6lo
Internet-Draft
Updates: 6775 (if approved)
Intended status: Standards Track
Expires: March 24, 2018

P. Thubert, Ed.
cisco
E. Nordmark

S. Chakrabarti

September 20, 2017

An Update to 6LoWPAN ND
draft-ietf-6lo-rfc6775-update-09

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.

Table of Contents

1. Introduction

The scope of this draft is an IPv6 Low Power Networks 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 such as:

- o Support for indicating mobility vs retry (T-bit)
- o Ease up requirement of registration for link-local addresses
- o Enhancement to Address Registration Option (ARO)
- o Permitting registration of target address
- o Clarification of support of privacy and temporary addresses

The applicability of 6LoWPAN ND registration is discussed in Section 2, and new extensions and updates to RFC 6775 are presented in Section 4. Considerations on Backward Compatibility, Security and Privacy are also elaborated upon in Section 7, Section 8 and in Section 9, respectively.

2. Applicability of Address Registration Options

The original purpose of the Address Registration Option (ARO) in the original 6LoWPAN ND specification is to facilitate duplicate address detection (DAD) for hosts as well as populate Neighbor Cache Entries (NCE) [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 registration can fail or become useless 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 which 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. However, the ability to return errors to address registrations is not intended to be used to restrict the ability of hosts to form and use addresses, as recommended in "Host Address Availability Recommendations" [RFC7934].

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

In the classical IPv6 ND [RFC4861], a router must have enough storage to hold neighbor cache entries for all the addresses to which it may forward. A router using 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. For this reason, the number of registrations supported by a 6LoWPAN Router (6LR) or 6LoWPAN Border Router (6LBR) must be clearly documented.

A network administrator should deploy adapted 6LR/6LBRs to support the number and type of devices in his network, based on the number of IPv6 addresses that those devices require and their renewal rate and behaviour.

3. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

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

- "Neighbor Discovery for IP version 6" [RFC4861],
- "IPv6 Stateless Address Autoconfiguration" [RFC4862],
- "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals" [RFC4919],
- "Neighbor Discovery Optimization for Low-power and Lossy Networks" [RFC6775] and
- "Multi-link Subnet Support in IPv6" [I-D.ietf-ipv6-multilink-subnets],

as well as the following terminology:

Backbone Link An IPv6 transit link that interconnects two or more Backbone Routers. It is expected to be of a relatively high speed compared to the LLN in order to support the trafic that is required to federate multiple segments of the potentially large LLN into a single IPv6 subnet. Also referred to as a to as a Backbone, a LLN Backbone, and a Backbone Network.

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

Extended LLN The aggregation of multiple LLNs as defined in RFC 4919 [RFC4919], interconnected by a Backbone Link via Backbone Routers, and forming a single IPv6 MultiLink Subnet.

Registration The process during which a wireless Node registers its address(es) with the Border Router so the 6BBR can serve as proxy for ND operations over the Backbone.

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

Registered Node The node for which the registration is performed, and which owns the fields in the EARO option.

Registering Node The node that performs the registration to the 6BBR, which may proxy for the registered node.

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

legacy and original vs. updated In the context of this specification, the terms "legacy" and "original" relate to the support of the RFC 6775 by a 6LN, a 6LR or a 6LBR, whereas the term "updated" refers to the support of this specification.

classical In the context of this specification, the term "classical" relates to the support of the IPv6 Neighbor Discovery (IPv6 ND) protocol as specified in RFC 4861 and RFC 4862. This specification does not deprecate the classical IPv6 ND Protocol.

4. Updating RFC 6775

This specification introduces the Extended Address Registration Option (EARO) based on the ARO as defined in RFC 6775 [RFC6775]; in particular a "T" flag is added that MUST be set is NS messages when this specification is used, and echoed in NA messages to confirm that the protocol is supported.

