            Registration Extensions for 6LoWPAN Neighbor Discovery
                    draft-ietf-6lo-rfc6775-update-16

Abstract

   This specification updates RFC 6775 - 6LoWPAN Neighbor Discovery, to
   clarify the role of the protocol as a registration technique,
   simplify the registration operation in 6LoWPAN routers, as well as to
   provide enhancements to the registration capabilities and mobility
   detection for different network topologies including the backbone
   routers performing proxy Neighbor Discovery in a low power network.

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 September 19, 2018.

Copyright Notice

Table of Contents

1. Introduction

   The scope of this draft is an IPv6 Low-Power Network including star
   and mesh topologies. This specification modifies and extends the
   behavior and protocol elements of "Neighbor Discovery Optimization
   for IPv6 over Low-Power Wireless Personal Area Networks" (6LoWPAN ND)
   [RFC6775] to enable additional capabilities and enhancements
   including:

   o determining the freshest location in case of mobility (TID)
   o Simplifying the registration flow for Link-Local Addresses
   o Support of a Leaf Node in a Route-Over network
   o Proxy registration in a Route-Over network
   o Registration to a IPv6 ND proxy over a Backbone Link (6BBR)
   o Clarification of support for privacy and temporary addresses

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. Subset of a 6LoWPAN Glossary

   This document often uses the following acronyms:

   6BBR: 6LoWPAN Backbone Router (proxy for the registration)
   6LBR: 6LoWPAN Border Router (authoritative on DAD)
   6LN: 6LoWPAN Node
   6LR: 6LoWPAN Router (relay to the registration process)

   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
   DODAG: Destination-Oriented Directed Acyclic Graph
   LLN: Low-Power and Lossy Network (a typical IoT network)
   NA: Neighbor Advertisement
   NCE: Neighbor Cache Entry
   ND: Neighbor Discovery
   NDP: Neighbor Discovery Protocol
   NS: Neighbor Solicitation
   ROVR: Registration Ownership Verifier (pronounced rover)
   RPL: IPv6 Routing Protocol for LLNs (pronounced ripple)
   RA: Router Advertisement
   RS: Router Solicitation
   TSCH: Timeslotted Channel Hopping
   TID: Transaction ID (a sequence counter in the EARO)

2.3. References

   The Terminology used in this document is consistent with and
   incorporates that described in Terms Used in Routing for Low-Power
   and Lossy Networks (LLNs). [RFC7102].

   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

   o "Neighbor Discovery for IP version 6" [RFC4861],
   o "IPv6 Stateless Address Autoconfiguration" [RFC4862],
   o "Problem Statement and Requirements for IPv6 over Low-Power
      Wireless Personal Area Network (6LoWPAN) Routing" [RFC6606],
   o "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs):
      Overview, Assumptions, Problem Statement, and Goals" [RFC4919] and
   o "Neighbor Discovery Optimization for Low-power and Lossy Networks"
      [RFC6775].

2.4. New Terms

   This specification introduces the following terminology:

   Backbone Link: An IPv6 transit link that interconnects two or more
        Backbone Routers. It is expected to be of high speed compared
        to the LLN in order to carry the traffic that is required to

federate multiple segments of the potentially large LLN into a
single IPv6 subnet.

Backbone Router: A logical network function in an IPv6 router that
federates an LLN over a Backbone Link. In order to do so, the
Backbone Router (6BBR) proxies the 6LoWPAN ND operations
detailed in this document onto the matching operations that run
over the backbone, typically IPv6 ND. Note that 6BBR is a
logical function, just like 6LR and 6LBR, and that the same
physical router may operate all three.

Extended LLN: Multiple LLNs as defined in [RFC6550], interconnected
by a Backbone Link via Backbone Routers, and forming a single
IPv6 Multi-Link Subnet.

Registration: The process during which a 6LN registers an IPv6
Address with a 6LR in order to obtain services such as DAD and
routing back. In a Route-Over network, a router that provides
connectivity to the LLN (typically a 6LBR, e.g., collocated
with a RPL Root) may serve as proxy for the registration of the
6LN to the 6BBR so the 6BBR can provide IPv6 ND proxy services
over the Backbone.

Binding: The association between an IP address, a MAC address, a
port, and other information about the node that owns the IP
Address.

Registered Node: The 6LN for which the registration is performed,
and which owns the fields in the Extended ARO option.

Registering Node: The node that performs the registration; this may
be the Registered Node, or a proxy such as a 6LBR performing a
registration to a 6BBR, on behalf of the Registered Node.

Registered Address: An address owned by the Registered Node that was
or is being registered.

RFC6775-only: Applied to a type of node or a type of message, this
adjective indicates a behavior that is strictly as specified by
[RFC6775] as opposed to updated with this specification.

updated: Qualifies a 6LN, a 6LR, or a 6LBR that supports this
specification.

3. Applicability of Address Registration Options

The purpose of the Address Registration Option (ARO) in [RFC6775] is
to facilitate duplicate address detection (DAD) for hosts as well as
to populate Neighbor Cache Entries (NCEs) [RFC4861] in the routers.
This reduces the reliance on multicast operations, which are often as
intrusive as broadcast, in IPv6 ND operations.

With this specification, a failed or useless registration can be
detected by a 6LR or a 6LBR for reasons other than address
duplication. Examples include: the router having run out of space; a
registration bearing a stale sequence number perhaps denoting a
movement of the host after the registration was placed; a host

   misbehaving and attempting to register an invalid address such as the
   unspecified address [RFC4291]; or a host using an address that is not
   topologically correct on that link.

   In such cases the host will receive an error to help diagnose the
   issue and may retry, possibly with a different address, and possibly
   registering to a different router, depending on the returned error.
   The ability to return errors to address registrations is not intended
   to be used to restrict the ability of hosts to form and use multiple
   addresses. Rather, the intention is to conform to "Host Address
   Availability Recommendations" [RFC7934].

   In particular, the freedom to form and register addresses is needed
   for enhanced privacy; each host may register a number of addresses
   using mechanisms such as "Privacy Extensions for Stateless Address
   Autoconfiguration (SLAAC) in IPv6" [RFC4941].

   In IPv6 ND [RFC4861], a router needs enough storage to hold NCEs for
   all the addresses to which it can currently forward packets. A
   router using the Address Registration mechanism also needs enough
   storage to hold NCEs for all the addresses that may be registered to
   it, regardless of whether or not they are actively communicating.
   The number of registrations supported by a 6LoWPAN Router (6LR) or
   6LoWPAN Border Router (6LBR) MUST be clearly documented by the vendor
   and the dynamic use of associated resources SHOULD be made available
   to the network operator, e.g., to a management console.

   A network administrator MUST deploy updated 6LR/6LBRs to support the
   number and type of devices in their network, based on the number of
   IPv6 addresses that those devices require and their address renewal
   rate and behavior.

4. Updating RFC 6775

   This specification introduces the Extended Address Registration
   Option (EARO) based on the ARO as defined [RFC6775]. A 'T' flag is
   added to indicate that a new field, the Transaction ID (TID) is
   populated. The 'T' flag MUST be set in NS messages when this
   specification is used, and echoed in NA messages to confirm that the
   protocol is supported. The EUI-64 field is overloaded to carry
   different types of information and its size may be increased when
   backward compatibility is not an issue.

   The extensions to the ARO option are used in the Duplicate Address
   messages, the Duplicate Address Request (DAR) and Duplicate Address
   Confirmation (DAC), so as to convey the additional information all
   the way to the 6LBR. In turn the 6LBR may proxy the registration
   using IPv6 ND over a Backbone Link as illustrated in Figure 1. Note

that this specification avoids the Duplicate Address message flow for
Link-Local Addresses in a Route-Over [RFC6606] topology.

```
       6LN                6LR                6LBR               6BBR
        |                  |                  |                  |
        |    NS(EARO)      |                  |                  |
        |--------------->|                  |                  |
        |                  | Extended DAR    |                  |
        |                  |-------------->|                  |
        |                  |                  |                  |
        |                  |                  | proxy NS(EARO)  |
        |                  |                  |--------------->|
        |                  |                  |                  | NS(DAD)
        |                  |                  |                  | ------>
        |                  |                  |                  | <wait>
        |                  |                  |                  |
        |                  |                  | proxy NA(EARO)  |
        |                  |                  |<---------------|
        |                  | Extended DAC    |                  |
        |                  |<--------------|                  |
        |    NA(EARO)      |                  |                  |
        |<---------------|                  |                  |
        |                  |                  |                  |
```
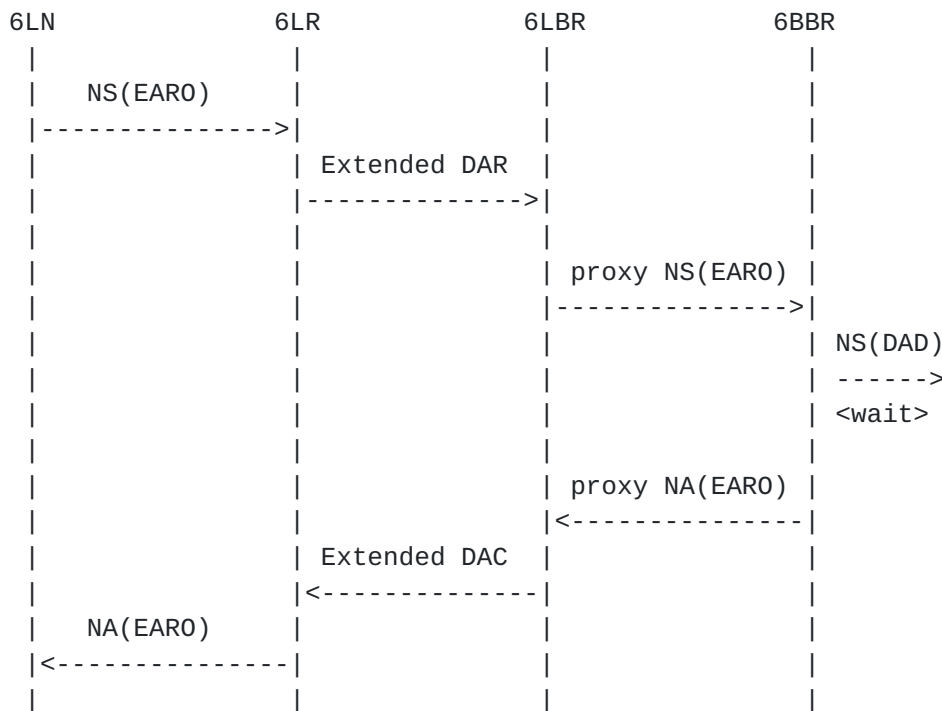
                  Figure 1: (Re-)Registration Flow

In order to support various types of link layers, this specification
allows multiple registrations, including for privacy / temporary
addresses and provides new mechanisms to help clean up stale
registration state as soon as possible, e.g., after a movement (see
Section 8).

