Workgroup: ROLL
Updates: 6550, 8505 (if approved)
Published: 31 October 2019
Intended Status: Standards Track
Expires: 3 May 2020
Authors: P. Thubert, Ed. M. Richardson
Cisco Systems Sandelman

Eliding and Querying RPL Information

Abstract

This specification extends RFC6550 and RFC8505 to provide unicast and multicast routing services in a RPL domain to 6LNs that are plain hosts and do not participate to RPL.

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 3 May 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

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

Table of Contents

1. Introduction

2. Terminology

2.1. BCP 14

2.2. References

2.3. Glossary

3. 6LoWPAN Neighbor Discovery

3.1. RFC 6775

3.2. RFC 8505 Extended ARO

3.2.1. R Flag

3.2.2. TID, I Field and Opaque Fields

3.2.3. ROVR

3.3. RFC 8505 Extended DAR/DAC

4. Updating RFC 6550

5. Updating RFC 8505

6. 6LN Requirements to be a RPL-Unware Leaf

6.1. Support of 6LoWPAN ND

6.2. External Routes and RPL Artifacts

6.2.1. Support of the HbH Header

6.2.2. Support of the Routing Header

6.2.3. Support of IPv6 Encapsulation

7. Updated RPL Status

8. Updated RPL Target option

9. Protocol Operations for Unicast Addresses

9.1. General Flow

9.1.1. In RPL Non-Storing-Mode

9.1.2. In RPL Storing-Mode

9.2. Operation

9.2.1. By the 6LN

9.2.2. By the 6LR

9.2.3. By the RPL Root

9.2.4. By the 6LBR

10. Protocol Operations for Multicast Addresses

11. Implementation Status

12. Security Considerations

13. IANA Considerations

13.1. RPL Target Option Flags

13.2. New Subsubregistry for the RPL Non-Rejection Status values

13.3. New Subsubregistry for the RPL Rejection Status values

14. Acknowledgments

15. Normative References

16. Informative References

Appendix A. Example Compression

Authors' Addresses

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 is a Distance-Vector protocol, which, compared to link-state protocols, limits the amount of topological knowledge that needs to be installed and maintained in each node. In order to operate in constrained networks, RPL allows a Routing Stretch (see [RFC6687]), whereby routing is only performed along a

DODAG 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.

In order to cope with lossy transmissions, RPL forms Direction-Oriented Directed Acyclic Graphs (DODAGs) using DODAG Information Solicitation (DIS) and DODAG Information Object (DIO) messages. For most 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 routes proactively but only fixes them when they are used by actual traffic. The result is that RPL provides reachability for most of the LLN nodes, most of the time, but may not really converge in the classical sense. RPL provides unicast and multicast routing services back to RPL-Aware nodes (RANs). A RAN will inject routes to itself using Destination Advertisement Object (DAO) messages sent to either parent-nodes in Storing Mode or to the Root indicating their parent in 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.

When a routing protocol such as RPL is used to maintain reachability within a Non-Broadcast Multi-Access (NBMA) subnet, some nodes may act as routers and participate to the routing operations whereas others may be plain hosts. 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, a RPL-Unaware Leaf (RUL) designates a leaf does not participate to RPL at all. In that case, the 6LN is a plain host that needs an interface to its RPL router to obtain routing services over the LLN. This specification enables a RPL-Unaware Leaf (RUL) to announce itself as a host and request that 6LRs that accept the registration also inject the relevant routing information for the Registered Address in the RPL domain on its behalf. The unicast packet forwarding operation by the 6LR serving a Leaf 6LN is described in [USEofRPLinfo].

Examples of routing-agnostic 6LN may include lightly-powered sensors such as window smash sensor (alarm system), or the kinetically powered light switch. Other application of this specification may include a smart grid network that controls appliances - such as

washing machines or the heating system - in the home. Applicances may not participate to the RPL protocol operated in the smart grid network but can still receive control packet from the smart grid.

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.

The term "byte" is used in its now customary sense as a synonym for "octet".

"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 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 a RAL or a RPL router. As opposed to a RUL, a RAN manages the reachability of its addresses and prefixes by injecting them in RPL by itself.

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

Readers are expected to be familiar with all the terms and concepts that are discussed in

* "Neighbor Discovery for IP version 6" [RFC4861],

* "IPv6 Stateless Address Autoconfiguration" [RFC4862],

* "Problem Statement and Requirements for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Routing" [RFC6606],

* "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [RFC4919],

* "Neighbor Discovery Optimization for Low-power and Lossy Networks" [RFC6775], and

* "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery" [RFC8505].

2.3. Glossary

This document often uses the following acronyms:

AR: Address Resolution (aka Address Lookup)

6LBR: 6LoWPAN Border Router

6LN: 6LoWPAN Node (a Low Power host or router)

6LR: 6LoWPAN Router

6CIO: Capability Indication Option

(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

DCO: Destination Cleanup Object

DIS: DODAG Information Solicitation

DIO: DODAG Information Object

DODAG: Destination-Oriented Directed Acyclic Graph

LLN: Low-Power and Lossy Network

NA: Neighbor Advertisement

NCE: Neighbor Cache Entry

ND:
Neighbor Discovery

NDP: Neighbor Discovery Protocol

NS: Neighbor Solicitation

RA: Router Advertisement

ROVR: Registration Ownership Verifier

RPI: RPL Packet Information (an Option in the Hop-By_Hop Header)

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

The "IPv6 Neighbor Discovery (IPv6 ND) Protocol" (NDP) suite [RFC4861] [RFC4862] was defined for transit media such a Ethernet, and relies heavily on multicast operations for address discovery and duplicate address detection (DAD).

