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

M. Sethi, Ed.
Ericsson
P. Thubert
Cisco
B. Sarikaya, Ed.
Huawei USA

August 22, 2016

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

Abstract

This document defines an extension to 6LoWPAN Neighbor Discovery. This extension is designed for low-power and lossy network environments and it supports multi-hop operation. Nodes supporting this extension compute a Cryptographically Unique Interface ID and associate it with one or more of their Registered Addresses. The Cryptographic ID (Crypto-ID) uniquely identifies the owner of the Registered Address. It is used in place of the EUI-64 address that is specified in RFC 6775. Once an address is registered with a Cryptographic ID, only the owner of that ID can modify the state information of the Registered Address in the 6LR and 6LBR.

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 February 23, 2017.

Copyright Notice

Table of Contents

1. Introduction

Neighbor discovery for IPv6 [RFC4861] and stateless address autoconfiguration [RFC4862] are together referred to as neighbor discovery protocols (NDP). They are defined for regular hosts that have sufficient memory and computation capabilities. These protocols are however not suitable for resource-constrained devices. Therefore, they require adaptation to work on resource-constrained hosts operating over a low-power and lossy network (LLN). Neighbor Discovery optimizations for 6LoWPAN networks include simple optimizations such as a host address registration feature. This feature uses the address registration option (ARO) which is sent in the unicast Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages [RFC6775].

With 6LoWPAN ND [RFC6775], the ARO option includes a EUI-64 interface ID to uniquely identify the interface of the Registered Address on the registering device, so as to correlate further registrations for the same address and avoid address duplication. The EUI-64 interface ID is not secure and its ownership cannot be verified. Consequently,

any device claiming the same EUI-64 interface ID may take over an existing registration and attract the traffic for that address. The address registration mechanism in [RFC6775] is limited as it does not require a node to prove its ownership of the EUI-64 Interface ID. Therefore, any node connected to the subnet and aware of the registered address to EUI-64 interface ID mapping may effectively fake the same interface ID and steal an address.

In this document, we extend 6LoWPAN ND to protect the address ownership with cryptographic material, but as opposed to Secure Neighbor Discovery (SEND) [RFC3971] and Cryptographically Generated Addresses (CGAs) [RFC3972], the cryptographic material generated is not embedded in the Interface ID (IID) as an IPv6 address. Instead, the generated cryptographic ID is used as a correlator associated with the registration of the IP address. This approach is made possible with 6LoWPAN ND [RFC6775], where the 6LR and the 6LBR maintain state information for each Registered Address. If a cryptographic ID is associated with the first 6LoWPAN ND registration, then it can be used to validate any future updates to the registration.

In order to achieve this ownership verification, in this extension specification, the EUI-64 interface ID used in 6LoWPAN ND is replaced with cryptographic material whose ownership can be verified. The extension also provides new means for the 6LR to validate ownership of the registration, and thus, the ownership of registered address. The resulting protocol is called Protected Address Registration protocol (ND-PAR).

In ND-PAR, a node typically generates one 64-bit cryptographic ID (Crypto-ID) and uses it as Unique Interface ID in the registration of one (or more) of its addresses with the 6LR, which it attaches to and uses as default router. The 6LR validates ownership of the cryptographic ID typically upon creation or update of a registration state, for instance following an apparent movement from one point of attachment to another. The ARO option is modified to carry the Unique Interface ID, and through the DAR/DAC exchange.

Compared with SeND, this specification saves ~1Kbyte in every NS/NA message. Also SeND requires one cryptographic address per IPv6 address. This specification separates the cryptographic identifier from the 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 an IID. 6LoWPAN derives the IPv6 address from other things like a short address in 802.15.4 to enable a better compression.

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.

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.

This document uses [RFC7102] for Terminology in Low power And Lossy Networks.

3. Requirements

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

- 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.

- 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.

- 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.

- 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.

- The Address Registration Option used in the ND registration SHOULD be extended to carry the relevant forms of Unique Interface IDentifier.

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

4. Protocol Interactions

Protected address and registration neighbor discovery protocol (ND-PAR) modifies Neighbor Discovery Optimization for Low-power and Lossy Networks [RFC6775] as explained in this section.

4.1. Overview

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].

