6Lo
Internet-Draft
Intended status: Standards Track
Expires: February 21, 2015

P. Thubert, Ed.
cisco

August 22, 2014

Requirements for an update to 6LoWPAN ND draft-thubert-6lo-rfc6775-update-reqs-04

Abstract

Work presented at the ROLL, 6lo, 6TiSCH and 6MAN Working Groups suggest that enhancements to the 6LoWPAN ND mechanism are now needed. This document elaborates on those requirements and suggests approaches to serve them.

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 http://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 February 21, 2015.

Table of Contents

1. Introduction 2
2. Terminology 3
3. Overview 3
  3.1. RPL Leaf Support in 6LoWPAN ND 5

3.2. registration Failures Due to Movement 6
3.3. Proxy registration 6
3.4. Target Registration 6
3.5. RPL root vs. 6LBR 7
3.6. Securing the Registration 7
4. Requirements 8
4.1. Requirements Related to Mobility 8
4.2. Requirements Related to Routing Protocols 9
4.3. Requirements Related to the Variety of Low-Power Link types 9
4.4. Requirements Related to Proxy Operations 10
4.5. Requirements Related to Security 10
4.6. Requirements Related to Low-Power devices 11
5. Suggested Changes to Protocol Elements 11
5.1. ND Neighbor Solicitation (NS) 11
5.2. ND Router Advertisement (RA) 12
5.3. RPL DODAG Information Object (DIO) 12
5.4. ND Enhanced Address Registration Option (EARO) 12
6. Security Considerations 13
7. IANA Considerations 14
8. Acknowledgments 14
9. References 14
9.1. Normative References 14
9.2. Informative References 15
Author's Address 16

1. Introduction

A number of use cases, including the Industrial Internet, require a large scale deployment of sensors that can not be realized with wires and is only feasible over wireless Low power and Lossy Network (LLN) technologies. When simpler hub-and-spoke topologies are not sufficient for the expected throughput and density, mesh networks must be deployed, which implies the concepts of hosts and routers, whether operated at Layer-2 or Layer-3.

The IETF has designed the LLN host-to-router and router-to-router protocol that supports address assignment and the router-to-router protocol that supports reachability across Route-Over LLNs in different Areas. It was clear for both efforts that the scalability requirements could only be met with IPv6 [RFC2460], and there is no fundamental contradiction between those protocols to that regard.

While DHCPv6 is still a viable option in LLNs, the new IETF standard that supports address assignment specifically for LLNs is 6LoWPAN ND, the Neighbor Discovery Optimization for Low-power and Lossy Networks [RFC6775]. 6LoWPAN ND was designed as a stand-alone mechanism separately from its IETF routing counterpart, the IPv6 Routing Protocol for Low power and Lossy Networks [RFC6550] (RPL), and the interaction between the 2 protocols was not defined.

The 6TiSCH WG is now considering an architecture [I-D.ietf-6tisch-architecture] whereby a 6LowPAN ND host could connect to the Internet via a RPL Network, but this requires additions to the protocol to support mobility and reachability in a secured and manageable

environment.

At the same time, new work at 6MAN on Efficiency aware IPv6 Neighbor Discovery Optimizations [I-D.chakrabarti-nordmark-6man-efficient-nd] suggests that 6LoWPAN ND can be extended to other types of networks on top of the Low power and Lossy Networks (LLNs) for which it was already defined. The value of such extension is especially apparent in the case of mobile wireless devices, to reduce the multicast operations that are related to classical ND ([RFC4861], [RFC4862]) and plague the wireless medium. In this context also, there is a need for additions to the protocol.

The Optimistic Duplicate Address Detection [RFC4429] (ODAD) specification details how an address can be used before a Duplicate Address Detection (DAD) is complete, and insists that an address that is TENTATIVE should not be associated to a Source Link-Layer Address Option in a Neighbor Solicitation message. As we expect the 6LoWPAN ND protocol for a more general use, it can make sense to keep respecting that rule, which is another change to the specification.

This document suggests a limited evolution to [RFC6775] so as to allow operation of a 6LoWPAN ND node as a leaf in a RPL network. It also suggests a more generalized use of the information in the ARO option outside of the strict LLN domain, for instance over a converged backbone.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

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], "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 "Transmission of IPv6 Packets over IEEE 802.15.4 Networks" [RFC4944].