"Neighbor Discovery Optimizations for 6LoWPAN networks" [RFC6775] (6LoWPAN ND) adapts IPv6 ND for operations over energy-constrained LLNs. In particular, 6LoWPAN ND introduces a unicast host address registration mechanism that contributes to reducing the use of multicast messages that are present in the classical IPv6 ND protocol. 6LoWPAN ND 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).

6LoWPAN ND 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.

The main functions of [RFC6775] are to proactively establish the Neighbor Cache Entry in the 6LR and to avoid address duplication. There is no concept of registering the address for an external

service such as RPL routing. That feature is introduced with "Registration Extensions for 6LoWPAN Neighbor Discovery" [RFC8505].

3.2. RFC 8505 Extended ARO

[RFC8505] updates the behavior of RFC 6775 to enable a generic registration to services such as routing, and defines an Extended Address Registration Option (EARO). The format of the EARO is shown in Figure 1:

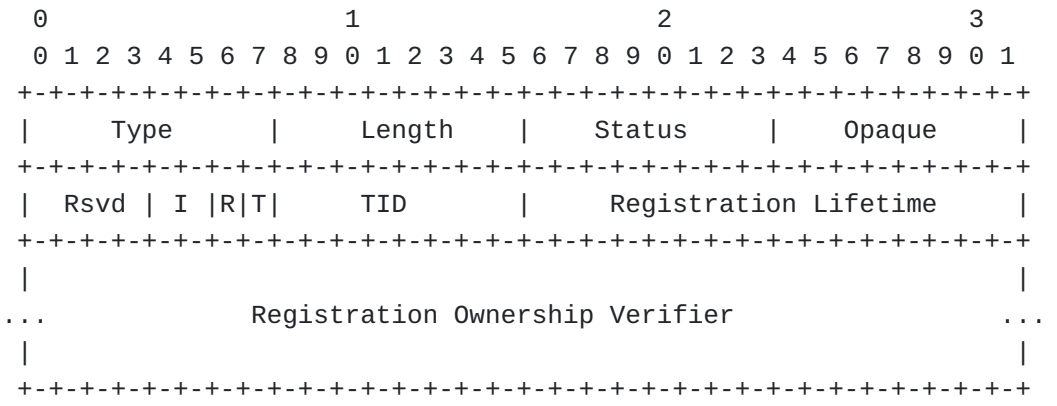


Figure 1: EARO Option Format

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, e.g., by means of routing or proxying ND. If the R flag is not set, then the Registering Node is expected to be a RAN that handles the reachability of the Registered Address by itself.

This document specifies how the R flag is used in the context of RPL. A 6LN operates as a RUL for an IPv6 address iff it sets the R flag in the NS(EARO) used to register the address. The RPL router generates a DAO message for the Registered Address upon an NS(EARO) iff the R flag in the EARO is set. Conversely, this document specifies a behavior of a RPL router acting as 6LR for the registration 6LR that depends on the setting of the R flag in the NS(EARO).

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 a variable length from 64 to 256 bits. The ROVR is a replacement of the EUI-64 field in the ARO [RFC6775] that was used to identify uniquely a registration based on 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] 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, which means that nodes that are aware of the host route to the 6LN are now 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. The Extended Duplicate Address messages can carry the ROVR field of variable size. The periodic EDAR/EDAC exchange is triggered by a NS(EARO) message and is intended to create and then refresh the corresponding state in the 6LBR for a lifetime that is indicated by the 6LN. Conversely, 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 a lifetime that is indicated by the source of the DAO. This means that there are two periodic messages that traverse the whole network to indicate that an address is still reachable, one to the Root and one to the 6LBR. This represents a waste of bandwidth and energy that can be undesirable in an LLN.

This specification saves the support of RPL in a 6LN called a RUL and avoids an extraneous periodic flow across the LLN. The RUL only needs to perform a [RFC8505] registration to the 6LR. The 6LR turns it into a DAO message to the Root on behalf of the RUL. Upon the new DAO, the Root proxies the EDAR exchange to the 6LBR on behalf of the 6LR. This is illustrated in Figure 5.

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 Targets are exposed as External addresses. An IP-in-IP encapsulation that terminates at the border 6LR is used to remove RPL artifacts and compression techniques that may not be processed correctly outside of the RPL domain.

This document 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).

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 a keep-alive EDAR message and a keep-alive NS(EARO) message. The keep-alive messages are used for backward compatibility, when the DAO does not transport a ROVR as specified in Section 8. The keep-alive messages have a zero ROVR field and can only be used to refresh a pre-existing state associated to the Registered Address. More specifically, a keep-alive message can only increase the lifetime and/or increment the TID of the existing state in a 6LBR.

Upon the renewal of a 6LoWPAN ND registration, this specification changes the behavior of a RPL router acting as 6LR for the registration as follows. 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.

