Workgroup: ROLL
Updates: 6550, 8505 (if approved)
Published: 15 April 2020
Intended Status: Standards Track
Expires: 17 October 2020
Authors: P. Thubert, Ed. M. Richardson
Cisco Systems Sandelman

Routing for RPL Leaves

Abstract

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

Status of This Memo

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

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

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

This Internet-Draft will expire on 17 October 2020.

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.

To save signaling and routing state in constrained networks, RPL allows a routing stretch (see [RFC6687]), whereby routing is only performed along an acyclic graph optimized to reach a Root node, as opposed to straight along a 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 a any-to-any shortest path protocol. Finally, 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.

To provide alternate paths in lossy networks, RPL forms Direction-Oriented Directed Acyclic Graphs (DODAGs) using DODAG Information Solicitation (DIS) and DODAG Information Object (DIO) messages. For many of the nodes, though not all, a 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.

[RFC6550] provides unicast and multicast routing services to RPL-Aware nodes (RANs), either as a collection tree or with routing back. In the latter case, an RAN injects routes to itself using Destination Advertisement Object (DAO) messages sent either to parent-nodes, in the RPL Storing Mode, or to the Root indicating their parent, in the Non-Storing Mode. This process effectively forms a DODAG back to the device that is a subset of the DODAG to the Root with all links reversed.

RPL can be deployed as an extension to IPv6 Neighbor Discovery (ND) [RFC4861][RFC4862] and 6LoWPAN ND [RFC6775][RFC8505] to maintain reachability within a Non-Broadcast Multi-Access (NBMA) subnet. In that mode, some nodes may act as Routers and participate to the forwarding operations whereas others will only terminate packets, acting as Hosts in the data-plane. In [RFC6550] terms, a Host that is reachable over the RPL network is called a Leaf.

"When to use RFC 6553, 6554 and IPv6-in-IPv6" [USEofRPLinfo] introduces the term RPL-Aware-Leaf (RAL) for a Leaf that injects

routes in RPL to manage the reachability of its own IPv6 addresses. In contrast, the term RPL-Unaware Leaf (RUL) designates a Leaf that does not participate to RPL at all. A RUL is an IPv6 Host [RFC8504] that needs a RPL-Aware Router to obtain routing services over the RPL network.

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

The Non-Storing Mode mechanisms are used to extend the routing state with connectivity to RULs even when the DODAG is operated in Storing-Mode DODAGs. The unicast packet forwarding operation by the 6LR serving a 6LN that is a RPL Leaf is described in [USEofRPLinfo].

Examples of routing-agnostic 6LNs include lightly-powered sensors such as window smash sensor (alarm system), and kinetically powered light switches. Other applications of this specification may include a smart grid network that controls appliances - such as washing machines or the heating system - in the home. Appliances may not participate to the RPL protocol operated in the Smartgrid network but can still interact with the Smartgrid for control and/or metering.

2. Terminology

2.1. BCP 14

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. 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 2.3. Other terms in use in LLNs are found in "Terminology for Constrained-Node Networks" [RFC7228].

"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, an RAN manages the reachability of its addresses and prefixes by injecting them in RPL by itself.

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

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

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

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

2.3. Glossary

This document often uses the following acronyms:

AR: Address Resolution (aka Address Lookup)

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)

3. 6LoWPAN Neighbor Discovery

3.1. RFC 6775 Address Registration

The classical "IPv6 Neighbor Discovery (IPv6 ND) Protocol" [RFC4861] [RFC4862] was defined for transit media such a 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.

3.2. 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:

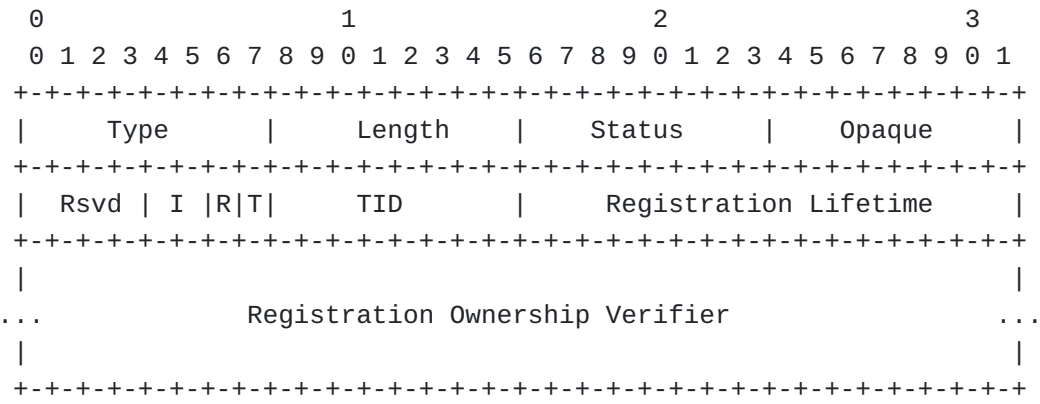

Figure 1: EARO Option Format

3.2.1. R Flag

[RFC8505] introduces the "R" flag in the EARO. The Registering Node sets the "R" flag to indicate whether the 6LR should ensure reachability for the Registered Address. If the "R" flag is not set, then the Registering Node handles the reachability of the Registered Address by other means, which means in a RPL network that it is an RAN 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 6LN is a RUL that requires reachability services for an IPv6 address if and only if it sets the "R" flag in the NS(EARO) used to

register the address to a RPL border router acting as 6LR. Upon receiving the NS(EARO), the RPL router generates a DAO message for the Registered Address if and only if the "R" flag is set.

3.2.2. TID, I Field and Opaque Fields

The EARO also includes a sequence counter called Transaction ID (TID), which maps to the Path Sequence Field found in Transit Options in RPL DAO messages. 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 6.1). The EARO also transports an Opaque field and an "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 of the Opaque field by a RUL.

3.2.3. ROVR

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

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

This specification does not address how the protection by [AP-ND] could be extended to RPL. On the other hand, it adds the ROVR to the DAO to build the proxied EDAR at the Root (see Section 8), which means that nodes that are aware of the Host route to the 6LN are made aware of the associated ROVR as well.

3.3. RFC 8505 Extended DAR/DAC

[RFC8505] updates the periodic DAR/DAC exchange that takes place between the 6LR and the 6LBR using Extended DAR/DAC messages which can carry a ROVR field of variable size. The exchange is triggered by an NS(EARO) message and is intended to create, refresh and delete the corresponding state in the 6LBR for a lifetime that is indicated by the 6LN. It is protected by the ARQ mechanism 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 from the 6LR to 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 removes the extraneous keep-alive across the LLN. The 6LR turns the periodic Address Registration 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. Upon a refresher DAO, the Root proxies the EDAR exchange to refresh the state at the 6LBR on behalf of the 6LR, as illustrated in Figure 7.

