

6lo
Internet-Draft
Updates: [6775](#) (if approved)
Intended status: Standards Track
Expires: May 18, 2018

B. Sarikaya
P. Thubert
Cisco
M. Sethi
Ericsson
November 14, 2017

Address Protected Neighbor Discovery for Low-power and Lossy Networks
draft-ietf-6lo-ap-nd-04

Abstract

This document defines an extension to 6LoWPAN Neighbor Discovery [RFC 6775](#). Nodes supporting this extension compute a cryptographic Owner Unique Interface ID and associate it with one or more of their Registered Addresses. Once an address is registered with a Cryptographic ID, only the owner of that ID can modify the anchor state information of the Registered Address, and Source Address Validation can be enforced.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

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

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

This Internet-Draft will expire on May 18, 2018.

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 (<https://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	2
2.	Terminology	4
3.	Updating RFC 6775	4
4.	New Fields and Options	5
4.1.	New Crypto-ID	5
4.2.	Updated EARO	6
4.3.	New Crypto-ID Parameters Option	7
5.	Protocol Overview	9
5.1.	Protocol Scope	9
5.2.	Protocol Flows	10
5.3.	Multihop Operation	12
6.	Security Considerations	12
7.	IANA considerations	13
7.1.	Crypto Type Registry	13
8.	Acknowledgements	14
9.	References	14
9.1.	Normative References	14
9.2.	Informative references	14
Appendix A.	Requirements Addressed in this Document	16
	Authors' Addresses	17

[1.](#) Introduction

"Neighbor Discovery Optimizations for 6LoWPAN networks" [[RFC6775](#)] (6LoWPAN ND) adapts the classical IPv6 ND protocol [[RFC4861](#)][[RFC4862](#)] (IPv6 ND) for operations over a constrained low-power and lossy network (LLN). In particular, 6LoWPAN ND introduces a unicast host address registration mechanism that contributes to reduce the use of multicast messages that are present in the classical IPv6 ND protocol. 6LoWPAN ND defines a new Address Registration Option (ARO) that is carried in the unicast Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages between the 6LoWPAN Node (6LN) and the 6LoWPAN Router (6LR). Additionally, it also defines the Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC) messages between the 6LR and the 6LoWPAN Border Router (6LBR). In LLN networks, the 6LBR is the central repository of all the registered addresses in its domain.

The registration mechanism in 6LoWPAN ND [[RFC6775](#)] prevents the use of an address if that address is already present in the subnet (first

come first serve). In order to validate address ownership, the registration mechanism enables the 6LR and 6LBR to validate claims for a registered address with an associated Owner Unique Interface Identifier (OUI). 6LoWPAN ND specifies that the OUI is derived from the MAC address of the device (EUI-64), which can be spoofed. Therefore, any node connected to the subnet and aware of a registered-address-to-OUI mapping could effectively fake the OUI, steal the address and redirect traffic for that address towards a different 6LN. The "Update to 6LoWPAN ND" [\[I-D.ietf-6lo-rfc6775-update\]](#) defines an Extended ARO (EARO) option that allows to transport alternate forms of OUIs, and is a prerequisite for this specification.

According to this specification, a 6LN generates a cryptographic ID (Crypto-ID) and places it in the OUI field in the registration of one (or more) of its addresses with the 6LR(s) that the 6LN uses as default router(s). Proof of ownership of the cryptographic ID (Crypto-ID) is passed with the first registration to a given 6LR, and enforced at the 6LR, in a new Crypto-ID Parameters Option (CIPO). The 6LR validates ownership of the cryptographic ID upon the creation of a registration state, or a change in the anchor information, such as Link-Layer Address and associated Layer-2 cryptographic material.

The protected address registration protocol proposed in this document enables the enforcement of Source Address Validation (SAVI) [\[RFC7039\]](#), which ensures that only the correct owner uses a registered address in the source address field in IPv6 packets. Consequently, a 6LN that sources a packet has to use a 6LR to which the source address of the packet is registered to forward the packet. The 6LR maintains state information for the registered address, including the MAC address, and a link-layer cryptographic key associated with the 6LN. In SAVI-enforcement mode, the 6LR allows only packets from a connected Host if the connected Host owns the registration of the source address of the packet.