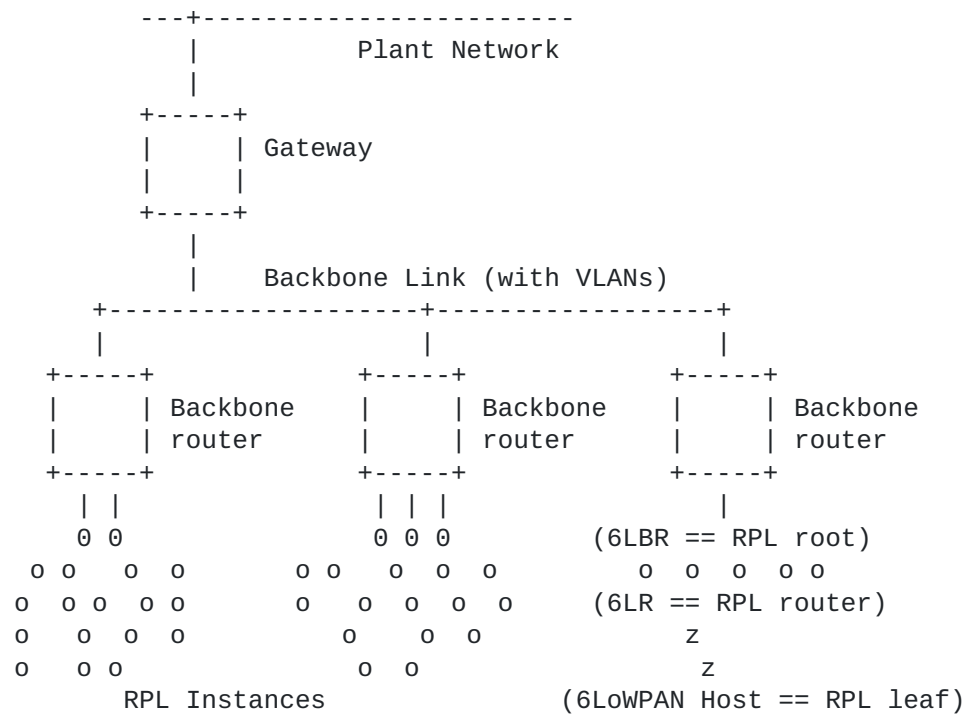
Additionally, this document uses terminology from 6TiSCH [I-D.ietf-6tisch-terminology] and ROLL [RFC7102].

3. Overview

The 6TiSCH architecture [I-D.ietf-6tisch-architecture] expects that a 6LoWPAN device can connect as a leaf to a RPL network, where the leaf support is the minimal functionality to connect as a host to a RPL network without the need to participate to the full routing protocol. The support of leaf can be implemented as a minor

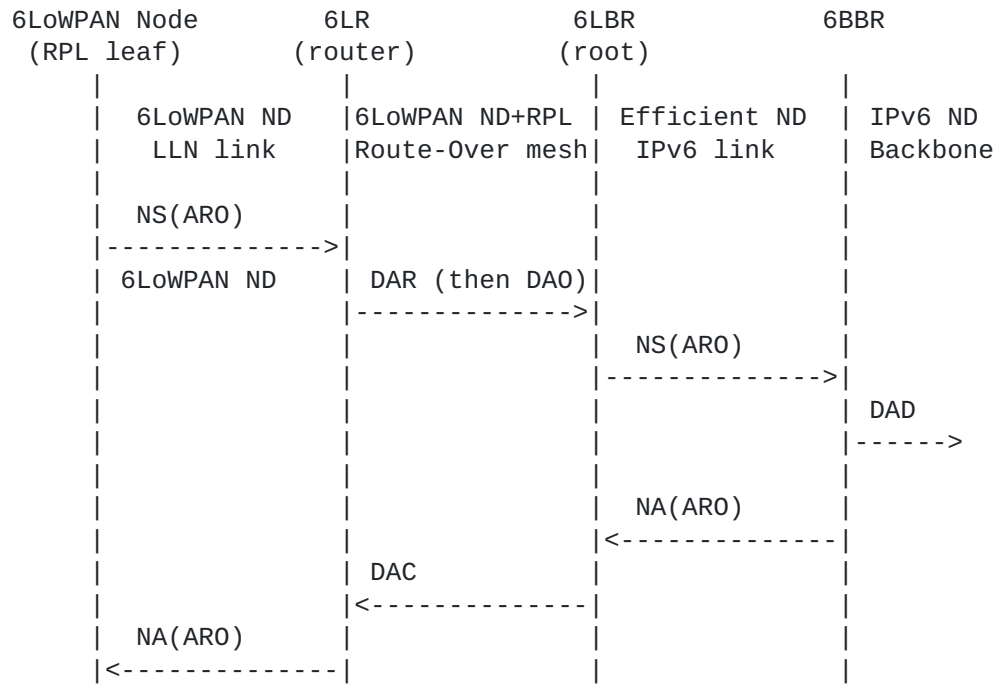
increment to 6LoWPAN ND, with the additional capability to carry a sequence number that is used to track the movements of the device, and optionally some information about the RPL topology that this device will join.

