6lo
Internet-Draft
Updates: 6775 (if approved)
Intended status: Standards Track
Expires: December 23, 2017

P. Thubert, Ed.
cisco
E. Nordmark
S. Chakrabarti

June 21, 2017

An Update to 6LoWPAN ND
draft-ietf-6lo-rfc6775-update-06

Abstract

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

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 23, 2017.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must

include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 3
2. Applicability of Address Registration Options 3
3. Terminology 4
4. Updating RFC 6775 5
4.1. Extended Address Registration Option 6
4.2. Transaction ID 6
4.3. Owner Unique ID 7
4.4. Registering the Target Address 7
4.5. Link-Local Addresses and Registration 8
4.6. Maintaining the Registration States 9
5. Detecting Enhanced ARO Capability Support 10
6. Updated ND Options 11
6.1. The Enhanced Address Registration Option (EARO) 11
6.2. New 6LoWPAN capability Bits in the Capability Indication Option 14
7. Backward Compatibility 14
7.1. Discovering the capabilities of an ND peer 14
7.1.1. Using the E Flag in the CIO 14
7.1.2. Using the T Flag in the EARO 15
7.2. Legacy 6LoWPAN Node 15
7.3. Legacy 6LoWPAN Router 16
7.4. Legacy 6LoWPAN Border Router 16
8. Security Considerations 16
9. Privacy Considerations 18
10. IANA Considerations 18
11. Acknowledgments 20
12. References 20
12.1. Normative References 20
12.2. Informative References 21
12.3. External Informative References 23
Appendix A. Applicability and Requirements Served 24
Appendix B. Requirements 24
B.1. Requirements Related to Mobility 25
B.2. Requirements Related to Routing Protocols 25
B.3. Requirements Related to the Variety of Low-Power Link types 26
B.4. Requirements Related to Proxy Operations 27
B.5. Requirements Related to Security 27
B.6. Requirements Related to Scalability 28
Authors' Addresses 29

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 RFC 6775 "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)" [RFC6775] to enable additional capabilities such as:

* Support the indication of mobility vs retry (T-bit)

* Ease up requirement of registration for link-local addresses

* Introducing Enhancement to Address Registration Option (ARO)

* Permitting regitration of target address

* Clarification of support of privacy and temporary addresses

The following sections will discuss applicability of 6LoWPAN ND registration, new extensions and updates to RFC 6775. Finally, we will discuss how the extensions of registration framework can be useful for a scenario such as Backbone router(6BBR) proxy ND operations.

2. Applicability of Address Registration Options

The purpose of the Address Registration Option (ARO) [RFC6775] and of the Extended ARO (EARO) that is introduced in this document is to facilitate duplicate address detection (DAD) for hosts and pre-populate Neighbor Cache Entries (NCE) [RFC4861] in the routers to reduce the need for sending 'multicast neighbor solicitations' which may be harmful in low power constrained nodes networks where multicast is most often treated as broadcasts.

In some cases the address registration can fail or becomes useless for reasons other than a duplicate address. Examples are the router having run out of space, a registration bearing a stale sequence number (e.g. denoting a movement of the host after this registration was placed), a host misbehaving and attempting to register an invalid address such as the unspecified address [RFC4291], or the 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 6LR, depending on the returned error.

However, the ability to return errors to address registrations MUST NOT be used to restrict the ability of hosts to form and use addresses as recommended in "Host Address Availability

Recommendations" [RFC7934]. In particular, this is needed for enhanced privacy, which implies that each host will register a multiplicity of address as part mechanisms like "Privacy Extensions for Stateless Address Autoconfiguration (SLAAC) in IPv6" [RFC4941]. This implies that the capabilities of 6LR and 6LBRs in terms of number of registrations must be clearly announced in the router documentation, and that 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.

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 this additional terminology:

Backbone This is an IPv6 transit link that interconnects 2 or more Backbone Routers. It is expected to be deployed as a high speed Backbone in order to federate a potentially large set of LLNS. Also referred to as a LLN Backbone or Backbone network.

Backbone Router An IPv6 router that federates the LLN using a Backbone link as a Backbone. A 6BBR acts as a 6LoWPAN Border Routers (6LBR) and an Energy Aware Default Router (NEAR).

Extended LLN This is 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 proxy ND for it over the Backbone.

Binding The state in the 6BBR that associates an IP address with a MAC address, a port and some other information about the node that owns the IP address.