The 6lo adaptation layer framework ([\[RFC4944\]](#), [\[RFC6282\]](#)) expects that a device forms its IPv6 addresses based on Layer-2 address, so as to enable a better compression. This is incompatible with "Secure Neighbor Discovery (SEND)" [\[RFC3971\]](#) and "Cryptographically Generated Addresses (CGAs)" [\[RFC3972\]](#), which derive the Interface ID (IID) in the IPv6 addresses from cryptographic material. "Privacy Considerations for IPv6 Address Generation Mechanisms" [\[RFC7721\]](#) places additional recommendations on the way addresses should be formed and renewed.

This document specifies that a device may form and register addresses at will, without a constraint on the way the address is formed or the number of addresses that are registered in parallel. It enables to

protect multiple addresses with a single cryptographic material and to send the proof only once to a given 6LR for multiple addresses and refresher registrations.

2. Terminology

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

Readers are expected to be familiar with all the terms and concepts that are discussed in [\[RFC3971\]](#), [\[RFC3972\]](#), [\[RFC4861\]](#), [\[RFC4919\]](#), [\[RFC6775\]](#), and [\[I-D.ietf-6lo-backbone-router\]](#) which proposes an evolution of [\[RFC6775\]](#) for wider applicability.

This document defines Crypto-ID as an identifier of variable size which in most cases is 64 bits long. It is generated using cryptographic means explained later in this document [Section 4.1](#). "Elliptic Curves for Security" [\[RFC7748\]](#) and "Edwards-Curve Digital Signature Algorithm (EdDSA)" [\[RFC8032\]](#) provides information on Elliptic Curve Cryptography (ECC) and a (twisted) Edwards curve, Ed25519, which can be used with this specification. "Alternative Elliptic Curve Representations" [\[I-D.struik-lwip-curve-representations\]](#) provides additional information on how to represent Montgomery curves and (twisted) Edwards curves as curves in short-Weierstrass form and illustrates how this can be used to implement elliptic curve computations using existing implementations that already implement, e.g., ECDSA and ECDH using NIST [\[FIPS186-4\]](#) prime curves.

The document also conforms to the terms and models described in [\[RFC5889\]](#) and uses the vocabulary and the concepts defined in [\[RFC4291\]](#) for the IPv6 Architecture. Finally, common terminology related to Low power And Lossy Networks (LLN) defined in [\[RFC7102\]](#) is also used.

3. Updating [RFC 6775](#)

This specification defines a cryptographic identifier (Crypto-ID) that can be used as a replacement to the MAC address in the OUI field of the EARO option; the computation of the Crypto-ID is detailed in [Section 4.1](#). A node in possession of the necessary cryptographic material SHOULD use Crypto-ID by default as OUI in its registration. Whether a OUI is a Crypto-ID is indicated by a new "C" flag in the NS(EARO) message.

This specification introduces a new option, the CIP0, that is used to prove ownership of the Crypto-ID. A node that registers for the

first time to a 6LR SHOULD place a CIP0 option in its registration. However, it is not expected to place the option in the periodic refresher registrations for that address, or to register other addresses with the same OUID. When a 6LR receives a NS(EAR0) registration with a new Crypto-ID as a OUID, it SHOULD challenge by responding with a NA(EAR0) with a status of "Validation Requested". This process of validation MAY be skipped in networks where there is no mobility.

The challenge MUST also be triggered in the case of a registration for which the Source Link-Layer Address is not consistent with a state that already exists either at the 6LR or the 6LBR. In the latter case, the 6LBR returns a status of "Validation Requested" in the DAR/DAC exchange, which is echoed by the 6LR in the NA (EAR0) back to the registering node. This flow should not alter a preexisting state in the 6LR or the 6LBR.

Upon receiving a NA(EAR0) with a status of "Validation Requested", the registering node SHOULD retry its registration with a CIP0 option that proves its ownership of the Crypto-ID.

If the 6LR cannot validate the CIP0, it responds with a status of "Validation Failed". After receiving a NA(EAR0) with a status of "Validation Failed", the registering node MUST NOT use this Crypto-ID for registering with that 6LR.