6. 6LN Requirements to be a RPL-Unware Leaf

This document provides RPL routing for a RUL, that is a 6LN acting as a plain host and not aware of RPL. Still, a minimal RPL-independent functionality is expected from the 6LN in order to obtain routing services from the 6LR.

6.1. Support of 6LoWPAN ND

A RUL MUST implement [RFC8505] and set the R flag in the EARO option. A 6LN is considered to be a RUL if and only if it sets the R flag in the EARO.

A RUL MUST register to all the 6LRs from which it expects to get routing services. The registrations SHOULD be performed in a rapid sequence, using the exact same EARO for a same Address. Gaps between the registrations will invalidate some of the routes till the 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 refrain from using the Registered Address as specified by [RFC8505] depending on the Status value.

A RUL SHOULD support [AP-ND] to protect the ownership of its addresses.

6.2. External Routes and RPL Artifacts

Section 4.1. of [USEofRPLinfo] provides a set of rules that MUST be followed when forwarding packets over an external route:

RPL data packets are often encapsulated using IP-in-IP and in Non-Storing Mode, packets going down will carry an SRH as well. RPL data packets also typically carry a Hop-by-Hop Header to transport a RPL Packet Information (RPI) [RFC6550]. These additional headers are called RPL artifacts. When IP-in-IP is used and the outer headers terminate at a 6LR down the path (see Figure 9 for the compressed format in Storing Mode), then the 6LR decapsulates the IP-in-IP and the packet that is forwarded to the external destination is free of RPL artifacts - but possibly an RPI if packet was generated by a RAN in the same RPL domain as the destination RUL.

Non-Storing Mode DAO messages are used to signal external routes to the Root, even if the DODAG is operated in Storing Mode. This enables to advertise the 6LR that injects the route for use as tunnel endpoint in the data path. For all external routes, the Root should use an IP-in-IP tunnel to that 6LR, with the RPL artifacts in the outer header to be stripped by the 6LR. The IP-in-IP encapsulation may be avoided in Storing Mode if the path to the

external destination beyond the 6LR is known to handle or ignore the RPL artifacts properly [RFC8200]. A RUL is an example of a destination that is reachable via an external (host) route for which IP-in-IP tunneling may be avoided as it ignores the RPI and the consumed SRH artifacts. The use of non-Storing Mode signaling in Storing Mode and the associated IP-in-IP encapsulation are transparent to intermediate routers that only see packets back and forth between the Root and the 6LR and do not need a special support for external routes.

A RUL may not support IP-in-IP tunneling [RFC8504], so if IP-in-IP is used, and unless the Root as a better knowledge, the tunnel should terminate at the 6LR that injected the external route to the RUL.

Additionally, the RUL is not expected to support the compression method defined in [RFC8138]. The 6LR that injected the route should uncompress the packet before forwarding over an external route, even when delivering to a RUL, even when it is not the destination in the outer header of the incoming packet.

6.2.1. 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.

6.2.2. 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 [RFC6553] is ignored when the Segments Left is zero, and dropped otherwise.

6.2.3. 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.

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 status values defined for use in the IPv6 ND Extended Address Registration Option (EARO) and listed in table 1 of [RFC8505] in a RPL status. Only EARO status values in the range 0-63 can be transported.

The resulting RPL status is as follows:

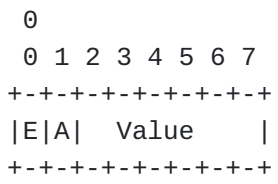


Figure 2: RPL status Format

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. 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 as illustrated in Figure 3. This enables the RPL Root to generate a full EDAR Message as opposed to a keep-alive EDAR that has restricted properties. The Target Prefix MUST be aligned to the next 4-byte boundary after the size indicated by the Prefix Length. if necessary it is padded with zeros. The size of the ROVR is indicated in a new ROVR Type field that is encoded to map the CodePfx in the EDAR message (see section 4.2 of [RFC8505]). With this specification the ROVR is the remainder of the RPL Target Option.

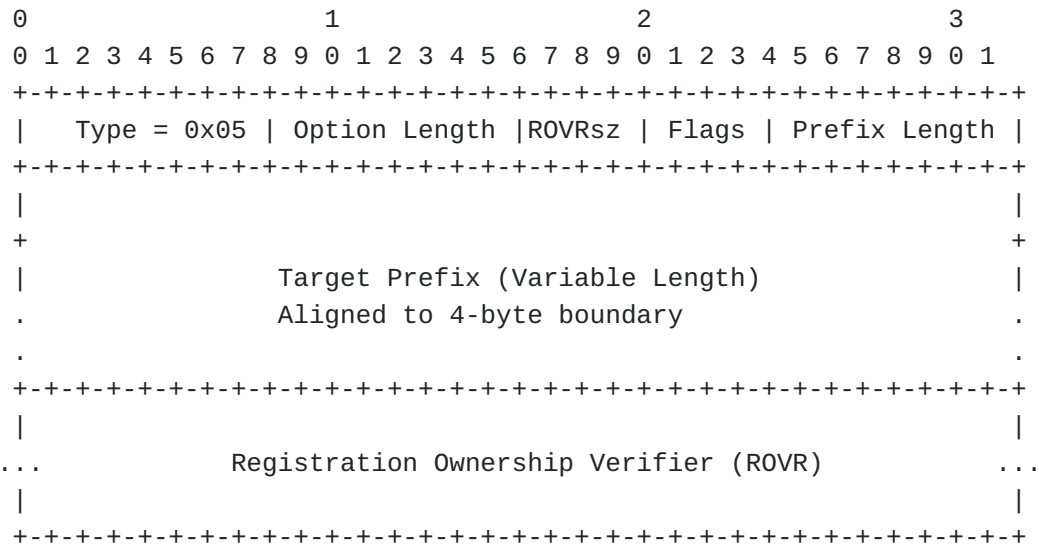


Figure 3: Updated Target Option

New fields:

