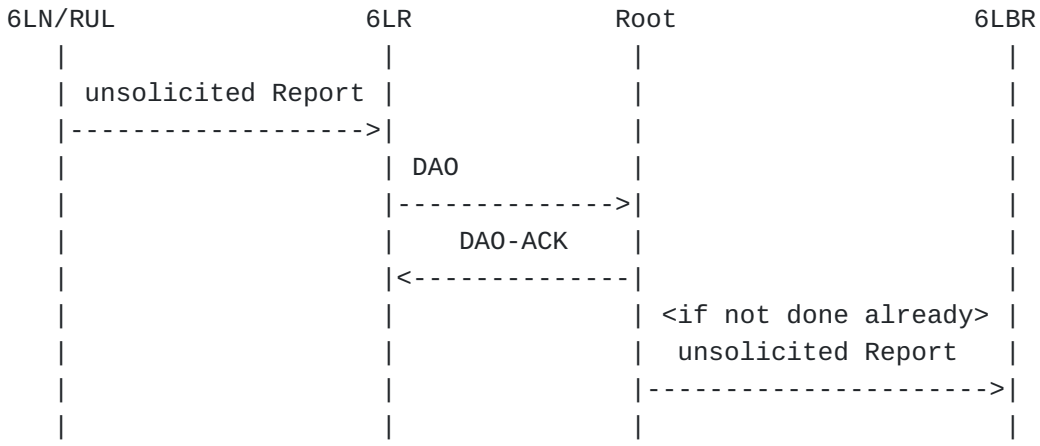

Figure 10: First Multicast Registration Flow

The equivalent of the registration refresh is pulled periodically by the 6LR acting as 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, and gets a Report back that is mapped into a DAO one by one. Optionally, the 6LR MAY send a General Query, where the Multicast Address field is set to zero. 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 11:

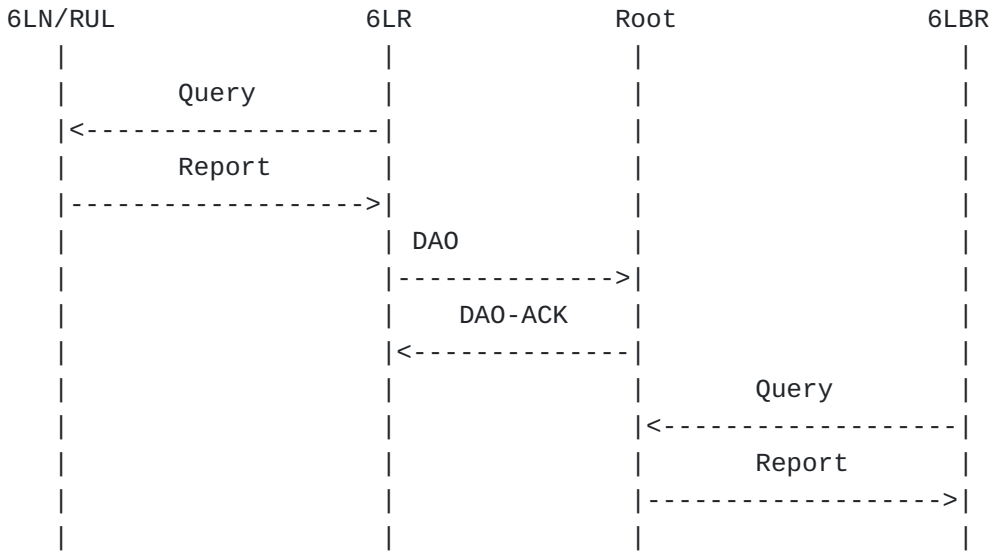

Figure 11: Next Registration Flow

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

11. Security Considerations

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

The LLN nodes depend on the 6LBR and the RPL participants for their operation. A trust model must be put in place to ensure that the right devices are acting in these roles, so as to avoid threats such as black-holing, (see [RFC7416] section 7), Denial-Of-Service attacks whereby a rogue 6LR creates a high churn in the RPL network by advertising and removing many forged addresses, or bombing attack whereby an impersonated 6LBR would destroy state in the network by using the status code of 4 ("Removed").

This trust model could be at a minimum based on a Layer-2 Secure joining and the Link-Layer security. This is a generic 6LoWPAN requirement, see Req5.1 in Appendix of [RFC8505].

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

The Link-Layer security is needed in particular to prevent Denial-Of-Service attacks whereby a rogue 6LN creates a high churn in the RPL network by constantly registering and deregistering addresses with the R Flag set to 1 in the EARO.

[RFC8928] updated 6LoWPAN ND with the called Address-Protected Neighbor Discovery (AP-ND). AP-ND protects the owner of an address against address theft and impersonation attacks in a Low-Power and Lossy Network (LLN). Nodes supporting th 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 a proof of ownership is provided, only the owner of that address can modify the registration information, thereby enforcing Source Address Validation. [RFC8928] reduces even more the attack perimeter that is available to the edge nodes and its use is suggested in this specification.

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

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 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 RPLInstance is to be used for the traffic coming from the RUL, per its own policy.

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 the overusing that channel could be detected. An implementation SHOULD

notify the network management when a RPL Target Option is receives with an unknown ROVR field size, to ensure that the situation is known to the network administrator.

