        Address Protected Neighbor Discovery for Low-power and Lossy Networks
                       draft-sarikaya-6lo-ap-nd-01

Abstract

   This document defines an extension of 6LoWPAN Neighbor Discovery for
   application in low-power and lossy networks. The protocol is
   specified to be protected and to support multi-hop operation. A node
   computes its Cryptographic, Unique Interface ID, and associates one
   or more of its Registered Addresses with that Cryptographic ID in
   place of the EUI-64 that is used in RFC 6775 to uniquely identify the
   interface of the Registered Address. Once an address is registered
   with a Cryptographic ID, only the owner of that ID can modify the
   state in the 6LR and 6LBR regarding the Registered Address.

Status of This Memo

Copyright Notice

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

   Neighbor discovery for IPv6 [RFC4861] and stateless address
   autoconfiguration [RFC4862], together referred to as neighbor
   discovery protocols (NDP), are defined for regular hosts operating
   with wired/wireless links. These protocols are not suitable and
   require optimizations for resource constrained, low power hosts
   operating with LLN for low-power and lossy networks. Neighbor
   Discovery optimizations for 6LoWPAN networks include simple
   optimizations such as a host address registration feature using the
   address registration option (ARO) which is sent in unicast Neighbor
   Solicitation (NS) and Neighbor Advertisement (NA) messages [RFC6775].
   With 6LoWPAN ND [RFC6775], the ARO option includes a EUI-64 address
   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 address is
   not secured and its ownership cannot be verified. It results that
   any device claiming the same EUI-64 address may take over a
   registration and attract the traffic for that 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], [RFC3972], the cryptographic
   material is not embedded in the Interface ID (IID) in an IPv6 address

but used as a correlator associated to the registration of the IPv6 address. This approach is made possible with 6LoWPAN ND [RFC6775], where the 6LR and the 6LBR maintain a state for each Registered Address. If a cryptographic ID is associated with an original 6LoWPAN ND registration and stored in the registration state, then it can be used to validate that any update to the registration state is made by the owner of that ID.

To achieve this, this specification replaces the EUI-64 address, that is used in 6LoWPAN ND to avoid address duplication, with cryptographic material whose ownership can be verified; it also provides new means for the 6LR to validate ownership of the registration thus that of the registered address by the registering device. The resulting protocol is called Protected address autoconfiguration and registration protocol (ND-PAAR).

A node generates one 64-bit cryptographic 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 a point of attachment to another. The ARO option is modified to carry the Unique Interface ID, and through the DAR/DAC exchange, the 6LBR is kept aware that this is the case, i.e. unique and whether the 6LR has verified the claim.

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], "neighbor Discovery for IP version 6" [RFC4861], "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] where the 6LoWPAN Router (6LR) and the 6LoWPAN Border Router (6LBR) are introduced, and [I-D.chakrabarti-nordmark-6man-efficient-nd], which proposes an evolution of [RFC6775] for a larger applicability.

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] due to the
   host-initiated interactions to allow for sleeping hosts, elimination
   of multicast-based address resolution for hosts, etc.

   New options to be added to Neighbor Solicitation messages MUST lead
   to small packet sizes. Smaller packet sizes facilitate low-power
   transmission by resource constrained nodes on lossy links.

   The support of the registration mechanism SHOULD be extended to more
   LLN links than IEEE 802.15.4, matching at least the LLN links for
   which a 6lo "IPv6 over foo" specification exists, as well as Low-
   Power Wi-Fi.

   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.