RVRsz: 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

9.1. General Flow

This specification enables to save the exchange of Extended Duplicate Address messages, EDAR and EDAC, from a 6LN all the way to the 6LBR across a RPL mesh, for the sole purpose of refreshing an existing state in the 6LBR. Instead, the EDAR/EDAC exchange is proxied by the RPL Root upon a DAO message that refreshes the RPL routing state. 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 registration lifetime in the NS(EARO) message from the 6LN.

In that flow, the RPL Root acts as a proxy to refresh the state in the 6LBR. The proxy operation applies to both RUL and RAN. This means that 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. 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.

From the perspective of the 6LN, the registration flow happens transparently; it is not delayed by the proxy RPL operation, so the device does not need to change the amount of time it waits based upon whether RPL proxy operation happens or not.

On the first registration, illustrated in Figure 4, from the perspective of the 6LR in Non-Storing Mode, the Extended Duplicate Address message takes place as prescribed by [RFC8505]. When successful, the flow creates a Neighbor Cache Entry (NCE) in the 6LR, and the 6LR injects the Registered Address in RPL using DAO/DAO-ACK exchanges all the way to the RPL DODAG Root. The protocol does not carry a specific information that the Extended Duplicate Address messages were already exchanged, so the Root proxies them anyway.

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.

9.1.1. In RPL Non-Storing-Mode

In Non-Storing Mode, the flows can be nested as illustrated in Figure 4 and it is possible to carry information such as an updated lifetime from the 6LBR all the way to the 6LN.

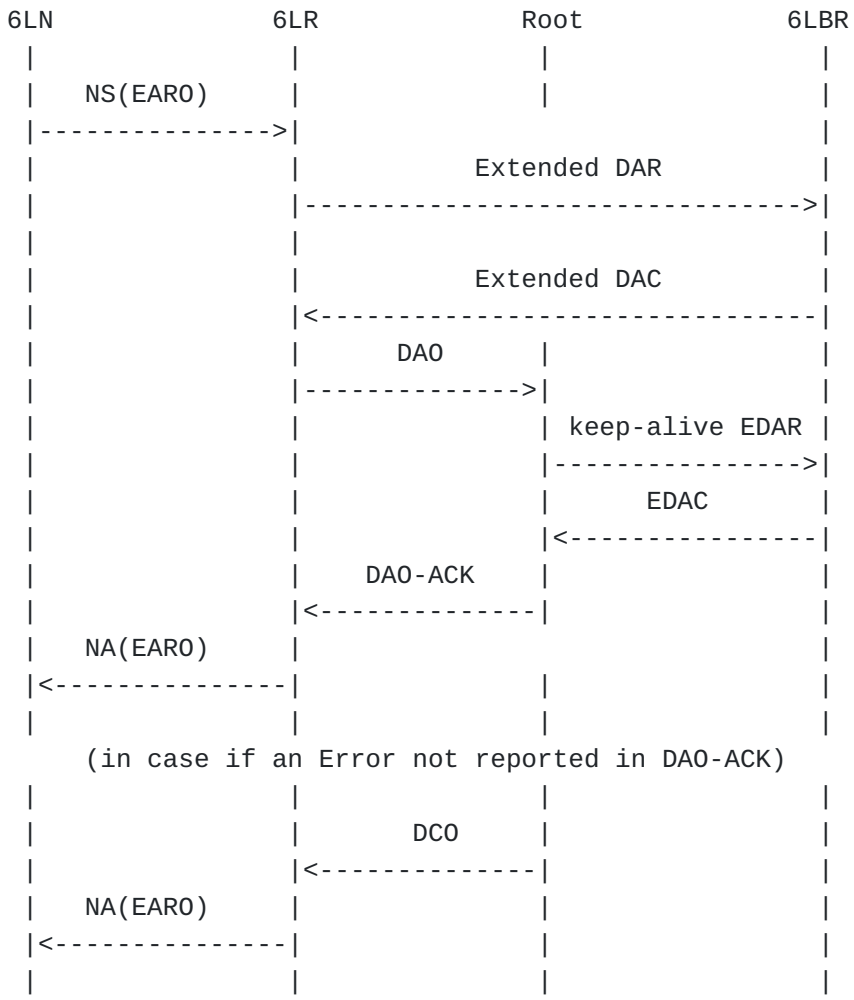


Figure 4: First Registration Flow in Non-Storing Mode

A re-registration is performed by the 6LN to maintain the NCE in the 6LR alive before lifetime expires. Upon a re-registration, as illustrated in Figure 5, the 6LR redistributes the Registered Address NS(EARO) in RPL.