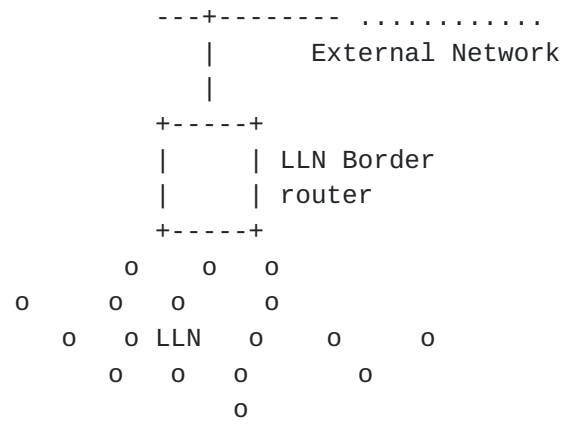

Figure 1: Basic Configuration

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].

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.

[I-D.ietf-6tisch-architecture] suggests to use of RPL [RFC6550] as the routing protocol between the 6LRs and the 6LBR, and leveraging a backbone router [I-D.ietf-6lo-backbone-router] to extend the LLN in a larger multilink subnet [RFC4903]. In that model, a registration flow happens as shown in Figure 2. Note that network beyond the 6LBR is out of scope for this document.

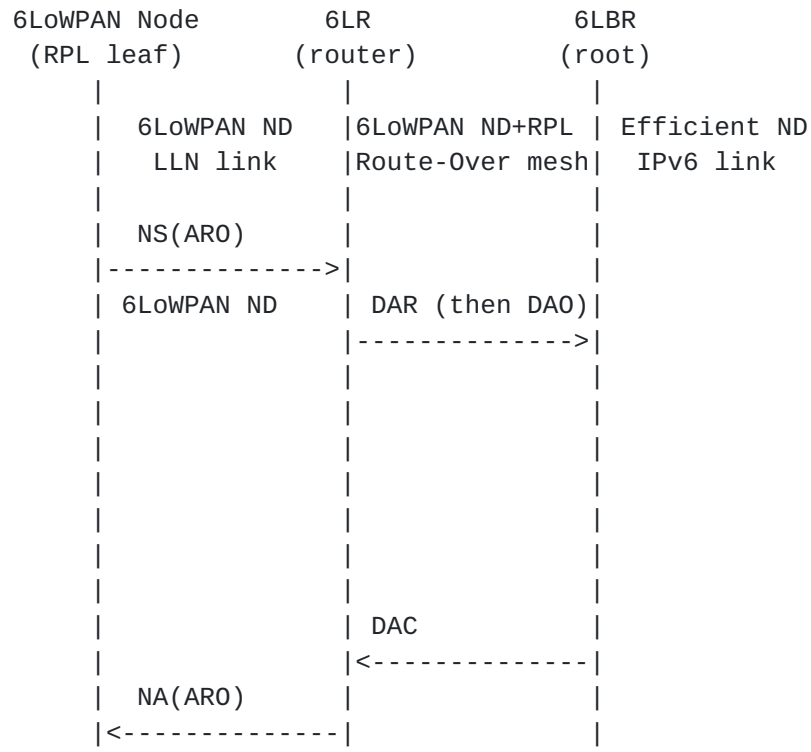

Figure 2: (Re-)Registration Flow over Multi-Link Subnet

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 a new Address Registration Option (ARO) [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.

The registration mechanism in [RFC6775] was created for the original purpose of Duplicate Address Detection (DAD), whereby use of an address would be granted as long as the address is not already present in the subnet. But [RFC6775] does not require that the 6LR use the registration for source address validation (SAVI) [RFC7039].

Protected address registration protocol proposed in this document enforces SAVI. With this we ensure that only the correct owner uses the registered address in the source address field. Therefore a destination node can trust that the source is the real owner without using SeND. All packets destined for a node go through the 6LR to which it is attached. The 6LR maintains state information for the registered addressed along with the MAC address, and link-layer cryptographic key associated with that node. The 6LR therefore only delivers packets to the real owner based on its state information.

In order to validate address ownership, the registration mechanism (that goes all the way to the 6LBR with the DAR/DAC) enables the 6LBR to correlate further claims for a registered address from the device to which it is granted, based on a Unique Interface IDentifier (UID). This UID is derived from the MAC address of the device (EUI-64).