4. New Fields and Options

4.1. New Crypto-ID

Elliptic Curve Cryptography (ECC) is used to calculate the Crypto-ID. Each 6LN using a Crypto-ID for registration MUST have a public/private key pair. The digital signature is constructed by using the 6LN's private key over its EUI-64 (MAC) address. The signature value is computed using the ECDSA signature algorithm and the hash function used is SHA-256 [RFC6234]. Public Key is the most important parameter in CGA Parameters (sent by 6LN in an NS message). ECC Public Key could be in uncompressed form or in compressed form where the first octet of the OCTET STRING is 0x04 and 0x02 or 0x03, respectively. Point compression can further reduce the key size by about 32 octets.

To support cryptographic algorithm agility [RFC7696], Edwards-Curve Digital Signature Algorithm (EdDSA) curve Ed25519ph (pre-hashing) [RFC8032] can also be used as an alternate to the default NIST P-256 [FIPS186-4]. This is indicated by 6LN using the Crypto Type field in the CIP0 option. The document currently only defines two possible values for the Crypto Type field. A value of 0 indicates that NIST

P-256 is used for the signature operation and SHA-256 as the hash algorithm. A value of 1 indicates that Ed25519ph is used for the signature operation and SHA-256 as the hash algorithm. New values for the Crypto Type maybe defined in the future for new curves.

The Crypto-ID is computed as follows:

1. the modifier is set to a random or pseudo-random 128-bit value
2. the modifier, 9 zero octets and the ECC public key are concatenated from left to right.
3. the SHA-256 algorithm is applied on the concatenation
4. the 112 leftmost bits of the hash value are retained
5. the modifier value, the EUI-64 transformation of the device Link Layer Address and the encoded public key are concatenated from left to right
6. Digital signature (NIST P-256 or EdDSA) is executed on the concatenation
7. the leftmost bits of the resulting signature are used as the Crypto-ID.

With this specification, only 64 bits are retained, but it could be expanded to more bits in the future by increasing the size of the OUID field.

4.2. Updated EARO

This specification updates the EARO option as follows:

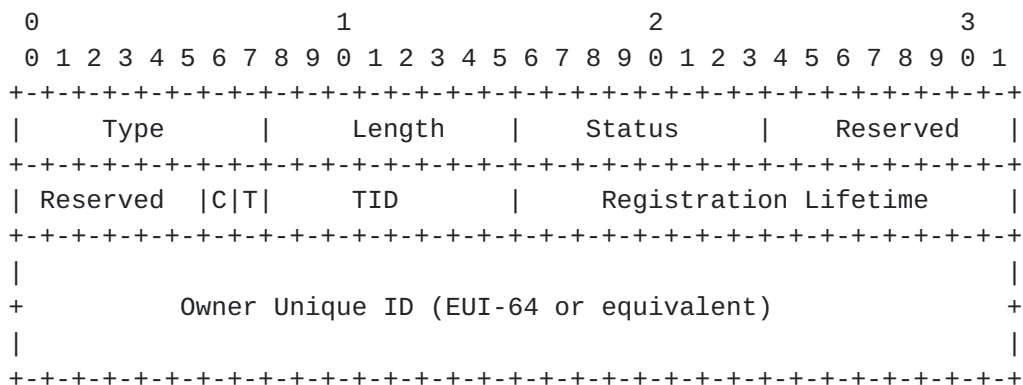


Figure 1: Enhanced Address Registration Option

Type: 33

Length: 8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 bytes.

Status: 8-bit unsigned integer. Indicates the status of a registration in the NA response. MUST be set to 0 in NS messages. This specification uses values introduced in the update to 6LoWPAN ND [[I-D.ietf-6lo-rfc6775-update](#)], such as "Validation Requested" and "Validation Failed". No additional value is defined.

Reserved: This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

C: This "C" flag is set to indicate that the Owner Unique ID field contains a Crypto-ID.

T and TID: Defined in [[I-D.ietf-6lo-rfc6775-update](#)].

Owner Unique ID: When the "C" flag is set, this field contains a Crypto-ID.

[4.3.](#) New Crypto-ID Parameters Option

This specification introduces a new option, the Crypto-ID Parameters Option (CIP0), that carries the proof of ownership of a crypto-ID.