   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 autoconfiguration and registration neighbor
   discovery protocol (ND-PAAR) 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].

```
        ---+-------- ............ ------------
           |        External Network         |
           |
      +-----+
      |     | LLN Border
      |     | router
      +-----+
         o     o     o
       o     o    o      o
      o   o LLN   o    o      o
        o    o    o        o
             o
```
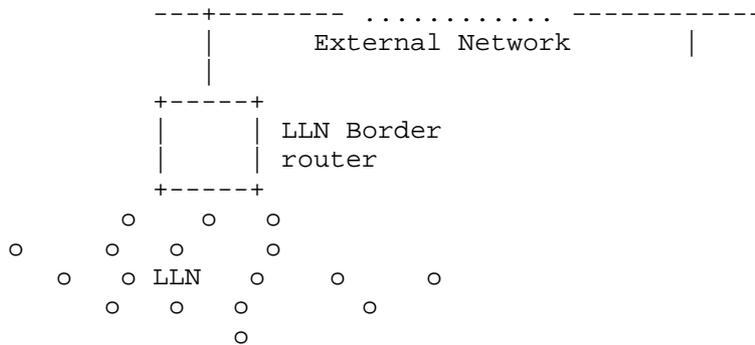
Figure 1: Basic Configuration

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 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 route-over mesh network, the 6LR is directly connected to the
host device; this specification expects that peer-wise Layer-2
security is deployed so that all the packets from a particular host
are identified as such 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 and 6LBR.

The [I-D.ietf-6tisch-architecture] suggests to use RPL [RFC6550] as
the routing protocol between the 6LRs and the 6LBR, and to leverage
[I-D.chakrabarti-nordmark-6man-efficient-nd] to extend the LLN in a
larger multilink subnet [RFC4903]. In that model, a registration
flow happens as shown in Figure 2:

```
6LoWPAN Node          6LR              6LBR              6BBR
  (RPL leaf)        (router)          (root)
    |                 |                 |                 |
    |    6LoWPAN ND   |6LoWPAN ND+RPL   | Efficient ND    |IPv6 ND
    |     LLN link    |Route-Over mesh  |   IPv6 link     |Backbone
    |                 |                 |                 |
    |    NS(ARO)       |                 |                 |
    |--------------->|                 |                 |
    |    6LoWPAN ND   |  DAR (then DAO) |                 |
    |                 |-------------->|                 |
    |                 |                 |    NS(ARO)       |
    |                 |                 |-------------->|
    |                 |                 |                 |  DAD
    |                 |                 |                 |------>
    |                 |                 |                 |
    |                 |                 |    NA(ARO)       |
    |                 |                 |<--------------|
    |                 |  DAC            |                 |
    |                 |<--------------|                 |
    |    NA(ARO)       |                 |                 |
    |<--------------|                 |                 |
```
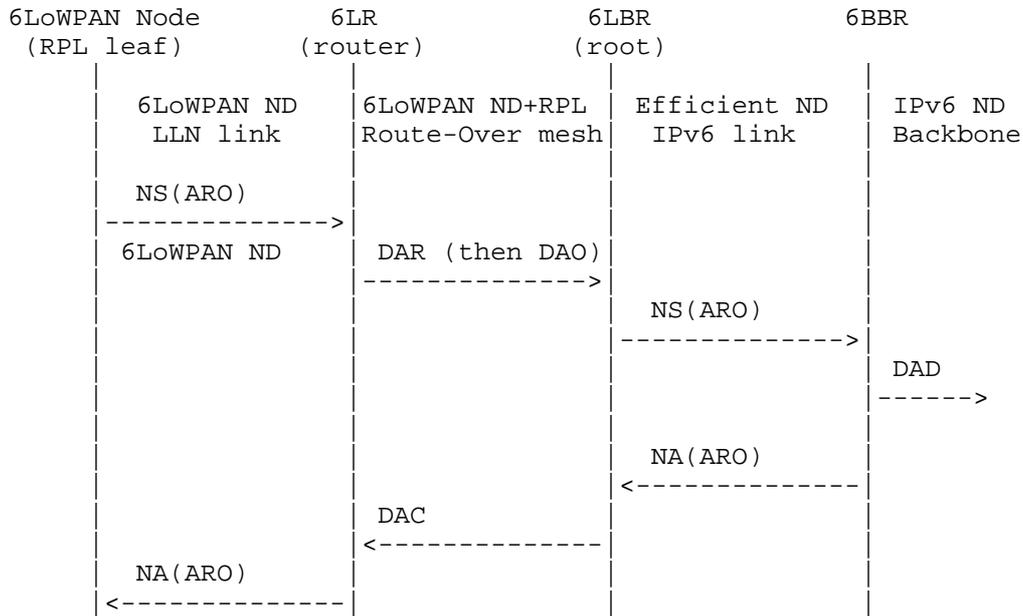
            Figure 2: (Re-)Registration Flow over Multi-Link Subnet

   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 infirms) 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).