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

```
        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, it is RECOMMENDED to allow multiple registrations, including for privacy / temporary addresses, and provides new mechanisms to help clean up stale registration states as soon as possible.

A Registering Node SHOULD prefer registering to a 6LR that is found to support this specification, as discussed in Section 7.1, over a legacy one.

4.1. Extended Address Registration Option (EARO)

The Extended ARO (EARO) deprecates the ARO and is backward compatible with it. More details on backward compatibility can be found in Section 7.

The semantics of the ARO are modified as follows:

o The address that is being registered with a Neighbor Solicitation (NS) with an EARO is now the Target Address, as opposed to the Source Address as specified in RFC 6775 [RFC6775] (see Section 4.5). This change enables a 6LBR to use one of its addresses as source to 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 Unique ID in the EARO Option is no longer required to be a MAC address (see Section 4.3). This enables in particular the use of a Provable Temporary UID (PT-UID) as opposed to burn-in MAC address; the PT-UID provides an anchor trusted by the 6LR and 6LBR to protect the state associated to the node.

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 a new "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 Transaction ID (TID) is a sequence number that is incremented with each re-registration. The TID is used to detect the freshness of the registration request and useful 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 track the sequence of movements of a node in order to route to the current (freshest known) location of a moving node.

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

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 consider the comparison as if it has evaluated in such a way so as to give precedence to the sequence number that has most recently been observed to increment. Failing this, the node should consider the comparison as if it has evaluated in such a way so as to minimize the resulting changes to its own state.

4.3. Owner Unique ID

The Owner Unique ID (OUID) enables a duplicate address registration to be distinguished from a double registration or a movement. An ND message from the 6BBR over the Backbone that is proxied on behalf of a Registered Node must carry the most recent EARO option seen for that node. A NS/NA with an EARO and a NS/NA without a EARO thus represent different nodes; if they relate to a same target then an address duplication is likely.

With RFC 6775, the Owner Unique ID carries an EUI-64 burn-in address, which implies that duplicate EUI-64 addresses are avoided. With this specification, the Owner Unique ID is allowed to be extended to different types of identifier, as long as the type is clearly

indicated. For instance, the type can be a cryptographic string and used to prove the ownership of the registration as discussed in "Address Protected Neighbor Discovery for Low-power and Lossy Networks" [I-D.ietf-6lo-ap-nd].

In any fashion, it is recommended that the node stores the unique Id or the keys used to generate that ID in persistent memory. Otherwise, it will be prevented to re-register a same address after a reboot that would cause a loss of memory until the 6LBR times out the registration.

4.4. Extended Duplicate Address Messages

In order to map the new EARO content in the DAR/DAC messages, a new TID field is added to the Extended DAR (EDAR) and the Extended DAC (EDAC) messages as a replacement to a Reserved field, and an odd value of the ICMP Code indicates support for the TID, to transport the "T" flag.

In order to prepare for new extensions, and though no option had been earlier defined for the Duplicate Address messages, implementations SHOULD expect ND options after the main body, and SHOULD ignore them.

As for the EARO, the Extended Duplicate Address messages are backward compatible with the original versions, and remarks concerning backwards compatibility 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 inherited from RFC 6775, 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 a 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 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.

The reason for this change is to enable proxy-registrations on behalf of other nodes, for instance to enable a RPL root to register addresses on behalf of other LLN nodes, as discussed in Appendix B.4. In that case, the Registering Node MUST indicate its own address as source of the ND message and its MAC address in the Source Link-Layer Address Option (SLLAO), since it still expects to receive and route the packets. Since the Registered Address belongs to the Registered Node, that address is indicated in the Target Address field of the NS message.

With this convention, a TLLA option indicates the link-layer address of the 6LN that owns the address, whereas the SLLA Option in a NS message indicates that of the Registering Node, which can be the owner device, or a proxy.