Public Key: ECC public key of 6LN.

Padding: A variable-length field making the option length a multiple of 8, containing as many octets as specified in the Pad Length field.

5. Protocol Overview

5.1. Protocol Scope

The scope of the present work is a 6LoWPAN Low Power Lossy Network (LLN), typically a stub network connected to a larger IP network via a Border Router called a 6LBR per [RFC6775].

The 6LBR maintains a registration state for all devices in the attached LLN, and, in conjunction with the first-hop router (the 6LR), is in a position to validate uniqueness and grant ownership of an IPv6 address before it can be used in the LLN. This is a fundamental difference with a classical network that relies on IPv6 address auto-configuration [RFC4862], where there is no guarantee of ownership from the network, and any IPv6 Neighbor Discovery packet must be individually secured [RFC3971].

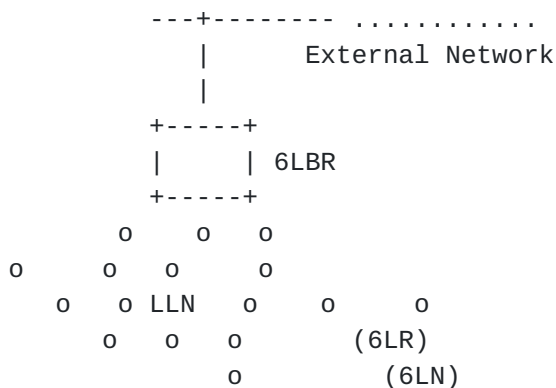


Figure 3: Basic Configuration

In a mesh network, the 6LR is directly connected to the host device. This specification expects that the peer-wise layer-2 security is deployed so that all the packets from a particular host are securely identifiable by the 6LR. The 6LR may be multiple hops away from the 6LBR. Packets are routed between the 6LR and the 6LBR via other 6LRs. This specification expects that a chain of trust is established so that a packet that was validated by the first 6LR can be safely routed by the next 6LRs to the 6LBR.

5.2. Protocol Flows

Figure 4 illustrates a registration flow all the way to a 6LowPAN Backbone Router (6BBR).

A new device that joins the network auto-configures an address and performs an initial registration to an on-link 6LR with an NS message that carries an Address Registration Option (EARO) [RFC6775]. The 6LR validates the address with the central 6LBR using a DAR/DAC exchange, and the 6LR confirms (or denies) the address ownership with an NA message that also carries an Address Registration Option.

In a multihop 6LoWPAN, the registration with Crypto-ID is propagated to 6LBR as described in [Section 5.3](#). If a chain of trust is present between the 6LR and the 6LBR, then there is no need to propagate the proof of ownership to the 6LBR. All the 6LBR needs to know is that this particular OUID is randomly generated, so as to enforce that any update via a different 6LR is also random.