Section 5 of [RFC6775] specifies how a 6LN bootstraps an interface
and locates available 6LRs. A Registering Node prefers registering
to a 6LR that is found to support this specification, as discussed in
Section 5, over an RFC6775-only one, and operates in a backward-
compatible fashion when attaching to an RFC6775-only 6LR.

4.1. Extended Address Registration Option (EARO)

The Extended ARO (EARO) replaces the ARO and is backward compatible
with the ARO if and only if the Length of the option is set to 2.
Its format is presented in Section 6.1. More details on backward
compatibility can be found in Section 7.

The semantics of the Neighbor Solicitation (NS) and the ARO are
modified as follows:

   o The address that is being registered with an NS with an EARO is
      now the Target Address, as opposed to the Source Address as
      specified in [RFC6775] (see Section 4.5). This change enables a
      6LBR to use one of its addresses as source of the proxy-
      registration of an address that belongs to a LLN Node to a 6BBR.
      This also limits the use of an address as source address before it
      is registered and the associated DAD process is complete.
   o The EUI-64 field in the ARO Option is renamed Registration
      Ownership Verifier (ROVR) and is not required to be derived from a
      MAC address (see Section 4.3).
   o The option Length MAY be different than 2 and take a value between
      3 and 5, in which case the EARO is not backward compatible with an
      ARO. The increase of size corresponds to a larger ROVR field, so
      the size of the ROVR is inferred from the option Length.
   o This document specifies a new flag in the EARO, the 'R' flag. If
      the 'R' flag is set, the Registering Node expects that the 6LR
      ensures reachability for the Registered Address, e.g., by means of
      routing or proxying ND. Conversely, when it is not set, the 'R'
      flag indicates that the Registering Node is a router, which for
      instance participates to a Route-Over routing protocol such as the
      IPv6 Routing Protocol for Low-Power and Lossy Networks [RFC6550]
      (RPL) and that it will take care of injecting its Address over the
      routing protocol by itself. A 6LN that acts only as a host, when
      registering, MUST set the 'R' flag to indicate that it is not a
      router and that it will not handle its own reachability. A 6LR
      that manages its reachability SHOULD NOT set the 'R' flag; if it
      does, routes towards this router may be installed on its behalf
      and may interfere with those it injects.
   o The specification introduces a Transaction ID (TID) field in the
      EARO (see Section 4.2). The TID MUST be provided by a node that
      supports this specification and another new flag, the 'T' flag,
      MUST be set to indicate so.
   o Finally, this specification introduces new status codes to help
      diagnose the cause of a registration failure (see Table 1).

4.2. Transaction ID

   The TID is a sequence number that is incremented by the 6LN with each
   re-registration to a 6LR. The TID is used to detect the freshness of
   the registration request and to detect one single registration by
   multiple 6LoWPAN border routers (e.g., 6LBRs and 6BBRs) supporting
   the same 6LoWPAN. The TID may also be used by the network to route
   to the current (freshest known) location of a moving node by spotting
   the most recent TID.

   When a Registered Node is registered with multiple 6BBRs in parallel,
   the same TID MUST be used. This enables the 6BBRs to determine that
   the registrations are the same, and distinguish that situation from a

movement (see section 4 of [I-D.ietf-6lo-backbone-router] and
Section 4.7 below).

4.2.1. Comparing TID values

The TID is a sequence counter and its operation is the exact match of
the path sequence specified in RPL, the IPv6 Routing Protocol for
Low-Power and Lossy Networks [RFC6550] specification.

In order to keep this document self-contained and yet compatible, the
text below is an exact copy from section 7.2. "Sequence Counter
Operation" of [RFC6550].

A TID is deemed to be fresher than another when its value is greater
per the operations detailed in this section.

The TID range is subdivided in a 'lollipop' fashion ([Perlman83]),
where the values from 128 and greater are used as a linear sequence
to indicate a restart and bootstrap the counter, and the values less
than or equal to 127 used as a circular sequence number space of size
128 as in [RFC1982]. Consideration is given to the mode of operation
when transitioning from the linear region to the circular region.
Finally, when operating in the circular region, if sequence numbers
are detected to be too far apart then they are not comparable, as
detailed below.

A window of comparison, SEQUENCE_WINDOW = 16, is configured based on
a value of 2^N, where N is defined to be 4 in this specification.

For a given sequence counter,

1. The sequence counter SHOULD be initialized to an implementation
    defined value which is 128 or greater prior to use. A
    recommended value is 240 (256 - SEQUENCE_WINDOW).
2. When a sequence counter increment would cause the sequence
    counter to increment beyond its maximum value, the sequence
    counter MUST wrap back to zero. When incrementing a sequence
    counter greater than or equal to 128, the maximum value is 255.
    When incrementing a sequence counter less than 128, the maximum
    value is 127.
3. When comparing two sequence counters, the following rules MUST be
    applied:

    1. When a first sequence counter A is in the interval [128..255]
        and a second sequence counter B is in [0..127]:

1. If (256 + B - A) is less than or equal to
      SEQUENCE_WINDOW, then B is greater than A, A is less than
      B, and the two are not equal.
2. If (256 + B - A) is greater than SEQUENCE_WINDOW, then A
      is greater than B, B is less than A, and the two are not
      equal.

   For example, if A is 240, and B is 5, then (256 + 5 - 240) is
   21. 21 is greater than SEQUENCE_WINDOW (16), thus 240 is
   greater than 5. As another example, if A is 250 and B is 5,
   then (256 + 5 - 250) is 11. 11 is less than SEQUENCE_WINDOW
   (16), thus 250 is less than 5.

2. In the case where both sequence counters to be compared are
   less than or equal to 127, and in the case where both
   sequence counters to be compared are greater than or equal to
   128:

   1. If the absolute magnitude of difference between the two
         sequence counters is less than or equal to
         SEQUENCE_WINDOW, then a comparison as described in
         [RFC1982] is used to determine the relationships greater
         than, less than, and equal.
   2. If the absolute magnitude of difference of the two
         sequence counters is greater than SEQUENCE_WINDOW, then a
         desynchronization has occurred and the two sequence
         numbers are not comparable.

4. If two sequence numbers are determined to be not comparable,
   i.e., the results of the comparison are not defined, then a node
   should give precedence to the sequence number that was most
   recently incremented. Failing this, the node should select the
   sequence number in order to minimize the resulting changes to its
   own state.

4.3. Registration Ownership Verifier

The ROVR field generalizes the EUI-64 field of the ARO defined in
[RFC6775]. It is scoped to a registration and enables recognizing
and blocking an attempt to register a duplicate address, which is
characterized by a different ROVR in the conflicting registrations.
It can also be used to protect the ownership of a Registered Address,
if the proof-of-ownership of the ROVR can be obtained (more in
Section 4.6).

The ROVR can be of different types, as long as the type is signaled
in the message that carries the new type. For instance, the type can
be a cryptographic string and used to prove the ownership of the
registration as specified in "Address Protected Neighbor Discovery
for Low-power and Lossy Networks" [I-D.ietf-6lo-ap-nd]. In order to

support the flows related to the proof-of-ownership, this
specification introduces new status codes "Validation Requested" and
"Validation Failed" in the EARO.

Note on ROVR collision: different techniques for forming the ROVR
will operate in different name-spaces. [RFC6775] operates on EUI-
64(TM) addresses. [I-D.ietf-6lo-ap-nd] generates cryptographic
tokens. While collisions are not expected in the EUI-64 name-space
only, they may happen in the case of [I-D.ietf-6lo-ap-nd] and in a
mixed situation. An implementation that understands the name-space
MUST consider that ROVRs from different name-spaces are different
even if they have the same value. An RFC6775-only will confuse the
name-spaces, which slightly increases the risk of a ROVR collision.
A collision of ROVR has no effect if the two Registering Nodes
register different addresses, since the ROVR is only significant
within the context of one registration. A ROVR is not expected to be
unique to one registration, as this specification allows a node to
use the same ROVR to register multiple IPv6 addresses. This is why
the ROVR MUST NOT be used as a key to identify the Registering Node,
or as an index to the registration. It is only used as a match to
ensure that the node that updates a registration for an IPv6 address
is the node that made the original registration for that IPv6
address. Also, when the ROVR is not an EUI-64 address, then it MUST
NOT be used as the interface ID of the Registered Address. This way,
a registration that uses that ROVR will not collision with that of an
IPv6 Address derived from EUI-64 and using the EUI-64 as ROVR per
[RFC6775].