This document uses a randomly generated value as an alternate UID for the registration. Proof of ownership of the UID is passed with the first registration to a given 6LR, and enforced at the 6LR, which validates the proof. With this new operation, the 6LR allows only packets from a connected host if the connected host owns the registration of the source address of the packet.

In a multihop 6LoWPAN, the registration with Crypto-ID is propagated to 6LBR as described in Section 4.3. 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 UID is randomly generated, so as to enforce that any update via a different 6LR is also random.

4.2. Updating RFC 6775

Protocol interactions are as defined in Figure 2. The Crypto-ID is calculated as described in Section 4.2.1.

The Target Address field in NS message is set to the prefix concatenated with the node's address. This address does not need duplicate address detection as Crypto-ID is globally unique. So a host cannot steal an address that is already registered unless it has the key used for generating the Crypto-ID. The same Crypto-ID can thus be used to protect multiple addresses e.g. when the node receives a different prefix.

Local or on-link protocol interactions are shown in Figure 3. Crypto-ID and ARO are passed to and stored by the 6LR/6LBR 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. The node becomes owner of that address and the address is bound to the Crypto-ID in the 6LR/6LBR registry. This procedure avoids the constrained device to compute multiple keys for multiple addresses. The registration process allows the node to tie all the addresses to the same Crypto-ID and have the 6LR/6LBR enforce first-come first-serve after that.

A condition where a 6LN uses multiple IPv6 addresses may happen when the node moves at a different place and receives a different prefix. In this scenario, the node uses the same Crypto-ID to protect its new IPv6 address. This prevents other nodes from stealing the address and trying to use it as their source address.

Note that if the device that moves always forms new MAC and IP address [RFC6775], then this new address can be used for registration. In case of a collision of the new MAC and therefore IP address, the node can easily form a new IPv6 address. This is one case where the use of Crypto-ID would not be needed. Crypto-ID or ND-PAR should be activated when the IP address is claimed at another place, or for a different MAC address at the same place, e.g. for MAC address privacy [I-D.ietf-6man-ipv6-address-generation-privacy].

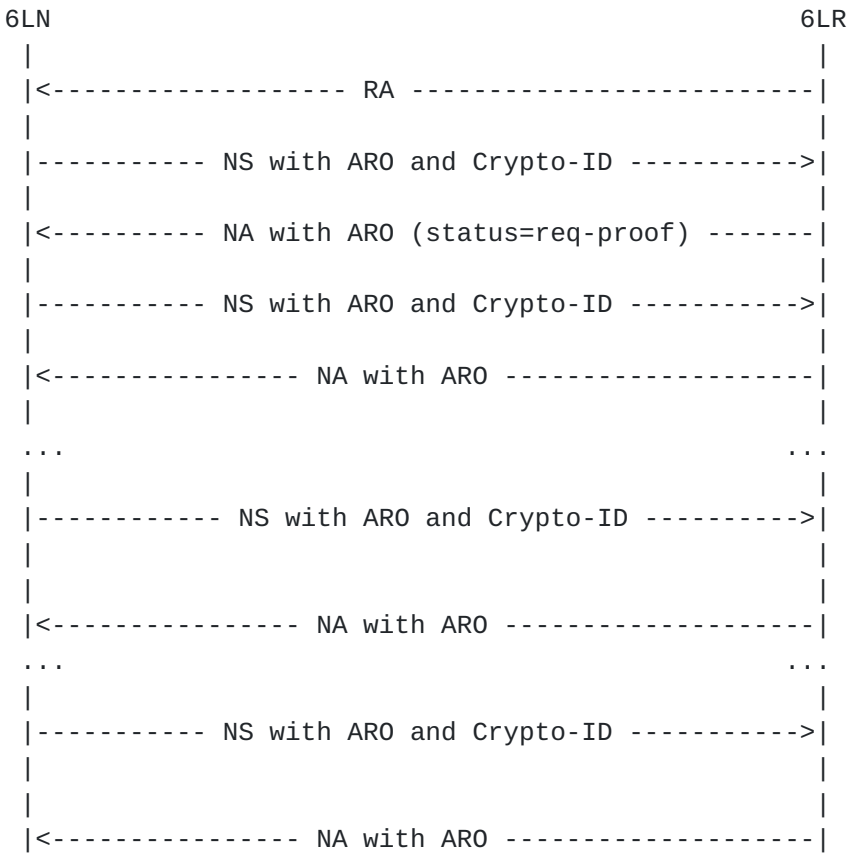

Figure 3: On-link Protocol Operation

Elliptic Curve Cryptography (ECC) is used in the calculation of cryptographic identifier (Crypto-ID). 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.