The Registering Node is reachable from the 6LR, and is also the one expecting packets for the 6LN. Therefore, 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 the original 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 RFC 6775, this specification only requires that a Link-Local address is unique from the perspective of the nodes that use it to communicate (e.g. the 6LN and the 6LR in an NS/NA exchange). This simplifies the DAD process for Link-Local addresses, and there is no exchange of Duplicate Address messages between the 6LR and a 6LBR for Link-Local addresses.

According to RFC 6775, a 6LoWPAN Node (6LN) uses the an address being registered as the source of the registration message. This generates complexities in the 6LR to be able to cope with a potential duplication, in particular for global addresses.

To simplify this, a 6LN and a 6LR that conform this specification MUST always use Link-Local addresses as source and destination addresses for the registration NS/NA exchange. As a result, the registration is globally faster, and some of the complexity is removed.

In more details:

An exchange between two nodes using Link-Local addresses implies that they are reachable over one hop and that at least one of the 2 nodes acts as a 6LR. 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, from the standpoint of this 6LR, this Link-Local address is unique and the registration is acceptable. Conversely, it may possibly happen that two different 6LRs expose the same Link-Local address but different link-layer addresses. In that case, a 6LN may only interact with one of the 6LRs so as to avoid confusion in the 6LN neighbor cache.

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

It is desired that a 6LR does not need to modify its state associated to the Source Address of an NS(EARO) message. For that reason, when possible, it is RECOMMENDED to use an address that is already registered with a 6LR

When registering to a 6LR that conforms this specification, 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 already registered, 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 burn-in MAC address. An EARO option in the response NA indicates that the 6LR supports this specification.

Since there is no Duplicate Address exchange 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 MUST be placed in the NS(EARO) message as required in RFC 6775 [RFC6775].

A node needs to register its IPv6 Global Unicast IPv6 Addresses (GUAs) to a 6LR in order to establish global reachability for these

addresses via that 6LR. When registering with a 6LR that conforms this specification, a Registering Node does not use its GUA as Source Address, in contrast to a node that complies to RFC 6775 [RFC6775]. For non-Link-Local addresses, the Duplicate Address exchange MUST conform to RFC 6775, 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, which, as discussed in Section 4.6, 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 in a 6LR. 6LBRs and 6BBRs may store additional registration information in more complex data structures and use protocols that are out of scope of this document to keep them synchonized when they are distributed.

When its Neighbor Cache is full, a 6LR cannot accept a new registration. In that situation, the EARO is returned in a NA message with a Status of 2, and the Registering Node may attempt to register to another 6LR.

Conversely the registry in the 6LBR may be saturated, in which case the LBR cannot guarantee that a new address is effectively not a duplicate. In that case, the 6LBR replies to a EDAR message with a EDAC message that carries a Status code 9 indicating "6LBR Registry saturated", and the address stays in TENTATIVE state. Note: this code is used by 6LBRs instead of Status 2 when responding to a Duplicate Address message exchange and 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, deregister other addresses first to make room, or keep the address in TENTATIVE state and retry later.

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

A node that ceases to use an address SHOULD attempt to deregister that address from all the 6LRs to which it has registered the address, which is achieved using an NS(EARO) message with a Registration Lifetime of 0.

A node that moves away from a particular 6LR SHOULD attempt to deregister 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 of 3 "Moved" SHOULD be used to clean up the state in the previous location. For instance, the "Moved" status can be used by a 6BBR in a NA(EARO) message to indicate that the ownership of the proxy state on the Backbone was transferred to another 6BBR, as the consequence of a movement of the device. The receiver of the message SHOULD propagate the status down the chain towards the Registered node and clean up its state.

Upon receiving a 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, or an alternate protocol, indicating the null Registration Lifetime and the latest TID that this 6LR is aware of.

Upon the Extended DAR message, the 6LBR evaluates if this is the freshest TID it has received for that particular registry entry. If it is, then the entry is scheduled to be removed, and the EDAR is answered with a EDAC message bearing a Status of 0 "Success". If it is not the freshest, then a Status 3 "Moved" is returned instead, and the existing entry is conserved.

Upon timing out a registration, a 6LR removes silently its binding cache entry, and a 6LBR schedules its entry to be removed.