The scope of the 6TiSCH Architecture is a Backbone Link that federates multiple LLNs as a single IPv6 Multi-Link Subnet. Each LLN in the subnet is anchored at a Backbone Router (6BBR). The Backbone Routers interconnect the LLNs over the Backbone Link and emulate that the LLN nodes are present on the Backbone by proxy-ND operations. An LLN node can move freely from an LLN Route-Over mesh anchored at a Backbone Router to another anchored at a same or a different Backbone Router inside the Multi-Link Subnet and conserve its addresses.



The root of the RPL topology is logically separated from the 6BBR that is used to connect the RPL topology to the backbone. The RPL root can use Efficient ND as the interface to register an LLN node in its topology to the 6BBR for whatever operation the 6BBR performs, such as ND proxy operations, or injection in a routing protocol. It results that, as illustrated in Figure 2, the periodic signaling could start at the leaf node with 6LoWPAN ND, then would be carried over RPL to the RPL root, and then with Efficient-ND to the 6BBR.

Efficient ND being an adaptation of 6LoWPAN ND, it makes sense to keep those two homogeneous in the way they use the source and the target addresses in the Neighbor Solicitation (NS) messages for registration, as well as in the options that they use for that process.



As the network builds up, a node should start as a leaf to join the RPL network, and may later turn into both a RPL-capable router and a 6LR, so as to accept leaf nodes to recursively join the network.

3.1. RPL Leaf Support in 6LoWPAN ND

RPL needs a set of information in order to advertise a leaf node through a DAO message and establish reachability.

At the bare minimum the leaf device must provide a sequence number that matches the RPL specification in section 7. [I-D.chakrabarti-nordmark-6man-efficient-nd] section "4.1. Address Registration Option" (ARO) already incorporates that addition with a new field in the option called the Transaction ID.

If for some reason the node is aware of RPL topologies, then providing the RPL InstanceID for the instances to which the node wishes to participate would be a welcome addition. In the absence of such information, the RPL router must infer the proper instanceID from external rules and policies.

On the backbone, the InstanceID is expected to be mapped onto a VLANID. Neither WiFi nor Efficient ND do provide a mapping to VLANIDs, and it is unclear, when a wireless node attaches to a backbone where VLANs are defined, which VLAN the wireless device attaches to. Considering that a VLAN is effectively the IP link on the backbone, adding the InstanceID to both specifications could be a welcome addition.

3.2. registration Failures Due to Movement

Registration to the 6LBR through DAR/DAC messages [RFC6775] may percolate slowly through an LLN mesh, and it might happen that in the meantime, the 6LoWPAN node moves and registers somewhere else. Both RPL and 6LoWPAN ND lack the capability to indicate that the same node is registered elsewhere, so as to invalidate states down the deprecated path.

In its current expression and functionality, 6LoWPAN ND considers that the registration is used for the purpose of DAD only as opposed to that of achieving reachability, and as long as the same node registers the IPv6 address, the protocol is functional. In order to act as a RPL leaf registration protocol and achieve reachability, the device must use the same TID for all its concurrent registrations, and registrations with a past TID should be declined. The state for an obsolete registration in the 6LR, as well as the RPL routers on the way, should be invalidated. This can only be achieved with the addition of a new Status in the DAC message, and a new error/clean-up flow in RPL.