This causes the RPL DODAG Root to refresh the state in the 6LBR with a keep-alive EDAC message. The keep-alive EDAC lacks the Registration Ownership Verifier (ROVR) information, since it is not present in RPL DAO messages, but the EDAC message sent in response by the 6LBR contains the actual value of the ROVR field for that registration.

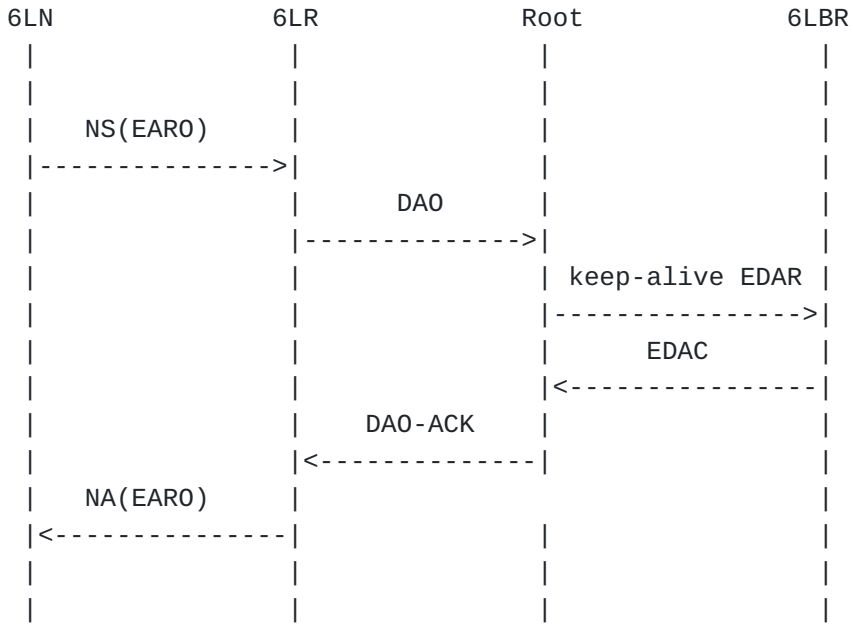


Figure 5: Next Registration Flow in Non-Storing Mode

In case of an error on the keep-alive EDAR flow, the error SHOULD be returned in the DAO-ACK - if one was requested - using the mapping of RPL Status and 6LoWPAN Status values discussed in Section 4.

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 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. So the 6LR must still expect a DAO-ACK even if it received a DCO while it was waiting for an acknowledgement for a short period of time, 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 a NA(EARO) and the 6LoWPAN ND Status value that is copied from the RPL status in the RPL message. An asynchronous DCO is also translated in an asynchronous NA(EARO) to the RUL with a copied Status value. The RPL Status values that are copied with 6LoWPAN ND are in the range 128 to 192 and listed in the same order (see Table 2). A RPL Status Value of 128 maps to 6LoWPAN ND Status Code of 1 and so on.

9.1.2. In RPL Storing-Mode

In 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 acknowledgement. A successful DAO-ACK is not a guarantee that the DAO has yet reached the Root or that the keep-alive EDAR has succeeded.

If the keep alive fails, the path is cleaned up asynchronously using a DCO message [EFFICIENT-NPDAO] as illustrated in Figure 6 and described in further details in Section 9.2.3.

