Internet Engineering Task Force (IETF)
Request for Comments: 8505
Updates: 6775
Category: Standards Track
ISSN: 2070-1721

P. Thubert, Ed.
Cisco
E. Nordmark
Zededa
S. Chakrabarti
Verizon
C. Perkins
Futurewei

November 2018

Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery

Abstract

This specification updates RFC 6775 -- the Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery specification -- to clarify the role of the protocol as a registration technique and 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 Routing Registrars performing routing for host routes and/or proxy Neighbor Discovery in a low-power network.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8505.

Table of Contents

1. Introduction

IPv6 Low-Power and Lossy Networks (LLNs) support star and mesh topologies. For such networks, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)" [RFC6775] (also referred to as "6LoWPAN Neighbor Discovery (ND)") defines a registration mechanism and a central IPv6 ND Registrar to ensure unique addresses. The 6LoWPAN ND mechanism reduces the dependency of the IPv6 ND protocol [RFC4861] [RFC4862] on network-layer multicast and link-layer broadcast operations.

This specification updates 6LoWPAN ND [RFC6775] to simplify and generalize registration in 6LoWPAN Routers (6LRs). In particular, this specification modifies and extends the behavior and protocol elements of 6LoWPAN ND to enable the following actions:

- Determining the most recent location in the case of node mobility
- Simplifying the registration flow for Link-Local Addresses
- Support for a routing-unaware leaf node in a route-over network
- Proxy registration in a route-over network

- Enabling verification for the registration, using the Registration Ownership Verifier (ROVR) (Section 5.3)

- Registration to an IPv6 ND proxy (e.g., a Routing Registrar)

- Better support for privacy and temporary addresses

These features satisfy the requirements listed in Appendix B.

2. Terminology

2.1. Requirements Language

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

2.2. Related Documents

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

- "Neighbor Discovery for IP version 6 (IPv6)" [RFC4861]

- "IPv6 Stateless Address Autoconfiguration" [RFC4862]

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

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

- "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)" [RFC6775]

2.3. Abbreviations

This document uses the following abbreviations:

6BBR: 6LoWPAN Backbone Router

6CIO: Capability Indication Option

6LBR: 6LoWPAN Border Router

6LN: 6LoWPAN Node

6LoWPAN: IPv6 over Low-Power Wireless Personal Area Network

6LR: 6LoWPAN Router

ARO: Address Registration Option

DAC: Duplicate Address Confirmation

DAD: Duplicate Address Detection

DAR: Duplicate Address Request

DODAG: Destination-Oriented Directed Acyclic Graph

EARO: Extended Address Registration Option

EDA: Extended Duplicate Address

EDAC: Extended Duplicate Address Confirmation

EDAR: Extended Duplicate Address Request

LLN: Low-Power and Lossy Network

NA: Neighbor Advertisement

NCE: Neighbor Cache Entry

ND: Neighbor Discovery

NS: Neighbor Solicitation

RA: Router Advertisement

ROVR: Registration Ownership Verifier (pronounced "rover")

RPL: IPv6 Routing Protocol for LLNs (pronounced "ripple") [RFC6550]

RS: Router Solicitation

TID: Transaction ID (a sequence counter in the EARO)

2.4. New Terms

Backbone Link: An IPv6 transit link that interconnects two or more Backbone Routers.

Binding: The association between an IP address, a Media Access Control (MAC) address, and other information about the node that owns the IP address.

Registration: The process by which a 6LN registers an IPv6 Address with a 6LR in order to establish connectivity to the LLN.

Registered Node: The 6LN for which the registration is performed, according to the fields in the EARO.

Registering Node: The node that performs the registration. Either the Registered Node or a proxy.

IPv6 ND Registrar: A node that can process a registration in either NS(EARO) or EDAR messages and consequently respond with an NA or EDAC message containing the EARO and appropriate status for the registration.

Registered Address: An address registered for the Registered Node.

RFC 6775-only: An implementation, a type of node, or a message that behaves only as specified by [RFC6775], as opposed to the behavior specified in this document.

Route-over network: A network for which connectivity is provided at the IP layer.

Routing Registrar: An IPv6 ND Registrar that also provides reachability services for the Registered Address, including DAD and proxy NA.

Backbone Router (6BBR): A Routing Registrar that proxies the 6LoWPAN ND operations specified in this document to ensure that multiple LLNs federated by a Backbone Link operate as a single IPv6 subnetwork.

updated: A 6LN, 6LR, or 6LBR that supports this specification, in contrast to an RFC 6775-only device.

3. Applicability of Address Registration Options

The ARO as described in [RFC6775] facilitates DAD for hosts and populates NCEs [RFC4861] in the routers. This reduces the reliance on multicast operations, which are often as intrusive as broadcast, in IPv6 ND operations (see [Multicast-over-IEEE802-Wireless]).

This document specifies new status codes for registrations rejected by a 6LR or 6LBR for reasons other than address duplication. Examples include:

- the router running out of space.
- a registration bearing a stale sequence number. This could happen if the host moves after the registration was placed.
- a host misbehaving and attempting to register an invalid address, such as the unspecified address as defined in [RFC4291].
- a host using an address that is not topologically correct on that link.

In such cases, the host will receive an error that will help diagnose the issue; the host may retry -- possibly with a different address or 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. Each host may form and register a number of addresses for enhanced privacy, using mechanisms such as those described in [RFC4941] ("Privacy Extensions for Stateless Address Autoconfiguration in IPv6"), e.g., Stateless Address Autoconfiguration (SLAAC), and SHOULD conform to [RFC7934] ("Host Address Availability Recommendations").

As indicated in IPv6 ND [RFC4861], a router needs enough storage to hold NCEs for all directly connected addresses to which it is currently forwarding packets (unused entries may be flushed). In contrast, a router serving the address-registration mechanism 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 6LR or 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. Network administrators need to ensure that 6LRs/6LBRs in their network support the number and types of devices that can register to them, based on the number of IPv6 Addresses that those devices require, as well as their address renewal rate and behavior.

4. Extended Neighbor Discovery Options and Messages

This specification does not introduce any new options; it modifies existing options and updates the associated behaviors.

4.1. Extended Address Registration Option (EARO)

The ARO is defined in Section 4.1 of [RFC6775].

This specification introduces the EARO; the EARO is based on the ARO for use in NS and NA messages. The EARO includes a sequence counter called the Transaction ID (TID), which is used to determine the latest location of a registering mobile device. A new T flag indicates that the presence of the TID field is populated and that the option is an EARO. A 6LN requests routing or proxy services from a 6LR using a new R flag in the EARO.