3.3. Proxy registration

The 6BBR provides the capability to defend an address that is owned by a 6LoWPAN Node, and attract packets to that address, whether it is done by proxying ND over a MultiLink Subnet, redistributing the address in a routing protocol or advertising it through an alternate proxy registration such as the Locator/ID Separation Protocol [RFC6830] (LISP) or Mobility Support in IPv6 [RFC6275] (MIPv6). In a LLN, it makes sense to piggyback the request to proxy/defend an address with its registration.

3.4. Target Registration

In their current incarnations, both 6LoWPAN ND and Efficient ND expect that the address being registered is the source of the NS(ARO) message and thus impose that a Source Link-Layer Address (SLLA) option be present in the message. In a mesh scenario where the 6LBR is physically separated from the 6LoWPAN Node, the 6LBR does not own the address being registered. This suggests that [I-D.chakrabarti-nordmark-6man-efficient-nd] should evolve to register the Target of the NS message as opposed to the Source Address. From another perspective, it may happen, in the use case of a Star topology, that the 6LR, 6LBR and 6BBR are effectively collapsed and should support 6LoWPAN ND clients. The convergence of efficient ND and 6LoWPAN ND into a single protocol is thus highly desirable.

In any case, as long as the DAD process is not complete for the address used as source of the packet, it is against the current practice to advertise the SLLA, since this may corrupt the ND cache of the destination node, as discussed in the Optimistic DAD specification [RFC4429] with regards to the TENTATIVE state.

This may look like a chicken and an egg problem, but in fact 6LoWPAN ND acknowledges that the Link-Local Address that is based on an EUI-64 address of a LLN node may be autoconfigured without the need for DAD. It results that a node could use that Address as source, with an SSLA option in the message if required, to register any other addresses, either Global or Unique-Local Addresses, which would be indicated in the Target.

The suggested change is to register the target of the NS message, and use Target Link-Layer Address (TLLA) in the NS as opposed to the SLLA in order to install a Neighbor Cache Entry. This would apply to both Efficient ND and 6LoWPAN ND in a very same manner, with the caveat that depending on the nature of the link between the 6LBR and the 6BBR, the 6LBR may resort to classical ND or DHCPv6 to obtain the address that it uses to source the NS registration messages, whether for itself or on behalf of LLN nodes.

3.5. RPL root vs. 6LBR

6LoWPAN ND is unclear on how the 6LBR is discovered, and how the liveliness of the 6LBR is asserted over time. On the other hand, the discovery and liveliness of the RPL root are obtained through the RPL protocol.

When 6LoWPAN ND is coupled with RPL, it makes sense to collocate the 6LBR and the RPL root functionalities. The DAR/DAC exchange becomes a preamble to the DAO messages that are used from then on to reconfirm the registration, thus eliminating a duplication of functionality between DAO and DAR messages.

3.6. Securing the Registration

A typical attack against IPv6 ND is address spoofing, whereby a rogue node claims the IPv6 Address of another node in and hijacks its traffic.

SEcure Neighbor Discovery (SEND) [RFC3971] is designed to protect each individual ND lookup/advertisement in a peer to peer model where each lookup may be between different parties. This is not the case in a 6LoWPAN ND LLN where, as illustrated in Figure 2, the 6LBR terminates all the flows and may store security information for later validation.

Additionally SEND requires considerably enlarged ND messages to carry cryptographic material, and requires that each protected address is generated cryptographically, which implies the computation of a different key for each Cryptographically Generated Address (CGA). SEND as defined in [RFC3971] is thus largely unsuitable for application in a LLN.

Once an Address is registered, the 6LBR maintains a state for that Address and is in position to bind securely the first registration with the Node that placed it, whether the Address is CGA or not. It should thus be possible to protect the ownership of all the addresses of a 6LoWPAN Node with a single key, and there should not be a need to carry the cryptographic material more than once to the 6LBR.