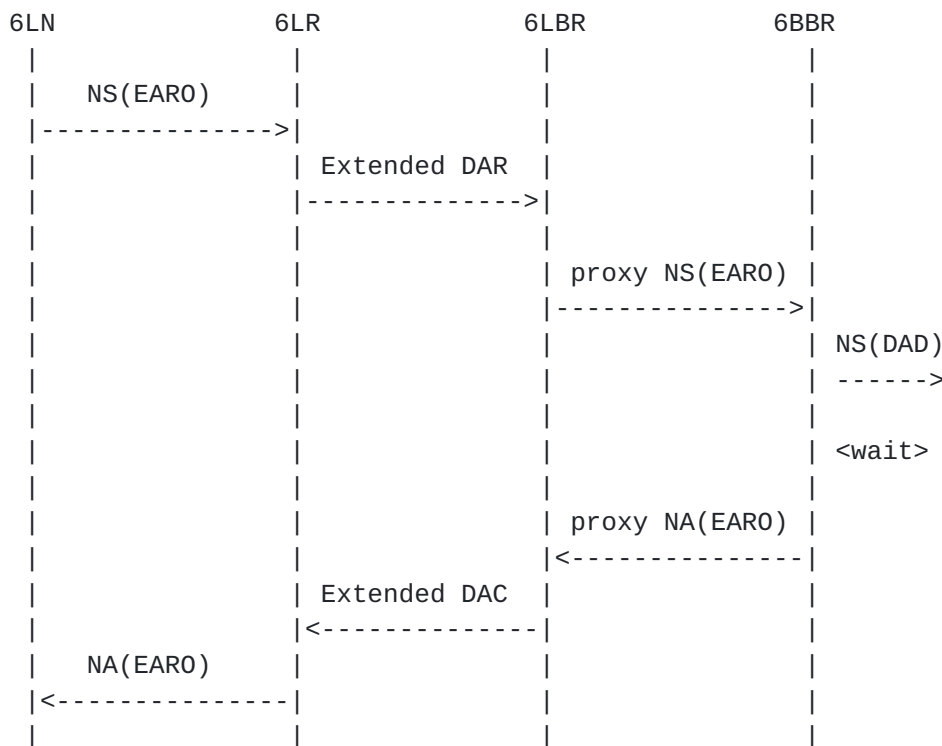


Figure 4: (Re-)Registration Flow

On-link (local) protocol interactions are shown in Figure 5. Crypto-ID and ARO are passed to and stored by the 6LR on the first NS and

not sent again in the next NS. The operation starts with 6LR sending a Router Advertisement (RA) message to 6LN.

The 6LR/6LBR ensures first-come/first-serve by storing the ARO and the Crypto-ID correlated to the node being registered. The node is free to claim any address it likes as long as it is the first to make such a claim. After a successful registration, the node becomes the owner of the registered address and the address is bound to the Crypto-ID in the 6LR/6LBR registry. This binding can be verified later, which prevents other nodes from stealing the address and trying to attract traffic for that address or use it as their source address.

A node may use multiple IPv6 addresses at the same time. The node may use the same Crypto-ID to protect multiple IPv6 addresses. The separation of the address and the Crypto-ID avoids the constrained device to compute multiple keys for multiple addresses. The registration process allows the node to bind all of its addresses to the same Crypto-ID.