The Registering Node SHOULD store the ROVR, or enough information to
regenerate it, in persistent memory. If this is not done and an
event such as a reboot causes a loss of state, re-registering the
same address could be impossible until the 6LRs and the 6LBR time out
the previous registration, or a management action is taken to clear
the relevant state in the network.

4.4. Extended Duplicate Address Messages

In order to map the new EARO content in the Extended Duplicate
Address (EDA) messages, a new TID field is added to the Extended DAR
(EDAR) and the Extended DAC (EDAC) messages as a replacement of the
Reserved field, and a non-null value of the ICMP Code indicates
support for this specification. The format of the EDA messages is
presented in Section 6.2.

As with the EARO, the Extended Duplicate Address messages are
backward compatible with the RFC6775-only versions as long as the
ROVR field is 64 bits long. Remarks concerning backwards

compatibility for the protocol between the 6LN and the 6LR apply
similarly between a 6LR and a 6LBR.

4.5. Registering the Target Address

The Registering Node is the node that performs the registration to
the 6BBR. As in [RFC6775], it may be the Registered Node as well, in
which case it registers one of its own addresses and indicates its
own MAC Address as Source Link Layer Address (SLLA) in the NS(EARO).

This specification adds the capability to proxy the registration
operation on behalf of a Registered Node that is reachable over an
LLN mesh. In that case, if the Registered Node is reachable from the
6BBR over a Mesh-Under mesh, the Registering Node indicates the MAC
Address of the Registered Node as the SLLA in the NS(EARO). If the
Registered Node is reachable over a Route-Over mesh from the
Registering Node, the SLLA in the NS(ARO) is that of the Registering
Node. This enables the Registering Node to attract the packets from
the 6BBR and route them over the LLN to the Registered Node.

In order to enable the latter operation, this specification changes
the behavior of the 6LN and the 6LR so that the Registered Address is
found in the Target Address field of the NS and NA messages as
opposed to the Source Address. With this convention, a TLLA option
indicates the link-layer address of the 6LN that owns the address.

If Registering Node expects packets for the 6LN, e.g., a 6LBR also
acting as RPL Root, then it MUST place its own Link Layer Address in
the SLLA Option that MUST always be placed in a registration NS(EARO)
message. This maintains compatibility with RFC6775-only 6LoWPAN ND
[RFC6775].

4.6. Link-Local Addresses and Registration

Considering that LLN nodes are often not wired and may move, there is
no guarantee that a Link-Local Address stays unique between a
potentially variable and unbounded set of neighboring nodes.

Compared to [RFC6775], this specification only requires that a Link-
Local Address be unique from the perspective of the two nodes that
use it to communicate (e.g., the 6LN and the 6LR in an NS/NA
exchange). This simplifies the DAD process in a Route-Over topology
for Link-Local Addresses by avoiding an exchange of EDA messages
between the 6LR and a 6LBR for those addresses.

In more details:

An exchange between two nodes using Link-Local Addresses implies that
they are reachable over one hop. A node MUST register a Link-Local
Address to a 6LR in order to obtain reachability from that 6LR beyond
the current exchange, and in particular to use the Link-Local Address
as source address to register other addresses, e.g., global
addresses.

If there is no collision with an address previously registered to
this 6LR by another 6LN, then the Link-Local Address is unique from
the standpoint of this 6LR and the registration is not a duplicate.
Alternatively, two different 6LRs might expose the same Link-Local
Address but different link-layer addresses. In that case, a 6LN MUST
only interact with at most one of the 6LRs.

The DAD process between the 6LR and a 6LBR, which is based on an
exchange of EDA messages, does not need to take place for Link-Local
Addresses.

When registering to a 6LR that conforms to this specification (see
Section 7.1, a node MUST use a Link-Local Address as the source
address of the registration, whatever the type of IPv6 address that
is being registered. That Link-Local Address MUST be either an
address that is already registered to the 6LR, or the address that is
being registered.

When a Registering Node does not have an already-registered Address,
it MUST register a Link-Local Address, using it as both the Source
and the Target Address of an NS(EARO) message. In that case, it is
RECOMMENDED to use a Link-Local Address that is (expected to be)
globally unique, e.g., derived from a globally unique EUI-64 address.
A 6LR that supports this specification replies with an NA(EARO),
setting the appropriate status.

Since there is no exchange of EDA messages for Link-Local Addresses,
the 6LR may answer immediately to the registration of a Link-Local
Address, based solely on its existing state and the Source Link-Layer
Option that is placed in the NS(EARO) message as required in
[RFC6775].

A node needs to register its IPv6 Global Unicast Addresses (GUAs) to
a 6LR in order to establish global reachability for these addresses
via that 6LR. When registering with an updated 6LR, a Registering
Node does not use a GUA as Source Address, in contrast to a node that
complies to [RFC6775]. For non-Link-Local Addresses, the exchange of
EDA messages MUST conform to [RFC6775], but the extended formats
described in this specification for the DAR and the DAC are used to
relay the extended information in the case of an EARO.

4.7. Maintaining the Registration States

   This section discusses protocol actions that involve the Registering
   Node, the 6LR, and the 6LBR. It must be noted that the portion that
   deals with a 6LBR only applies to those addresses that are registered
   to it; as discussed in Section 4.6, this is not the case for Link-
   Local Addresses. The registration state includes all data that is
   stored in the router relative to that registration, in particular,
   but not limited to, an NCE. 6LBRs and 6BBRs may store additional
   registration information in more complex abstract data structures and
   use protocols that are out of scope of this document to keep them
   synchronized when they are distributed.

   When its resource available to store registration states are
   exhausted, a 6LR cannot accept a new registration. In that
   situation, the EARO is returned in an NA message with a Status Code
   of "Neighbor Cache Full" (Table 1), and the Registering Node may
   attempt to register to another 6LR.

   If the registry in the 6LBR is saturated, then the 6LBR cannot decide
   whether a registration for a new address is a duplicate. In that
   case, the 6LBR replies to an EDAR message with an EDAC message that
   carries a new Status Code indicating "6LBR Registry saturated"
   (Table 1). Note: this code is used by 6LBRs instead of "Neighbor
   Cache Full" when responding to a Duplicate Address message exchange
   and is passed on to the Registering Node by the 6LR. There is no
   point for the node to retry this registration immediately via another
   6LR, since the problem is global to the network. The node may either
   abandon that address, de-register other addresses first to make room,
   or keep the address in TENTATIVE state and retry later.

   A node renews an existing registration by sending a new NS(EARO)
   message for the Registered Address. In order to refresh the
   registration state in the 6LBR, the registration MUST be reported to
   the 6LBR.

   A node that ceases to use an address SHOULD attempt to de-register
   that address from all the 6LRs to which it has registered the
   address. This is achieved using an NS(EARO) message with a
   Registration Lifetime of 0. If this is not done, a state will remain
   in the network for its Lifetime.

   A node that moves away from a particular 6LR SHOULD attempt to de-
   register all of its addresses registered to that 6LR and register to
   a new 6LR with an incremented TID. When/if the node shows up
   elsewhere, an asynchronous NA(EARO) or EDAC message with a Status
   Code of "Moved" SHOULD be used to clean up the state in the previous
   location. For instance, as described in

[I-D.ietf-6lo-backbone-router], the "Moved" status can be used by a 6BBR in an NA(EARO) message to indicate that the ownership of the proxy state on the Backbone Link was transferred to another 6BBR as the consequence of a movement of the device. If the receiver of the message has a state corresponding to the related address, it SHOULD propagate the status down the forwarding path to the Registered node (e.g., reversing an existing RPL [RFC6550] path as prescribed in [I-D.ietf-roll-efficient-npdao]). Whether it could do so or not, the receiver MUST clean up said state.

Upon receiving an NS(EARO) message with a Registration Lifetime of 0 and determining that this EARO is the freshest for a given NCE (see Section 4.2), a 6LR cleans up its NCE. If the address was registered to the 6LBR, then the 6LR MUST report to the 6LBR, through a Duplicate Address exchange with the 6LBR, indicating the null Registration Lifetime and the latest TID that this 6LR is aware of.

Upon receiving the EDAR message, the 6LBR evaluates if this is the most recent TID it has received for that particular registry entry. If so, then the EDAR is answered with an EDAC message bearing a Status of "Success" and the entry is scheduled to be removed. Otherwise, a Status Code of "Moved" is returned instead, and the existing entry is maintained.

When an address is scheduled to be removed, the 6LBR SHOULD keep its entry in a DELAY state for a configurable period of time, so as to protect a mobile node that de-registered from one 6LR and did not register yet to a new one, or the new registration did not yet reach the 6LBR due to propagation delays in the network. Once the DELAY time is passed, the 6LBR silently removes its entry.

5. Detecting Enhanced ARO Capability Support

"Generic Header Compression for IPv6 over 6LoWPANs" [RFC7400] introduces the 6LoWPAN Capability Indication Option (6CIO) to indicate a node's capabilities to its peers. The 6CIO MUST be present in both Router Solicitation (RS) and Router Advertisement (RA) messages, unless the information therein was already shared. This can have happened in recent exchanges. The information can also be implicit, or pre-configured in all nodes in a network. In any case, a 6CIO MUST be placed in an RA message that is sent in response to an RS with a 6CIO.