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

Registering Node The node that performs the registration to the 6BBR, either for one of its own addresses, in which case it is Registered Node and indicates its own MAC Address as Source Link Layer Address (SLLA) in the NS(EARO), or on behalf of a Registered Node that is reachable over a LLN mesh. In the latter 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). Otherwise, it is expected that the Registered Device is reachable over a Route-Over mesh from the Registering Node, in which case the SLLA in the NS(ARO) is that of the Registering Node, which causes it to attract the packets from the 6BBR to the Registered Node and route them over the LLN.

Registered Address The address owned by the Registered Node node that is being registered.

4. Updating RFC 6775

This specification extends the Address Registration Option (ARO) 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 echo'ed in NA messages to confirm that the protocol effectively supported. Support for this specification can thus be inferred from the presence of the Extended ARO ("T" flag set) in ND messages.

In order to support various types of link layers, this specification also adds recommendation 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 that supports this specification will favor registering to a 6LR that indicates support for this specification over that of RFC 6775 [RFC6775].

4.1. Extended Address Registration Option

This specification extends the ARO option that is used for the process of address registration. The new ARO is referred to as Extended ARO (EARO), and its semantics are modified as follows:

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 4.4 for more). This change enables a 6LBR to use an address of his 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 Duplicate Address Detection (DAD) is complete.

The Unique ID in the EARO option does no more have to be a MAC address (see Section 4.3 for more). This enables in particular the use of a Provable Temporary UID (PT-UID) as opposed to burn-in MAC address, the PT-UID providing a trusted anchor by the 6LR and 6LBR to protect the state associated to the node.

The specification introduces a Transaction ID (TID) field in the EARO (see Section 4.2 for more on TID). The TID MUST be provided by a node that supports this specification and a new T flag MUST be set to indicate so. The T bit can be used to determine whether the peer supports this specification.

Finally, this specification introduces a number of new Status codes to help diagnose the cause of a registration failure (more in Table 1).

4.2. Transaction ID

The specification expects that the Registered Node can provide a sequence number called Transaction ID (TID) 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 supporting the same large 6LOWPAN, as is the case for backbone routers (BBR).

For example, when a Registered Node is registered with multiple BBRs in parallel, it is expected that the same TID is used, to enable the 6BBRs to correlate the registrations as being a single one, and differentiate that situation from a movement.

Thus TID could be tracked to follow the sequence of mobility of a node. The details protocols of mobility verification by the border routers is not part of this specification.

4.3. Owner Unique ID

The Owner Unique ID (OUID) enables to differentiate a real duplicate address registration 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 and if they relate to a same target then they reflect an address duplication. The Owner Unique ID can be as simple as a EUI-64 burn-in address, if duplicate EUI-64 addresses are avoided.

Alternatively, the unique ID can be a cryptographic string that can can be 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 after a reboot that would cause a loss of memory until the Backbone Router times out the registration.

4.4. Registering the Target Address

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 in Route-Over meshes, for instance to enable that a RPL root registers addresses on behalf LLN nodes that are deeper in a 6TiSCH mesh, 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 get the packets and route them down the mesh. But the Registered Address belongs to another node, the Registered Node, and 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.

Since the Registering Node is the one that has reachability with the 6LR, and is the one expecting packets for the 6LN, it makes sense to maintain compatibility with RFC 6775 [RFC6775], and it is REQUIRED

that an SLLA Option is always placed in a registration NS(EARO) message.

4.5. 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 [RFC6775], this specification only requires that a Link-Local address is unique from the perspective of the peering nodes. This simplifies the Duplicate Address Detection (DAD) for Link-Local addresses, and there is no Duplicate Address Request (DAR) / Duplicate Address Confirmation (DAC) exchange between the 6LR and a 6LBR for Link-Local addresses.

Additionally, RFC 6775 [RFC6775] requires that a 6LoWPAN Node (6LN) uses 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 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 a same Link-Local address but different link-layer addresses. In that case, a 6LN may only interact with one of the 6LR so as to avoid confusion in the 6LN neighbor cache.

The DAD process between the 6LR and a 6LoWPAN Border Router (6LBR), which is based on a Duplicate Address Request (DAR) / Duplicate Address Confirmation (DAC) exchange as described in RFC 6775 [RFC6775], 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 DAR/DAC 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 (GUA) to a 6LR in order to obtain a global reachability for these addresses via that 6LR. As opposed to a node that complies to RFC 6775 [RFC6775], a Registering Node registering a GUA does not use that GUA as Source Address for the registration to a 6LR that conforms this specification. The DAR/DAC exchange MUST take place for non-Link-Local addresses as prescribed by RFC 6775 [RFC6775].