The energy constraint is usually a foremost factor, and attention should be paid to minimize the burden on the CPU. Hardware-assisted support of variants of the Counter with CBC-MAC [RFC3610] (CCM) authenticated encryption block cipher mode such as CCM* are common in LowPower ship-set implementations, and 6LoWPAN ND security mechanism should be capable to reuse them when applicable.

Finally, the code footprint in the device being also an issue, the capability to reuse not only hardware-assist mechanisms but also software across layers has to be considered. For instance, if code has to be present for upper-layer operations, e.g AES-CCM Cipher Suites for Transport Layer Security (TLS) [RFC6655], then the capability to reuse that code should be considered.

4. Requirements

4.1. Requirements Related to Mobility

Due to the nature of LLN networks, even a fixed 6LoWPAN Node may change its point of attachment (a 6LR) and may not be able to notify the 6LR that it has disconnected from. It results that the previous 6LR may still attract traffic that it cannot deliver any more. When the 6LR changes, there is thus a need to identify stale states and restore reachability timely.

Req1.1: Upon a change of point of attachment, connectivity via a new

6LR MUST be restored timely without the need to de-register from the previous 6LR.

Req1.2: For that purpose, the protocol MUST enable to differentiate multiple registrations from a same 6LoWPAN Node from two different 6LoWPAN Nodes claiming a same address.

Req1.3: This information MUST be passed from the 6LR to the 6LBR, and the 6LBR SHOULD be able to clean up the stale state asynchronously in the previous 6LR.

Req1.4: A 6LoWPAN Node SHOULD also be capable to register a same Address to multiple 6LRs, and this, concurrently.

4.2. Requirements Related to Routing Protocols

The point of attachment of a 6LoWPAN Node may be a 6LR in an LLN mesh. An LLN route-over mesh is typically based on RPL, which is the routing protocol that was defined at the IETF for this particular purpose. It derives that in this scenario, the 6LR would classically support RPL. One goal is that a 6LoWPAN Node attached via ND to a RPL-capable 6LR would not need to participate to the RPL protocol to obtain reachability via the 6LR. An additional goal would be to obtain reachability via other routing protocols through a same ND-based abstraction.

Related requirements are:

Req2.1: The ND registration method SHOULD be extended in such a fashion that the 6LR MAY advertise the Address of a 6LoWPAN Node over RPL and obtain reachability to that Address over the RPL domain.

Req2.2: The Address Registration Option that is used in the ND registration SHOULD be extended to carry enough information to generate a DAO message as specified in [RFC6550] section 6.4, in particular the capability to compute a DAOSequence and, as an option, a RPLInstanceID.

Req2.3: Depending on their applicability to LLNs, other standard mesh /MANET protocols MAY be considered as well.

4.3. Requirements Related to the Variety of Low-Power Link types

6LoWPAN ND [RFC6775] was defined with a focus on IEEE802.15.4 and in particular the capability to derive a unique Identifier from a globally unique MAC-64 address. At this point, the 6lo Working Group is extending the 6LoWPAN Header Compression (HC) [RFC6282] technique to other link types ITU-T G.9959 [I-D.brandt-6man-lowpanz], Master-

Slave/Token-Passing [I-D.ietf-6lo-6lobac], DECT Ultra Low Energy [I-D.ietf-6lo-dect-ule], Near Field Communication [I-D.hong-6lo-ipv6-over-nfc], as well as IEEE1901.2 Narrowband Powerline Communication Networks [I-D.popa-6lo-6loplc-ipv6-over-ieee19012-networks] and BLUETOOTH(R) Low Energy [I-D.ietf-6lo-btle].

Related requirements are:

Req3.1: The support of the registration mechanism SHOULD be extended to more LLN links, matching at least the links that are considered by 6lo as well as other popular Low-Power links such as Low-Power Wi-Fi.

Req3.2: As part of this extension, a mechanism to compute a unique Identifier should be provided, with the capability to form a Link-Local Address that can not be a duplicate. The Identifier SHOULD be unique at least to the domain where an Address formed by this device may be advertised through ND mechanisms.

Req3.3: The Address Registration Option used in the ND registration SHOULD be extended to carry the relevant forms of unique Identifier.

