6lo
Internet-Draft
Intended status: Standards Track
Expires: September 10, 2015

B. Sarikaya, Ed.
Huawei USA
F. Xia
Huawei Technologies Co., Ltd.
P. Thubert, Ed.
Cisco

March 9, 2015

Lightweight and Secure Neighbor Discovery for Low-power and Lossy Networks
draft-sarikaya-6lo-cga-nd-02

Abstract

This document defines a lightweight and secure version of 6LoWPAN Neighbor Discovery for application in low-power and lossy networks. Cryptographically Generated Address and digital signatures are calculated using Elliptic Curve Cryptography, so that the cryptographic operations are suitable for low power devices. An optimal version of this protocol is also specified which supports faster CGA calculation and multi-hop operation. A node computes a Cryptographically Generated Address to be used as a Unique Interface ID, and associate all its Registered Addresses with that Unique Interface 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 unique ID, only the owner of that ID can modify the state in the 6LR and 6LBR regarding the Registered Address.

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 lossy wireless links. 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 a 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.

Neighbor Discovery Protocols (NDP) are not secure especially when physical security on the link is not assured and vulnerable to attacks defined in [RFC3756]. Secure neighbor discovery protocol (SEND) is defined to secure NDP [RFC3971]. Cryptographically Generated Addresses (CGA) are used in SEND [RFC3972]. SEND mandates the use of the RSA signature algorithm which is computationally heavy and not suitable to use for low-power and resource constrained nodes. The use of an RSA public key and signature leads to long message sizes not suitable to use in low-bit rate, short range, asymmetric and non-transitive links such as IEEE 802.15.4.

In this document, we extend 6LoWPAN ND with CGA; but as opposed to SEND, the cryptographic address is not necessarily used as Interface ID (IID) in an IPv6 address but 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 CGA 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 CGA.

To achieve this, this specification replaces the EUI-64 address, that is used in 6LoWPAN ND to avoid address duplication, with a CGA address whose ownership can be verified; it also provides new means for the 6LR to validate ownership of the CGA address by the registering device. A node generates one 64-bit CGA address 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 CGA address 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 indicate that the Unique Interface ID is CGA-based, and through the DAR/DAC exchange, the 6LBR is kept aware that this is the case and whether the 6LR has verified the claim.

CGA generation is based on elliptic curve cryptography (ECC)and signature is calculated using elliptic curve digital signature

algorithm (ECDSA) known to be lightweight, leading to much smaller packet sizes. The resulting protocol is called Lightweight Secure Neighbor Discovery Protocol (LSEND).

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 draft also conforms to the terms and models described in [RFC5889] and uses the vocabulary and the concepts defined in [RFC4291] for the IPv6 Architecture.

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.

CGA generation, signature and key hash calculation MUST avoid the use of SHA-1 which is known to have security flaws. In this document, we use SHA-2 instead of SHA-1 and thus avoid SHA-1's flaws.

Public key and signature sizes MUST be minimized and signature calculation MUST be lightweight. In this document we adopt ECC and ECDSA with the P-256 curve in order to meet this requirement.

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.

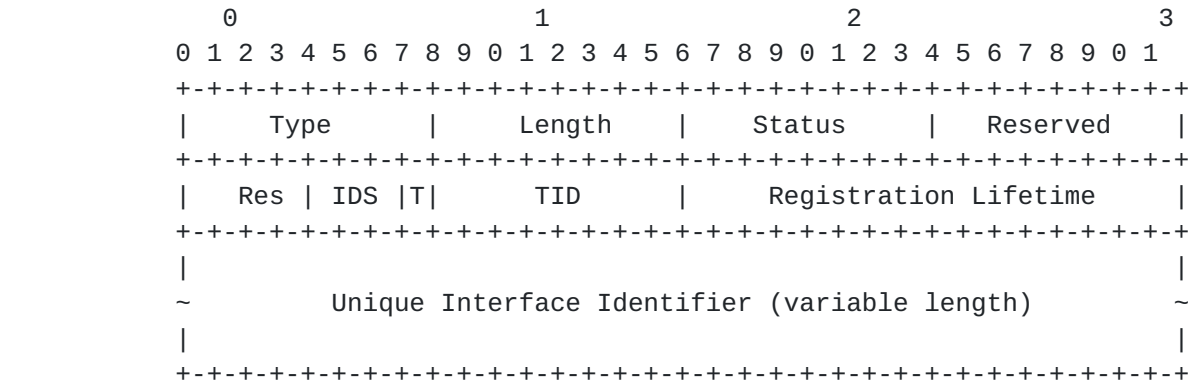
The Address Registration Option used in the ND registration SHOULD be extended to carry the relevant forms of Unique Interface IDentifier.

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

4. New and Modified Options

4.1. Modified Address Registration Option

The ARO option is modified to transport a CGA-based Unique Interface ID.



Track Forwarding, Transport Mode

Fields:

Type: 33 [RFC6775]

Length: 8-bit unsigned integer. Defined in [RFC6775]. The length of the option (including the type and length fields) in units of 8 bytes. The value 0 is invalid.