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

   The limitation of the mechanism in [RFC6775] is that it does not
   enable to prove the UID itself, so any node connected to the subnet
   and aware of the address/UID mapping may effectively fake the same
   UID and steal an address.

This draft 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.

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 need 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. Protocol Operations

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 for 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 given in Figure 3. Crypto
ID and ARO are passed to and stored by the 6LR/6LBR on the first NS
and not sent again the in the next NS.

The 6LR/6LBR ensures first-come/first-serve by storing the ARO and
the crypto ID correlated to the target being registered. Then, if
the node is the first to claim any address it likes, then it 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.

```
6LN                                                              6LR
 |                                                                |
 |<---------------------RA----------------------------------------|
 |                                                                |
 |--------------NS with ARO and Random UID  --------------->|
 |                                                                |
 |<---------------------NA with ARO (status=req-proof) --|
 |                                                                |
 |--------------NS with ARO and Random UID->|
 |                                                                |
 |<---------------------NA with ARO--------------------|
 |                                                                |
 ...                                                              |
 |                                                                |
 |--------------NS with ARO and Random UID  --------------->|
 |                                                                |
 |                                     |
 |<---------------------NA with ARO--------------------|
 ...                                                              |
 |                                                                |
 |--------------NS with ARO and Random UID  --------------->|
 |                                                                |
 |                                     |
 |<---------------------NA with ARO--------------------|
```
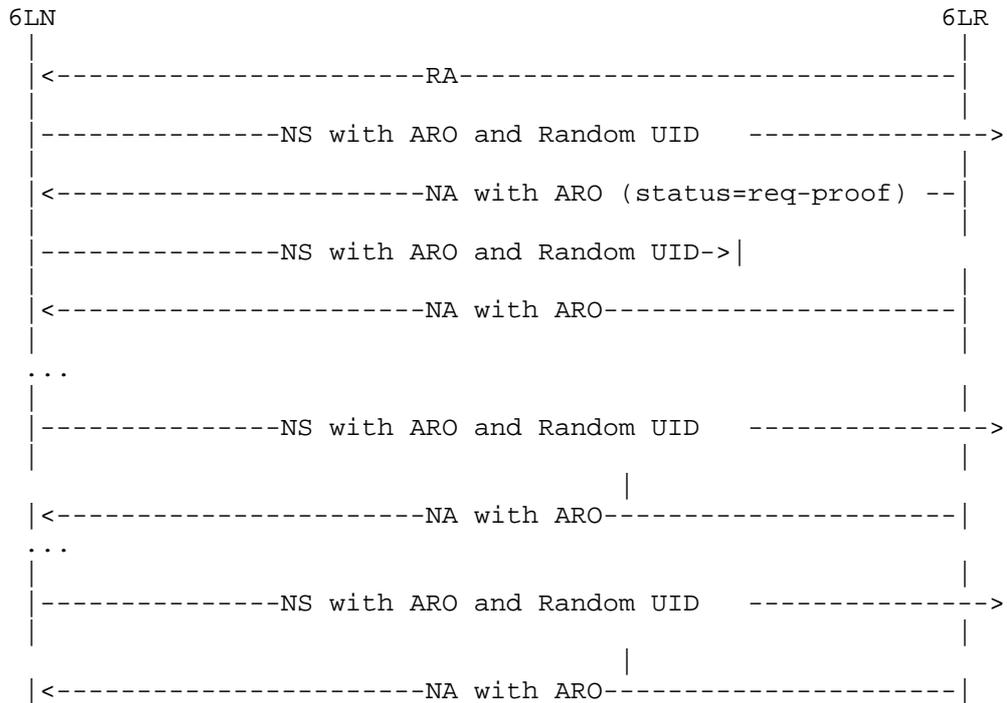
Figure 3: On-link Protocol Operation

4.2.1. Calculation of Cryptographic Identifier

   Elliptic Curve Cryptography (ECC) is used in the calculation of
   cryptographical identifier. The digital signature is constructed by
   using the 6LN's private key over its EUI-64, i.e. its MAC address.
   The signature value is computed using the ECDSA signature algorithm
   and hash function used is SHA-256. 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 using secp256r1 reduces the key size
   by 32 octets.