4.4. Requirements Related to Proxy Operations

Sleeping devices may not be able to answer themselves to a lookup from a node that uses classical ND on a backbone and may need a proxy operation by a 6BBR. Additionally, the device may need to rely on the 6LBR to perform that registration to the 6BBR.

Related requirements are:

Req4.1: The registration mechanism SHOULD enable a third party to proxy register an Address on behalf of a 6LoWPAN node that may be sleeping or located deeper in an LLN mesh.

4.5. Requirements Related to Security

In order to guarantee the operations of the 6LoWPAN ND flows, the spoofing of the 6LR, 6LBR and 6BBRs roles should be avoided. Once a node successfully registers an address, 6LoWPAN ND should provide energy-efficient means to protect that ownership even if the node is sleeping. In particular, the 6LR and the 6LBR then should be able to verify whether a subsequent registration for a same Address comes from a same node or is a duplicate.

Related requirements are:

Req5.1: 6LoWPAN ND security mechanisms SHOULD provide a mechanism for the 6LR, 6LBR and 6BBR to authenticate and authorize one another for their respective roles, as well as with the 6LoWPAN Node for the role

of 6LR.

Req5.2: 6LoWPAN ND security mechanisms SHOULD provide a mechanism for the 6LR and the 6LBR to validate whether a new registration corresponds to a same 6LoWPAN Node, and, if not, determine the rightful owner, and deny or clean-up the registration that is deemed in excess.

Req5.3: 6LoWPAN ND security mechanisms SHOULD lead to small packet sizes. In particular, the NS, NA, DAR and DAC messages for a re-registration flow SHOULD NOT exceed 80 octets so as to fit in a secured IEEE802.15.4 frame.

Req5.4: Recurrent 6LoWPAN ND security operations MUST NOT be computationally intensive on the LoWPAN Node CPU. When a Key hash calculation is employed, a mechanism lighter than SHA-1 SHOULD be preferred.

Req5.5: The number of Keys that the 6LoWPAN Node needs to manipulate SHOULD be minimized.

Req5.6: The 6LoWPAN ND security mechanisms SHOULD enable CCM* for use at both Layer 2 and Layer 3, and SHOULD enable the reuse of security code that has to be present on the device for upper layer security such as TLS.

Req5.7: Public key and signature sizes SHOULD be minimized while maintaining adequate confidentiality and data origin authentication for multiple types of applications with various degrees of criticality.

4.6. Requirements Related to Low-Power devices

The ND registration method is designed to save energy on Low-Power devices, and in particular enable duty-cycled devices that are sleeping most of the time and not capable to defend their own Addresses against always-on devices.

Related requirements are:

Req6.1: The registration mechanism SHOULD be applicable to a Low-Power device regardless of the link type, and enable a 6BBR to operate as a proxy to defend the registered Addresses on its behalf.

5. Suggested Changes to Protocol Elements

5.1. ND Neighbor Solicitation (NS)

The NS message used for registration should use a source address that respects the rules in [RFC6775], [RFC4861], and [RFC4429] for DAD. The SLLA Option may be present but only if the address passed DAD, and it is used to allow the 6LR to respond as opposed to as a registration mechanism.

The address that is being registered is the target address in the NS message and the TLLA Option must be present.

5.2. ND Router Advertisement (RA)

[I-D.chakrabarti-nordmark-6man-efficient-nd] adds an 'E' bit in the Router Advertisement flag, as well as a new Registrar Address Option (RAO). These fields are probably pertinent to LLNs inclusion into a revised 6LoWPAN ND should be studied. If the new 6LoWPAN flows require a change of behaviour (e.g. registering the Target of the NS message) then the RA must indicate that the router supports the new capability, and the NS must indicate that the Target is registered as opposed to the Source in an unequivocal fashion.

There is some amount of duplication between the options in the RPL DIO [RFC6550] and the options in the ND RA messages. At the same time, there are a number of options, including the 6LoWPAN Context Option (6CO) [RFC6775], the MTU and the SLLA Options [RFC4861] that can only be found in the RA messages. Considering that these options are useful for a joining node, the recommendation would be to associate the RA messages to the join beacon, and make them rare when the network is stable. On the other hand, the DIO message is to be used as the propagated heartbeat of the RPL network and provide the sense of time and liveliness.