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 deregistered from one 6LR and did not register yet to a new one, or the new registration did not reach yet the 6LBR due to propagation delays in the network. Once the DELAY time is passed, the 6LBR removes silently its entry.

5. Detecting Enhanced ARO Capability Support

The "Generic Header Compression for IPv6 over 6LoWPANs" [RFC7400] introduces the 6LoWPAN Capability Indication Option (6CIO) to indicate a node's capabilities to its peers. This specification extends the format defined in RFC 7400 to signal the support for EARO, as well as the node's capability to act as a 6LR, 6LBR and 6BBR.

With RFC 7400, the 6CIO is typically sent in a Router Solicitation (RS) message. When used to signal the capabilities above per this

specification, the 6CIO is typically present in Router Advertisement (RA) messages but can also be present in RS, Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages.

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. Enhanced Address Registration Option (EARO)

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

The Enhanced Address Registration Option (EARO) is intended to be used as a replacement to the ARO option within Neighbor Discovery NS and NA messages between a 6LN and its 6LR. Conversely, the Extended Duplicate Address messages, EDAR and EDAC, are to be used in replacement of the DAR and DAC messages so as to transport the new information between 6LRs and 6LBRs across LLNs meshes such as 6TiSCH networks.

An NS message with an EARO option is a registration if and only if it also carries an SLLAO option. The EARO option also used in NS and NA messages between Backbone Routers over the Backbone link to sort out the distributed registration state; in that case, it does not carry the SLLAO option and is not confused with a registration.

When using the EARO option, the address being registered is found in the Target Address field of the NS and NA messages. This differs from 6LoWPAN ND RFC 6775 [RFC6775] which specifies that the address being registered is the source of the NS.

The EARO extends the ARO and is recognized by the "T" flag set. The format of the EARO option 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 = 2   |    Status     |   Reserved    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |  Reserved  |T|     TID       |     Registration Lifetime     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    +         Owner Unique ID   (EUI-64 or equivalent)              +
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: EARO

Option Fields

Type: 33

Length: 8-bit unsigned integer. The length of the option in units of 8 bytes. Always 2.

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 RFC 6775 [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" should be used.
3	Moved: The registration fails 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 OUI 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 OUI collision.
4	Removed: The binding state was removed. This may be placed in an asynchronous NS(ARO) message, or as the rejection of a proxy registration to a Backbone Router
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 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.

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

TID: 1-byte integer; a transaction id that is maintained by the node and incremented with each transaction. The node SHOULD maintain the TID in a persistent storage.

Registration Lifetime: 16-bit integer; expressed in minutes. 0 means that the registration has ended and the associated state should be removed.

Owner Unique Identifier (OUI): A globally unique identifier for the node associated. This can be the EUI-64 derived IID of an interface, or some provable ID obtained cryptographically.

6.2. Extended Duplicate Address Message Formats

The Duplicate Address Request (DAR) and the Duplicate Address Confirmation (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.

The Duplicate Address Messages are extended to adapt to the Extended ARO 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     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+          Owner Unique ID   (EUI-64 or equivalent)             +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                       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 odd value of the ICMP Code indicates that the TID field is present and obeys this specification.

TID: 1-byte integer; same definition and processing as the TID in the EARO option as defined in Section 6.1.

Owner Unique Identifier (OUI): 8 bytes; same definition and processing as the OUI in the EARO option as defined in Section 6.1.

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

This specification defines a number of capability bits in the 6CIO that was introduced by RFC 7400 for use in IPv6 ND RA messages.

Routers that support this specification SHOULD set the "E" flag and 6LN SHOULD favor 6LR routers that support this specification over those that do not. Routers that are capable of acting as 6LR, 6LBR and 6BBR SHOULD set the "L", "B" and "P" flags, respectively. In particular, the function 6LR is usually collocated with that of 6LBR.

Those flags are not mutually exclusive and if a router is capable of running multiple functions, it SHOULD set all the related flags.