3.3.1. RFC 7400 Capability Indication Option

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

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

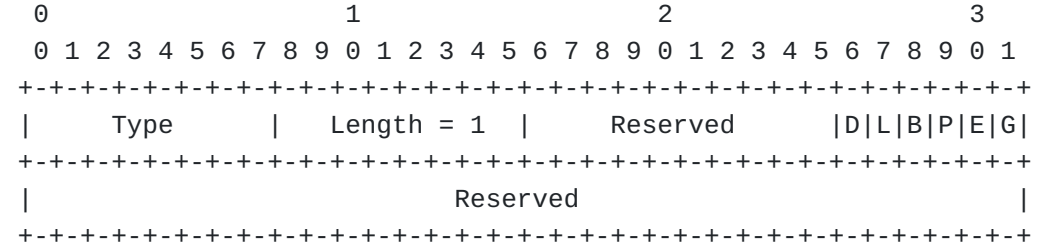

Figure 2: 6CIO flags

A 6LR that can provide reachability services for a RUL in a RPL network as specified in this document SHOULD include a 6CIO in its RA messages and set the L, P and E flags as prescribed by [RFC8505], see Section 6.1 for the behavior of the RUL.

4. Updating RFC 6550

This document specifies a new behavior whereby a 6LR injects DAO messages for unicast addresses (see Section 9) and multicast addresses (see Section 10) on behalf of leaves that are not aware of RPL. The addresses are exposed as external targets [RFC6550]. Per [USEofRPLinfo], an IP-in-IP encapsulation that terminates at the RPL

Root is used to remove RPL artifacts and compression techniques that may not be processed correctly outside of the RPL domain.

This document also synchronizes the liveness monitoring at the Root and the 6LBR. A 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 5), for any 6LN, RUL or RAN.

RPL defines a configuration option that is registered to IANA in section 20.14. of [RFC6550]. This specification defines a new flag "Root Proxies EDAR/EDAC" (P) that is encoded in one of the reserved control bits in the option. The new flag is set to indicate that the Root performs the proxy operation and that all nodes in the RPL network must refrain from renewing the 6LBR state directly. The bit position of the "P" flag is indicated in Section 12.2.

Section 6.3.1. of [RFC6550] defines a 3-bit Mode of Operation (MOP) in the DIO Base Object. The new "P" flag is defined only for MOP value between 0 to 6. For a MOP value of 7 or above, the flag MAY indicate something different and MUST NOT be interpreted as "Root Proxies EDAR/EDAC" unless the specification of the MOP indicates to do so.

The RPL Status defined in section 6.5.1. of [RFC6550] for use in the DAO-Ack message is extended to be used in the DCO messages [EFFICIENT-NPDAO] as well. Furthermore, this specification enables to use a RPL Status to transport the IPv6 ND Status defined for use in the EARO, more in Section 7.

Section 6.7. of [RFC6550] introduces the RPL Control message Options such as the RPL Target Option that can be included in a RPL Control message such as the DAO. Section 8 updates the RPL Target Option to optionally transport the ROVR used in the IPv6 Registration (see Section 3.2.3) so the RPL Root can generate a full EDAR message.

5. Updating RFC 8505

This document updates [RFC8505] to introduce the anonymous EDAR and NS(EARO) messages. The anonymous messages are used for backward compatibility. The anonymous messages are recognizable by a zero ROVR field and can only be used as a refresher for a pre-existing state associated to the Registered Address. More specifically, an anonymous message can only increase the lifetime and/or increment the TID of an existing state at the 6LBR.

Upon the renewal of a 6LoWPAN ND Address Registration, this specification changes the behavior of a RPL Router acting as 6LR for the registration. If the Root indicates the capability to proxy the EDAR/EDAC exchange to the 6LBR then the 6LR refrains from sending an EDAR message; if the Root is separated from the 6LBR, the Root regenerates the EDAR message to the 6LBR upon a DAO message that signals the liveliness of the Address. The regenerated message is anonymous iff the DAO is a legacy message that does not carry a ROVR as specified in Section 8.

6. Requirements on the RPL-Unware Leaf

This document provides RPL routing for a RUL, that is a 6LN acting as an IPv6 Host and not aware of RPL. Still, a minimal RPL-independent functionality is required from the RUL to obtain routing services.

6.1. Support of 6LoWPAN ND

In order to obtain routing services from a 6LR, a RUL MUST implement [RFC8505] and set the "R" flag in the EARO. The RUL SHOULD support [AP-ND] and use it to protect the ownership of its addresses. The RUL MUST NOT request routing services from a 6LR that does not originate RA messages with a CIO that has the L, P, and E flags all set as discussed in Section 3.3.1.

A RUL that has multiple potential routers MUST prefer those that provide routing services. The RUL MUST register to all the 6LRs from which it desires routing services. If there are no available routers, the connection of the RUL fails. The Address Registrations SHOULD be performed in an RApid sequence, using the exact same EARO for a same Address. Gaps between the Address Registrations will invalidate some of the routes till the Address Registration finally shows on those routes as well.

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

6.2. External Routes and RPL Artifacts

Section 4.1. of [USEofRPLinfo] provides a set of rules that MUST be followed for the routing operations to a RUL.

A 6LR that is upgraded to act 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. An upgraded 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 Mode signaling and the associated IP-in-IP encapsulated packets are normal traffic for 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 which happens to be a Host route.

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

In Non-Storing Mode, packets going down carry a Source Routing Header (SRH). The IP-in-IP encapsulation, the RPI and the SRH are collectively called the "RPL artifacts" and can be compressed using [RFC8138]. Figure 14 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 possibly an SRH in a Non-Storing Mode DODAG. [USEofRPLinfo] expects the RUL to support the basic "IPv6 Node Requirements" [RFC8504]. In particular the RUL is expected to ignore the RPL artifacts that are either consumed or not applicable to a Host.

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

6.2.1. Support of IPv6 Encapsulation

Section 2.1 of [USEofRPLinfo] sets the rules for forwarding IP-in-IP either to the final 6LN or to a parent 6LR. In order to enable IP-in-IP to the 6LN in Non-Storing Mode, the 6LN must be able to decapsulate the tunneled packet and either drop the inner packet if it is not the final destination, or pass it to the upper layer for further processing. Unless it is aware that the RUL can handle IP-in-IP properly, the Root that encapsulates a packet to a RUL

terminates the IP-in-IP tunnel at the parent 6LR . For that reason, it is beneficial but not necessary for a RUL to support IP-in-IP.

6.2.2. Support of the HbH Header

A RUL is expected to process an unknown Option Type in a Hop-by-Hop Header as prescribed by section 4.2 of [RFC8200]. This means in particular that an RPI with an Option Type of 0x23 [USEofRPLinfo] is ignored when not understood.

6.2.3. 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 means in particular that Routing Header with a Routing Type of 3 [RFC6554] is ignored when the Segments Left is zero, and the packet is dropped otherwise.

7. 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

This specification extends the scope of the RPL Status to be used in RPL DCO messages. Furthermore, this specification enables to carry the IPv6 ND Status values defined for use in the EARO and initially listed in table 1 of [RFC8505] in a RPL Status.

Section 12.1 reduces the range of EARO Status values to 0-63 ensure that they fit within a RPL Status as shown in Figure 3.