RAs should also be issued and the information therein propagated when a change occurs in the information therein, such as a router or a prefix lifetime.

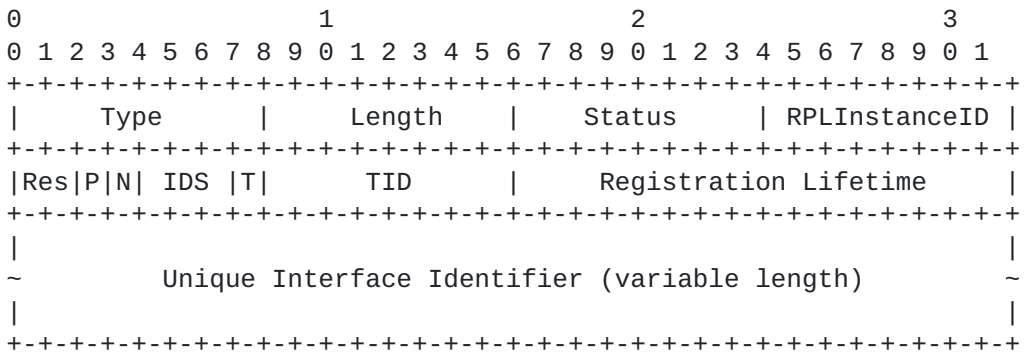
5.3. RPL DODAG Information Object (DIO)

If the RPL root serves as 6LBR, it makes sense to add at least a bit of information in the DIO to signal so. A Registrar Address Option (RAO) may also be considered for addition.

5.4. ND Enhanced Address Registration Option (EARO)

The ARO option contains a Unique ID that is supposed to identify the device across multiple registrations. It is envisioned that the device could form a single CGA-based Unique Interface ID (CUID) to securely bind all of its addresses. The CUID would be used as Unique Interface Identifier in the ARO option and to form a Link-Local address that would be deemed unique regardless of the Link type. Provided that the relevant cryptographic material is passed to the 6LBR upon the first registration or on-demand at a later time, the 6LBR can validate that a Node is effectively the owner of a CUID, and ensure that the ownership of an Address stays with the CUID that registered it first.

This option is designed to be used with standard NS and NA messages between backbone Routers as well as between nodes and 6LRs over the LLN and between the 6LBR and the 6BBR over whatever IP link they use to communicate.



The representation above is based on [I-D.chakrabarti-nordmark-6man-efficient-nd]. Only the proposed changes from that specification are discussed below but the expectation is that 6LoWPAN ND and Efficient ND converge on the ARO format.

Status: 8-bit integer. A new value of 3 is suggested to indicate a rejection due to an obsolete TID, typically an indication of a movement.

RPLInstanceID: 8-bit integer. This field is set to 0 when unused. Otherwise it contains the RPLInstanceID for which this address is registered, as specified in RPL [RFC6550], and discussed in particular in section 3.1.2.

P: One bit flag. When the bit is set, the address being registered is Target of the NS as opposed to the Source, for instance to enable ND proxy operation.

N: One bit flag. Set if the device moved. If not set, the 6BBR will refrain from sending gratuitous NA(O) or other form of distributed ND cache clean-up over the backbone. For instance, the flag should be reset after the DAD operation upon address formation.

6. Security Considerations

This specification expects that the link layer is sufficiently protected, either by means of physical or IP security for the Backbone Link or MAC sublayer cryptography. In particular, it is expected that the LLN MAC provides secure unicast to/from the Backbone Router and secure broadcast from the Backbone Router in a way that prevents tempering with or replaying the RA messages. Still, Section 4.5 has a requirement for a mutual authentication and authorization for a role for 6LRs, 6LBRs and 6BBRs.

This documents also suggests in Section 5.4 that a 6LoWPAN Node could form a single Unique Interface ID (CUID) based on cryptographic techniques similar to CGA. The CUID would be used as Unique Interface Identifier in the ARO option and new Secure ND procedures would be proposed to use it as opposed to the source IPv6 address to secure the binding between an Address and its owning Node, and enforce First/Come-First/Serve at the 6LBR.

7. IANA Considerations

A new type is requested for an ND option.