```
 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        |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, it can take registrations.

B: Node is a 6LBR.

P: Node is a 6BBR, proxying for nodes on this link.

E: This specification is supported and applied.

7. Backward Compatibility

7.1. Discovering the capabilities of an ND peer

7.1.1. Using the "E" Flag in the 6CIO Option

If the 6CIO is used in an ND message and the sending node supports this specification, then the "E" Flag MUST be set.

A router that supports this specification SHOULD indicate that with a 6CIO Option, but this might not be practical if the link-layer MTU is too small.

If the Registering Node (RN) receives a CIO in a Router Advertisement message, then the setting of the "E" Flag indicates whether or not this specification is supported. RN SHOULD favor a router that supports this specification over those that do not.

7.1.2. Using the "T" Flag in the EARO

One alternate way for a 6LN to discover the router's capabilities to first register a Link Local address, placing the same address in the Source and Target Address fields of the NS message, and setting the "T" Flag. The node may for instance register an address that is based on EUI-64. For such address, DAD is not required and using the SLLAO option in the NS is actually more consistent with existing ND specifications such as the "Optimistic Duplicate Address Detection (DAD) for IPv6" [RFC4429].

Once that first registration is complete, the node knows from the setting of the "T" Flag in the response whether the router supports this specification. If support is verified, the node may register other addresses that it owns, or proxy-register addresses on behalf some another node, indicating those addresses being registered in the Target Address field of the NS messages, while using one of its own previously registered addresses as source.

A node that supports this specification MUST always use an EARO as a replacement to an ARO in its registration to a router. This is harmless since the "T" flag and TID field are reserved in RFC 6775 are ignored by a legacy router. A router that supports this specification answers an ARO with an ARO and answers an EARO with an EARO.

This specification changes the behavior of the peers in a registration flows. To enable backward compatibility, a 6LB that registers to a 6LR that is not known to support this specification MUST behave in a manner that is compatible with RFC 6775. A 6LN can achieve that by sending a NS(EARO) message with a Link-Local Address used as both Source and Target Address, as described in Section 4.6. Once the 6LR is known to support this specification, the 6LN MUST obey this specification.

7.2. Legacy 6LoWPAN Node

A legacy 6LN will use the Registered Address as source and will not use an EARO option. An updated 6LR MUST accept that registration if it is valid per RFC 6775, and it MUST manage the binding cache accordingly. The updated 6LR MUST then use the original Duplicate Address messages as specified in RFC 6775 to indicate to the 6LBR that the TID is not present in the messages.

The main difference with RFC 6775 is that Duplicate Address exchange for DAD is avoided for Link-Local addresses. In any case, the 6LR SHOULD use an EARO in the reply, and may use any of the Status codes defined in this specification.

7.3. Legacy 6LoWPAN Router

The first registration by an updated 6LN MUST be for a Link-Local address, using that Link-Local address as source. A legacy 6LR will not make a difference and accept -or reject- that registration as if the 6LN was a legacy node.

An updated 6LN will always use an EARO option in the registration NS message, whereas a legacy 6LR will always reply with an ARO option in the NA message. So from that first registration, the updated 6LN can figure whether the 6LR supports this specification or not.

After detecting a legacy 6LR, an updated 6LN may attempt to find an alternate 6LR that is updated. In order to be backward compatible, after detecting that a 6LR is legacy, the 6LN MUST adhere to RFC 6775 in future protocol exchanges with that 6LR, and source the packet with the Registered Address.

Note that the updated 6LN SHOULD use an EARO in the request regardless of the type of 6LR, legacy or updated, which implies that the "T" flag is set.