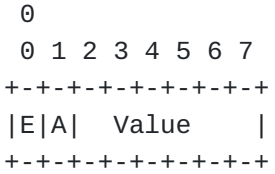

Figure 3: RPL Status Format

RPL Status subfields:

E:

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

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

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

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

Conversely, the 6LR MUST copy the value of the RPL Status unchanged in the EARO of an NA message that is built upon a RPL Status with the 'A' bit set in a DCO or a DAO-ACK message.

8. Updated RPL Target option

This specification updates the RPL Target option to transport the ROVR. This enables the RPL Root to generate a full EDAR message as opposed to an anonymous EDAR that has restricted properties.

The Target Prefix field MUST be aligned to the next 4-byte boundary after the size indicated by the Prefix Length. If necessary the transported prefix MUST be padded with zeros.

With this specification the ROVR is the remainder of the RPL Target Option. The size of the ROVR is indicated in a new ROVR Size field that is encoded to map one-to-one with the Code Suffix in the EDAR message (see table 4 of [RFC8505]).

The modified format is illustrated in Figure 4. It is backward compatible with the Target Option in [RFC6550] and SHOULD be used as a replacement.

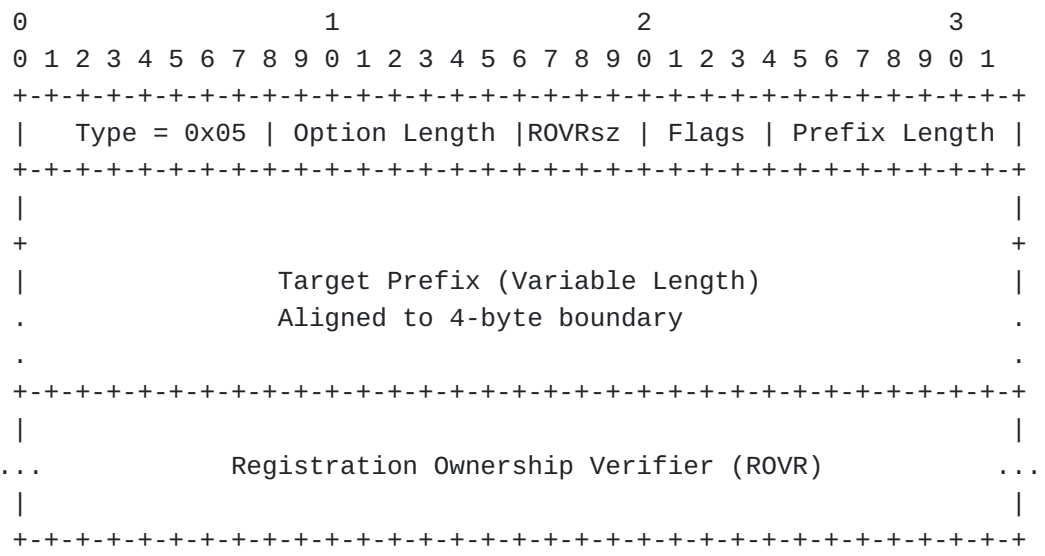

Figure 4: Updated Target Option

New fields:

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

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

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.

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 a DAO message that refreshes the RPL routing state. Any combination of the logical functions of 6LR, Root and 6LBR might be collapsed in a single node.

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

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 by the RPL Root. In a same fashion, if an additional routing protocol is

deployed on a same network, that additional routing protocol may need to handle the keep alive procedure for the addresses that it serves.

On the first Address Registration, illustrated in Figure 5 for RPL Non-Storing Mode, the Extended Duplicate Address exchange takes place as prescribed by [RFC8505]. If the exchange fails, the 6LR returns an NA message with a negative status to the 6LN, the NCE is not created and the address is not injected in RPL. If it is successful, the 6LR creates an NCE and injects the Registered Address in RPL using DAO/DAO-ACK exchanges all the way to the RPL DODAG Root.

The 6LN signals the termination of a registration with a 6LR using an NS(EARO) with a Registration Lifetime set to 0. Upon this, the 6LR MUST perform an EDAR/EDAC exchange to clean up the state at the 6LBR, as illustrated in Figure 8, unless it uses the ROVR in the RPL Target Option and, in Storing Mode, it is propagated to the Root.

9.1.1. In RPL Non-Storing-Mode

In Non-Storing Mode, the DAO message flow can be nested within the Address Registration flow as illustrated in Figure 5.

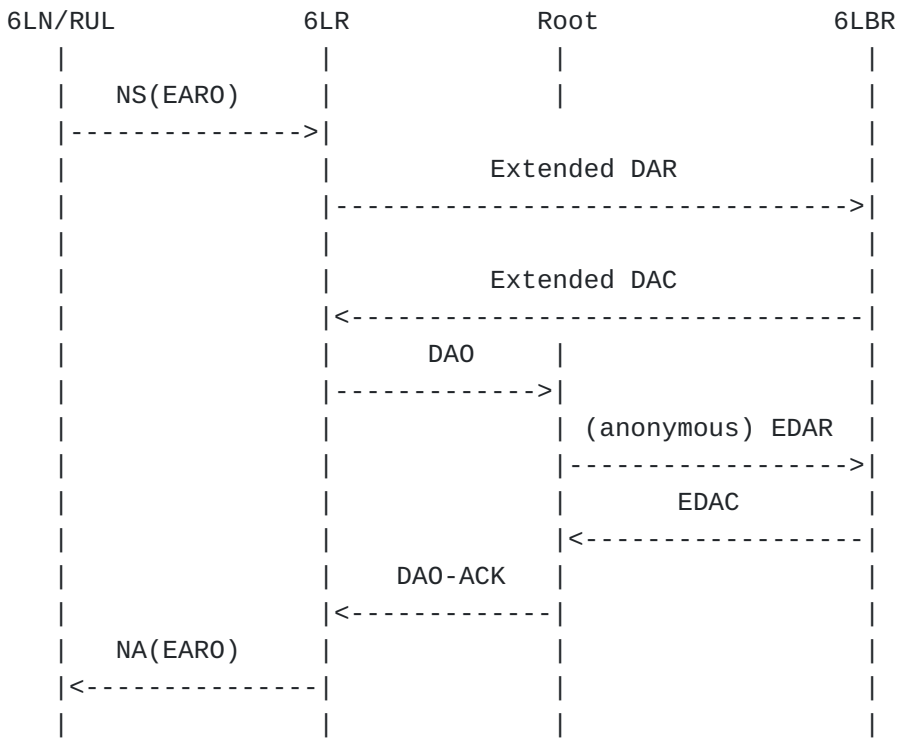

Figure 5: First Registration Flow in Non-Storing Mode

An issue may be detected later, e.g., the address moves within the LLN or to a different Root on a backbone [6BBR]. In that case the

value of the status that indicates the issue can be passed from 6LoWPAN ND to RPL and back as illustrated in Figure 6.