4.6. 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 4.5, 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 6LBR cannot guarantee that a new address is effectively not a duplicate. In that case, the 6LBR replies to a DAR message with a DAC message that carries a Status code 9 indicating "6LBR Registry saturated", and the address stays in TENTATIVE state.

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.

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 DAR/DAC 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 DAR message, the 6LBR evaluates if this is the freshest EARO it has received for that particular registry entry. If it is, then the entry is scheduled to be removed, and the DAR is answered with a DAC message bearing a Status of 0 "Success". If it is not the freshest, then a Status 2 "Moved" is returned instead, and the existing entry is conserved. The 6LBR SHOULD conserve the address 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.

5. Detecting Enhanced ARO Capability Support

The nodes and routers in a network may be mixed and if a node wants to use EARO feature for address registration, it has to find a router which supports it. Thus all implementations with EARO option MUST provide the capability detection method using 6CIO option to support both types of registrations (ARO and EARO) as described in later sections. Moreover, any new implementation of 6LOWPAN is also RECOMMENDED to support 6LoWPAN Capability Indication option(6CIO)in general.

RFC 7400 [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 capability to act as a 6LR, 6LBR and 6BBR.

With RFC 7400 [RFC7400], the 6CIO is typically sent Router Solicitation (RS) messages. When used to signal the capabilities above per this specification, the 6CIO is typically present Router Advertisement (RA) messages but can also be present in RS, Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages.

6. Updated ND Options

This specification does not introduce new options, but it modifies existing ones and updates the associated behaviors as follow:

6.1. The Enhanced Address Registration Option (EARO)

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 LLN node and its 6LoWPAN Router (6LR), as well as in Duplicate Address Request (DAR) and the Duplicate Address Confirmation (DAC) messages between 6LRs and 6LBRs in 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 AERO option also used in NS and NA messages between Backbone Routers over the Backbone link to sort out the distributed registration state, and in that case, it does not carry the SLLAO option and is not confused with a registration.

The EARO extends the ARO and is recognized by the "T" flag set.

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 format of the EARO option is as follows:

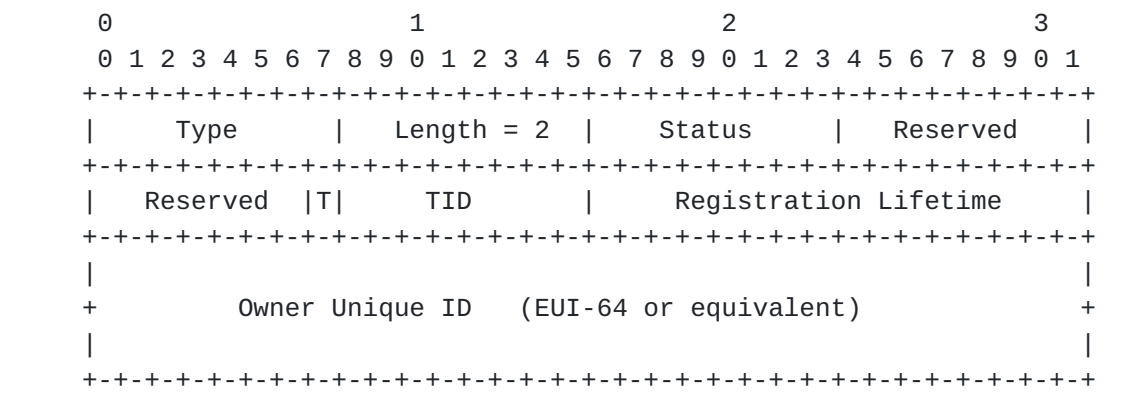


Figure 1: EARO

Option Fields

Type: 33

Length: 8-bit unsigned integer.

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.

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. it is recommended that the node maintains 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.

Value	Description
0..2	See RFC 6775 [RFC6775]. Note that 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	Proof 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 time out of a lifetime, or a movement. The receiver of the NA is the device that has performed a registration that is now stale and it should clean up its state.
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.
10	Incorrect proof: The proof of ownership of the registered address is not correct.

Table 1: EARO Status

Note: the code "6LBR Registry saturated" is used by 6LBRs instead of Status 2 when responding to a DAR/DAC 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.

6.2. New 6LoWPAN capability Bits in the Capability Indication Option

This specification defines a number of capability bits in the CIO that was introduced by RFC 7400 [RFC7400].

Support for this specification is indicated by setting the "E" flag in a CIO option. Routers that are capable of acting as 6LR, 6LBR and 6BBR SHOULD set the L, B and P flags, respectively.