Section 6.3 defines a new flag for the 6CIO to signal support for EARO by the issuer of the message and Section 7.1 specifies how the flag is to be used. New flags are also added to the 6CIO to signal the sender's capability to act as a 6LR, 6LBR, and 6BBR (see Section 6.3).

Section 6.3 also defines a new flag that indicates the support of EDA
messages by the 6LBR. This flag is valid in RA messages but not in
RS messages. More information on the 6LBR is found in a separate
Authoritative Border Router Option (ABRO). The ABRO is placed in RA
messages as prescribed by [RFC6775]; in particular, it MUST be placed
in an RA message that is sent in response to an RS with a 6CIO
indicating the capability to act as a 6LR, since the RA propagates
information between routers.

6. Extended ND Options and Messages

This specification does not introduce new options, but it modifies
existing ones and updates the associated behaviors as specified in
the following subsections.

6.1. Extended Address Registration Option (EARO)

The Address Registration Option (ARO) is defined in section 4.1 of
[RFC6775].

The Extended Address Registration Option (EARO) replaces the ARO used
within Neighbor Discovery NS and NA messages between a 6LN and its
6LR. Similarly, the EDA messages, EDAR and EDAC, replace the DAR and
DAC messages so as to transport the new information between 6LRs and
6LBRs across LLN meshes such as 6TiSCH networks.

An NS message with an EARO is a registration if and only if it also
carries an SLLA Option. The EARO is also used in NS and NA messages
between Backbone Routers [I-D.ietf-6lo-backbone-router] over the
Backbone Link to sort out the distributed registration state; in that
case, it does not carry the SLLA Option and is not confused with a
registration.

When using the EARO, the address being registered is found in the
Target Address field of the NS and NA messages.

The EARO extends the ARO and is indicated by the 'T' flag being set.
The format of the EARO is as follows:

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Type      |    Length     |     Status    |   Reserved    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | Reserved  |R|T|     TID       |     Registration Lifetime     |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 ...            Registration Ownership Verifier              ...
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
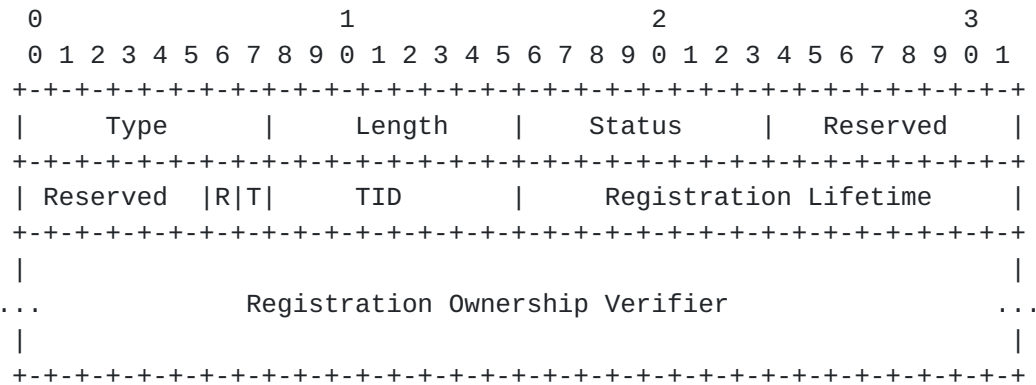
Figure 2: EARO

Option Fields

Type: 33
Length: 8-bit unsigned integer. The length of the option in
                units of 8 bytes. It MUST be 2 when operating in
                backward-compatible mode. It MAY be 3, 4 or 5,
                denoting a ROVR size of 128, 192 and 256 bits
                respectively.
Status: 8-bit unsigned integer. Indicates the status of a
                registration in the NA response. MUST be set to 0 in
                NS messages. See Table 1 below.

```
+-------+------------------------------------------------------------+
| Value | Description                                                |
+-------+------------------------------------------------------------+
|  0..2 | See [RFC6775].  Note: a Status of 1 ("Duplicate Address")  |
|       | applies to the Registered Address. If the Source Address   |
|       | conflicts with an existing registration, "Duplicate        |
|       | Source Address" MUST be used.                              |
|       |                                                            |
|   3   | Moved: The registration failed because it is not the       |
|       | freshest.  This Status indicates that the registration is  |
|       | rejected because another more recent registration was      |
|       | done, as indicated by a same ROVR and a more recent TID.   |
|       | One possible cause is a stale registration that has        |
|       | progressed slowly in the network and was passed by a more  |
|       | recent one.  It could also indicate a ROVR collision.      |
|       |                                                            |
|   4   | Removed: The binding state was removed. This status may    |
|       | be placed in an NA(EARO) message that is sent as the       |
|       | rejection of a proxy registration to a Backbone Router,    |
|       | or in an asynchronous NA(EARO) at any time.                |
|       |                                                            |
|   5   | Validation Requested: The Registering Node is challenged   |
```

```
|       | for owning the Registered Address or for being an     |
|       | acceptable proxy for the registration.  This Status is |
|       | expected in asynchronous messages from a registrar (6LR, |
|       | 6LBR, 6BBR) to indicate that the registration state is |
|       | removed, for instance, due to a movement of the device. |
|       |                                                        |
|   6   | Duplicate Source Address: The address used as source of |
|       | the NS(ARO) conflicts with an existing registration.   |
|       |                                                        |
|   7   | Invalid Source Address: The address used as source of the |
|       | NS(ARO) is not a Link-Local Address as prescribed by this |
|       | document.                                              |
|       |                                                        |
|   8   | Registered Address topologically incorrect: The address |
|       | being registered is not usable on this link, e.g., it is |
|       | not topologically correct                              |
|       |                                                        |
|   9   | 6LBR Registry saturated: A new registration cannot be  |
|       | accepted because the 6LBR Registry is saturated.  Note: |
|       | this code is used by 6LBRs instead of Status 2 when    |
|       | responding to a Duplicate Address message exchange and is |
|       | passed on to the Registering Node by the 6LR.          |
|       |                                                        |
|  10   | Validation Failed: The proof of ownership of the       |
|       | registered address is not correct.                     |
+-------+--------------------------------------------------------+
```

                   Table 1: EARO Status

   Reserved: This field is unused. It MUST be initialized to zero
                   by the sender and MUST be ignored by the receiver.
   R: One-bit flag. If the 'R' flag is set, the
                   Registering Node expects that the 6LR ensures
                   reachability for the registered address, e.g., by
                   injecting the address in a Route-Over routing
                   protocol or proxying ND over a Backbone Link.
   T: One-bit flag. Set if the next octet is used as a
                   TID.
   TID: One-byte integer; a Transaction ID that is maintained
                   by the node and incremented with each transaction.
   Registration Lifetime: 16-bit integer; expressed in minutes. 0
                   means that the registration has ended and the
                   associated state MUST be removed.
   Registration Ownership Verifier (ROVR): Enables the correlation
                   between multiple attempts to register a same IPv6
                   Address. This can be a unique ID of the Registering
                   Node, such as the EUI-64 address of an interface.
                   This can also be a token obtained with cryptographic

                        methods and used as proof of ownership of the
                        registration. The scope of a ROVR is the
                        registration of a particular IPv6 Address and it
                        cannot be used to correlate registrations of
                        different addresses.

6.2. Extended Duplicate Address Message Formats

   The DAR and DAC messages are defined in section 4.4 of [RFC6775].
   Those messages follow a common base format, which enables information
   from the ARO to be transported over multiple hops.

   Those messages are extended to adapt to the new EARO format, as
   follows:

      0   1   2   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
     +-+
     | Type | Code | Checksum |
     +-+
     | Status | TID | Registration Lifetime |
     +-+
     | |
     ...   Registration Ownership Verifier   ...
     | |
     +-+
     | |
     +   +
     | |
     +   Registered Address   +
     | |
     +   +
     | |
     +-+
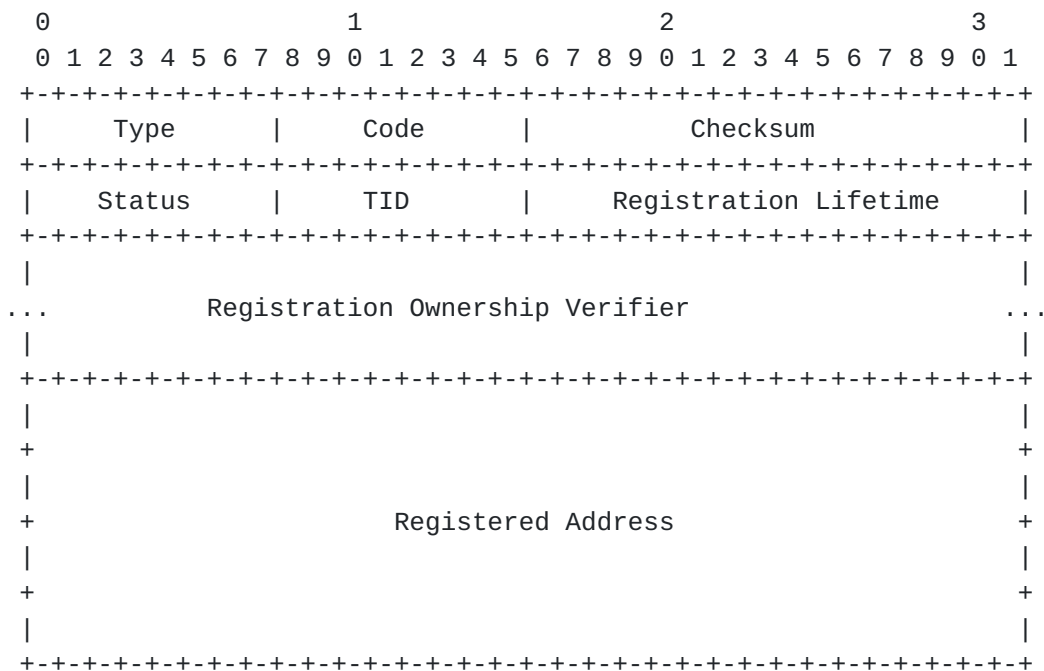
              Figure 3: Duplicate Address Messages Format

   Modified Message Fields

   Code: The ICMP Code as defined in [RFC4443]. The ICMP Code
                 MUST be set to 1 with this specification. An non-
                 null value of the ICMP Code indicates support for
                 this specification.
   TID: 1-byte integer; same definition and processing as the
                 TID in the EARO as defined in Section 6.1.
   Registration Ownership Verifier (ROVR): The size of the ROVR is
                 computed from the overall size of the IPv6 packet.