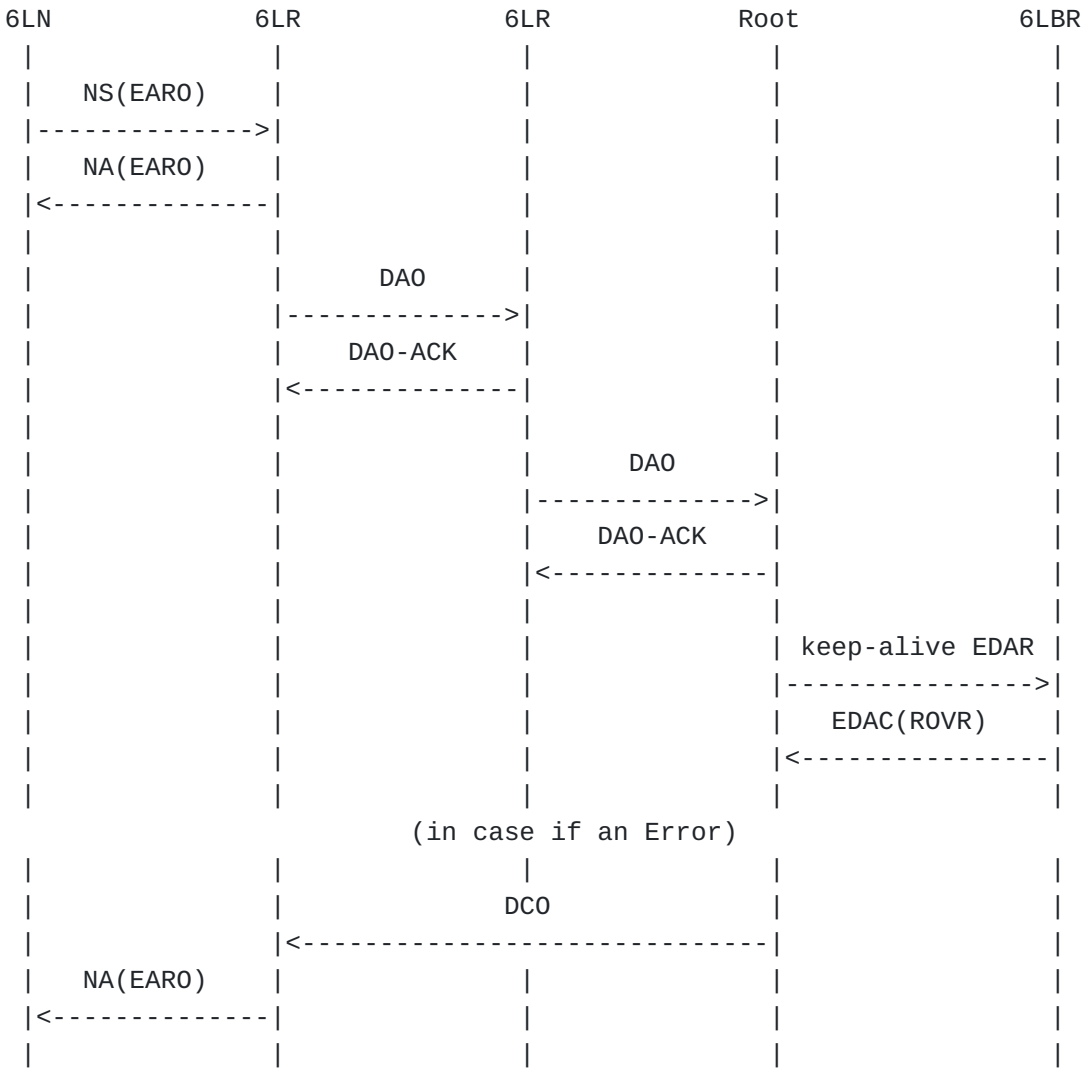


Figure 6: Next Registration Flow in Storing Mode

9.2. Operation

9.2.1. By the 6LN

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

- The 6LN obtains an IPv6 global address, for instance using autoconfiguration [RFC4862] based on a Prefix Information Option (PIO) [RFC4861] found in a Router Advertisement message or by some other means such as DHCPv6 [RFC3315].

- Once it has formed an address, the 6LN (re)registers its address periodically, within the Lifetime of the previous registration, as prescribed by [RFC6775].

- A 6LN acting as a RUL sets the R flag in the EARO whereas a 6LN acting as a RAN does not set the R flag as prescribed by [RFC8505] section 5.1.

- Upon each consecutive registration, the 6LN increases the TID field in the EARO, as prescribed by [RFC8505] section 5.2.

- The 6LN can register to more than one 6LR at the same time. In that case, a same value of TID is used for each registration.

- The 6LN may use any of the 6LRs to which it register to forward its packets. Using a 6LR to which the 6LN is not registered may result in packets dropped by a Source Address Validation function.

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. In any fashion the 6LN MUST set the "I" field to zero to indicate that topological information to be passed to a routing process as specified in [RFC8505] section 5.1.

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 and can build an RPI. A RUL that places an RPI in a data packet MUST indicate the RPLInstanceID that corresponds to the RPL Instance the packet should be injected into. All the flags and the Rank field are set to zero as specified by section 11.2 of [RFC6550].

9.2.2. By the 6LR

Also as prescribed by [RFC8505], the 6LR generates a DAR message upon reception of a valid NS(EARO) message for the registration of a new IPv6 Address by a 6LN. If the Duplicate Address exchange succeeds, then the 6LR installs a Neighbor Cache Entry (NCE). If the R flag was set in the EARO of the NS message, and this 6LR can manage the reachability of Registered Address, then the 6LR sets the R flag in the EARO of the NA message that is sent in response.

From then on, the 6LN periodically sends a new NS(EARO) to refresh the NCE state before the lifetime indicated in the EARO expires, with TID that is incremented each time till it wraps in a lollipop fashion (see section 5.2.1 of [RFC8505] which is fully compatible with section 7.2 of [RFC6550]). As long as the R flag is set and this router can still manage the reachability of Registered Address, the 6LR keeps setting the R flag in the EARO of the response NA message, but the exchange of Extended Duplicate Address messages is skipped.

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 RPL Packet Information (RPI) in the packet, in which case the 6LR SHOULD add one to the packet. if the "I" field is not zero, then the 6LR MUST consider that the Opaque field is zero. If the Opaque field is not set to zero, then it should carry a RPLInstanceID for the 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 empty. If the Opaque field is empty, the 6LR is free to use the default Instance (zero) for the registered address or to select an Instance of its choice; else, that is if the 6LR participates to the suggested Instance, then the 6LR SHOULD use that Instance for the registered address.

Upon a successful NS/NA(EARO) exchange: if the R flag was set in the EARO of the NS message, then the 6LR SHOULD inject the Registered Address in RPL by sending a DAO message on behalf of the 6LN; else the 6LR MUST NOT inject the Registered Address into RPL.

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

* The Registered Address is placed in a RPL Target Option in the DAO message as the Target Prefix, and the Prefix Length is set to 128;

* the External 'E' flag in the Transit Information Option (TIO) associated to the Target Option is set to indicate that the 6LR

redistributes an external target into the RPL network. When the Root has to use an IP-in-IP [USEofRPLinfo], then this flag indicates the IP-in-IP should be addressed to this node;

* the Path Lifetime in the TIO is computed from the Lifetime in the EARO Option to adapt 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;

* the Path Sequence in the TIO is set to the TID value found in the EARO option;

* Additionally, in Non-Storing Mode the 6LR indicates one of its global IPv6 unicast addresses as the Parent Address in the TIO.