The EUI-64 field is redefined and renamed "ROVR field" in order to carry different types of information, e.g., cryptographic information of variable size (see Section 5.3). A larger ROVR size MAY be used if and only if backward compatibility is not an issue in the particular LLN. The length of the ROVR field, expressed in units of 8 bytes, is the Length value of the option minus 1. A larger ROVR size MAY be used if and only if backward compatibility is not an issue in the particular LLN.

Section 5.1 discusses those changes in depth.

The format of the EARO is shown in Figure 1:

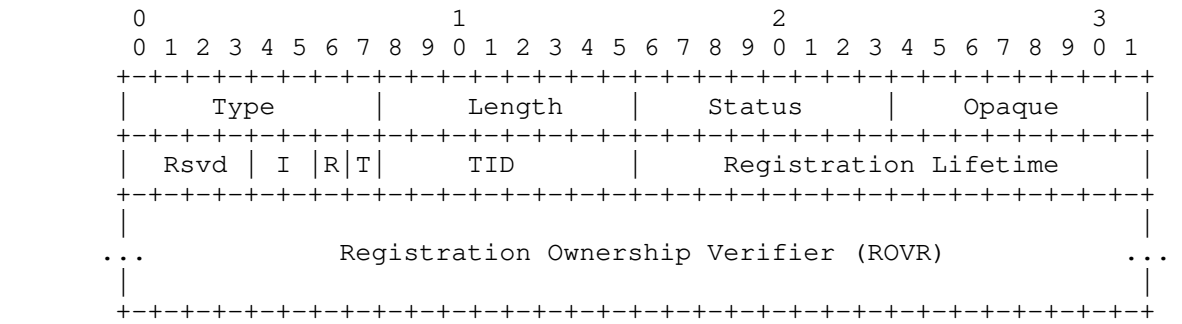

Figure 1: EARO Format

Option Fields:

Type: 33

Length: 8-bit unsigned integer. The length of the option in units of 8 bytes.

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.

Opaque: An octet opaque to ND. The 6LN MAY pass it transparently to another process. It MUST be set to 0 when not used.

Rsvd (Reserved):
This field is unused. It MUST be initialized to 0 by the sender and MUST be ignored by the receiver.

I: 2-bit integer. A value of 0 indicates that the Opaque field carries an abstract index that is used to decide in which routing topology the address is expected to be injected. In that case, the Opaque field is passed to a routing process with the indication that it carries topology information, and the value of 0 indicates default. All other values of "I" are reserved and MUST NOT be used.

R: The Registering Node sets the R flag to request reachability services for the Registered Address from a Routing Registrar.

T: 1-bit flag. Set if the next octet is used as a TID.

TID: 1-byte unsigned integer. A Transaction ID that is maintained by the node and incremented with each transaction of one or more registrations performed at the same time to one or more 6LRs. This field MUST be ignored if the T flag is not set.

Registration Lifetime:
16-bit integer, expressed in minutes. A value of 0 indicates that the registration has ended and that the associated state MUST be removed.

Registration Ownership Verifier (ROVR):
Enables the correlation between multiple attempts to register the same IPv6 Address. The ROVR size MUST be 64 bits when backward compatibility is needed; otherwise, the size MAY be 128, 192, or 256 bits.

Value	Description
0-2	As defined in [RFC6775]. Note: A Status value 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 most recent. This Status indicates that the registration is rejected because another more recent registration was done, as indicated by the 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 an IPv6 ND Registrar, 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. An IPv6 ND Registrar MAY place this Status in asynchronous DAC or NA messages.
6	Duplicate Source Address: The address used as the source of the NS(EARO) conflicts with an existing registration.
7	Invalid Source Address: The address used as the source of the NS(EARO) is not a Link-Local Address.
8	Registered Address Topologically Incorrect: The address being registered is not usable on this link.
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 Codes

4.2. Extended Duplicate Address Message Formats

The DAR and DAC messages share a common base format as defined in Section 4.4 of [RFC6775]. Those messages enable information from the ARO to be transported over multiple hops. The DAR and DAC are extended as shown in Figure 2:

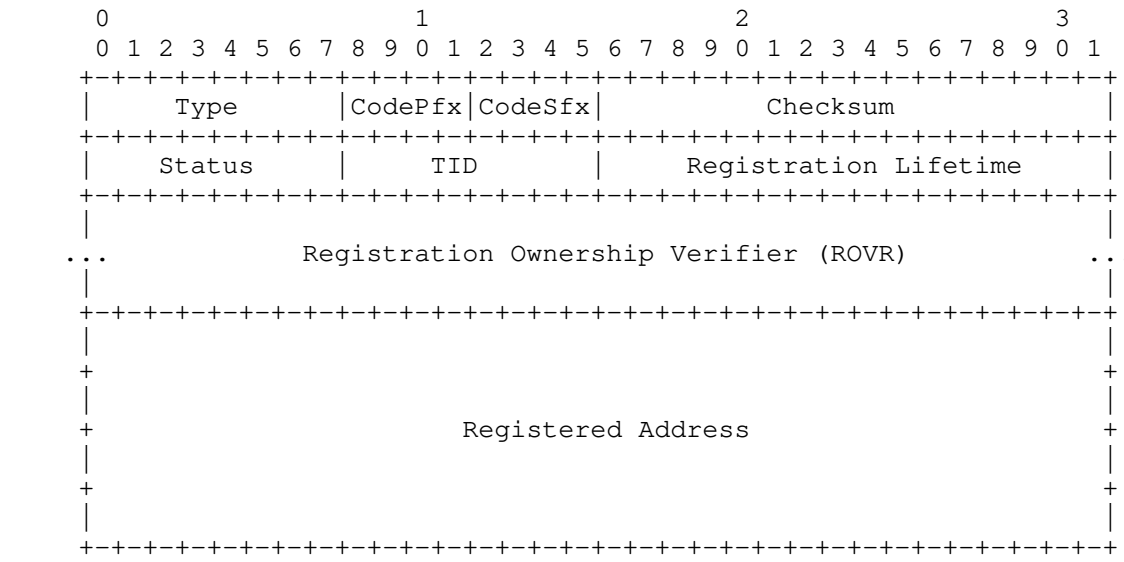

Figure 2: Extended Duplicate Address Message Format

Modified Message Fields:

Code: The ICMP Code [RFC4443] for Duplicate Address messages is split into two 4-bit fields: the Code Prefix and the Code Suffix. The Code Prefix MUST be set to 0 by the sender and MUST be ignored by the receiver. A non-null value of the Code Suffix indicates support for this specification. It MUST be set to 1 when operating in a backward-compatible mode, indicating a ROVR size of 64 bits. It MAY be 2, 3, or 4, denoting a ROVR size of 128, 192, or 256 bits, respectively.