   After the calculation, 6LN sends it along with the CGA parameters in
   the first NS message, see Figure 3. In order to send Cryptographical
   Identifier a neighbor discovery option 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 if it is used as IPv6 address.

   6LN also sends some other parameters to enable 6LR or 6LBR to verify
   the crypto ID. One of them is 6LN's MAC address which is sent in
   Address Registration Option (ARO) as defined in [RFC6775]. The next

one is shown in Figure 5. In that figure, CGA Parameters field
contains the public key, prefix and some other values. Digital
signature option contains the signature of the CGA calculated using
6LN's private key.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |     Type      |    Length     |    Status     |   Reserved    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |           Reserved            |     Registration Lifetime     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    +                          crypto ID                            +
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
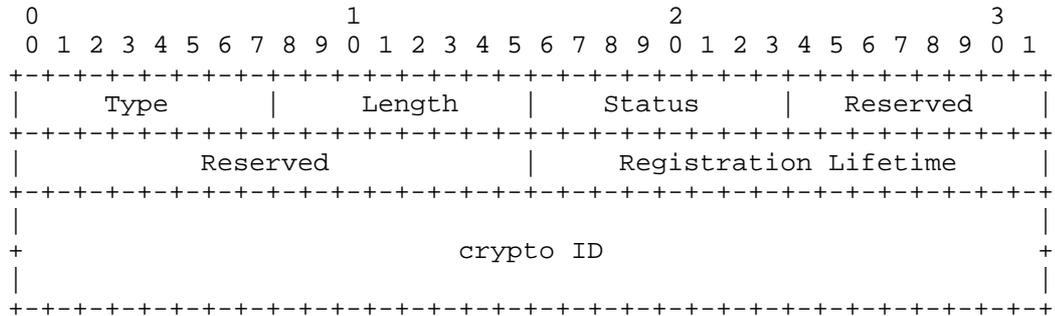
                      Figure 4: Crypto ID Option

   Type: TBA

   Length: 8-bit unsigned integer. The length of the option in units of
   8 bytes. It is 2 or 3, if crypto ID is 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.

   Registration Lifetime: 16-bit unsigned integer. The amount of time
   in units of 60 seconds that the router should retain the NCE for the
   sender of the NS that includes this option.