It MUST be 64bits long when operating in backward-
compatible mode. This field has the same definition
and processing as the ROVR in the EARO option as
defined in Section 6.1.

6.3. New 6LoWPAN Capability Bits in the Capability Indication Option

This specification defines 5 new capability bits for use in the 6CIO,
which was introduced by [RFC7400] for use in IPv6 ND RA messages.

This specification introduces the "E" flag to indicate that extended
ARO can be used in a registration. A 6LR that supports this
specification MUST set the "E" flag.

A similar flag "D" indicates the support of Extended Duplicate
Address Messages by the 6LBR; A 6LBR that supports this specification
MUST set the "D" flag. The "D" flag is learned from advertisements
by a 6LBR, and is propagated down a graph of 6LRs as a node acting as
6LN registers to a 6LR (which could be the 6LBR), and in turn becomes
a 6LR to which other 6LNs will register.

The new "L", "B", and "P" flags, indicate whether a router is capable
of acting as 6LR, 6LBR, and 6BBR, respectively. These flags are not
mutually exclusive and a node MUST set all the flags that are
relevant to it.

As an example, a 6LBR sets the "B" and "D" flags. If it acts as a
6LR, then it sets the "L" and "E" flags. If it is collocated with a
6BBR, then it also sets the "P" flag.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |  Length = 1   |    Reserved     |D|L|B|P|E|G|
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                           Reserved                           |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
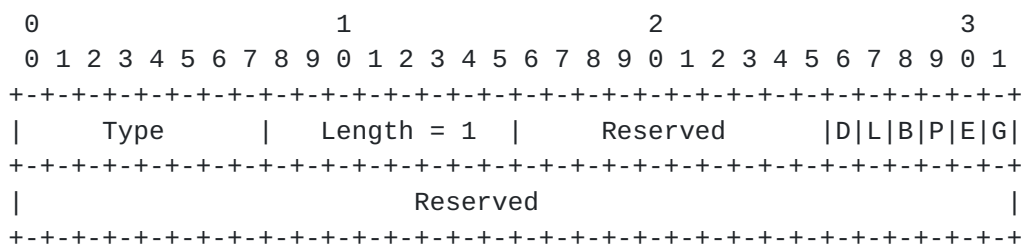
        Figure 4: New capability Bits L, B, P, E in the 6CIO

Option Fields

Type: 36
L: Node is a 6LR.
B: Node is a 6LBR.
P: Node is a 6BBR.
E: Node supports registrations based on EARO.

   D: 6LBR supports EDA messages.

7. Backward Compatibility

7.1. Discovering the Capabilities of Router

   A 6LR that supports this specification MUST place a 6CIO in its RA
   messages. A typical flow when a node starts up is that it sends a
   multicast RS and receives one or more unicast RA messages. If the
   6LR can process Extended ARO, then the "E" Flag is set in the RA.

   This specification changes the behavior of the peers in a
   registration flow. To enable backward compatibility, a 6LN that
   registers to a 6LR that is not known to support this specification
   MUST behave in a manner that is backward-compatible with [RFC6775].
   On the contrary, if the 6LR is known to support this specification,
   then the 6LN MUST conform to this specification when communicating
   with that 6LR.

   A 6LN that supports this specification MUST always use an EARO as a
   replacement for an ARO in its registration to a router. This is
   harmless since the 'T' flag and TID field are reserved in [RFC6775],
   and are ignored by an RFC6775-only router. A router that supports
   this specification MUST answer an NS(ARO) and an NS(EARO) with an
   NA(EARO). A router that does not support this specification will
   consider the ROVR as an EUI-64 address and treat it the same, which
   has no consequence if the Registered Addresses are different.

7.2. RFC6775-only 6LoWPAN Node

   An RFC6775-only 6LN will use the Registered Address as the source
   address of the NS message and will not use an EARO. An updated 6LR
   MUST accept that registration if it is valid per [RFC6775], and it
   MUST manage the binding cache accordingly. The updated 6LR MUST then
   use the RFC6775-only EDA messages as specified in [RFC6775] to
   indicate to the 6LBR that the TID is not present in the messages.

   The main difference from [RFC6775] is that the exchange of EDA
   messages for the purpose of DAD is avoided for Link-Local Addresses.
   In any case, the 6LR MUST use an EARO in the reply, and can use any
   of the Status codes defined in this specification.

7.3. RFC6775-only 6LoWPAN Router

   An updated 6LN discovers the capabilities of the 6LR in the 6CIO in
   RA messages from that 6LR; if the 6CIO was not present in the RA,
   then the 6LR is assumed to be a RFC6775-only 6LoWPAN Router.

An updated 6LN MUST use an EARO in the request regardless of the type of 6LR, RFC6775-only or updated, which implies that the 'T' flag is set. It MUST use a ROVR of 64 bits if the 6LR is an RFC6775-only 6LoWPAN Router.

If an updated 6LN moves from an updated 6LR to an RFC6775-only 6LR, the RFC6775-only 6LR will send an RFC6775-only DAR message, which cannot be compared with an updated one for freshness. Allowing RFC6775-only DAR messages to replace a state established by the updated protocol in the 6LBR would be an attack vector and that cannot be the default behavior. But if RFC6775-only and updated 6LRs coexist temporarily in a network, then it makes sense for an administrator to install a policy that allows so, and the capability to install such a policy should be configurable in a 6LBR though it is out of scope for this document.

7.4. RFC6775-only 6LoWPAN Border Router

With this specification, the Duplicate Address messages are extended to transport the EARO information. Similarly to the NS/NA exchange, an updated 6LBR MUST always use the EDA messages.

Note that an RFC6775-only 6LBR will accept and process an EDAR message as if it were an RFC6775-only DAR, as long as the ROVR is 64 bits long. An updated 6LR discovers the capabilities of the 6LBR in the 6CIO in RA messages from the 6LR; if the 6CIO was not present in any RA, then the 6LBR si assumed to be a RFC6775-only 6LoWPAN Border Router.

If the 6LBR is RFC6775-only, and the ROVR in the NS(EARO) was more than 64 bits long, then the 6LR MUST truncate the ROVR to the 64 rightmost bit and place the result in the EDAR message to maintain compatibility. This way, the support of DAD is preserved.

8. Security Considerations

This specification extends [RFC6775], and the security section of that document also applies to this as well. In particular, it is expected that the link layer is sufficiently protected to prevent rogue access, either by means of physical or IP security on the Backbone Link and link-layer cryptography on the LLN.

[RFC6775] does not protect the content of its messages and expects a lower layer encryption to defeat potential attacks. This specification also expects that the LLN MAC provides secure unicast to/from the Backbone Router and secure Broadcast or Multicast from the Backbone Router in a way that prevents tampering with or replaying the Neighbor Discovery messages.

This specification recommends using privacy techniques (see
Section 9) and protecting against address theft such as provided by
"Address Protected Neighbor Discovery for Low-power and Lossy
Networks" [I-D.ietf-6lo-ap-nd], which guarantees the ownership of the
Registered Address using a cryptographic ROVR.

The registration mechanism may be used by a rogue node to attack the
6LR or the 6LBR with a Denial-of-Service attack against the registry.
It may also happen that the registry of a 6LR or a 6LBR is saturated
and cannot take any more registrations, which effectively denies the
requesting node the capability to use a new address. In order to
alleviate those concerns, Section 4.7 provides a number of
recommendations that ensure that a stale registration is removed as
soon as possible from the 6LR and 6LBR. In particular, this
specification recommends that:

o A node that ceases to use an address SHOULD attempt to de-register
   that address from all the 6LRs to which it is registered. See
   Section 4.2 for the mechanism to avoid replay attacks and avoiding
   the use of stale registration information.
o The Registration lifetimes SHOULD be individually configurable for
   each address or group of addresses. The nodes SHOULD be
   configured with a Registration Lifetime that reflects their
   expectation of how long they will use the address with the 6LR to
   which it is registered. In particular, use cases that involve
   mobility or rapid address changes SHOULD use lifetimes that are
   larger yet of a same order as the duration of the expectation of
   presence.
o The router (6LR or 6LBR) SHOULD be configurable so as to limit the
   number of addresses that can be registered by a single node, but
   as a protective measure only. A node may be identified by MAC
   address, but a stronger identification (e.g., by security
   credentials) is RECOMMENDED. When that maximum is reached, the
   router should use a Least-Recently-Used (LRU) algorithm to clean
   up the addresses, keeping at least one Link-Local Address. The
   router SHOULD attempt to keep one or more stable addresses if
   stability can be determined, e.g., because they are used over a
   much longer time span than other (privacy, shorter-lived)
   addresses. Address lifetimes SHOULD be individually configurable.
o In order to avoid denial of registration for the lack of
   resources, administrators should take great care to deploy
   adequate numbers of 6LRs to cover the needs of the nodes in their
   range, so as to avoid a situation of starving nodes. It is
   expected that the 6LBR that serves an LLN is a more capable node
   than the average 6LR, but in a network condition where it may
   become saturated, a particular deployment should distribute the
   6LBR functionality, for instance by leveraging a high speed

      Backbone Link and Backbone Routers to aggregate multiple LLNs into
      a larger subnet.