After calculating its Crypto-ID, a 6LN sends it along with the CGA parameters in the first NS message, see Figure 3. In order to send Crypto-ID, a modified address registration option called Enhanced Address Registration Option (EARO) is defined in Figure 4. As defined in the figure this ID is variable length, varying between 64 to 128 bits. This ID is 128 bits long only if it is used as IPv6 address. This may happen when some application uses one IP address of the device as device ID. It would make sense in that case to build a real CGA IPv6 address. The prefix of the address would be obtained from prefix information option (PIO in RA) [RFC4861].

6LN also sends some other parameters to enable 6LR or 6LBR to verify the Crypto-ID. The option shown in Figure 5 can be used. In the figure, CGA Parameters field contains the public key, prefix and some other values. It is a simplified form of CGA Option defined in [RFC3971].

4.2.1. Crypto-ID Calculation

First, the modifier is set to a random or pseudo-random 128-bit value. Next, concatenate from left to right the modifier, 9 zero octets and the ECC public key. SHA-256 algorithm is applied on the concatenation. The 112 leftmost bits of the hash value is taken. Concatenate from left to right the modifier value, the subnet prefix and the encoded public key. NIST P-256 is executed on the concatenation. The leftmost bits of the result is used as the Crypto-ID. The length is normally 64 bits, however it could be 128 bits.

In respecting the cryptographical algorithm agility [RFC7696], Curve 25519 [RFC7748] can also be used instead of NIST P-256. This is indicated by 6LN by setting the Crypto Type field in CGA Parameters Option to a value of 1. If 6LBR does not support Curve 25519, it will set Crypto Type field to zero. This means that the default algorithm (NIST P-256) will be used.

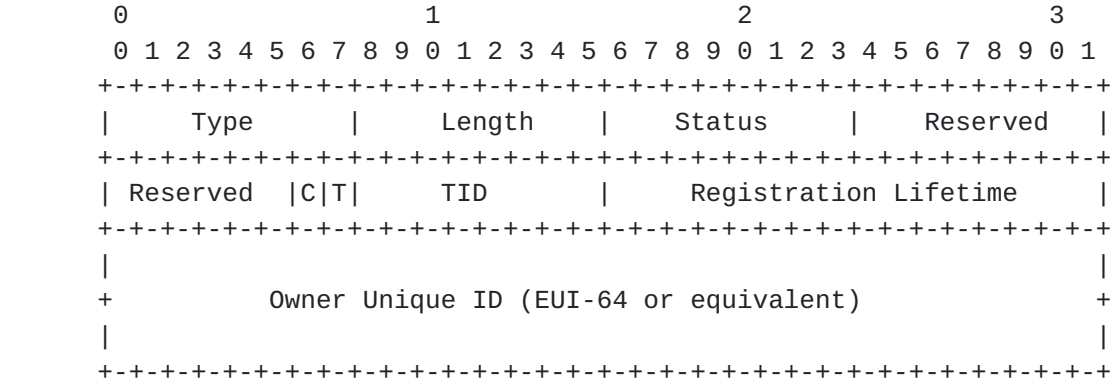

Figure 4: Enhanced Address Registration Option

Type:

TBA1

Length:

8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 bytes. The value 0 is invalid. A value of 3 with the C flag set indicates a Crypto-ID of 128 bits.

Status:

8-bit unsigned integer. Indicates the status of a registration in the NA response. MUST be set to 0 in NS messages. See below.

Reserved:

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

C:

C bit when set is used to indicate that Owner Unique ID fields contains Crypto-ID.

T and TID:

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

Owner Unique ID:

In this specification, this field contains Crypto-ID, a variable length field to carry the Crypto-ID or random UID. This field is normally 64 bits long. It could be 128 bits long if IPv6 address is used as the Crypto-ID.