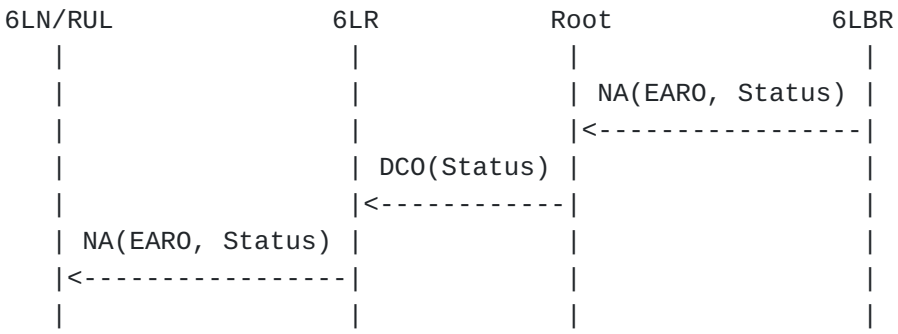

Figure 6: Asynchronous Issue

An Address re-Registration is performed by the 6LN to maintain the NCE in the 6LR alive before lifetime expires. Upon an Address re-Registration, as illustrated in Figure 7, the 6LR redistributes the Registered Address NS(EARO) in RPL.

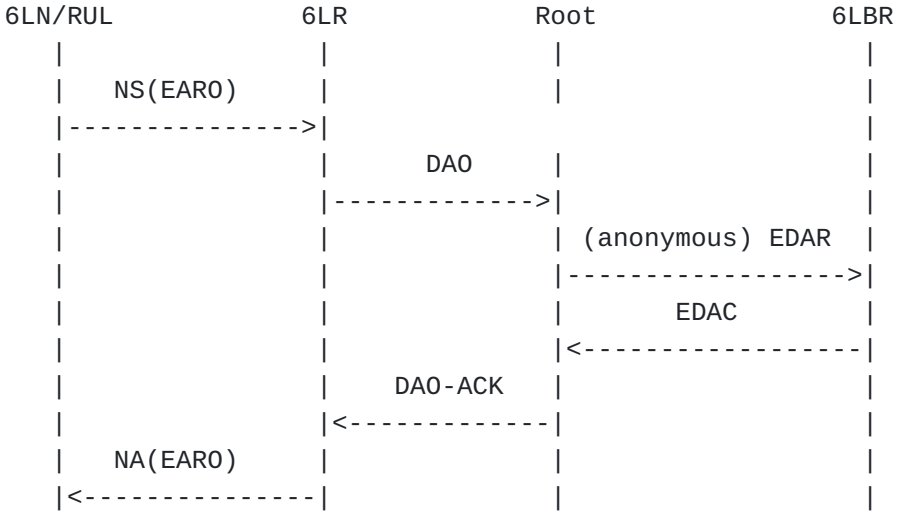

Figure 7: Next Registration Flow in Non-Storing Mode

This causes the RPL DODAG Root to refresh the state in the 6LBR with an EDAC message or an anonymous EDAC if the ROVR is not indicated in the Target Option. In both cases, the EDAC message sent in response by the 6LBR contains the actual value of the ROVR field for that Address Registration. In case of an error on the proxied EDAR flow, the error MUST be returned in the DAO-ACK - if one was requested - using a RPL Status with the 'A' flag set that imbeds a 6LoWPAN Status value as discussed in Section 7.

If the Root could not return the negative Status in the DAO-ACK then it sends an asynchronous Destination Cleanup Object (DCO) message

[EFFICIENT-NPDAO] to the 6LR by placing the negative Status in the RPL Status with the 'A' flag set. Note that if both are used in a short interval of time, the DAO-ACK and DCO messages are not guaranteed to arrive in the same order at the 6LR.

The 6LR may receive a requested DAO-ACK even after it received a DCO, but the negative Status in the DCO supercedes a positive Status in the DAO-ACK regardless of the order in which they are received. Upon the DAO-ACK - or the DCO if it arrives first - the 6LR responds to the RUL with an NA(EARO). If the RPL Status has the 'A' flag set, then the ND Status is extracted and passed in the EARO; else, if the 'E' flag is set, indicating a rejection, then the status 4 "Removed" is used; else, the ND Status of 0 indicating "Success" is used.

The RUL may terminate the registration at anytime by using a Registration Lifetime of 0. This specification expects that the RPL Target option transports a ROVR. If that is the case, the normal heartbeat flow is sufficient to inform the 6LBR using the Root as proxy as illustrated in Figure 7. If the 6LR could not add the ROVR to the DAO message, then it MUST inform the 6LBR separately using as illustrated in Figure 8.

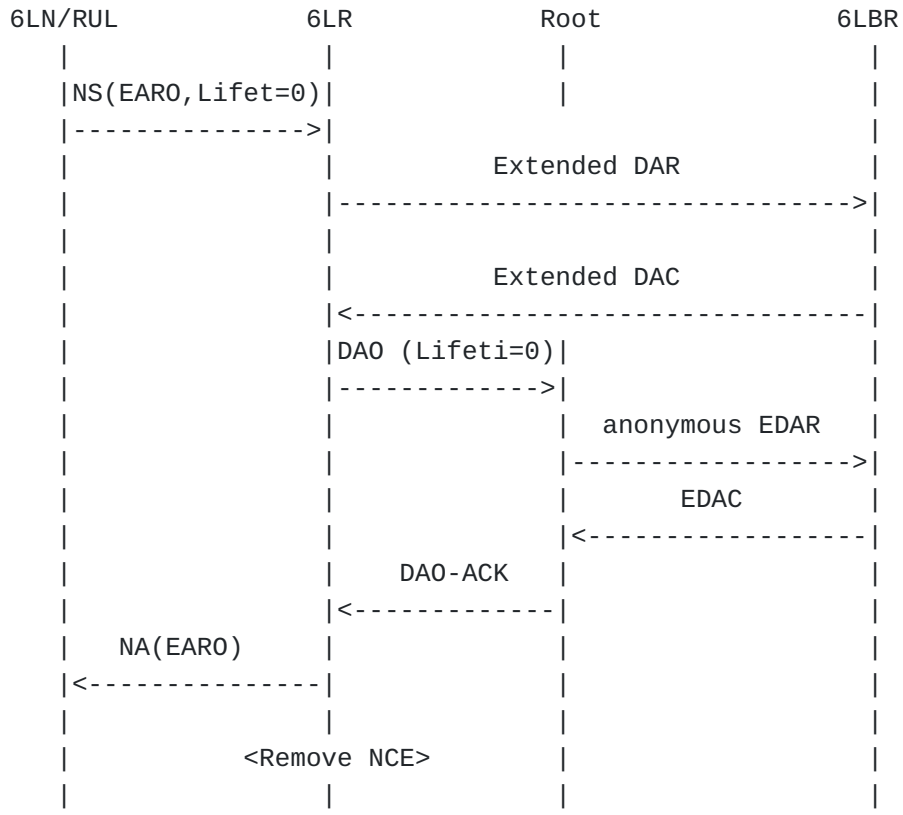

Figure 8: Last Registration Flow in Non-Storing Mode, No ROVR

9.1.2. In RPL Storing-Mode

In RPL Storing Mode, the DAO-ACK is optional. When it is used, it is generated by the RPL parent, which does not need to wait for the grand-parent to send the acknowledgment. A successful DAO-ACK is not a guarantee that the DAO has yet reached the Root or that the EDAR was successfully proxied by the Root.