   The LLN nodes depend on the 6LBR and the 6BBR 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 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 (see Req5.1 in Appendix B.5).

9. Privacy Considerations

   As indicated in Section 3, this protocol does not inherently limit
   the number of IPv6 addresses that each device can form. However, to
   mitigate denial-of-service attacks, it can be useful as a protective
   measure to have a limit that is high enough not to interfere with the
   normal behavior of devices in the network. A host should be able to
   form and register any address that is topologically correct in the
   subnet(s) advertised by the 6LR/6LBR.

   This specification does not mandate any particular way for forming
   IPv6 addresses, but it discourages using EUI-64 for forming the
   Interface ID in the Link-Local Address because this method prevents
   the usage of "SEcure Neighbor Discovery (SEND)" [RFC3971],
   "Cryptographically Generated Addresses (CGA)" [RFC3972], and that of
   address privacy techniques.

   "Privacy Considerations for IPv6 Adaptation-Layer Mechanisms"
   [RFC8065] explains why privacy is important and how to form privacy-
   aware addresses. All implementations and deployments must consider
   the option of privacy addresses in their own environments.

   The IPv6 address of the 6LN in the IPv6 header can be compressed
   statelessly when the Interface Identifier in the IPv6 address can be
   derived from the Lower Layer address. When it is not critical to
   benefit from that compression, e.g., the address can be compressed
   statefully, or it is rarely used and/or it is used only over one hop,
   then privacy concerns should be considered. In particular, new
   implementations should follow the IETF "Recommendation on Stable IPv6
   Interface Identifiers" [RFC8064]. [RFC8064] recommends the use of "A
   Method for Generating Semantically Opaque Interface Identifiers with
   IPv6 Stateless Address Autoconfiguration (SLAAC)" [RFC7217] for
   generating Interface Identifiers to be used in SLAAC.

10. IANA Considerations

   Note to RFC Editor, to be removed: please replace "This RFC"
   throughout this document by the RFC number for this specification
   once it is allocated.

   IANA is requested to make a number of changes under the "Internet
   Control Message Protocol version 6 (ICMPv6) Parameters" registry, as
   follows.

10.1. ARO Flags

   IANA is requested to create a new subregistry for "ARO Flags". This
   specification defines 8 positions, bit 0 to bit 7, and assigns bit 6
   for the 'R' flag and bit 7 for the 'T' flag (see Section 6.1). The
   policy is "IETF Review" or "IESG Approval" [RFC8126]. The initial
   content of the registry is as shown in Table 2.

   New subregistry for ARO Flags under the "Internet Control Message
          Protocol version 6 (ICMPv6) [RFC4443] Parameters"

```
          +-------------+--------------+-----------+
          |  ARO Status | Description  | Document  |
          +-------------+--------------+-----------+
          |     0..5    | Unassigned   |           |
          |             |              |           |
          |      6      | 'R' Flag     | This RFC  |
          |             |              |           |
          |      7      | 'T' Flag     | This RFC  |
          +-------------+--------------+-----------+
```

                     Table 2: new ARO Flags

10.2. ICMP Codes

   IANA is requested to create 2 new subregistries of the ICMPv6 "Code"
   Fields registry, which itself is a subregistry of the Internet
   Control Message Protocol version 6 (ICMPv6) Parameters for the ICMP
   codes. The new subregistries relate to the ICMP type 157, Duplicate
   Address Request (shown in Table 3), and 158, Duplicate Address
   Confirmation (shown in Table 4), respectively. The range of an
   ICMPv6 "Code" Field is 0..255 in all cases. The policy is "IETF
   Review" or "IESG Approval" [RFC8126] for both subregistries. The new
   subregistries are initialized as follows:

New entries for ICMP types 157 DAR message

```
+---------+----------------------+------------+
| Code    | Name                 | Reference  |
+---------+----------------------+------------+
| 0       | Original DAR message | RFC 6775   |
|         |                      |            |
| 1       | Extended DAR message | This RFC   |
|         |                      |            |
| 2...255 | Unassigned           |            |
+---------+----------------------+------------+
```

Table 3: new ICMPv6 Code Fields

New entries for ICMP types 158 DAC message

```
+---------+----------------------+------------+
| Code    | Name                 | Reference  |
+---------+----------------------+------------+
| 0       | Original DAC message | RFC 6775   |
|         |                      |            |
| 1       | Extended DAC message | This RFC   |
|         |                      |            |
| 2...255 | Unassigned           |            |
+---------+----------------------+------------+
```

Table 4: new ICMPv6 Code Fields

10.3. New ARO Status values

   IANA is requested to make additions to the Address Registration
   Option Status Values Registry as follows:

Address Registration Option Status Values Registry

```
+-------------+------------------------------------------+-----------+
| ARO Status  | Description                              | Document  |
+-------------+------------------------------------------+-----------+
|      3      | Moved                                    | This RFC  |
|             |                                          |           |
|      4      | Removed                                  | This RFC  |
|             |                                          |           |
|      5      | Validation Requested                     | This RFC  |
|             |                                          |           |
|      6      | Duplicate Source Address                 | This RFC  |
|             |                                          |           |
|      7      | Invalid Source Address                   | This RFC  |
|             |                                          |           |
|      8      | Registered Address topologically         | This RFC  |
|             | incorrect                                |           |
|             |                                          |           |
|      9      | 6LBR Registry saturated                  | This RFC  |
|             |                                          |           |
|     10      | Validation Failed                        | This RFC  |
+-------------+------------------------------------------+-----------+
```

Table 5: New ARO Status values

10.4. New 6LoWPAN capability Bits

IANA is requested to make additions to the Subregistry for "6LoWPAN
capability Bits" as follows:

Subregistry for "6LoWPAN capability Bits" under the "Internet Control
        Message Protocol version 6 (ICMPv6) Parameters"

```
+-----------------+----------------------+-----------+
| Capability Bit  | Description          | Document  |
+-----------------+----------------------+-----------+
|       10        | EDA  Support (D bit) | This RFC  |
|                 |                      |           |
|       11        | 6LR  capable (L bit) | This RFC  |
|                 |                      |           |
|       12        | 6LBR capable (B bit) | This RFC  |
|                 |                      |           |
|       13        | 6BBR capable (P bit) | This RFC  |
|                 |                      |           |
|       14        | EARO support (E bit) | This RFC  |
+-----------------+----------------------+-----------+
```

Table 6: New 6LoWPAN capability Bits

11. Acknowledgments

   Kudos to Eric Levy-Abegnoli who designed the First Hop Security
   infrastructure upon which the first backbone router was implemented.
   Many thanks to Sedat Gormus, Rahul Jadhav, Tim Chown, Juergen
   Schoenwaelder, Chris Lonvick, Dave Thaler, Adrian Farrel, Peter Yee,
   and Lorenzo Colitti for their various contributions and reviews.
   Also, many thanks to Thomas Watteyne for the world first
   implementation of a 6LN that was instrumental to the early tests of
   the 6LR, 6LBR and Backbone Router.

12. References

12.1. Normative References

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

   [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing
              Architecture", RFC 4291, DOI 10.17487/RFC4291, February
              2006, <https://www.rfc-editor.org/info/rfc4291>.

   [RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet
              Control Message Protocol (ICMPv6) for the Internet
              Protocol Version 6 (IPv6) Specification", STD 89,
              RFC 4443, DOI 10.17487/RFC4443, March 2006,
              <https://www.rfc-editor.org/info/rfc4443>.

   [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>.

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

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

[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>.

[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>.

[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>.

12.2. Informative References

[I-D.chakrabarti-nordmark-6man-efficient-nd]
           Chakrabarti, S., Nordmark, E., Thubert, P., and M.
           Wasserman, "IPv6 Neighbor Discovery Optimizations for
           Wired and Wireless Networks", draft-chakrabarti-nordmark-
           6man-efficient-nd-07 (work in progress), February 2015.

[I-D.delcarpio-6lo-wlanah]
          Vega, L., Robles, I., and R. Morabito, "IPv6 over
          802.11ah", draft-delcarpio-6lo-wlanah-01 (work in
          progress), October 2015.

[I-D.hou-6lo-plc]
          Hou, J., Hong, Y., and X. Tang, "Transmission of IPv6
          Packets over PLC Networks", draft-hou-6lo-plc-03 (work in
          progress), December 2017.

[I-D.ietf-6lo-ap-nd]
          Thubert, P., Sarikaya, B., and M. Sethi, "Address
          Protected Neighbor Discovery for Low-power and Lossy
          Networks", draft-ietf-6lo-ap-nd-06 (work in progress),
          February 2018.

[I-D.ietf-6lo-backbone-router]
          Thubert, P., "IPv6 Backbone Router", draft-ietf-6lo-
          backbone-router-06 (work in progress), February 2018.

[I-D.ietf-6lo-nfc]
          Choi, Y., Hong, Y., Youn, J., Kim, D., and J. Choi,
          "Transmission of IPv6 Packets over Near Field
          Communication", draft-ietf-6lo-nfc-09 (work in progress),
          January 2018.