TID: 1-byte integer. Same definition and processing as the TID in the EARO as defined in Section 4.1. This field MUST be ignored if the ICMP Code is null.

Registration Ownership Verifier (ROVR):
The size of the ROVR is known from the ICMP Code Suffix. This field has the same definition and processing as the ROVR in the EARO as defined in Section 4.1.

4.3. Extensions to the Capability Indication Option

This specification defines five new capability bits for use in the 6CIO as defined by [RFC7400] ("6LoWPAN-GHC: Generic Header Compression for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)"), for use in IPv6 ND messages. (The G flag is defined in Section 3.3 of [RFC7400].)

The D flag indicates that the 6LBR supports EDAR and EDAC messages. A 6LR that learns the D flag from advertisements can then exchange EDAR and EDAC messages with the 6LBR, and it also sets the D flag as well as the L flag in the 6CIO in its own advertisements. In this way, 6LNs will be able to prefer registration with a 6LR that can make use of new 6LBR features.

The new L, B, and P flags indicate whether a router is capable of acting as a 6LR, 6LBR, or Routing Registrar (e.g., 6BBR) (or some combination thereof), respectively. These flags are not mutually exclusive; an updated node can advertise multiple collocated functions.

The E flag indicates that the EARO can be used in a registration. A 6LR that supports this specification MUST set the E flag.

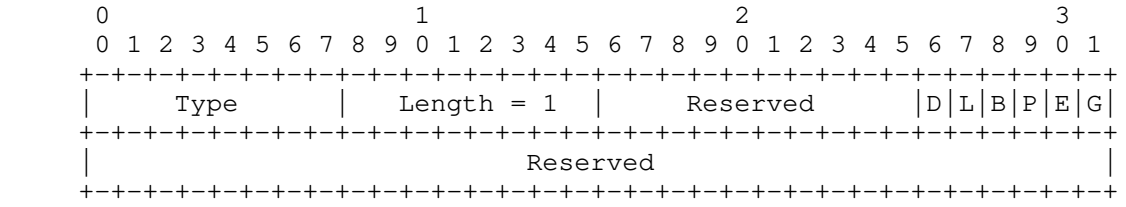

Figure 3: New Capability Bits in the 6CIO

Option Fields:

Type: 36

D: The 6LBR supports EDAR and EDAC messages.

L: The node is a 6LR.

B: The node is a 6LBR.

P: The node is a Routing Registrar.

E: The node is an IPv6 ND Registrar; i.e., it supports registrations based on the EARO.

5. Updating RFC 6775

The EARO (see Section 4.1) updates the ARO used within NS and NA messages between a 6LN and a 6LR. The update enables a registration to a Routing Registrar in order to obtain additional services, such as return routability to the Registered Address by such means as routing and/or proxy ND, as illustrated in Figure 4.

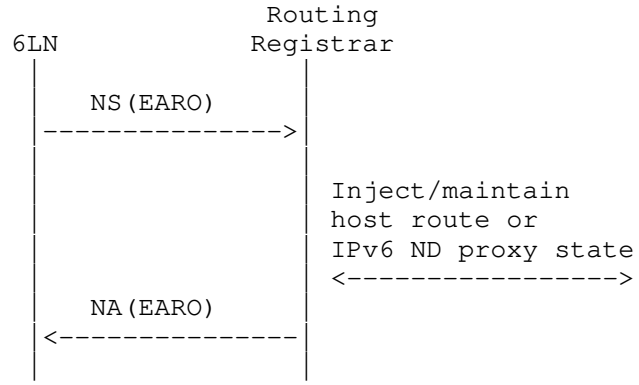

Figure 4: (Re-)Registration Flow

Similarly, the EDAR and EDAC update the DAR and DAC messages so as to transport the new information between 6LRs and 6LBRs across an LLN mesh. The extensions to the ARO are the DAR and the DAC, as used in the Duplicate Address messages. They convey the additional information all the way to the 6LBR.

In turn, the 6LBR may proxy the registration to obtain reachability services from a Routing Registrar such as a 6BBR, as illustrated in Figure 5. This specification avoids the Duplicate Address message flow for Link-Local Addresses in a route-over [RFC6606] topology (see Section 5.6).

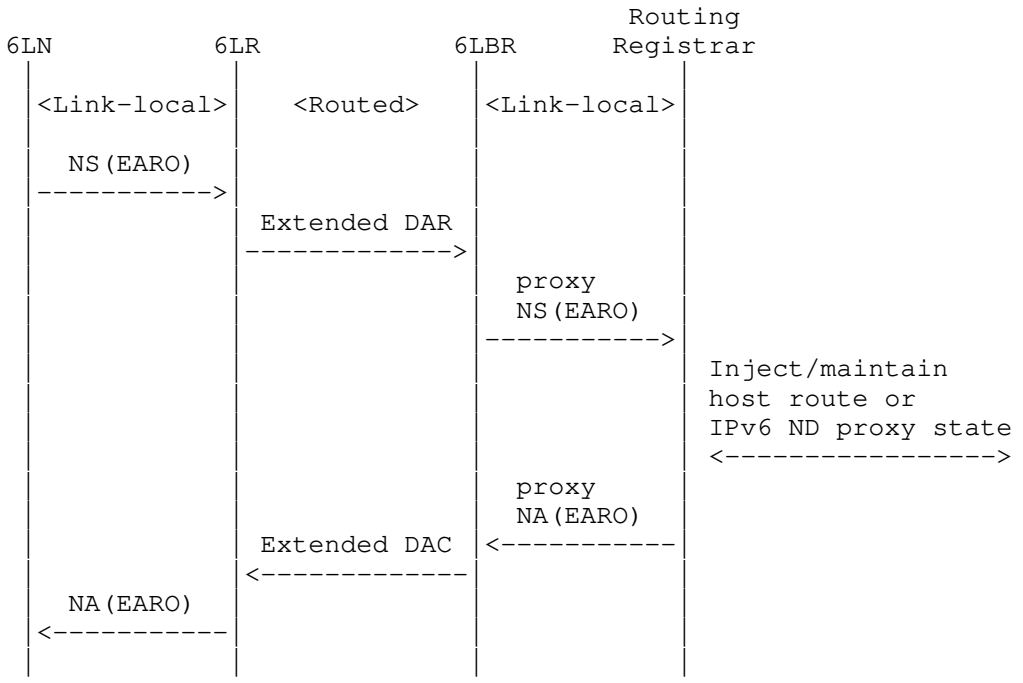

Figure 5: (Re-)Registration Flow

This specification allows multiple registrations, including registrations for privacy and temporary addresses, and provides a mechanism to help clean up stale registration state as soon as possible, e.g., after a movement (see Section 7).