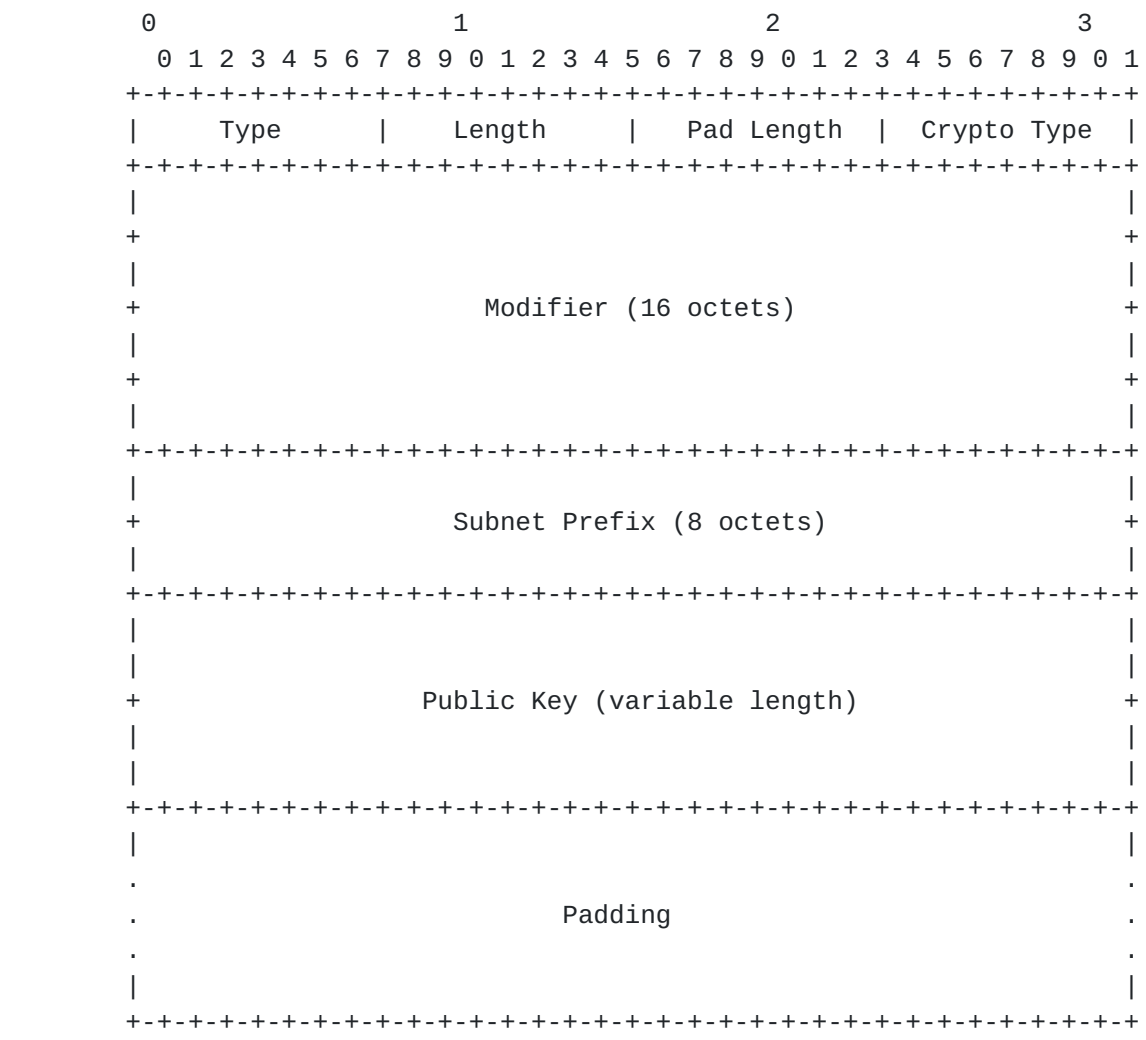

Figure 5: CGA Parameters Option

Type:

TBA2

Length:

The length of the option in units of 8 octets.

Pad Length:

The length of the Padding field.