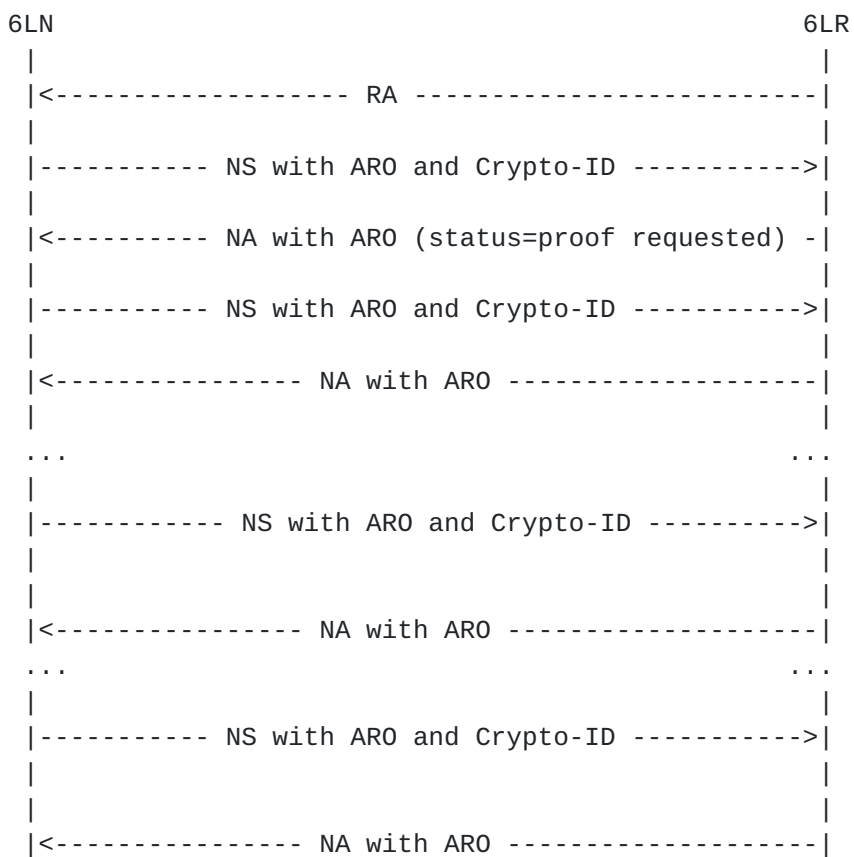


Figure 5: On-link Protocol Operation

5.3. Multihop Operation

In a multihop 6LoWPAN, a 6LBR sends RAs with prefixes downstream and the 6LR receives and relays them to the nodes. 6LR and 6LBR communicate using ICMPv6 Duplicate Address Request (DAR) and Duplicate Address Confirmation (DAC) messages. The DAR and DAC use the same message format as NS and NA, but have different ICMPv6 type values.

In ND-PAR we extend DAR/DAC messages to carry cryptographically generated OUID. In a multihop 6LoWPAN, the node exchanges the messages shown in Figure 4. The 6LBR must identify who owns an address (EUI-64) to defend it, if there is an attacker on another 6LR. Because of this the content that the source signs and the signature needs to be propagated to the 6LBR in the DAR message. For this purpose the DAR message sent by 6LR to 6LBR MUST contain the CIP0 option. The DAR message also contains ARO.

Occasionally, a 6LR might miss the node's OUID (that it received in ARO). 6LR should be able to ask for it again. This is done by restarting the exchanges shown in Figure 5. The result enables 6LR to refresh the information that was lost. The 6LR MUST send DAR message with ARO to 6LBR. The 6LBR replies with a DAC message with the information copied from the DAR, and the Status field is set to zero. With this exchange, the 6LBR can (re)validate and store the information to make sure that the 6LR is not a fake.

In some cases, the 6LBR may use a DAC message to solicit a Crypto-ID from a 6LR and also requests 6LR to verify the EUI-64 6LR received from 6LN. This may happen when a 6LN node is compromised and a fake node is sending the Crypto-ID as if it is the node's EUI-64. Note that the detection in this case can only be done by 6LBR not by 6LR.

6. Security Considerations

The observations regarding the threats to the local network in [\[RFC3971\]](#) also apply to this specification.

The threats discussed in 6LoWPAN ND [\[RFC6775\]](#) and its update [\[I-D.ietf-6lo-rfc6775-update\]](#) also apply here. Compared with SeND, this specification saves about 1Kbyte in every NS/NA message. Also, this specification separates the cryptographic identifier from the registered IPv6 address so that a node can have more than one IPv6 address protected by the same cryptographic identifier. SeND forces the IPv6 address to be cryptographic since it integrates the CGA as the IID in the IPv6 address. This specification frees the device to form its addresses in any fashion, so as to enable the classical 6LoWPAN compression which derives IPv6 addresses from Layer-2

addresses, as well as privacy addresses. The threats discussed in [Section 9.2 of \[RFC3971\]](#) are countered by the protocol described in this document as well.

Collisions of Owner Unique Interface IDentifier (OUID) (which is the Crypto-ID in this specification) is a possibility that needs to be considered. The formula for calculating the probability of a collision is $1 - e^{-K^2/(2n)}$ where n is the maximum population size (2^{64} here, $1.84E19$) and K is the actual population (number of nodes). If the Crypto-ID is 64-bit long, then the chance of finding a collision is 0.01% when the network contains 66 million nodes. It is important to note that the collision is only relevant when this happens within one stub network (6LBR). A collision of Crypto-ID is a rare event. In the case of a collision, an attacker may be able to claim the registered address of an another legitimate node. However for this to happen, the attacker would also need to know the address which was registered by the legitimate node. This registered address is however never broadcasted on the network and therefore it provides an additional entropy of 64-bits that an attacker must correctly guess. To prevent such a scenario, it is RECOMMENDED that nodes derive the address being registered independently of the OUID.

7. IANA considerations

IANA is requested to assign two new option type values for the CIP0 under the subregistry "IPv6 Neighbor Discovery Option Formats".

7.1. Crypto Type Registry

The following Crypto Type values are defined in this document:

+-----+-----+	
Crypto Type value	Algorithms
+-----+-----+	
0	NIST P-256 [FIPS186-4] , SHA-256 [RFC6234]
1	Ed25519ph [RFC8032], SHA-256 [RFC6234]
+-----+-----+	

Table 1: Crypto Types

Assignment of new values for new Crypto Type MUST be done through IANA with "Specification Required" and "IESG Approval" as defined in [\[RFC8126\]](#).