Section 5 of [RFC6775] specifies how a 6LN bootstraps an interface and locates available 6LRs. A Registering Node SHOULD register to a 6LR that supports this specification if one is found, as discussed in Section 6.1, instead of registering to an RFC 6775-only 6LR; otherwise, the Registering Node operates in a backward-compatible fashion when attaching to an RFC 6775-only 6LR.

5.1. Extending the Address Registration Option

The EARO updates the ARO and is backward compatible with the ARO if and only if the Length value of the option is set to 2. The format of the EARO is presented in Section 4.1. More details on backward compatibility can be found in Section 6.

The NS message and the ARO are modified as follows:

- The Target Address field in the NS containing the EARO is now the field that indicates the address that is being registered, as opposed to the Source Address field in the NS as specified in [RFC6775] (see Section 5.5). This change enables a 6LBR to send a proxy registration for a 6LN's address to a Routing Registrar and in most cases also avoids the use of an address as the Source Address before it is registered.

- The EUI-64 field in the ARO is renamed "Registration Ownership Verifier (ROVR)" and is not required to be derived from a MAC address (see Section 5.3).

- The option's Length value 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 in size corresponds to a larger ROVR field, so the size of the ROVR is inferred from the option's Length value.

- A new Opaque field is introduced to carry opaque information in cases where the registration is relayed to another process, e.g., to be advertised by a routing protocol. A new "I" field provides a type for the opaque information and indicates the other process to which the 6LN passes the opaque value. A value of 0 for the "I" field indicates topological information to be passed to a routing process if the registration is redistributed. In that case, a value of 0 for the Opaque field (1) is backward compatible with the reserved fields that are overloaded and (2) indicates that the default topology is to be used.

- This document specifies a new flag in the EARO: the R flag. If the R flag is set, the Registering Node requests that the 6LR ensure reachability for the Registered Address, e.g., by means of routing or proxy ND. Conversely, when it is not set, the R flag indicates that the Registering Node is a router and that it will advertise reachability to the Registered Address via a routing protocol (such as RPL [RFC6550]).

- A node that supports this specification MUST provide a TID field in the EARO and set the T flag to indicate the presence of the TID (see Section 5.2).

- Finally, this specification introduces new status codes to help diagnose the cause of a registration failure (see Table 1).

When registering, a 6LN that acts only as a host 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 advertises.

5.2. 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 determine the recency of the registration request. The network uses the most recent TID to determine the most recent known location(s) of a moving 6LN. When a Registered Node is registered with multiple 6LRs in parallel, the same TID MUST be used. This enables the 6LBRs and/or Routing Registrars to determine whether the registrations are identical and to distinguish that situation from a movement (for example, see Section 5.7 and Appendix A).

5.2.1. Comparing TID Values

The operation of the TID is fully compatible with that of the RPL Path Sequence counter as described in Section 7.2 of [RFC6550] ("RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks").

A TID is deemed to be more recent than another when its value is greater as determined by 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 are used as a circular sequence number space of size 128 as mentioned 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 determined 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. Prior to use, the sequence counter SHOULD be initialized to an implementation-defined value of 128 or greater. 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 0. 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 the interval [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.

5.3. Registration Ownership Verifier (ROVR)

The ROVR field replaces the EUI-64 field of the ARO defined in [RFC6775]. It is associated in the 6LR and the 6LBR with the registration state. The ROVR 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 that can be used in additional protocol exchanges to associate a cryptographic identity (key) with this registration to ensure that only the owner can modify it later, if the proof of ownership of the ROVR can be obtained. The scope of a ROVR is the registration of a particular IPv6 Address, and it MUST NOT be used to correlate registrations of different addresses.

The ROVR can be of different types; the type is signaled in the message that carries the new type. For instance, the type can be a cryptographic string and can be used to prove the ownership of the registration as specified in [AP-ND] ("Address Protected Neighbor Discovery for Low-power and Lossy Networks"). 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 regarding ROVR collisions: Different techniques for forming the ROVR will operate in different namespaces. [RFC6775] specifies the use of EUI-64 addresses. [AP-ND] specifies the generation of cryptographic tokens. While collisions are not expected in the EUI-64 namespace only, they may happen if [AP-ND] is implemented by at least one of the nodes. An implementation that understands the namespace MUST consider that ROVRs from different namespaces are different even if they have the same value. An RFC 6775-only 6LBR or 6LR will confuse the namespaces; this slightly increases the risk of a ROVR collision. A ROVR collision 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 Identifier of the Registered Address. This way, a registration that uses that ROVR will not collide with that of an IPv6 Address derived from EUI-64 and using the EUI-64 as the 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 (1) the 6LRs and the 6LBR time out the previous registration or (2) a management action clears the relevant state in the network.

5.4. Extended Duplicate Address Messages

In order to map the new EARO content in the EDA messages, a new TID field is added to the EDAR and EDAC messages as a replacement for the Reserved field, and a non-null value of the ICMP Code indicates support for this specification. The format of the EDAR and EDAC messages is presented in Section 4.2.

As with the EARO, the EDA messages are backward compatible with the RFC 6775-only versions, as long as the ROVR field is 64 bits long. Remarks concerning backward compatibility for the protocol between the 6LN and the 6LR apply similarly between a 6LR and a 6LBR.

5.5. Registering the Target Address

An NS message with an EARO is a registration if and only if it also carries an SLLA Option ("SLLAO") [RFC6775] ("SLLA" stands for "Source Link-Layer Address"). The EARO can also be used in NS and NA messages between Routing Registrars to determine the distributed registration state; in that case, it does not carry the SLLA Option and is not confused with a registration.

The Registering Node is the node that performs the registration to the Routing Registrar. As also described 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 the 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 Routing Registrar via a mesh-under configuration, 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 configuration 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 Routing Registrar 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 field. With this convention, a TLLA Option (Target Link-Layer Address Option, or "TLLAO") indicates the link-layer address of the 6LN that owns the address.

A Registering Node (e.g., a 6LBR also acting as a RPL root) that advertises reachability for the 6LN MUST place its own link-layer address in the SLLA Option of the registration NS(EARO) message. This maintains compatibility with RFC 6775-only 6LoWPAN ND.

5.6. Link-Local Addresses and Registration

LLN nodes are often not wired and may move. There is no guarantee that a Link-Local Address will remain unique among a huge and potentially variable 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.

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 further reachability by way of that 6LR and, in particular, to use the Link-Local Address as the Source Address to register other addresses, e.g., global addresses.