If a DAO-ACK is not requested, or has a Status that is less than 128, indicating the DAO was accepted, respectively by a parent in Storing Mode or by the Root in non-Storing Mode,, the 6LR replies with a NA(EARO) to the RUL with a status of 0 (Success).

In case of a DAO-ACK or a DCO with a status of 132 (Validation Requested) the 6LR challenges the 6LN for ownership of the address, as described in section 6.1 of [RFC8505]. 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 MUST refrain from injecting the address in RPL and may take actions to protect itself against DoS attacks by a rogue 6LN, see Section 12

Other status values above 128 indicate that the 6LR failed to inject the address into the RPL network. In that case the the 6LR MUST send a NA(EARO) to the RUL with the copied Status value. If for any other reason the 6LR fails to inject the address into the RPL network, the 6LR SHOULD send a NA(EARO) to the RUL with a status of 2 (Out of Storage) which indicates a possibility to retry later.

If a 6LR receives a valid NS(EARO) message with the R flag reset 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 Node to maintain the corresponding route from then on, either keeping it active by sending further DAO messages, or destroying it using a No-Path DAO.

Upon 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 copied Status value.

9.2.3. By the RPL Root

In RPL Storing Mode of Operation (MOP), the DAO message is propagated from child to parent all the way to the Root along the DODAG, populating routing state as it goes. In Non-Storing Mode, The DAO message is sent directly to the RPL Root. Upon reception of a DAO message, for each RPL Target option that creates or updates an existing RPL state:

- the Root notifies the 6LBR using an internal API if they are co-located, or performs an EDAR/EDAC exchange on behalf of the 6LR if they are separated. If the Target option transports a ROVR, then the Root MUST use it to build a full EDAR message as the 6LR would. Else, a keep-alive EDAR is used with the ROVR field set to zero.

An EDAR message MUST be constructed as follows:

- The Target IPv6 address from in the RPL Target Option is placed in the Registered Address field of the EDAR message and in the Target field of the NS message, respectively;

- 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;

- the RPL Root indicates its own MAC Address as Source Link Layer Address (SLLA) in the NS(EARO);

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

- when present in the RPL Target option, the ROVR field is used 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 length of the ROVR field. If it is not present the ROVR field in the EDAR is set to zero indicating that this is a keep-alive EDAR. The actual value of the ROVR for that registration is expected from the 6LBR in the response EDAC.

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 placed in the DCO.

9.2.4. By the 6LBR

Upon reception of an EDAR message with the ROVR field is set to zero indicating a keep-alive EDAR, the 6LBR checks whether an entry exists for the and computes whether the TID in the DAR message is fresher than that in the entry as prescribed in section 4.2.1. of [RFC8505].

If the entry does not exist, the 6LBR does not create the entry, and answers with a Status "Removed" in the EDAC message.

If the entry exists but is not fresher, the 6LBR does not update the entry, and answers with a Status "Success" in the EDAC message.

If the entry exists and the TID in the DAR message is fresher, the 6LBR updates the TID in the entry, and if the lifetime of the entry is extended by the Registration Lifetime in the DAR message, it also updates the lifetime of the entry. In that case, the 6LBR replies with a Status "Success" in the DAC message.

The EDAC that is constructed is the same as if the keep-alive EDAR was a full EDAR, and includes the ROVR that is associated to the registration.

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 if 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 registration, as illustrated in Figure 7, the 6LN, as an MLD listener, sends an unsolicited Report to the 6LR in order to start receiving the flow immediately. 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 an Layer-2 acknoledgement, 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 echange as 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.

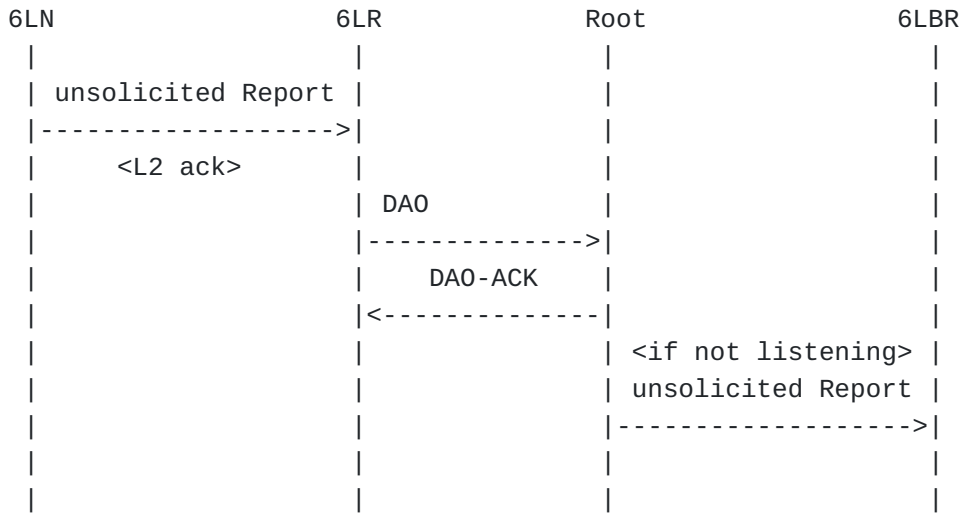


Figure 7: First Multicast Registration Flow

A re-registration is pulled by 6LR acting as querier. Note that the message may 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 8,