If an updated 6LN moves from an updated 6LR to a legacy 6LR, the legacy 6LR will send a legacy DAR message, which can not be compared with an updated one for freshness.

Allowing legacy 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 legacy 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. Legacy 6LoWPAN Border Router

With this specification, the Duplicate Address messages are extended to transport the EARO information. Similarly to the NS/NA exchange, updated 6LBR devices always use the Extended Duplicate Address messages and all the associated behavior so they can amlways be differentiated from legacy ones.

Note that a legacy 6LBR will accept and process an EDAR message as if it was an original one, so the original support of DAD is preserved.

8. Security Considerations

This specification extends RFC 6775 [RFC6775], and the security section of that draft also applies to this as well. In particular, it is expected that the link layer is sufficiently protected to prevent a rogue access, either by means of physical or IP security on the Backbone Link and link layer cryptography on the LLN.

This specification also expects that the LLN MAC provides secure unicast to/from the Backbone Router and secure Broadcast from the Backbone Router in a way that prevents tempering with or replaying the RA messages.

This specification recommends to using privacy techniques (see Section 9, and protection 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 OUID.

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 registration, which effectively denies the requesting a 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 deregister that address from all the 6LRs to which it is registered. The flow is propagated to the 6LBR when needed, and a sequence number is used to make sure that only the freshest command is acted upon.

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.

- The router (6LR or 6LBR) SHOULD be configurable so as to limit the number of addresses that can be registered by a single node, as identified at least by MAC address and preferably by security credentials. When that maximum is reached, the router should use a Least-Recently-Used (LRU) logic so as to clean up the addresses that were not used for the longest time, keeping at least one Link-Local address, and attempting to keep one or more stable addresses if such can be recognized, e.g. from the way the IID is formed or because they are used over a much longer time span than other (privacy, shorter-lived) addresses. The address lifetimes SHOULD be individually configurable.

- 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 a LLN is a more capable node then 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 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.

9. Privacy Considerations

As indicated in section Section 2, this protocol does not aim at limiting the number of IPv6 addresses that a device can form. 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] and "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 such addresses. All implementations and deployment must consider the option of privacy addresses in their own environment. Also future specifications involving 6LOWPAN Neighbor Discovery should consult "Recommendation on Stable IPv6 Interface Identifiers" [RFC8064] for default interface identifaction.

10. IANA Considerations

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 7 for the "T" flag in 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..6	Unassigned	
7	"T" Flag	RFC This

Table 2: new ARO Flags

10.2. ICMP Codes

IANA is requested to create a new entry in the ICMPv6 "Code" Fields subregistry of the Internet Control Message Protocol version 6 (ICMPv6) Parameters for the ICMP codes related to the ICMP type 157 and 158 Duplicate Address Request (shown in Table 3) and Confirmation (shown in Table 4), respectively, as follows:

New entries for ICMP types 157 DAR message

Code	Name	Reference
0	Original DAR message	RFC 6775
1	Extended DAR message	RFC This

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	RFC This

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	RFC This
4	Removed	RFC This
5	Validation Requested	RFC This
6	Duplicate Source Address	RFC This
7	Invalid Source Address	RFC This
8	Registered Address topologically incorrect	RFC This
9	6LBR registry saturated	RFC This
10	Validation Failed	RFC This

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
11	6LR capable (L bit)	RFC This
12	6LBR capable (B bit)	RFC This
13	6BBR capable (P bit)	RFC This
14	EARO support (E bit)	RFC This

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 Charlie Perkins for his in-depth reviews and constructive suggestions, as well as to Sedat Gormus, Rahul Jadhav and Lorenzo Colitti for their various contributions and reviews. Also many thanks to Thomas Watteyne for his early 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>.

[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>.

[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>.