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

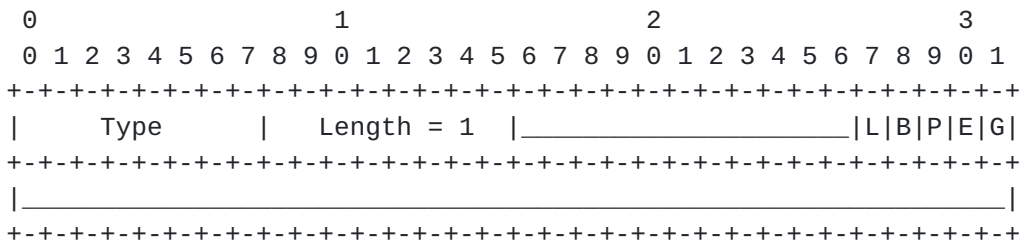


Figure 2: New capability Bits L, B, P, E in the CIO

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 CIO

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

It is RECOMMENDED that a router that supports this specification indicates so with a CIO option, but this might not be practical if the link-layer MTU is too small.

If the Registering Node receives a CIO in a RA, then the setting of the E" Flag indicates whether or not this specification is supported.

A node which does not implement this draft or parse 6CIO option, MUST ignore the packet and the sender of option SHOULD use legacy registration method according to RFC 6775 [RFC6775] after a timeout period.

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 amenable 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 this 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, already 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 [RFC6775] are ignored by a legacy router. A router that supports this specification answers to an ARO with an ARO and to an EARO with an EARO.

This specification changes the behavior of the peers in a registration flows. To enable backward compatibility, a node that registers to a router that is not known to support this specification MUST behave as prescribed by RFC 6775. Once the router is known to support this specification, the node 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. In order to be backward compatible, an updated 6LR needs to accept that registration if it is valid per the RFC 6775 [RFC6775] specification, and manage the binding cache accordingly.

The main difference with RFC 6775 is that DAR/DAC exchange for DAD may be avoided for Link-Local addresses. Additionally, 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 a an updated 6LN is for a Link-Local address, using that Link-Local address as source. A legacy 6LN will not makes 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 6LN will always areply 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.

When facing a legacy 6LR, an updated 6LN may attempt to find an alternate 6LR that is updated. In order to be backward compatible, based on the discovery that a 6LR is legacy, the 6LN needs to fallback to legacy behavior and source the packet with the Registered Address.

The main difference is that the updated 6LN SHOULD use an EARO in the request regardless of the type of 6LN, legacy or updated

7.4. Legacy 6LoWPAN Border Router

With this specification, the DAR/DAC transports an EARO option as opposed to an ARO option. As described for the NS/NA exchange, devices that support this specification always use an EARO option and all the associated behavior.

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 (more in section 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 4.6 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 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.

- 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 homogeneous with 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.

- Administrators should take great care to deploy adequate numbers of 6LR 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.

When the ownership of the OUID cannot be assessed, this specification limits the cases where the OUID and the TID are multicasted, and obfuscates them in responses to attempts to take over an address.

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 recognizes that use of EUI-64 for forming the Interface ID in the Link-Local address 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] addresses 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 create a new subregistry for "ARO Flags" under the "Internet Control Message Protocol version 6 (ICMPv6) Parameters". 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" [RFC5226]. 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) Parameters"

ARO Status	Description	Document
0..6	Unassigned	
7	"T" Flag	RFC This

Table 2: new ARO Flags

IANA is requested to make additions to existing registries as follows:

Address Registration Option Status Values Registry

ARO Status	Description	Document
3	Moved	RFC This
4	Removed	RFC This
5	Proof 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	Incorrect proof	RFC This

Table 3: New ARO Status values

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 4: New 6LoWPAN capability Bits

11. Acknowledgments

Kudos to Eric Levy-Abegnoli who designed the First Hop Security infrastructure at Cisco.

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, <http://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, <http://www.rfc-editor.org/info/rfc4291>.

[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, <http://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, <http://www.rfc-editor.org/info/rfc4862>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc7400>.

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-03 (work in progress), January 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-11 (work in progress), January 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-07 (work in progress), June 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.

[RFC3610] Whiting, D., Housley, R., and N. Ferguson, "Counter with CBC-MAC (CCM)", RFC 3610, DOI 10.17487/RFC3610, September 2003, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc3971>.

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

[RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006, <http://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, <http://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, <http://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, <http://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, <http://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, <http://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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc8064>.

[RFC8065] Thaler, D., "Privacy Considerations for IPv6 Adaptation-Layer Mechanisms", RFC 8065, DOI 10.17487/RFC8065, February 2017, <http://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, <http://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, <http://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/>.

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