Status: 8-bit unsigned integer. Extended from [RFC6775]. Indicates the status of a registration in the NA response. MUST be set to 0 in NS messages. A new status for req-proof of to-be-defined-by-iana (4

suggested) indicates that the cryptographic material that proves the CGA ownership is requested in a new NS.

Reserved: 8 bits. This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

Res: 4 bits. This field is unused. It MUST be initialized to zero by the sender and MUST be ignored by the receiver.

IDS: Identifier name Space. Indicates the name space for the Unique Interface Identifier. IDS of 0 means EUI-64 UID. A new IDS to be assigned by IANA (a value of 2 is suggested) is defined for CGA-based Unique Interface ID.

T bit: 1 bit flag. Set if the TID octet is valid.

TID: 8-bit integer. It is a transaction id maintained by the host and used by the 6LR to indicate the registration that is being validated

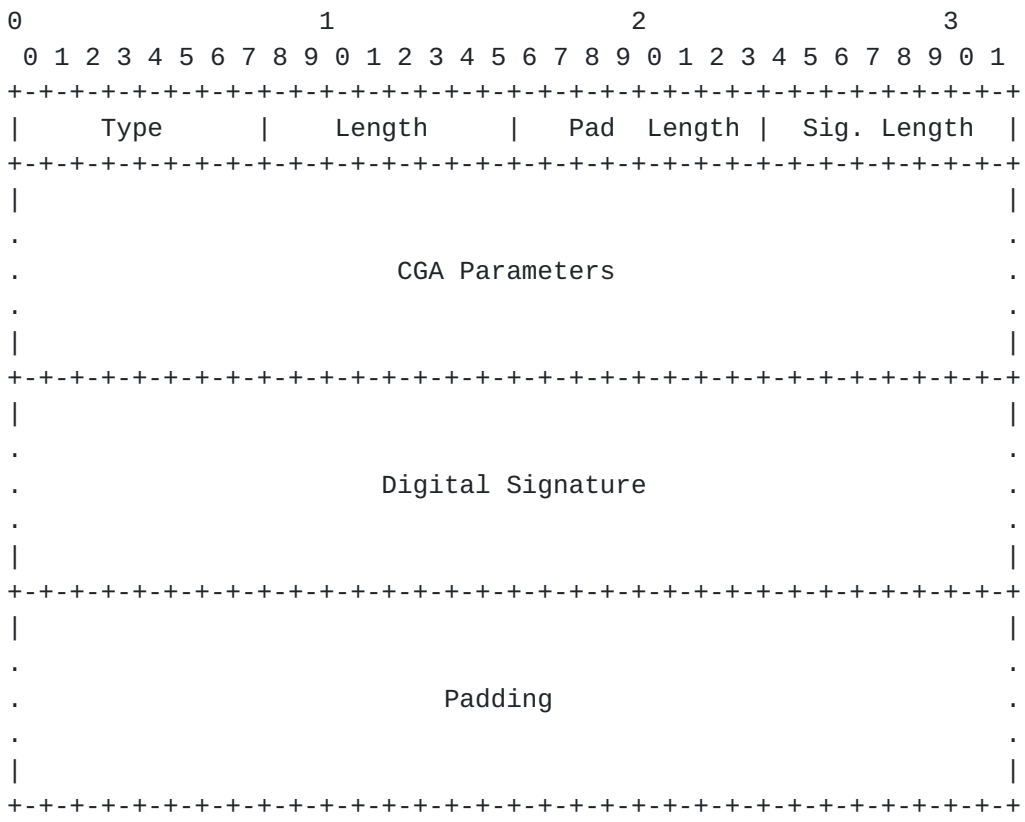
Registration Lifetime: 16-bit unsigned integer. Defined in [RFC6775]. The amount of time in a unit of 60 seconds that the router should retain the Neighbor Cache entry for the sender of the NS that includes this option. A value of zero means to remove the registration.

Unique Interface Identifier: 8 bytes. May be CGA-based with this specification.

4.2. CGA Parameters and Digital Signature Option

This option contains both CGA parameters and the digital signature.

A summary of the CGA Parameters and Digital Signature Option format is shown below.



Type

TBA1 for CGA Parameters and Digital Signature

Length

The length of the option (including the Type, Length, Pad Length, Signature Length, CGA Parameters, Digital Signature and Padding fields) 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 described in Section 4 of [RFC3972].

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]). Digital signature is constructed as explained in Section 4.4.