Crypto Type:

The type of cryptographic algorithm used in calculation Crypto-ID. Default value of all zeros indicate NIST P-256. A value of 1 is assigned for Curve 25519. New values may be defined later.

Modifier:

128 bit random value.

Subnet Prefix:

64 bit subnet prefix.

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.

4.3. Multihop Operation

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

In ND-PAR we extend DAR/DAC messages to carry cryptographically generated UID. In a multihop 6LoWPAN, the node exchanges the messages shown in Figure 2. The 6LBR must be aware of who owns an address (EUI-64) to defend the first node 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 DAR message. For this purpose the DAR message sent by 6LR to 6LBR MUST contain CGA Parameters and Digital Signature Option carrying the CGA that the node calculates and its public key. DAR message also contains ARO.

It is possible that occasionally, 6LR may miss the node's UID (that it received in ARO). 6LR should be able to ask for it again. This is done by restarting the exchanges shown in Figure 3. The result enables 6LR to refresh the information that was lost. 6LR MUST send DAR message with ARO to 6LBR. 6LBR as a reply forms 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 6LBR may use DAC message to signal to 6LR that it expects Crypto-ID from 6LR also asks 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.

5. Security Considerations

The same considerations regarding the threats to the Local Link Network covered in [RFC3971] apply.

The threats discussed in Section 9.2 of [RFC3971] are countered by the protocol described in this document as well.

Collisions of Crypto-ID is a possibility that needs to be considered. The formula for calculating probability of a collision is 1 - e^{-k^2/(2n)}. 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 ID in ND-PAR is a rare event. However, when such a collision does happen, the protocol operation is not affected, although it opens a window for a node to hijack an address from another. The link-layer security ensures that the nodes would normally not be aware of a collision on the subnet. If a malicious node is able to gain knowledge of a collision through other means, the only thing that it could do is to steal addresses from the other honest node. This would be no different from what is already possible in a 6lo network today.

6. IANA considerations

IANA is requested to assign two new option type values, TBA1 and TBA2 under the subregistry "IPv6 Neighbor Discovery Option Formats".

7. Acknowledgements

We are grateful to Rene Struik and Robert Moskowitz for their comments that lead to many improvements to this document.

8. References

8.1. 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>.

[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>.

[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>.

[RFC4903] Thaler, D., "Multi-Link Subnet Issues", RFC 4903, DOI 10.17487/RFC4903, June 2007, <http://www.rfc-editor.org/info/rfc4903>.

[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>.

[RFC5889] Baccelli, E., Ed. and M. Townsley, Ed., "IP Addressing Model in Ad Hoc Networks", RFC 5889, DOI 10.17487/RFC5889, September 2010, <http://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, <http://www.rfc-editor.org/info/rfc6234>.

[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>.

[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>.

[RFC7102] Vasseur, JP., "Terms Used in Routing for Low-Power and Lossy Networks", RFC 7102, DOI 10.17487/RFC7102, January 2014, <http://www.rfc-editor.org/info/rfc7102>.

[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, <http://www.rfc-editor.org/info/rfc7039>.

[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>.

[RFC7696] Housley, R., "Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms", BCP 201, RFC 7696, DOI 10.17487/RFC7696, November 2015, <http://www.rfc-editor.org/info/rfc7696>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <http://www.rfc-editor.org/info/rfc7748>.

8.2. Informative references

[I-D.ietf-6lo-backbone-router]
Thubert, P., "IPv6 Backbone Router", draft-ietf-6lo-backbone-router-01 (work in progress), March 2016.

[I-D.ietf-6tisch-architecture]
Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", draft-ietf-6tisch-architecture-10 (work in progress), June 2016.

[I-D.ietf-6man-ipv6-address-generation-privacy]
Cooper, A., Gont, F., and D. Thaler, "Privacy Considerations for IPv6 Address Generation Mechanisms", draft-ietf-6man-ipv6-address-generation-privacy-08 (work in progress), September 2015.

Authors' Addresses

Mohit Sethi (editor)
Ericsson
Hirsalantie
Jorvas 02420

Email: mohit@piuha.net

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

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

Behcet Sarikaya (editor)
Huawei USA
5340 Legacy Dr. Building 3
Plano, TX 75024

Email: sarikaya@ieee.org