If there is no collision with a previously registered address, then the Link-Local Address is unique from the standpoint of this 6LR and the registration is not a duplicate. Two different 6LRs might claim 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 exchange of EDAR and EDAC messages between the 6LR and a 6LBR, which ensures that an address is unique across the domain covered by the 6LBR, does not need to take place for Link-Local Addresses.

When sending an NS(EARO) to a 6LR, a 6LN 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 6LN starts up, it typically multicasts an RS and receives one or more unicast RA messages from 6LRs. If the 6LR can process EARO messages, then it places a 6CIO in its RA message with the E flag set as required in Section 6.1.

When a Registering Node does not have an already-registered address, it MUST register a Link-Local Address, using it as both the Source Address and the Target Address of an NS(EARO) message. In that case, it is RECOMMENDED to use an address for which DAD is not required (see [RFC6775]), e.g., derived from a globally unique EUI-64 address; using the SLLA Option in the NS is consistent with existing ND specifications such as [RFC4429] ("Optimistic Duplicate Address Detection (DAD) for IPv6"). The 6LN MAY then use that address to register one or more other addresses.

A 6LR that supports this specification replies with an NA(EARO), setting the appropriate status. Since there is no exchange of EDAR or EDAC 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 SLLA Option that is placed in the NS(EARO) message as required in [RFC6775].

A node registers 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 the Source Address, in contrast to a node that complies with [RFC6775]. For non-Link-Local Addresses, the exchange of EDAR and EDAC 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.

5.7. 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 5.6, 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 Routing Registrars may store additional registration information and use synchronization protocols that are out of scope for this document.

A 6LR cannot accept a new registration when its registration storage space is exhausted. In that situation, the EARO is returned in an NA message with a status code of "Neighbor Cache Full" (Status 2; see [RFC6775] and Table 1), and the Registering Node may attempt to register to another 6LR.

If the registry in the 6LBR is full, 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 in the node retrying this registration via another 6LR, since the problem is network-wide. The node may abandon that address, de-register other addresses first to make room, or keep the address "tentative" [RFC4861] and retry later.

A node renews an existing registration by sending a new NS(EARO) message for the Registered Address, and the 6LR MUST report the new registration 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, the associated state will remain in the network until the current Registration Lifetime expires; this may lead to a situation where the 6LR resources become saturated, even if they were correctly planned to start with. The 6LR may then take defensive measures that may prevent this node or some other nodes from owning as many addresses as they request (see Section 7).

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 appears 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. The "Moved" status can be used by a Routing Registrar in an NA(EARO) message to indicate that the ownership of the proxy state was transferred to another Routing Registrar due to movement of the device. If the receiver of the message has registration 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 [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 most recent for a given NCE (see Section 5.2), 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 determines 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 code of 0 ("Success") [RFC6775], 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 NCE in a DELAY state [RFC4861] for a configurable period of time, so as to prevent a scenario where (1) a mobile node that de-registered from one 6LR did not yet register to a new one or (2) the new registration did not yet reach the 6LBR due to propagation delays in the network. Once the DELAY time has passed, the 6LBR silently removes its entry.

6. Backward Compatibility

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]. Conversely, if the 6LR is found 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 behavior is backward compatible, since the T flag and TID field occupy fields that are reserved in [RFC6775] and are thus ignored by an RFC 6775-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; this scenario has no consequence if the Registered Addresses are different.

6.1. Signaling EARO Support

[RFC7400] specifies the 6CIO, which indicates a node's capabilities to the node's peers. The 6CIO MUST be present in both RS and RA messages, unless the 6CIO information was already shared in recent exchanges 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 4.3 defines a new flag for the 6CIO to signal EARO support by the issuer of the message. New flags are also added to the 6CIO to signal the sender's capability to act as a 6LR, 6LBR, and Routing Registrar (see Section 4.3).

Section 4.3 also defines a new flag that indicates the support of EDAR and EDAC 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.

6.2. RFC 6775-Only 6LN

An RFC 6775-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 RFC 6775-only DAR and DAC 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 DAR and DAC 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.

6.3. RFC 6775-Only 6LR

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 RFC 6775-only.

An updated 6LN MUST use an EARO in the request, regardless of the type of 6LR -- RFC 6775-only or updated; this implies that the T flag is set. It MUST use a ROVR of 64 bits if the 6LR is RFC 6775-only.

If an updated 6LN moves from an updated 6LR to an RFC 6775-only 6LR, the RFC 6775-only 6LR will send an RFC 6775-only DAR message, which cannot be compared with an updated one for recency. Allowing RFC 6775-only DAR messages to update a state established by the updated protocol in the 6LBR would be an attack vector; therefore, this cannot be the default behavior. But if RFC 6775-only and updated 6LRs coexist temporarily in a network, then it makes sense for an administrator to install a policy that allows this behavior, using some method that is out of scope for this document.

6.4. RFC 6775-Only 6LBR

With this specification, the Duplicate Address messages are extended to transport the EARO information. As with the NS/NA exchange, an updated 6LBR MUST always use the EDAR and EDAC messages.

Note that an RFC 6775-only 6LBR will accept and process an EDAR message as if it were an RFC 6775-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 is assumed to be RFC 6775-only.

If the 6LBR is RFC 6775-only, the 6LR MUST use only the 64 leftmost bits of the ROVR and place the result in the EDAR message to maintain compatibility. This way, the support of DAD is preserved.

7. Security Considerations

This specification extends [RFC6775], and the Security Considerations section of that document also applies to this document. In particular, the link layer SHOULD be sufficiently protected to prevent rogue access.

[RFC6775] does not protect the content of its messages and expects lower-layer encryption to defeat potential attacks. This specification requires the LLN MAC layer to provide secure unicast to/from a Routing Registrar and secure broadcast or multicast from the Routing Registrar in a way that prevents tampering with or replaying the ND messages.

This specification recommends using privacy techniques (see Section 8) and protecting against address theft via methods that are outside the scope of this document. As an example, [AP-ND] 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 6LBR with a denial-of-service attack against the registry. It may also happen that the registry of a 6LR or 6LBR is saturated and cannot take any more registrations; this scenario effectively denies the requesting node the capability to use a new address. In order to alleviate those concerns, (1) Section 5.2 provides a sequence counter that keeps incrementing to detect and clean up stale registration information and that contributes to defeat replay attacks and (2) Section 5.7 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:

- A node that ceases to use an address SHOULD attempt to de-register that address from all the 6LRs to which it is registered.