8. Acknowledgments

The author wishes acknowledge the contributions by Samita Chakrabarti, Erik Normark, JP Vasseur, Eric Levy-Abegnoli, Patrick Wetterwald, Thomas Watteyne, and Behcet Sarikaya.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] Deering, S.E. and R.M. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC3775] Johnson, D., Perkins, C. and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, April 2006.

[RFC4443] Conta, A., Deering, S. and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W. and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T. and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J. and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[RFC6275] Perkins, C., Johnson, D. and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC6282] Hui, J. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, September 2011.

[RFC6550] Winter, T., Thubert, P., 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, March 2012.

[RFC6655] McGrew, D. and D. Bailey, "AES-CCM Cipher Suites for Transport Layer Security (TLS)", RFC 6655, July 2012.

[RFC6775] Shelby, Z., Chakrabarti, S., Nordmark, E. and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, November 2012.

[RFC6830] Farinacci, D., Fuller, V., Meyer, D. and D. Lewis, "The Locator/ID Separation Protocol (LISP)", RFC 6830, January 2013.

9.2. Informative References

[I-D.brandt-6man-lowpanz]
Brandt, A. and J. Buron, "Transmission of IPv6 packets over ITU-T G.9959 Networks", Internet-Draft draft-brandt-6man-lowpanz-02, June 2013.

[I-D.chakrabarti-nordmark-6man-efficient-nd]
Chakrabarti, S., Nordmark, E., Thubert, P. and M. Wasserman, "Wired and Wireless IPv6 Neighbor Discovery Optimizations", Internet-Draft draft-chakrabarti-nordmark-6man-efficient-nd-04, October 2013.

[I-D.hong-6lo-ipv6-over-nfc]
Hong, Y., Choi, Y., Youn, J., Kim, D. and J. Choi, "Transmission of IPv6 Packets over Near Field Communication", Internet-Draft draft-hong-6lo-ipv6-over-nfc-01, August 2014.

[I-D.ietf-6lo-6lobac]
Lynn, K., Martocci, J., Neilson, C. and S. Donaldson, "Transmission of IPv6 over MS/TP Networks", Internet-Draft draft-ietf-6lo-6lobac-00, July 2014.

[I-D.ietf-6lo-btle]
Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z. and C. Gomez, "Transmission of IPv6 Packets over BLUETOOTH(R) Low Energy", Internet-Draft draft-ietf-6lo-btle-02, June 2014.

[I-D.ietf-6lo-dect-ule]
Mariager, P., Petersen, J., Shelby, Z., Logt, M. and D. Barthel, "Transmission of IPv6 Packets over DECT Ultra Low Energy", Internet-Draft draft-ietf-6lo-dect-ule-00, June 2014.

[I-D.ietf-6tisch-architecture]
Thubert, P., Watteyne, T. and R. Assimiti, "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4e", Internet-Draft draft-ietf-6tisch-architecture-01, February 2014.

[I-D.ietf-6tisch-terminology]
Palattella, M., Thubert, P., Watteyne, T. and Q. Wang, "Terminology in IPv6 over the TSCH mode of IEEE 802.15.4e", Internet-Draft draft-ietf-6tisch-terminology-00, November 2013.

[I-D.popa-6lo-6loplc-ipv6-over-ieee19012-networks]
Popa, D. and J. Hui, "6LoPLC: Transmission of IPv6 Packets over IEEE 1901.2 Narrowband Powerline Communication Networks", Internet-Draft draft-popa-6lo-6loplc-ipv6-over-ieee19012-networks-00, March 2014.

[RFC3610] Whiting, D., Housley, R. and N. Ferguson, "Counter with CBC-MAC (CCM)", RFC 3610, September 2003.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A. and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[RFC3971] Arkko, J., Kempf, J., Zill, B. and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[RFC4389] Thaler, D., Talwar, M. and C. Patel, "Neighbor Discovery Proxies (ND Proxy)", RFC 4389, April 2006.

[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, August 2007.

[RFC7102] Vasseur, JP., "Terms Used in Routing for Low-Power and Lossy Networks", RFC 7102, January 2014.

Author's Address

Pascal Thubert, editor
Cisco Systems, Inc
Building D
45 Allee des Ormes - BP1200
MOUGINS - Sophia Antipolis, 06254
FRANCE

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