[I-D.ietf-6tisch-architecture]
          Thubert, P., "An Architecture for IPv6 over the TSCH mode
          of IEEE 802.15.4", draft-ietf-6tisch-architecture-13 (work
          in progress), November 2017.

[I-D.ietf-mboned-ieee802-mcast-problems]
          Perkins, C., McBride, M., Stanley, D., Kumari, W., and J.
          Zuniga, "Multicast Considerations over IEEE 802 Wireless
          Media", draft-ietf-mboned-ieee802-mcast-problems-01 (work
          in progress), February 2018.

[I-D.ietf-roll-efficient-npdao]
          Jadhav, R., Sahoo, R., and Z. Cao, "No-Path DAO
          modifications", draft-ietf-roll-efficient-npdao-01 (work
          in progress), October 2017.

[I-D.perkins-intarea-multicast-ieee802]
          Perkins, C., Stanley, D., Kumari, W., and J. Zuniga,
          "Multicast Considerations over IEEE 802 Wireless Media",
          draft-perkins-intarea-multicast-ieee802-03 (work in
          progress), July 2017.

   [I-D.struik-lwip-curve-representations]
              Struik, R., "Alternative Elliptic Curve Representations",
              draft-struik-lwip-curve-representations-00 (work in
              progress), October 2017.

   [RFC1958] Carpenter, B., Ed., "Architectural Principles of the
              Internet", RFC 1958, DOI 10.17487/RFC1958, June 1996,
              <https://www.rfc-editor.org/info/rfc1958>.

   [RFC1982] Elz, R. and R. Bush, "Serial Number Arithmetic", RFC 1982,
              DOI 10.17487/RFC1982, August 1996,
              <https://www.rfc-editor.org/info/rfc1982>.

   [RFC3610] Whiting, D., Housley, R., and N. Ferguson, "Counter with
              CBC-MAC (CCM)", RFC 3610, DOI 10.17487/RFC3610, September
              2003, <https://www.rfc-editor.org/info/rfc3610>.

   [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>.

   [RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander,
              "SEcure Neighbor Discovery (SEND)", RFC 3971,
              DOI 10.17487/RFC3971, March 2005,
              <https://www.rfc-editor.org/info/rfc3971>.

   [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)",
              RFC 3972, DOI 10.17487/RFC3972, March 2005,
              <https://www.rfc-editor.org/info/rfc3972>.

   [RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD)
              for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006,
              <https://www.rfc-editor.org/info/rfc4429>.

   [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy
              Extensions for Stateless Address Autoconfiguration in
              IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007,
              <https://www.rfc-editor.org/info/rfc4941>.

   [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>.

   [RFC7217] Gont, F., "A Method for Generating Semantically Opaque
              Interface Identifiers with IPv6 Stateless Address
              Autoconfiguration (SLAAC)", RFC 7217,
              DOI 10.17487/RFC7217, April 2014,
              <https://www.rfc-editor.org/info/rfc7217>.

   [RFC7428] Brandt, A. and J. Buron, "Transmission of IPv6 Packets
              over ITU-T G.9959 Networks", RFC 7428,
              DOI 10.17487/RFC7428, February 2015,
              <https://www.rfc-editor.org/info/rfc7428>.

   [RFC7668] Nieminen, J., Savolainen, T., Isomaki, M., Patil, B.,
              Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low
              Energy", RFC 7668, DOI 10.17487/RFC7668, October 2015,
              <https://www.rfc-editor.org/info/rfc7668>.

   [RFC7934] Colitti, L., Cerf, V., Cheshire, S., and D. Schinazi,
              "Host Address Availability Recommendations", BCP 204,
              RFC 7934, DOI 10.17487/RFC7934, July 2016,
              <https://www.rfc-editor.org/info/rfc7934>.

   [RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu,
              "Recommendation on Stable IPv6 Interface Identifiers",
              RFC 8064, DOI 10.17487/RFC8064, February 2017,
              <https://www.rfc-editor.org/info/rfc8064>.

   [RFC8065] Thaler, D., "Privacy Considerations for IPv6 Adaptation-
              Layer Mechanisms", RFC 8065, DOI 10.17487/RFC8065,
              February 2017, <https://www.rfc-editor.org/info/rfc8065>.

   [RFC8105] Mariager, P., Petersen, J., Ed., Shelby, Z., Van de Logt,
              M., and D. Barthel, "Transmission of IPv6 Packets over
              Digital Enhanced Cordless Telecommunications (DECT) Ultra
              Low Energy (ULE)", RFC 8105, DOI 10.17487/RFC8105, May
              2017, <https://www.rfc-editor.org/info/rfc8105>.

   [RFC8163] Lynn, K., Ed., Martocci, J., Neilson, C., and S.
              Donaldson, "Transmission of IPv6 over Master-Slave/Token-
              Passing (MS/TP) Networks", RFC 8163, DOI 10.17487/RFC8163,
              May 2017, <https://www.rfc-editor.org/info/rfc8163>.

   [RFC8279] Wijnands, IJ., Ed., Rosen, E., Ed., Dolganow, A.,
              Przygienda, T., and S. Aldrin, "Multicast Using Bit Index
              Explicit Replication (BIER)", RFC 8279,
              DOI 10.17487/RFC8279, November 2017,
              <https://www.rfc-editor.org/info/rfc8279>.

12.3. External Informative References

[IEEEstd802154]
          IEEE, "IEEE Standard for Low-Rate Wireless Networks",
          IEEE Standard 802.15.4, DOI 10.1109/IEEE
          P802.15.4-REVd/D01, June 2017,
          <http://ieeexplore.ieee.org/document/7460875/>.

[Perlman83]
          Perlman, R., "Fault-Tolerant Broadcast of Routing
          Information", North-Holland Computer Networks 7: 395-405,
          1983, <http://www.cs.illinois.edu/~pbg/courses/cs598fa09/
          readings/p83.pdf>.

Appendix A. Applicability and Requirements Served (Not Normative)

This specification extends 6LoWPAN ND to provide a sequence number to
the registration and serves the requirements expressed in
Appendix B.1 by enabling the mobility of devices from one LLN to the
next based on the complementary work in the "IPv6 Backbone Router"
[I-D.ietf-6lo-backbone-router] specification.

IEEE Std. 802.15.4 [IEEEstd802154], the "6TiSCH architecture"
[I-D.ietf-6tisch-architecture] introduces how a 6LoWPAN ND host could
connect to the Internet via a RPL mesh network, but this requires
additions to the 6LoWPAN ND protocol to support mobility and
reachability in a secured and manageable environment. This
specification details the new operations that are required to
implement the 6TiSCH architecture and serves the requirements listed
in Appendix B.2.

The term LLN is used loosely in this specification to cover multiple
types of WLANs and WPANs, including Low-Power IEEE Std. 802.11
networking, Bluetooth Low Energy, IEEE Std. 802.11ah, and IEEE Std.
802.15.4 wireless meshes, so as to address the requirements discussed
in Appendix B.3.

This specification can be used by any wireless node to associate at
Layer-3 with a 6BBR and register its IPv6 addresses to obtain routing
services including proxy-ND operations over a Backbone Link,
effectively providing a solution to the requirements expressed in
Appendix B.4.

This specification is extended by "Address Protected Neighbor
Discovery for Low-power and Lossy Networks" [I-D.ietf-6lo-ap-nd] to
providing a solution to some of the security-related requirements
expressed in Appendix B.5.

"Efficiency aware IPv6 Neighbor Discovery Optimizations"
[I-D.chakrabarti-nordmark-6man-efficient-nd] suggests that 6LoWPAN ND
[RFC6775] can be extended to other types of links beyond IEEE Std.
802.15.4 for which it was defined. The registration technique is
beneficial when the Link-Layer technique used to carry IPv6 multicast
packets is not sufficiently efficient in terms of delivery ratio or
energy consumption in the end devices, in particular to enable
energy-constrained sleeping nodes. The value of such extension is
especially apparent in the case of mobile wireless nodes, to reduce
the multicast operations that are related to IPv6 ND ([RFC4861],
[RFC4862]) and affect the operation of the wireless medium
[I-D.ietf-mboned-ieee802-mcast-problems]
[I-D.perkins-intarea-multicast-ieee802]. This serves the scalability
requirements listed in Appendix B.6.

Appendix B. Requirements (Not Normative)

This section lists requirements that were discussed discussed by the
6lo WG for an update to 6LoWPAN ND. How those requirements are
matched with existing specifications at the time of this writing is
shown in Appendix B.8.

B.1. Requirements Related to Mobility

Due to the unstable nature of LLN links, even in an LLN of immobile
nodes a 6LN may change its point of attachment from 6LR-a to 6LR-b,
and may not be able to notify 6LR-a. Consequently, 6LR-a may still
attract traffic that it cannot deliver any more. When links to a 6LR
change state, there is thus a need to identify stale states in a 6LR
and restore reachability in a timely fashion, e.g., by using some
signaling upon the detection of the movement, or using a keep-alive
mechanism with a period that is consistent with the application
needs.

Req1.1: Upon a change of point of attachment, connectivity via a new
6LR MUST be restored in a timely fashion without the need to de-
register from the previous 6LR.

Req1.2: For that purpose, the protocol MUST enable differentiating
between multiple registrations from one 6LoWPAN Node and
registrations from different 6LoWPAN Nodes claiming the same address.

Req1.3: Stale states MUST be cleaned up in 6LRs.

Req1.4: A 6LoWPAN Node SHOULD also be able to register its Address
concurrently to multiple 6LRs.