- The registration lifetimes SHOULD be individually configurable for each address or group of addresses. A node SHOULD be configured for each address (or address category) with a Registration Lifetime that reflects the expectation of how long it will use the address with the 6LR to which the address is registered. In particular, use cases that involve mobility or rapid address changes SHOULD use lifetimes that are the same order of magnitude as the duration of the expectation of presence but that are still longer.

- 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. In any case, a router MUST be able to keep a minimum number of addresses per node. That minimum depends on the type of device and ranges between 3 for a very constrained LLN and 10 for a larger device. A node may be identified by its MAC address, as long as it is not obfuscated by privacy measures. A stronger identification (e.g., by security credentials) is RECOMMENDED. When the 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.

- In order to avoid denial of registration due to a 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 LLN should distribute the 6LBR functionality -- for instance, by leveraging a high-speed Backbone Link and Routing Registrars to aggregate multiple LLNs into a larger subnet.

The LLN nodes depend on a 6LBR and may use the services of a Routing Registrar for their operation. A trust model MUST be put in place to ensure that only authorized 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. At a minimum, this trust model could be based on Layer 2 access control or could provide role validation as well (see Req-5.1 in Appendix B.5).

8. Privacy Considerations

As indicated in Section 3, this protocol does not 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 Identifier in the Link-Local Address because this method prevents the usage of Secure Neighbor Discovery (SEND) [RFC3971], Cryptographically Generated Addresses (CGAs) [RFC3972], and other address privacy techniques.

[RFC8065] ("Privacy Considerations for IPv6 Adaptation-Layer Mechanisms") 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, privacy concerns should be considered. In particular, new implementations should follow [RFC8064] ("Recommendation on Stable IPv6 Interface Identifiers"). [RFC8064] recommends the mechanism specified in [RFC7217] ("A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)") for generating Interface Identifiers to be used in SLAAC.

9. IANA Considerations

IANA has made a number of changes under the "Internet Control Message Protocol version 6 (ICMPv6) Parameters" registry, as follows.

9.1. Address Registration Option Flags

IANA has created a new subregistry for "Address Registration Option Flags" under the "Internet Control Message Protocol version 6 (ICMPv6) Parameters" registry. (See [RFC4443] for information regarding ICMPv6.)

This specification defines eight positions -- bit 0 to bit 7 -- and assigns bit 6 for the R flag and bit 7 for the T flag (see Section 4.1). The registration procedure is "IETF Review" or "IESG Approval" (see [RFC8126]).

The initial contents of the registry are shown in Table 2.

ARO Status	Description	Reference
0-5	Unassigned	
6	R Flag	RFC 8505
7	T Flag	RFC 8505

Table 2: New Address Registration Option Flags

9.2. Address Registration Option I-Field

IANA has created a new subregistry for "Address Registration Option I-Field" under the "Internet Control Message Protocol version 6 (ICMPv6) Parameters" registry.

This specification defines four integer values from 0 to 3 and assigns value 0 to "Abstract Index for Topology Selection" (see Section 4.1). The registration procedure is "IETF Review" or "IESG Approval" [RFC8126].

The initial contents of the registry are shown in Table 3.

Value	Meaning	Reference
0	Abstract Index for Topology Selection	RFC 8505
1-3	Unassigned	

Table 3: New Subregistry for the EARO I-Field

9.3. ICMP Codes

IANA has created two new subregistries of the 'ICMPv6 "Code" Fields' registry, which itself is a subregistry of ICMPv6 codes in the "Internet Control Message Protocol version 6 (ICMPv6) Parameters" registry.

The new subregistries relate to ICMP Types 157 (Duplicate Address Request) (shown in Table 4) and 158 (Duplicate Address Confirmation) (shown in Table 5), respectively. For those two ICMP types, the ICMP Code field is split into two subfields: the Code Prefix and the Code Suffix. The new subregistries relate to the Code Suffix portion of the ICMP Code. The range of the Code Suffix is 0-15 in all cases. The registration procedure is "IETF Review" or "IESG Approval" [RFC8126] for both subregistries.

The initial contents of these subregistries are as follows:

Code Suffix	Meaning	Reference
0	DAR message	RFC 6775
1	EDAR message with 64-bit ROVR field	RFC 8505
2	EDAR message with 128-bit ROVR field	RFC 8505
3	EDAR message with 192-bit ROVR field	RFC 8505
4	EDAR message with 256-bit ROVR field	RFC 8505
5-15	Unassigned	

Table 4: Code Suffixes for ICMP Type 157 DAR Message

Code Suffix	Meaning	Reference
0	DAC message	RFC 6775
1	EDAC message with 64-bit ROVR field	RFC 8505
2	EDAC message with 128-bit ROVR field	RFC 8505
3	EDAC message with 192-bit ROVR field	RFC 8505
4	EDAC message with 256-bit ROVR field	RFC 8505
5-15	Unassigned	

Table 5: Code Suffixes for ICMP Type 158 DAC Message

9.4. New ARO Status Values

IANA has made additions to the "Address Registration Option Status Values" subregistry, as follows:

Value	Description	Reference
3	Moved	RFC 8505
4	Removed	RFC 8505
5	Validation Requested	RFC 8505
6	Duplicate Source Address	RFC 8505
7	Invalid Source Address	RFC 8505
8	Registered Address Topologically Incorrect	RFC 8505
9	6LBR Registry Saturated	RFC 8505
10	Validation Failed	RFC 8505

Table 6: New ARO Status Values

9.5. New 6LoWPAN Capability Bits

IANA has made additions to the "6LoWPAN Capability Bits" subregistry, as follows:

Bit	Description	Reference
10	EDA Support (D bit)	RFC 8505
11	6LR capable (L bit)	RFC 8505
12	6LBR capable (B bit)	RFC 8505
13	Routing Registrar (P bit)	RFC 8505
14	EARO support (E bit)	RFC 8505

Table 7: New 6LoWPAN Capability Bits

10. References

10.1. 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>.

[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>.

10.2. Informative References

[Alternative-Ellip-Curve-Reps]
Struik, R., "Alternative Elliptic Curve Representations", Work in Progress, draft-struik-lwip-curve-representations-00, October 2017.

[AP-ND] Thubert, P., Ed., Sarikaya, B., Sethi, M., and R. Struik, "Address Protected Neighbor Discovery for Low-power and Lossy Networks", Work in Progress, draft-ietf-6lo-ap-nd-08, October 2018.

[Arch-for-6TiSCH]
Thubert, P., Ed., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", Work in Progress, draft-ietf-6tisch-architecture-17, November 2018.

[Efficient-NPDAO]
Jadhav, R., Ed., Thubert, P., Sahoo, R., and Z. Cao, "Efficient Route Invalidation", Work in Progress, draft-ietf-roll-efficient-npdao-09, October 2018.