[EFFICIENT-NPDAO] 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 a 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] creates a Registry for the 8-bit Address Registration Option Flags field. IANA is requested to rename the first column of the table from "ARO Status" to "Bit number".

12.2. Resizing the ARO Status values

Section 12 of [RFC6775] creates the Address Registration Option Status values Registry with a range 0-255.

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

IANA is requested to modify the Address Registration Option Status values Registry so that the upper bound of the unassigned values is 63. This document should be added as a reference. The registration procedure does not change.

12.3. New RPL DODAG Configuration Option Flag

IANA is requested to assign a flag from the "DODAG Configuration Option Flags for MOP 0..6" [USEofRPLinfo] registry as follows:

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

Table 2: New DODAG Configuration Option Flag

It is suggested to IANA to indicate that the Flag fields in RPL options are indexed starting counting from bit 0 as the most significant bit.

12.4. RPL Target Option Registry

This document modifies the "RPL Target Option Flags" registry initially created in Section 20.15 of [RFC6550] . The registry now includes only 4 bits (Section 6.1) and should point to this document as an additional reference. The registration procedure doesn't change.

Section 6.1 also defines a new entry in the Registry as follows:

Bit Number	Capability Description	Reference
0 (suggested)	Advertiser address in Full (F)	THIS RFC

Table 3: RPL Target Option Registry

12.5. New Subregistry for RPL Non-Rejection Status values

This specification creates 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, under the RPL registry.

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

*Registration procedure is "IETF Review" [RFC8126].

*Initial allocation is as indicated in Table 4:

Value	Meaning	Reference
0	Unqualified acceptance	THIS RFC / RFC 6550
1..63	Unassigned	

Table 4: Acceptance values of the RPL Status

12.6. New Subregistry for RPL Rejection Status values

This specification creates 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, under the RPL registry.

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

*Registration procedure is "IETF Review" [RFC8126].

*Initial allocation is as indicated in Table 5:

Value	Meaning	Reference
0	Unqualified rejection	THIS RFC
1..63	Unassigned	

Table 5: Rejection values of the RPL Status

13. Acknowledgments

The authors wish to thank Ines Robles, Georgios Papadopoulos and especially Rahul Jadhav and Alvaro Retana for their reviews and contributions to this document. Also many thanks to Peter Van der Stok and Carl Wallace for their reviews and useful comments during the IETF Last Call and the IESG review sessions.

14. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[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>.

[USEofRPLinfo] Robles, 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", Work in Progress, Internet-Draft, draft-ietf-roll-useofrplinfo-42, 12 November 2020, <https://tools.ietf.org/html/draft-ietf-roll-useofrplinfo-42>.

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

15. Informative References

[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>.

[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>.

[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>.

[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>.

[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>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282,

DOI 10.17487/RFC6282, September 2011, <https://www.rfc-editor.org/info/rfc6282>.

[RFC6687] Tripathi, J., Ed., de Oliveira, J., Ed., and JP. Vasseur, Ed., "Performance Evaluation of the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6687, DOI 10.17487/RFC6687, October 2012, <https://www.rfc-editor.org/info/rfc6687>.

[RFC7416] Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., and M. Richardson, Ed., "A Security Threat Analysis for the Routing Protocol for Low-Power and Lossy Networks (RPLs)", RFC 7416, DOI 10.17487/RFC7416, January 2015, <https://www.rfc-editor.org/info/rfc7416>.

[RFC8025] Thubert, P., Ed. and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging Dispatch", RFC 8025, DOI 10.17487/RFC8025, November 2016, <https://www.rfc-editor.org/info/rfc8025>.

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

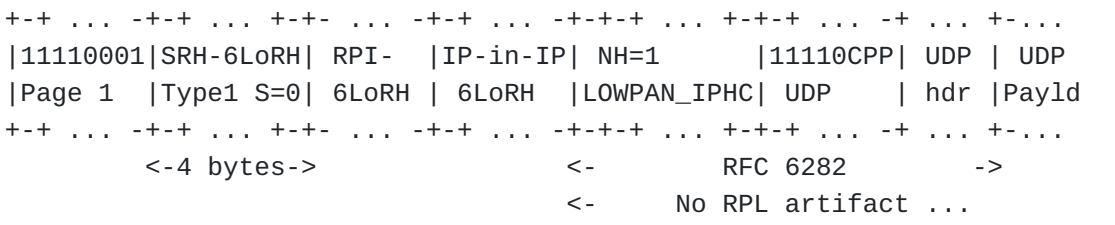

Figure 12: Encapsulation to Parent 6LR in Storing Mode

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

In Figure 12, the source of the IP-in-IP encapsulation is the Root, so it is elided in the IP-in-IP 6LoRH. The destination is the parent 6LR of the destination of the 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. It results that the total length of the SRH-6LoRH is 4 bytes.

In Non-Storing Mode, the encapsulation from the Root would be similar to that represented in Figure 12 with possibly more hops in the SRH-6LoRH and possibly multiple SRH-6LoRHs if the various addresses in the routing header are not compressed to the same format. Note that on the last hop to the parent 6LR, the RH3 is consumed and removed from the compressed form, so the use of Non-Storing Mode vs. Storing Mode is indistinguishable from the packet format.

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

Authors' Addresses

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

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

Michael C. Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca
URI: http://www.sandelman.ca/