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.ietf-6lo-ap-nd]
Sarikaya, B., Thubert, P., and M. Sethi, "Address Protected Neighbor Discovery for Low-power and Lossy Networks", draft-ietf-6lo-ap-nd-02 (work in progress), May 2017.

[I-D.ietf-6lo-backbone-router]
Thubert, P., "IPv6 Backbone Router", draft-ietf-6lo-backbone-router-04 (work in progress), July 2017.

[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-07 (work in progress), June 2017.

[I-D.ietf-6tisch-architecture]
Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", draft-ietf-6tisch-architecture-12 (work in progress), August 2017.

[I-D.ietf-bier-architecture]
Wijnands, I., Rosen, E., Dolganow, A., Przygienda, T., and S. Aldrin, "Multicast using Bit Index Explicit Replication", draft-ietf-bier-architecture-08 (work in progress), September 2017.

[I-D.ietf-ipv6-multilink-subnets]
Thaler, D. and C. Huitema, "Multi-link Subnet Support in IPv6", draft-ietf-ipv6-multilink-subnets-00 (work in progress), July 2002.

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

[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>.

[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>.

[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>.

12.3. External Informative References

[IEEEstd802154]
IEEE, "IEEE Standard for Low-Rate Wireless Networks", IEEE Standard 802.15.4, DOI 10.1109/IEEESTD.2016.7460875, <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

This specification extends 6LoWPAN ND to sequence the registration and serves the requirements expressed 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.

In the context of the the TimeSlotted Channel Hopping (TSCH) mode of 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 Wi-Fi, BLUETOOTH(R) 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 the Backbone, effectively providing a solution to the requirements expressed in Appendix B.4.

"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 classical ND ([RFC4861], [RFC4862]) and plague the wireless medium. This serves scalability requirements listed in Appendix B.6.

Appendix B. Requirements

This section lists requirements that were discussed at 6lo for an update to 6LoWPAN ND. This specification meets most of them, but those listed in Appendix B.5 which are deferred to a different specification such as [I-D.ietf-6lo-ap-nd], and those related to multicast.

B.1. Requirements Related to Mobility

Due to the unstable nature of LLN links, even in a LLN of immobile nodes a 6LN may change its point of attachment to a 6LR, say 6LR-a, 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.

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

Req1.2: For that purpose, the protocol MUST enable to differentiate 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 capable to register its Address to multiple 6LRs, and this, concurrently.

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 a LLN can be based on RPL, which is the routing protocol that was defined at the IETF for this particular purpose. Other routing protocols than RPL are also considered by Standard Defining Organizations (SDO) on the basis of the expected network characteristics. It is required that a 6LoWPAN Node attached via ND to a 6LR would need to participate in the selected routing protocol to obtain reachability via the 6LR.

Next to 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 [I-D.ietf-bier-architecture] proposes an optimized technique to enable multicast in a LLN with a very limited requirement for routing state in the nodes.

Related requirements are:

Req2.1: The ND registration method SHOULD be extended in such a fashion that the 6LR MAY advertise the Address of a 6LoWPAN Node over 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 [RFC6550] section 6.4, 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 MAC-64 address. At this point, the 6lo Working Group is extending the 6LoWPAN Header Compression (HC) [RFC6282] technique to other link types ITU-T G.9959 [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 IEEE1901.2 Narrowband Powerline Communication Networks [I-D.popa-6lo-6loplc-ipv6-over-ieee19012-networks] and BLUETOOTH(R) Low Energy [RFC7668].

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 Neighbour 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 classical ND on a Backbone 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 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, in 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 a 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 impossible.

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

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 6LoWPAN Node 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 and more hops.

Authors' Addresses

Pascal Thubert (editor)
Cisco Systems, Inc
Sophia Antipolis
FRANCE

Email: pthubert@cisco.com

Erik Nordmark
Santa Clara, CA
USA

Email: nordmark@sonic.net

Samita Chakrabarti
San Jose, CA
USA

Email: samitac.ietf@gmail.com