[IEEE-802-15-4]
IEEE, "IEEE Standard for Low-Rate Wireless Networks", IEEE Standard 802.15.4, DOI 10.1109/IEEESTD.2016.7460875, <https://ieeexplore.ieee.org/document/7460875/>.

[IPv6-Backbone-Router]
Thubert, P., Ed. and C. Perkins, "IPv6 Backbone Router", Work in Progress, draft-ietf-6lo-backbone-router-08, October 2018.

[IPv6-over-802.11ah]
Del Carpio Vega, L., Robles, M., and R. Morabito, "IPv6 over 802.11ah", Work in Progress, draft-delcarpio-6lo-wlanah-01, October 2015.

[IPv6-over-NFC]
Choi, Y., Ed., Hong, Y-G., Youn, J-S., Kim, D-K., and J-H. Choi, "Transmission of IPv6 Packets over Near Field Communication", Work in Progress, draft-ietf-6lo-nfc-12, November 2018.

[IPv6-over-PLC]
Hou, J., Liu, B., Hong, Y-G., Tang, X., and C. Perkins, "Transmission of IPv6 Packets over PLC Networks", Work in Progress, draft-hou-6lo-plc-05, October 2018.

[Multicast-over-IEEE802-Wireless]
Perkins, C., McBride, M., Stanley, D., Kumari, W., and JC. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", Work in Progress, draft-ietf-mboned-ieee802-mcast-problems-03, October 2018.

[ND-Optimizations]
Chakrabarti, S., Nordmark, E., Thubert, P., and M. Wasserman, "IPv6 Neighbor Discovery Optimizations for Wired and Wireless Networks", Work in Progress, draft-chakrabarti-nordmark-6man-efficient-nd-07, February 2015.

[Perlman83]
Perlman, R., "Fault-Tolerant Broadcast of Routing Information", North-Holland Computer Networks 7: pp. 395-405, DOI 10.1016/0376-5075(83)90034-X, 1983, <http://www.cs.illinois.edu/~pbg/courses/cs598fa09/readings/p83.pdf>.

[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>.

[Routing-for-RPL-Leaves] Thubert, P., Ed., "Routing for RPL Leaves", Work in Progress, draft-thubert-roll-unaware-leaves-05, May 2018.

Appendix A. Applicability and Fulfilled Requirements (Not Normative)

This specification extends 6LoWPAN ND to provide a sequence number to the registration and fulfills the requirements expressed in Appendix B.1 by enabling the mobility of devices from one LLN to the next. A full specification for enabling mobility based on the use of the EARO and the registration procedures defined in this document can be found in subsequent work [IPv6-Backbone-Router] ("IPv6 Backbone Router"). The 6BBR is an example of a Routing Registrar that acts as an IPv6 ND proxy over a Backbone Link that federates multiple LLNs as well as the Backbone Link itself into a single IPv6 subnet. The expected registration flow in that case is illustrated in Figure 6, noting that any combination of 6LR, 6LBR, and 6BBR may be collocated.

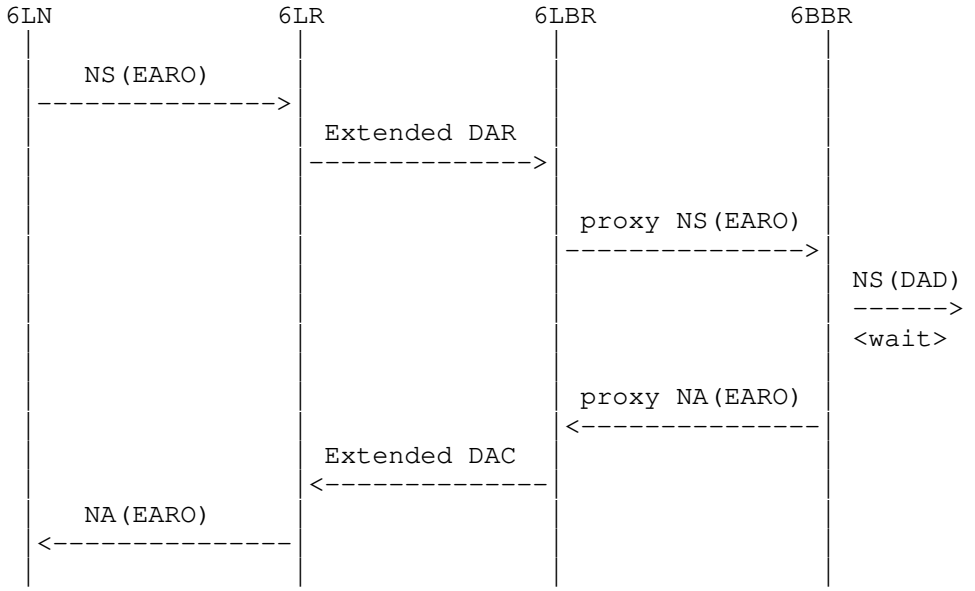

Figure 6: (Re-)Registration Flow

[Arch-for-6TiSCH] ("An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4") describes how a 6LoWPAN ND host using the Time-Slotted Channel Hopping (TSCH) mode of IEEE Std. 802.15.4 [IEEE-802-15-4] can connect to the Internet via a RPL mesh network. Doing so requires additions to the 6LoWPAN ND protocol to support mobility and reachability in a secure and manageable network environment. This document specifies those new operations and fulfills the requirements listed in Appendix B.2.

The term "LLN" is used loosely in this document and is intended 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 register its IPv6 Addresses with a Routing Registrar and to obtain routing services such as proxy ND operations over a Backbone Link. This satisfies the requirements expressed in Appendix B.4.

This specification is extended by [AP-ND] to provide a solution to some of the security-related requirements expressed in Appendix B.5.

[ND-Optimizations] ("IPv6 Neighbor Discovery Optimizations for Wired and Wireless Networks") 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 an 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 [Multicast-over-IEEE802-Wireless]. This fulfills the scalability requirements listed in Appendix B.6.

Appendix B. Requirements (Not Normative)

This appendix lists requirements that were discussed by the 6lo Working Group 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, say, 6LR-a to 6LR-b but 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 type of signaling upon detection of the movement or using a keep-alive mechanism with a period that is consistent with the needs of the application.

Req-1.1: 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.

Req-1.2: For that purpose, the protocol MUST enable differentiating between multiple registrations from one 6LN and registrations from different 6LNs claiming the same address.

Req-1.3: Stale states MUST be cleaned up in 6LRs.