The 6LR uses the EDAR/EDAC exchange as in Non-Storing Mode, for the initial registration, and also possibly at the termination in the case the 6LR could not add the ROVR to the RPL Target option of the DAO message.

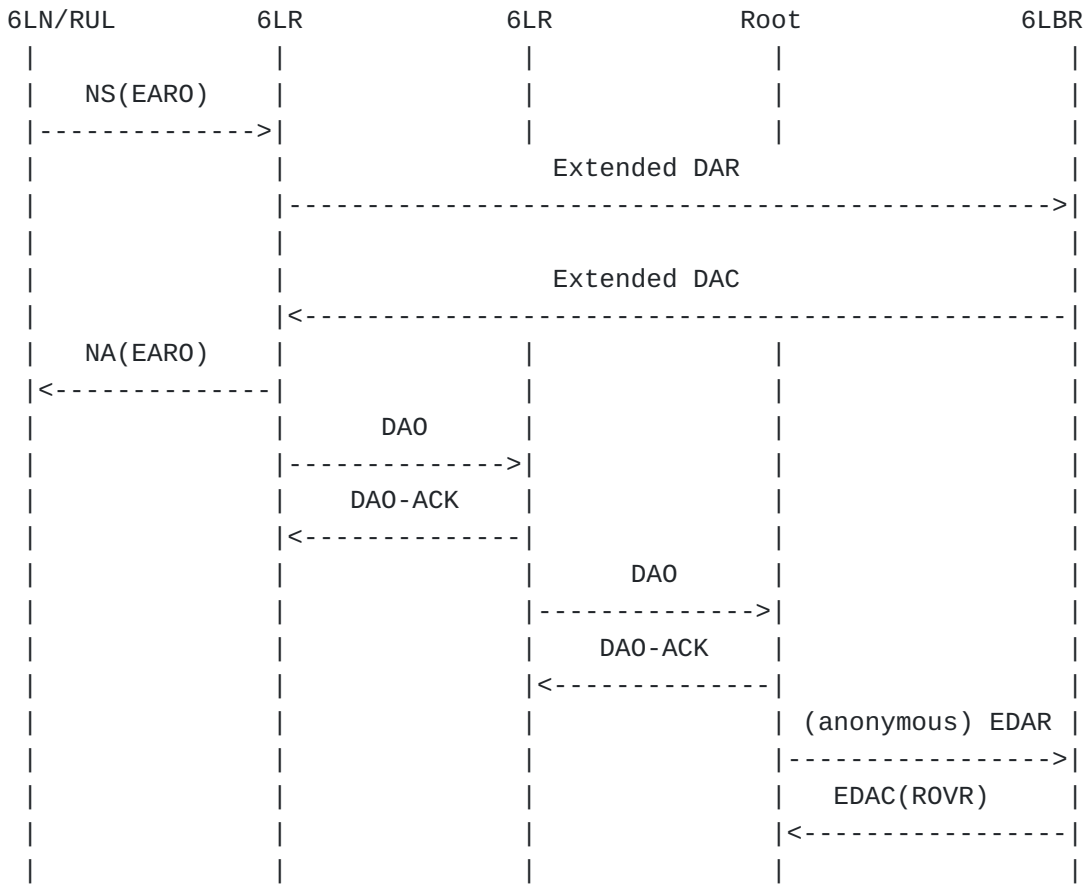

Figure 9: First Registration Flow in Storing Mode

The Storing Mode of RPL does not provide and end-to-end confirmation that a DAO reached the root. When the 6LR has just joined, and later if DAO messages are lost before reaching the Root, the 6LR might not be reachable back from the Root. Performing an EDAR/EDAC exchange on behalf of a RUL provides that confirmation. On the other hand, if the 6LR retries an EDAR and never gets and EDAC back, it SHOULD resend a DAO to become reachable again, before it tries another sequence of EDAR.

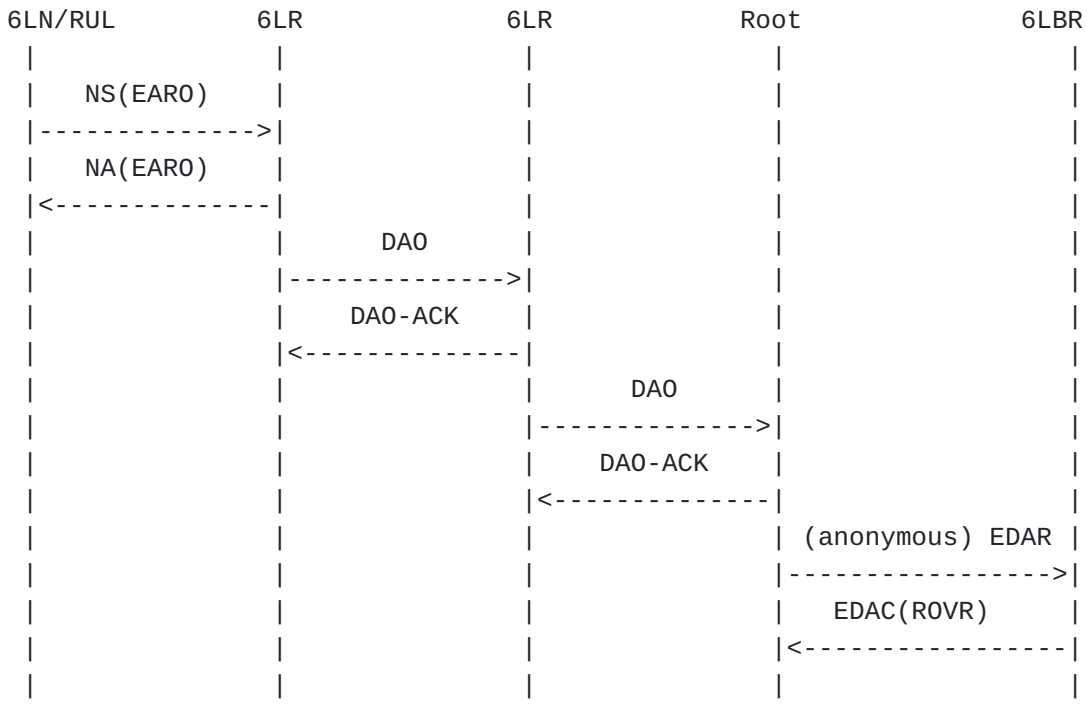

Figure 10: Next Registration Flow in Storing Mode

If the keep-alive fails, or an asynchronous issue is reported, the path can be cleaned up asynchronously using a DCO message [EFFICIENT-NPDAO] as illustrated in Figure 11 and described in further details in Section 9.2.3.