   Crypto ID Variable length field to carry the cryptographical
   identifier 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.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |      Type      |     Length    |   Pad  Length | Sig. Length   |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    .                                                               .
    .                        CGA Parameters                         .
    .                                                               .
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    .                                                               .
    .                       Digital Signature                       .
    .                                                               .
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    .                                                               .
    .                           Padding                             .
    .                                                               .
    |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
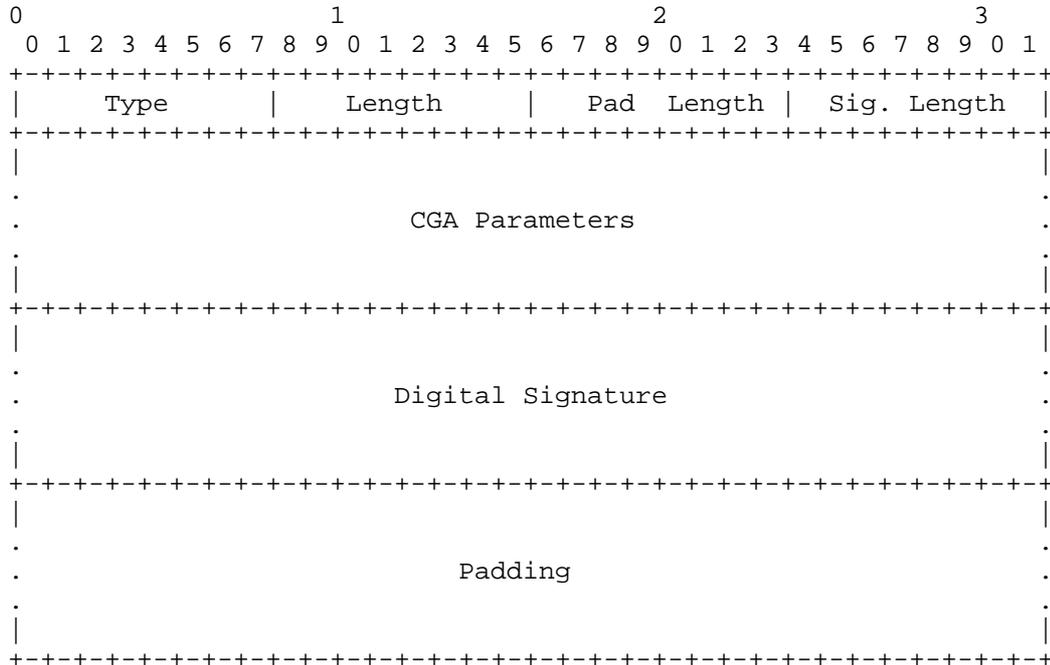
Figure 5: CGA Parameters Option

Type TBA

Length The length of the option in units of 8 octets.

Pad Length The length of the Padding field.

Sig Length The length of the Digital Signature field.

CGA Parameters The CGA Parameters field is variable-length containing
the CGA Parameters data structure.

Digital Signature The Digital Signature field is a variable length
field containing a Elliptic Curve Digital Signature Algorithm (ECDSA)
signature (with SHA-256 and P-256 curve of [FIPS-186-3]).

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-PAAR 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 user 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
we need 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.

5. Security Considerations

The same considerations regarding the threats to the Local Link Not
Covered (as in [RFC3971]) apply.

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

As to the attacks to the protocol itself, denial of service attacks
that involve producing a very high number of packets are deemed
unlikely because of the assumptions on the node capabilities in low-
power and lossy networks.

A collision of ID in ND-PAAR is a really rare event that does not
prevent the protocol operation though it opens a window for a node to
hijack an address from another. The nodes would normally not be
aware that they are in this situation, and the only thing they could
do if they knew would be to steal addresses from one another, so the
damage is limited to these 2 nodes.

6. IANA considerations

    TBD.

7. Acknowledgements

    TBD.

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>.

   [RFC3756]   Nikander, P., Ed., Kempf, J., and E. Nordmark, "IPv6
               Neighbor Discovery (ND) Trust Models and Threats",
               RFC 3756, DOI 10.17487/RFC3756, May 2004,
               <http://www.rfc-editor.org/info/rfc3756>.

   [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>.

   [RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk,
              "Elliptic Curve Cryptography Subject Public Key
              Information", RFC 5480, DOI 10.17487/RFC5480, March 2009,
              <http://www.rfc-editor.org/info/rfc5480>.

   [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>.

   [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>.

   [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>.

   [Guide]   "Guidelines for 64-bit global Identifier (EUI-64TM)",
              November 2012,
              <http://standards.ieee.org/develop/regauth/tut/eui64.pdf>.

8.2. Informative references

   [I-D.rafiee-6man-ssas]
              Rafiee, H. and C. Meinel, "A Simple Secure Addressing
              Scheme for IPv6 AutoConfiguration (SSAS)", draft-rafiee-
              6man-ssas-11 (work in progress), September 2014.

   [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.ietf-6tisch-architecture]
             Thubert, P., "An Architecture for IPv6 over the TSCH mode
             of IEEE 802.15.4", draft-ietf-6tisch-architecture-08 (work
             in progress), May 2015.

Authors' Addresses

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

   Email: sarikaya@ieee.org

   Pascal Thubert (editor)
   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