Req-1.4: A 6LN 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 (SDOs) on the basis of the expected network characteristics. It is required that a 6LN attached via ND to a 6LR indicate whether or not it (1) participates in the selected routing protocol to obtain reachability via the 6LR or (2) expects the 6LR to manage its reachability.

The specified updates enable other specifications to define new services such as Source Address Validation Improvement (SAVI) (via [AP-ND]), participation as an unaware leaf to a routing protocol (such as the protocol described in [RFC6550] (RPL)) (via [Routing-for-RPL-Leaves]), and registration to Backbone Routers performing proxy ND in an LLN (via [IPv6-Backbone-Router]).

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 subtree), 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 as follows:

Req-2.1: 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.

Req-2.2: Considering RPL, the ARO 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.

Req-2.3: Multicast operations SHOULD be supported and optimized -- for instance, using BIER or the Multicast Protocol for Low-Power and Lossy Networks (MPL). Whether ND is appropriate for the registration to the Routing Registrar is to be defined, considering the additional burden of supporting Multicast Listener Discovery Version 2 (MLDv2) for IPv6 [RFC3810].

B.3. Requirements Related to Various 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) technique [RFC6282] to other link types, including ITU-T G.9959 [RFC7428], Master-Slave/Token-Passing [RFC8163], Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy [RFC8105], Near Field Communication [IPv6-over-NFC], and IEEE Std. 802.11ah [IPv6-over-802.11ah], as well as Bluetooth low energy [RFC7668] and Power Line Communication (PLC) Networks [IPv6-over-PLC].

Related requirements are as follows:

Req-3.1: 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.

Req-3.2: 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.

Req-3.3: The ARO used in the ND registration SHOULD be extended to carry the relevant forms of the unique identifier.

Req-3.4: ND should specify the formation of a site-local address that follows the security recommendations in [RFC7217].

B.4. Requirements Related to Proxy Operations

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

The ND registration method SHOULD defend the addresses of duty-cycled devices that are sleeping most of the time and incapable of defending their own addresses.

Related requirements are as follows:

Req-4.1: The registration mechanism SHOULD enable a third party to proxy-register an address on behalf of a 6LN that may be sleeping or located deeper in an LLN mesh.

Req-4.2: The registration mechanism SHOULD be applicable to a duty-cycled device regardless of the link type and SHOULD enable a Routing Registrar to operate as a proxy to defend the Registered Addresses on its behalf.

Req-4.3: 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, spoofing the roles of the 6LR, 6LBR, and Routing Registrar 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 should then 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 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, the ability to route packets between the JA/CT and the joining node is needed.

Related requirements are as follows:

Req-5.1: 6LoWPAN ND security mechanisms SHOULD provide a mechanism for the 6LR, 6LBR, and Routing Registrar to authenticate and authorize one another for their respective roles, as well as with the 6LN for the role of 6LR.

Req-5.2: 6LoWPAN ND security mechanisms SHOULD provide a mechanism for the 6LR and the 6LBR to validate new registrations of authorized nodes. Joining of unauthorized nodes MUST be prevented.

Req-5.3: The use of 6LoWPAN ND security mechanisms SHOULD NOT result in 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 [IEEE-802-15-4] frame.

Req-5.4: Recurrent 6LoWPAN ND security operations MUST NOT be computationally intensive on the 6LN's CPU. When calculation of a key hash is employed, a mechanism lighter than SHA-1 SHOULD be used.

Req-5.5: The number of keys that the 6LN needs to manipulate SHOULD be minimized.

Req-5.6: 6LoWPAN ND security mechanisms SHOULD enable (1) the variation of CCM ("Counter with CBC-MAC") [RFC3610] called "CCM*" for use at both Layer 2 and Layer 3 and (2) the reuse of a security code that has to be present on the device for upper-layer security (e.g., TLS). Algorithm agility and support for large keys (e.g., 256-bit key sizes) are also desirable.

Req-5.7: 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.

Req-5.8: Routing of packets should continue when links pass from the unsecured state to the secured state.

Req-5.9: 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 if it is a duplicate.

B.6. Requirements Related to Scalability

Use cases from Automatic Meter Reading (AMR) (collection-tree operations) and Advanced Metering Infrastructure (AMI) (bidirectional communication to the meters) indicate the need 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 as follows:

Req-6.1: The registration mechanism SHOULD enable a single 6LBR to register multiple thousands of devices.

Req-6.2: The timing of the registration operation should allow for long latency, such as that found in LLNs with ten or more hops.

B.7. Requirements Related to Operations and Management

Guideline 3.8 in Section 3 of [RFC1958] ("Architectural Principles of the Internet") recommends the following: "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 dynamic configuration of LLN devices can also be constrained by network and power limitations.

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 registrations, so the administrator can take actions such as adding a Backbone Link with additional 6LBRs and Routing Registrars to the network.

Related requirements are as follows:

Req-7.1: A management model SHOULD be provided that enables access to the 6LBR, monitors its usage vs. capacity, and sends alerts in the case of congestion. It is recommended that the 6LBR be reachable over a non-LLN link.

Req-7.2: A management model SHOULD be provided that enables access to the 6LR and its capacity to host additional NCEs. This management model SHOULD avoid polling individual 6LRs in a way that could disrupt the operation of the LLN.

Req-7.3: Information on successful and failed registrations 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.

Req-7.4: In the 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

Requirement	Document
Req-1.1	[IPv6-Backbone-Router]
Req-1.2	[RFC6775]
Req-1.3	[RFC6775]
Req-1.4	RFC 8505
Req-2.1	RFC 8505
Req-2.2	RFC 8505
Req-2.3	
Req-3.1	Technology Dependent
Req-3.2	Technology Dependent
Req-3.3	Technology Dependent
Req-3.4	Technology Dependent

Req-4.1	RFC 8505
Req-4.2	RFC 8505
Req-4.3	[RFC6775]
Req-5.1	
Req-5.2	[AP-ND]
Req-5.3	
Req-5.4	
Req-5.5	[AP-ND]
Req-5.6	[Alternative-Ellip-Curve-Reps]
Req-5.7	[AP-ND]
Req-5.8	
Req-5.9	[AP-ND]
Req-6.1	RFC 8505
Req-6.2	RFC 8505
Req-7.1	
Req-7.2	
Req-7.3	
Req-7.4	

Table 8: Documents That Address Requirements

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, Warren Kumari, Benjamin Kaduk, Mirja Kuehlewind, Ben Campbell, Eric Rescorla, and Lorenzo Colitti for their various contributions and reviews. Also, many thanks to Thomas Watteyne for the world's first implementation of a 6LN that was instrumental to the early tests of the 6LR, 6LBR, and Backbone Router.

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, CA 95050
United States of America

Email: charliep@computer.org