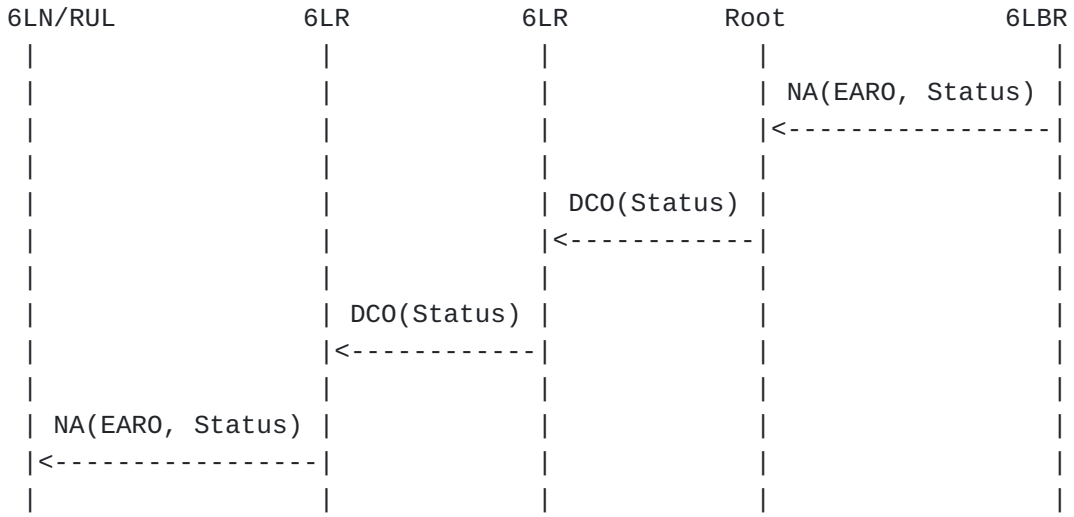

Figure 11: Issue in Storing Mode

In the case illustrated here, the issue is actually detected in the ND protocol and reported in the State of a NA(EARO) message. That

statis is transported in the DCO message as a RPL Status with the 'A' and typically the 'E' flags set.

9.2. Detailed Operation

9.2.1. By the RUL Acting as 6LN

This specification does not alter the operation of a 6LoWPAN ND-compliant 6LN, and a RUL is expected to operate as follows:

1. The 6LN obtains an IPv6 global address, either using Stateless Address Autoconfiguration (SLAAC) [RFC4862] based on a Prefix Information Option (PIO) [RFC4861] found in an RA message, or some other means such as DHCPv6 [RFC3315].

2. Once it has formed an address, the 6LN (re)registers its address periodically, within the Lifetime of the previous Address Registration, as prescribed by [RFC6775] and [RFC8505], to refresh the NCE before the lifetime indicated in the EARO expires. The TID is incremented each time and wraps in a lollipop fashion (see section 5.2.1 of [RFC8505] which is fully compatible with section 7.2 of [RFC6550]).

3. As stated in section 5.2 of [RFC8505], the 6LN can register to more than one 6LR at the same time. In that case, it MUST use the same value of TID for all of the parallel Address Registrations. The 6LN should send the registration(s) with a non-zero Registration Lifetime and ensure that one succeeds before it terminates other registrations to maintain the state in the network and at the 6LBR and minimize the churn.

4. Following section 5.1 of [RFC8505], a 6LN acting as a RUL sets the "R" flag in the EARO of at least one registration, whereas acting as an RAN it never does. If the "R" flag is not echoed in the NA, the RUL SHOULD attempt to use another 6LR. The 6LN should send the registration(s) with the "R" flag set and ensure that one succeeds before it sends the registrations with the flag reset. In case of a conflict with the preceeding rule on lifetime, the rule on lifetime has precedence.

5. The 6LN may use any of the 6LRs to which it registered as default gateway. Using a 6LR to which the 6LN is not registered may result in packets dropped at the 6LR by a Source Address Validation function (SAVI) so it is not recommended.

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

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

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

9.2.2. By the RPL Border Router Acting as 6LR

Also as prescribed by [RFC8505], the 6LR generates an EDAR message upon reception of a valid NS(EARO) message for the registration of a new IPv6 Address by a 6LN. If the initial EDAR/EDAC exchange succeeds, then the 6LR installs an NCE for the Registration Lifetime. For the refreshes of the registration, if the RPL Root has indicated that it proxies the keep-alive EDAR/EDAC exchange with the 6LBR (see Section 4), the 6LR MUST refrain from sending the keep-alive EDAR itself.

If the "R" flag is set in the NS(EARO), the 6LR SHOULD attempt to inject the host route in RPL, unless this is barred for other reasons, like a saturation of the network or if its RPL parent. The 6LR MUST set "R" flag in the NA(EARO) back if and only if it successfully injected the Registered Address in RPL.

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

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

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

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

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

1. The Registered Address is signaled as Target Prefix in the RPL Target Option in the DAO message; the Prefix Length is set to 128

2. RPL Non-Storing Mode is to be used. The 6LR indicates one of its global or unique-local IPv6 unicast addresses as the Parent Address in the associated RPL Transit Information Option (TIO)

3. the External 'E' flag in the TIO is set to indicate that the 6LR redistributes an external target into the RPL network

4. the Path Lifetime in the TIO is computed from the Lifetime in the EARO Option. This adapts it to the Lifetime Units used in the RPL operation; note that if the lifetime is 0, then the 6LR generates a No-Path DAO message that cleans up the routes down to the Address of the 6LN; 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.

The NCE is removed if the 6LR tries to inject the route is RPL and fails for reasons related to ND, which is recognized by both the 'E' and the 'A' flags set in the RPL Status of the DAO-ACK or the DCO, as detailed below.

Otherwise, success injecting the route is assumed if a DAO-ACK was not requested or if it is received with a RPL Status that is not a rejection (i.e., the 'E' flag not set).

In case of success, if the 'A' flag is set in the RPL Status of the DAO-ACK, then the 6LR MUST use the Status Value in the RPL Status for the Status in the NA(EARO), else a Status of 0 (Success) is returned.

The status of 0 MUST also be used if the 6LR could not even try to inject the route - note that the "R" flag is reset in that case.

In a network where Address Protected Neighbor Discovery (AP-ND) is enabled, in case of a DAO-ACK or a DCO indicating transporting an EARO Status Value of 5 (Validation Requested), the 6LR MUST challenge the 6LN for ownership of the address, as described in

section 6.1 of [AP-ND], before the Registration is complete. This ensures that the address validated before it is injected in RPL.

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

The other rejection codes indicate that the 6LR failed to inject the address into the RPL network. If an EARO Status is transported, the 6LR MUST send a NA(EARO) to the RUL with that Status value, and the "R" flag not set. Similarly, upon receiving a DCO message indicating that the address of a RUL should be removed from the routing table, the 6LR issues an asynchronous NA(EARO) to the RUL with the embedded ND Status value if there was one, and the "R" flag not set.

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

9.2.3. By the RPL Root

A RPL Root SHOULD set the "P" flag in the RPL configuration option of the DIO messages that it generates (see Section 4) to signal that it proxies the keep-alive EDAR/EDAC echange. The remainder of this section assumes that it does.