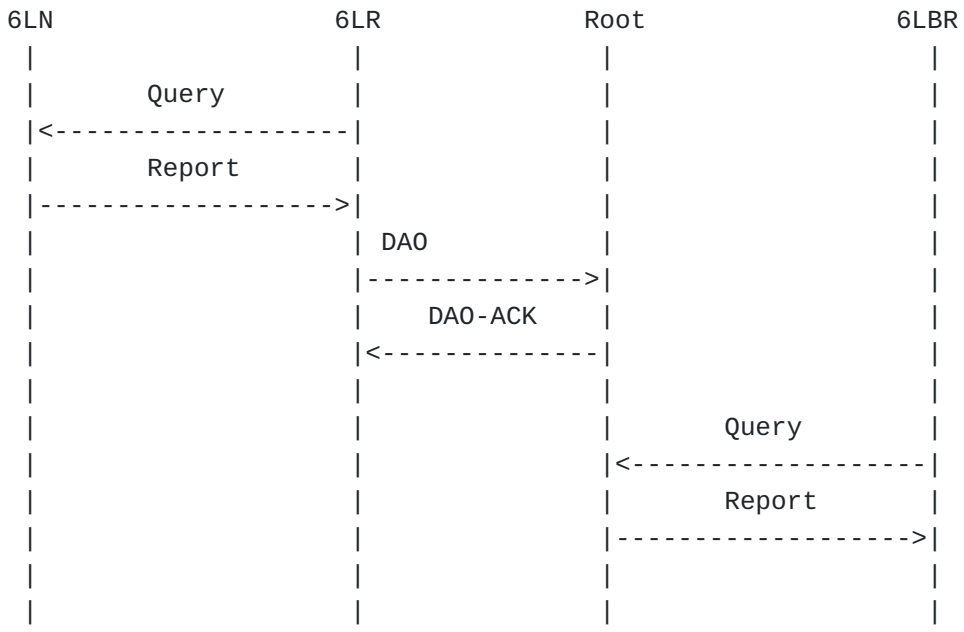


Figure 8: Next Registration Flow

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. Implementation Status

12. Security Considerations

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 access control, or could provide role validation as well. This is a generic 6LoWPAN requirement, see Req5.1 in Appendix of [RFC8505].

The keep-alive EDAR message does not carry a valid Registration Unique ID [RFC8505] and it cannot be used to create a binding state in the 6LBR. The 6LBR MUST NOT create an entry based on a keep-alive EDAR that does not match an existing entry. All it can do is refresh the lifetime and the TID of an existing entry.

At the time of this writing RPL does not have a zerotrust model whereby the 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.

13. IANA Considerations

13.1. 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.

13.2. New Subsubregistry for the RPL Non-Rejection Status values

This specification creates a new subsubregistry for the RPL Non-Rejection Status values for use in RPL DAO-ACK and RCO Messages, 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 2:

Value	Meaning	Defining Spec
0	Unqualified acceptance	RFC 6550

Table 2: Status values of the RPL DAO-ACK Message

13.3. New Subsubregistry for the RPL Rejection Status values

This specification creates a new subsubregistry for the RPL Non-Rejection Status values for use in RPL DAO-ACK and RCO Messages, under the ICMPv6 parameters registry.

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

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

*There is no initial allocation

14. Acknowledgments

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

15. 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>.

[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>.

[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>.

[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-12, 10 April 2019, <https://tools.ietf.org/html/draft-ietf-6lo-ap-nd-12>.

[USEofRPLinfo] Robles, I., Richardson, M., and P. Thubert, "Using RPL 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-31, 7 August 2019, <https://tools.ietf.org/html/draft-ietf-roll-useofrplinfo-31>.

[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>.

16. Informative References

[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>.

[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>.

[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>.

Appendix A. Example Compression

Figure 9 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]. The difference with the format presented in Figure 19 of [RFC8138] is the addition of a SRH-6LoRH before the RPI-6LoRH to transport the destination address of the outer IPv6 header.

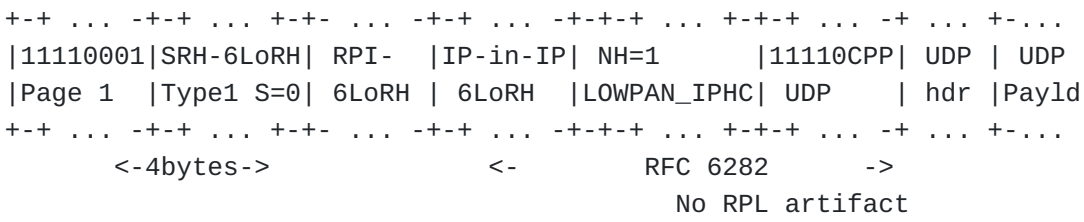


Figure 9: Encapsulation to Parent 6LR in Storing Mode

In Figure 9, 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 9 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.

Follows the RPI-6LoRH and then the IP-in-IP 6LoRH. When the IP-in-IP 6LoRH is removed, all the router 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/