B.2. Requirements Related to Routing Protocols

   The point of attachment of a 6LN may be a 6LR in an LLN mesh. IPv6
   routing in an LLN can be based on RPL, which is the routing protocol
   that was defined by the IETF for this particular purpose. Other
   routing protocols are also considered by Standards Development
   Organizations (SDO) on the basis of the expected network
   characteristics. It is required that a 6LN attached via ND to a 6LR
   indicates whether it participates in the selected routing protocol to
   obtain reachability via the 6LR, or whether it expects the 6LR to
   manage its reachability.

   Beyond the 6LBR unicast address registered by ND, other addresses
   including multicast addresses are needed as well. For example, a
   routing protocol often uses a multicast address to register changes
   to established paths. ND needs to register such a multicast address
   to enable routing concurrently with discovery.

   Multicast is needed for groups. Groups may be formed by device type
   (e.g., routers, street lamps), location (Geography, RPL sub-tree), or
   both.

   The Bit Index Explicit Replication (BIER) Architecture [RFC8279]
   proposes an optimized technique to enable multicast in an LLN with a
   very limited requirement for routing state in the nodes.

   Related requirements are:

   Req2.1: The ND registration method SHOULD be extended so that the 6LR
   is instructed whether to advertise the Address of a 6LN over the
   selected routing protocol and obtain reachability to that Address
   using the selected routing protocol.

   Req2.2: Considering RPL, 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 section 6.4 of [RFC6550],
   in particular the capability to compute a Path Sequence and, as an
   option, a RPLInstanceID.

   Req2.3: Multicast operations SHOULD be supported and optimized, for
   instance, using BIER or MPL. Whether ND is appropriate for the
   registration to the 6BBR is to be defined, considering the additional
   burden of supporting the Multicast Listener Discovery Version 2
   [RFC3810] (MLDv2) for IPv6.

B.3. Requirements Related to the Variety of Low-Power Link types

   6LoWPAN ND [RFC6775] was defined with a focus on IEEE Std.802.15.4
   and in particular the capability to derive a unique identifier from a
   globally unique EUI-64 address. At this point, the 6lo Working Group
   is extending the 6LoWPAN Header Compression (HC) [RFC6282] technique
   to other link types including ITU-T G.9959 [RFC7428], Master-Slave/
   Token-Passing [RFC8163], DECT Ultra Low Energy [RFC8105], Near Field
   Communication [I-D.ietf-6lo-nfc], IEEE Std. 802.11ah
   [I-D.delcarpio-6lo-wlanah], as well as Bluetooth(R) Low Energy
   [RFC7668], and Power Line Communication (PLC) [I-D.hou-6lo-plc]
   Networks.

   Related requirements are:

   Req3.1: The support of the registration mechanism SHOULD be extended
   to more LLN links than IEEE Std.802.15.4, matching at least the LLN
   links for which an "IPv6 over foo" specification exists, as well 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 SHOULD be unique at least within the LLN connected
   to a 6LBR discovered by ND in each node within the LLN.

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

   Req3.4: The Neighbor Discovery should specify the formation of a
   site-local address that follows the security recommendations from
   [RFC7217].

B.4. Requirements Related to Proxy Operations

   Duty-cycled devices may not be able to answer themselves to a lookup
   from a node that uses IPv6 ND on a Backbone Link and may need a
   proxy. Additionally, the duty-cycled device may need to rely on the
   6LBR to perform registration to the 6BBR.

   The ND registration method SHOULD defend the addresses of duty-cycled
   devices that are sleeping most of the time and not capable to defend
   their own addresses.

   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.

Req4.2: The registration mechanism SHOULD be applicable to a duty-cycled device regardless of the link type and SHOULD enable a 6BBR to operate as a proxy to defend the Registered Addresses on its behalf.

Req4.3: The registration mechanism SHOULD enable long sleep durations, on the order of multiple days to a month.

B.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 for the 6LBR to protect that ownership even when the node that registered the address is sleeping.

In particular, the 6LR and the 6LBR then should be able to verify whether a subsequent registration for a given address comes from the original node.

In an LLN it makes sense to base security on Layer-2 security. During bootstrap of the LLN, nodes join the network after authorization by a Joining Assistant (JA) or a Commissioning Tool (CT). After joining, nodes communicate with each other via secured links. The keys for the Layer-2 security are distributed by the JA/CT. The JA/CT can be part of the LLN or be outside the LLN. In both cases it is needed that packets are routed between JA/CT and the joining node.

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 new registration of authorized nodes. Joining of unauthorized nodes MUST be prevented.

Req5.3: 6LoWPAN ND security mechanisms SHOULD NOT lead to large 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 IEEE Std.802.15.4 [IEEEstd802154] 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 the variation of CCM [RFC3610] called 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. Algorithm agility and support for large keys (e.g., 256-bit key sizes) is also desirable, following at Layer-3 the introduction of those capabilities at Layer-2.

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.

Req5.8: Routing of packets should continue when links pass from the unsecured to the secured state.

Req5.9: 6LoWPAN ND security mechanisms SHOULD provide a mechanism for the 6LR and the 6LBR to validate whether a new registration for a given address corresponds to the same 6LN that registered it initially, and, if not, determine the rightful owner and deny or clean up the registration that is duplicate.

B.6. Requirements Related to Scalability

Use cases from Automatic Meter Reading (AMR, collection tree operations) and Advanced Metering Infrastructure (AMI, bi-directional communication to the meters) indicate the needs for a large number of LLN nodes pertaining to a single RPL DODAG (e.g., 5000) and connected to the 6LBR over a large number of LLN hops (e.g., 15).

Related requirements are:

Req6.1: The registration mechanism SHOULD enable a single 6LBR to register multiple thousands of devices.

Req6.2: The timing of the registration operation should allow for a large latency such as found in LLNs with ten to more hops.

B.7. Requirements Related to Operations and Management

Section 3.8 of "Architectural Principles of the Internet" [RFC1958] recommends to: "avoid options and parameters whenever possible. Any options and parameters should be configured or negotiated dynamically rather than manually". This is especially true in LLNs where the number of devices may be large and manual configuration is

infeasible. Capabilities for a dynamic configuration of LLN devices
can also be constrained by the network and power limitation.

A Network Administrator should be able to validate that the network
is operating within capacity, and that in particular a 6LBR does not
get overloaded with an excessive amount of registration, so the
administrator can take actions such as adding a Backbone Link with
additional 6LBRs and 6BBRs to the network.

Related requirements are:

Req7.1: A management model SHOULD be provided that enables access to
the 6LBR, monitor its usage vs. capacity, and alert in case of
congestion. It is recommended that the 6LBR be reachable over a non-
LLN link.

Req7.2: A management model SHOULD be provided that enables access to
the 6LR and its capacity to host additional NCE. This management
model SHOULD avoid polling individual 6LRs in a way that could
disrupt the operation of the LLN.

Req7.3: Information on successful and failed registration SHOULD be
provided, including information such as the ROVR of the 6LN, the
Registered Address, the address of the 6LR, and the duration of the
registration flow.

Req7.4: In case of a failed registration, information on the failure
including the identification of the node that rejected the
registration and the status in the EARO SHOULD be provided.

B.8. Matching Requirements with Specifications

I-drafts/RFCs addressing requirements

Requirement	Document
Req1.1	[I-D.ietf-6lo-backbone-router]
Req1.2	[RFC6775]
Req1.3	[RFC6775]
Req1.4	This RFC
Req2.1	This RFC
Req2.2	This RFC

```
|            |                                         |
| Req2.3     |                                         |
|            |                                         |
| Req3.1     | Technology Dependent                    |
|            |                                         |
| Req3.2     | Technology Dependent                    |
|            |                                         |
| Req3.3     | Technology Dependent                    |
|            |                                         |
| Req3.4     | Technology Dependent                    |
|            |                                         |
| Req4.1     | This RFC                                 |
|            |                                         |
| Req4.2     | This RFC                                 |
|            |                                         |
| Req4.3     | [RFC6775]                                |
|            |                                         |
| Req5.1     |                                         |
|            |                                         |
| Req5.2     | [I-D.ietf-6lo-ap-nd]                    |
|            |                                         |
| Req5.3     |                                         |
|            |                                         |
| Req5.4     |                                         |
|            |                                         |
| Req5.5     | [I-D.ietf-6lo-ap-nd]                    |
|            |                                         |
| Req5.6     | [I-D.struik-lwip-curve-representations] |
|            |                                         |
| Req5.7     | [I-D.ietf-6lo-ap-nd]                    |
|            |                                         |
| Req5.8     |                                         |
|            |                                         |
| Req5.9     | [I-D.ietf-6lo-ap-nd]                    |
|            |                                         |
| Req6.1     | This RFC                                 |
|            |                                         |
| Req6.2     | This RFC                                 |
|            |                                         |
| Req7.1     |                                         |
|            |                                         |
| Req7.2     |                                         |
|            |                                         |
| Req7.3     |                                         |
|            |                                         |
| Req7.4     |                                         |
+------------+-----------------------------------------+
```

                     Table 7: Work Addressing requirements

Authors' Addresses

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

   Phone: +33 4 97 23 26 34
   Email: pthubert@cisco.com

   Erik Nordmark
   Zededa
   Santa Clara, CA
   United States of America

   Email: nordmark@sonic.net

   Samita Chakrabarti
   Verizon
   San Jose, CA
   United States of America

   Email: samitac.ietf@gmail.com

   Charles E. Perkins
   Futurewei
   2330 Central Expressway
   Santa Clara 95050
   United States of America

   Email: charliep@computer.org