Upon reception of a DAO message, for each RPL Target option that creates or updates an existing RPL state, the Root notifies the 6LBR. This can be done using an internal API if they are co-located, or using a proxied EDAR/EDAC exchange if they are separated.

If the RPL Target option transports a ROVR, then the Root MUST use it to build a full EDAR message; else, an anonymous EDAR is used with the ROVR field set to zero.

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. If the ROVR is present in the RPL Target option, it 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; else, the ROVR field in the EDAR is set to zero indicating an anonymous EDAR.

Upon a Status value in an EDAC message that is not "Success", the Root SHOULD destroy the formed paths using either a DAO-ACK (in Non-Storing Mode) or a DCO downwards as specified in [EFFICIENT-NPDAO]. Failure to destroy the former path would result in Stale routing state and local black holes if the address belongs to another party elsewhere in the network. The RPL Status value that maps the 6LoWPAN ND Status value MUST be embedded in the RPL Status in the DCO.

9.2.4. By the 6LBR

Upon reception of an EDAR message with the ROVR field set to a non-zero value, the 6LBR acts as prescribed by [RFC8505]. If the ROVR is set to 0, indicating an anonymous EDAR, the 6LBR MUST act as below:

1. The 6LBR checks whether an entry exists for the address. If the entry does not exist, the 6LBR MUST NOT create the entry, and it MUST answer with a Status "Removed" in the EDAC message. If the entry exists, the 6LBR computes whether the TID in the EDAR message is fresher than the one in the entry as prescribed in section 4.2.1. of [RFC8505], and continues as follows:

2. If the anonymous EDAR message is fresher, the 6LBR updates the TID in the entry, restarts the heartbeat timer for the entry, and answers with a Status "Success" in the EDAC message. If the value of the Registration Lifetime is smaller than the value in the entry, then the latter value MUST be used for the heartbeat; this means in particular that the Registration Lifetime of 0 is ignored. Conversely, if the duration of the Lifetime is extended by the Registration Lifetime in the EDAR message, it is used for the hearbeat and to the value in the entry is updated.

3. If the TID in the entry is the same or fresher, the 6LBR does not update the entry, and answers with a Status "Success" and "Moved" in the EDAC message, respectively.

The EDAC that is constructed is the same as if the anonymous EDAR was a full EDAR, but for the ROVR that is set to zero.

10. Protocol Operations for Multicast Addresses

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

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

On the first Address Registration, as illustrated in Figure 12, the 6LN, as an MLD listener, sends an unsolicited Report to the 6LR in order to start receiving the flow immediately.

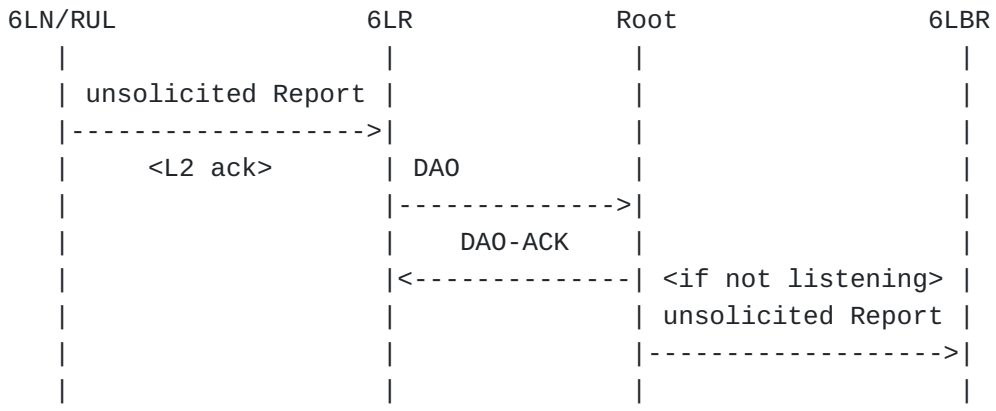

Figure 12: First Multicast Registration Flow

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

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

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

if it is already registered as a listener for that address, and if not, it performs its own unsolicited Report for the multicast target.

An Address re-Registration is pulled periodically by 6LR acting as querier. Note that the message may be sent unicast to all the known individual listeners. Upon a time out of the Query Interval, the 6LR sends a Query to each of its listeners, and gets a Report back that is mapped into a DAO, as illustrated in Figure 13:

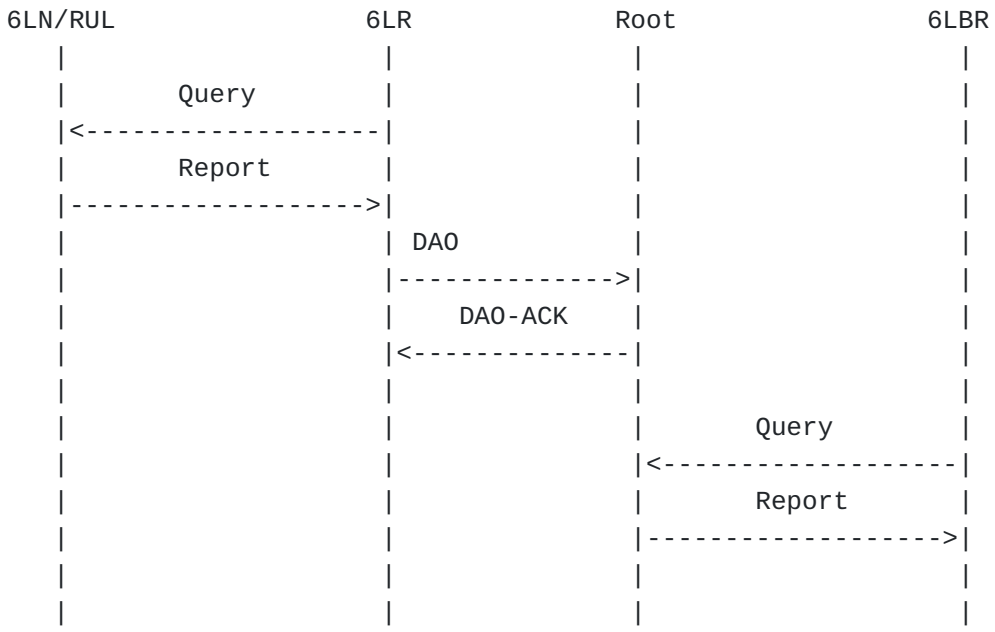

Figure 13: Next Registration Flow

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

11. Security Considerations

First of all, it is worth noting that with [RFC6550], every node in the LLN is RPL-aware and can inject any RPL-based attack in the network. This specification isolates edge nodes that can only interact with the RPL routers using 6LoWPAN ND, meaning that they cannot perform RPL insider attacks. 6LoWPAN ND can optionally provide SAVI features, which reduces even more the attack perimeter that is available to the edge nodes.

The LLN nodes depend on the 6LBR and the RPL participants for their operation. A trust model must be put in place to ensure that the right devices are acting in these roles, so as to avoid threats such as black-holing, (see [RFC7416] section 7) or bombing attack whereby

an impersonated 6LBR would destroy state in the network by using the "Removed" Status code.