8. Acknowledgements

Many thanks to Charlie Perkins for his in-depth review and constructive suggestions. We are also especially grateful to Rene Struik and Robert Moskowitz for their comments that lead to many improvements to this document, in particular WRT ECC computation and references.

9. References

9.1. Normative References

- [I-D.ietf-6lo-rfc6775-update]
Thubert, P., Nordmark, E., Chakrabarti, S., and C. Perkins, "An Update to 6LoWPAN ND", [draft-ietf-6lo-rfc6775-update-10](#) (work in progress), October 2017.
- [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>>.
- [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>>.
- [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>>.

9.2. Informative references

- [FIPS186-4]
"FIPS Publication 186-4: Digital Signature Standard", July 2013, <<http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf>>.

[I-D.ietf-6lo-backbone-router]

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

[I-D.struik-lwip-curve-representations]

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

[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>>.

[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>>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", [RFC 4944](#), DOI 10.17487/RFC4944, September 2007, <<https://www.rfc-editor.org/info/rfc4944>>.

[RFC5889] Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing Model in Ad Hoc Networks", [RFC 5889](#), DOI 10.17487/RFC5889, September 2010, <<https://www.rfc-editor.org/info/rfc5889>>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", [RFC 6234](#), DOI 10.17487/RFC6234, May 2011, <<https://www.rfc-editor.org/info/rfc6234>>.

[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>>.

[RFC7039] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, Ed., "Source Address Validation Improvement (SAVI) Framework", [RFC 7039](#), DOI 10.17487/RFC7039, October 2013, <<https://www.rfc-editor.org/info/rfc7039>>.

- [RFC7102] Vasseur, JP., "Terms Used in Routing for Low-Power and Lossy Networks", [RFC 7102](#), DOI 10.17487/RFC7102, January 2014, <<https://www.rfc-editor.org/info/rfc7102>>.
- [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>>.
- [RFC7696] Housley, R., "Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms", [BCP 201](#), [RFC 7696](#), DOI 10.17487/RFC7696, November 2015, <<https://www.rfc-editor.org/info/rfc7696>>.
- [RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", [RFC 7721](#), DOI 10.17487/RFC7721, March 2016, <<https://www.rfc-editor.org/info/rfc7721>>.
- [RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", [RFC 7748](#), DOI 10.17487/RFC7748, January 2016, <<https://www.rfc-editor.org/info/rfc7748>>.
- [RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", [RFC 8032](#), DOI 10.17487/RFC8032, January 2017, <<https://www.rfc-editor.org/info/rfc8032>>.
- [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>>.

[Appendix A](#). Requirements Addressed in this Document

In this section we state requirements of a secure neighbor discovery protocol for low-power and lossy networks.

- o The protocol MUST be based on the Neighbor Discovery Optimization for Low-power and Lossy Networks protocol defined in [[RFC6775](#)]. [RFC6775](#) utilizes optimizations such as host-initiated interactions for sleeping resource-constrained hosts and elimination of multicast address resolution.
- o New options to be added to Neighbor Solicitation messages MUST lead to small packet sizes, especially compared with existing protocols such as SEcure Neighbor Discovery (SEND). Smaller

packet sizes facilitate low-power transmission by resource-constrained nodes on lossy links.

- o The support for this registration mechanism SHOULD be extensible to more LLN links than IEEE 802.15.4 only. Support for at least the LLN links for which a 6lo "IPv6 over foo" specification exists, as well as Low-Power Wi-Fi SHOULD be possible.
- o 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.
- o The Address Registration Option used in the ND registration SHOULD be extended to carry the relevant forms of Unique Interface Identifier.
- o The Neighbour Discovery should specify the formation of a site-local address that follows the security recommendations from [[RFC7217](#)].

Authors' Addresses

Behcet Sarikaya
Plano, TX
USA

Email: sarikaya@ieee.org

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

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

Mohit Sethi
Ericsson
Hirsalantie
Jorvas 02420

Email: mohit@piuha.net