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

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 anonymous EDAR message does not carry a valid Registration Unique ID [RFC8505] in the form of a ROVR and may be played by any node on the network without the need to know the ROVR. The 6LBR MUST NOT create an entry based on a anonymous EDAR and it MUST NOT decrease the value of the lifetime. All it can do is refresh the lifetime and the TID of an existing entry. So the message cannot be used to create a binding state in the 6LBR but it can be used to maintain one active longer than expected.

Note that a full EDAR message with a lifetime of 0 will destroy that state and the anonymous message will not recreate it. Note also that a rogue that has access to the network can attack the 6LBR with other (forged) addresses and ROVR, and that this is a much easier DoS attack than trying to keep existing state alive longer.

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

12. IANA Considerations

12.1. Resizing the ARO Status values

IANA is requested to modify the Address Registration Option Status Values Registry as follows: The unassigned values range is reduced from 11-255 to 11-63.

12.2. New DODAG Configuration Option Flag

This specification updates the Registry for the "DODAG Configuration Option Flags" that was created for [RFC6550] as follows:

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

Table 2: New DODAG Configuration Option Flag

12.3. RPL Target Option Flags

Section 20.15 of [RFC6550] creates a registry for the 8-bit RPL Target Option Flags field. This specification reduces the field to 4 bits. The IANA is requested to reduce the size of the registry accordingly.

12.4. New Subregistry for the RPL Non-Rejection Status values

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

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

*Registration procedure is "Standards Action" [RFC8126].

*Initial allocation is as indicated in Table 3:

Value	Meaning	Reference
0	Unqualified acceptance	RFC 6550

Table 3: Acceptance values of the RPL Status

12.5. New Subregistry for the RPL Rejection Status values

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

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

*Registration procedure is "Standards Action" [RFC8126].

*Initial allocation is as indicated in Table 4:

Value	Meaning	Reference
0	Unqualified rejection	This document

Table 4: Rejection values of the RPL Status

13. acknowledgments

The authors wish to thank Georgios Papadopoulos and Rahul Jadhav for their early reviews of and contributions to this document

14. Normative References

[RFC2119]

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

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, DOI 10.17487/RFC2710, October 1999, <https://www.rfc-editor.org/info/rfc2710>.

[RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004, <https://www.rfc-editor.org/info/rfc3810>.

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, DOI 10.17487/RFC4919, August 2007, <https://www.rfc-editor.org/info/rfc4919>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <https://www.rfc-editor.org/info/rfc6550>.

[RFC6553] Hui, J. and JP. Vasseur, "The Routing Protocol for Low-Power and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams", RFC 6553, DOI 10.17487/RFC6553, March 2012, <https://www.rfc-editor.org/info/rfc6553>.

[RFC6554] Hui, J., Vasseur, JP., Culler, D., and V. Manral, "An IPv6 Routing Header for Source Routes with the Routing Protocol for Low-Power and Lossy Networks (RPL)", RFC 6554, DOI 10.17487/RFC6554, March 2012, <https://www.rfc-editor.org/info/rfc6554>.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012, <https://www.rfc-editor.org/info/rfc6775>.

[RFC7102] Vasseur, JP., "Terms Used in Routing for Low-Power and Lossy Networks", RFC 7102, DOI 10.17487/RFC7102, January 2014, <https://www.rfc-editor.org/info/rfc7102>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <https://www.rfc-editor.org/info/rfc7228>.

[RFC7400] Bormann, C., "6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 7400, DOI 10.17487/RFC7400, November 2014, <https://www.rfc-editor.org/info/rfc7400>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/info/rfc8126>.

[RFC8138] Thubert, P., Ed., Bormann, C., Toutain, L., and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing Header", RFC 8138, DOI 10.17487/RFC8138, April 2017, <https://www.rfc-editor.org/info/rfc8138>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8505] Thubert, P., Ed., Nordmark, E., Chakrabarti, S., and C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505, DOI 10.17487/RFC8505, November 2018, <https://www.rfc-editor.org/info/rfc8505>.

[AP-ND] Thubert, P., Sarikaya, B., Sethi, M., and R. Struik, "Address Protected Neighbor Discovery for Low-power and Lossy Networks", Work in Progress, Internet-Draft, draft-

ietf-6lo-ap-nd-20, 9 March 2020, <https://tools.ietf.org/html/draft-ietf-6lo-ap-nd-20>.

[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-38, 23 March 2020, <https://tools.ietf.org/html/draft-ietf-roll-useofrplinfo-38>.

[EFFICIENT-NPDAO]
Jadhav, R., Thubert, P., Sahoo, R., and Z. Cao, "Efficient Route Invalidation", Work in Progress, Internet-Draft, draft-ietf-roll-efficient-npdao-17, 30 October 2019, <https://tools.ietf.org/html/draft-ietf-roll-efficient-npdao-17>.

15. Informative References

[RFC6606] Kim, E., Kaspar, D., Gomez, C., and C. Bormann, "Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing", RFC 6606, DOI 10.17487/RFC6606, May 2012, <https://www.rfc-editor.org/info/rfc6606>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <https://www.rfc-editor.org/info/rfc3315>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <https://www.rfc-editor.org/info/rfc6282>.

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

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

[RFC8025] Thubert, P., Ed. and R. Cragie, "IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Paging

Dispatch", RFC 8025, DOI 10.17487/RFC8025, November 2016, <https://www.rfc-editor.org/info/rfc8025>.

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

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

Appendix A. Example Compression

Figure 14 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].

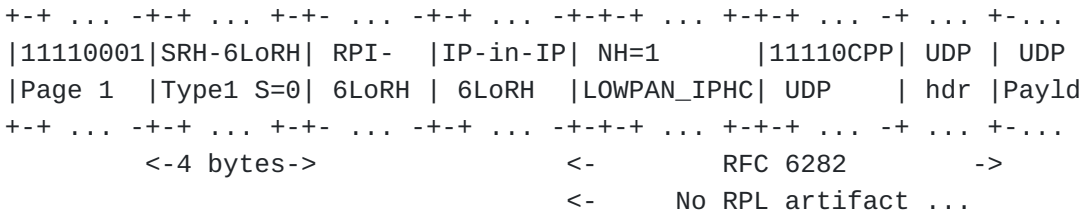

Figure 14: Encapsulation to Parent 6LR in Storing Mode

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

In Figure 14, the source of the IP-in-IP encapsulation is the Root, so it is elided in the IP-in-IP 6LoRH. The destination is the parent 6LR of the destination of the inner packet so it cannot be elided. In Storing Mode, it is placed as the single entry in an SRH-6LoRH as the first 6LoRH. Since there is a single entry so the SRH-6LoRH Size is 0. 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 14 with possibly more hops in the SRH-6LoRH and possibly multiple SRH-6LoRHs if the various addresses in the routing header are not compressed to the same format. Note that on the last hop to the parent 6LR, the RH3 is consumed and removed from the compressed form, so the use of Non-Storing Mode vs. Storing Mode is indistinguishable from the packet format.

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

Authors' Addresses

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

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

Michael C. Richardson
Sandelman Software Works

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