Padding

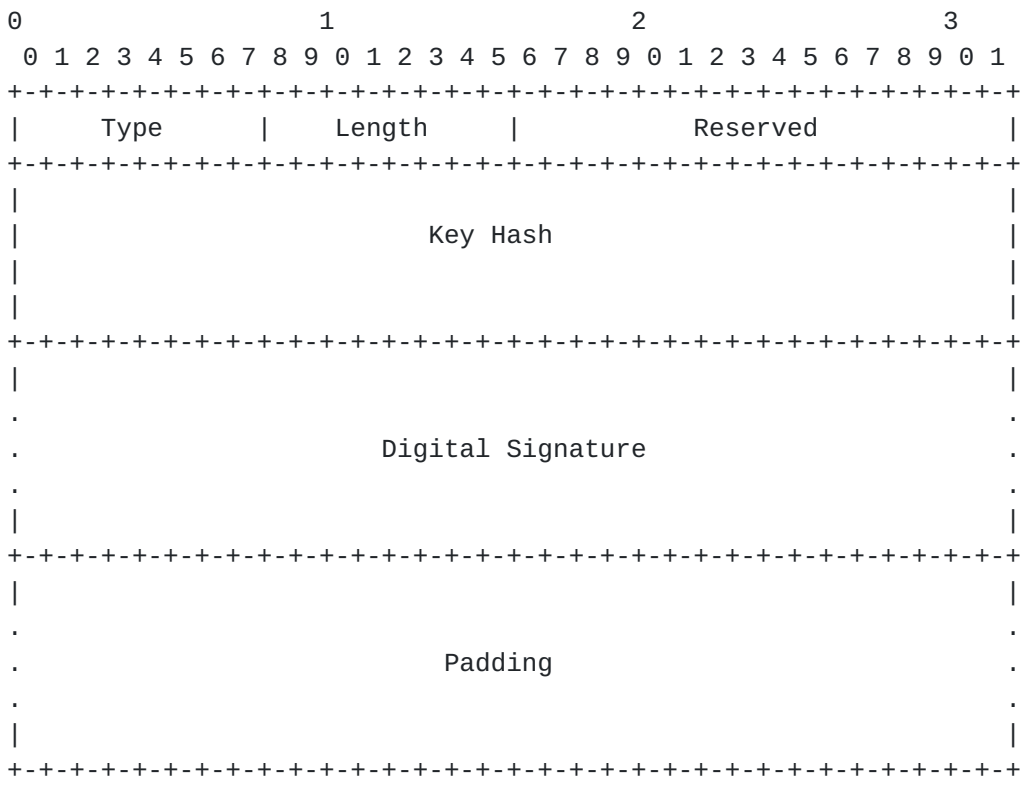
The Padding field contains a variable-length field making the CGA Parameters and Digital Signature Option length a multiple of 8.

4.3. Digital Signature Option

This option contains the digital signature.

A summary of the Digital Signature Option format is shown below. Note that this option has the same format as RSA Signature Option defined in [RFC3971]. The differences are that Digital Signature field carries an ECDSA signature not an RSA signature, and in calculating Key Hash field SHA-2 is used instead of SHA-1.

In the sequence of octets to be signed using the sender's private key includes 128-bit CGA Message Type tag. In LSEND, CGA Message Type tag of 0xE8C47FB7FD2BB885DAB2D31A0F2808B4 MUST be used.



Type

TBA2 for Digital Signature

Length

The length of the option (including the Type, Length, Reserved, Key Hash, Digital Signature and Padding fields) in units of 8 octets.

Key Hash

The Key Hash field is a 128-bit field containing the most significant (leftmost) 128 bits of a SHA-2 hash of the public key used for constructing the signature. This is the same as in [RFC3971] except for SHA-1 which has been replaced by SHA-2.

Digital Signature

Same as in Section 4.2.

Padding

The Padding field contains a variable-length field containing as many bytes long as remain after the end of the signature.

4.4. Calculation of the Digital Signature and CGA Using ECC

Due to the use of Elliptic Curve Cryptography, the following modifications are needed to [RFC3971] and [RFC3972].

The digital signature is constructed by using the sender's private key over the same sequence of octets specified in Section 5.2 of [RFC3971] up to all neighbor discovery protocol options preceding the Digital Signature option containing the ECC-based signature. The signature value is computed using the ECDSA signature algorithm as defined in [SEC1] and hash function SHA-256.

Public Key is the most important parameter in CGA Parameters defined in Section 4.2. Public Key MUST be DER-encoded ASN.1 structure of the type SubjectPublicKeyInfo formatted as ECC Public Key. The AlgorithmIdentifier, contained in ASN.1 structure of type SubjectPublicKeyInfo, MUST be the (unrestricted) id- ecPublicKey algorithm identifier, which is OID 1.2.840.10045.2.1, and the subjectPublicKey MUST be formatted as an ECC Public Key, specified in Section 2.2 of [RFC5480].

Note that the ECC key lengths are determined by the namedCurves parameter stored in ECParameters field of the AlgorithmIdentifier. The named curve to use is secp256r1 corresponding to P-256 which is OID 1.2.840.10045.3.1.7 [SEC2].

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. In LSEND, point compression MUST be supported.

5. Protocol Interactions

Lightweight Secure Neighbor Discovery for Low-power and Lossy Networks (LSEND for LLN) modifies Neighbor Discovery Optimization for Low-power and Lossy Networks [RFC6775] as explained in this section. Protocol interactions are shown in Figure 1.

6LoWPAN Nodes (6LN, or simply "nodes") receive RAs from adjacent 6LRs and generate their own cryptographically generated addresses using elliptic curve cryptography as explained in Section 4.4. The node sends a neighbor solicitation (NS) message with the address registration option (ARO) to 6LR. Such a NS is called an address registration NS.

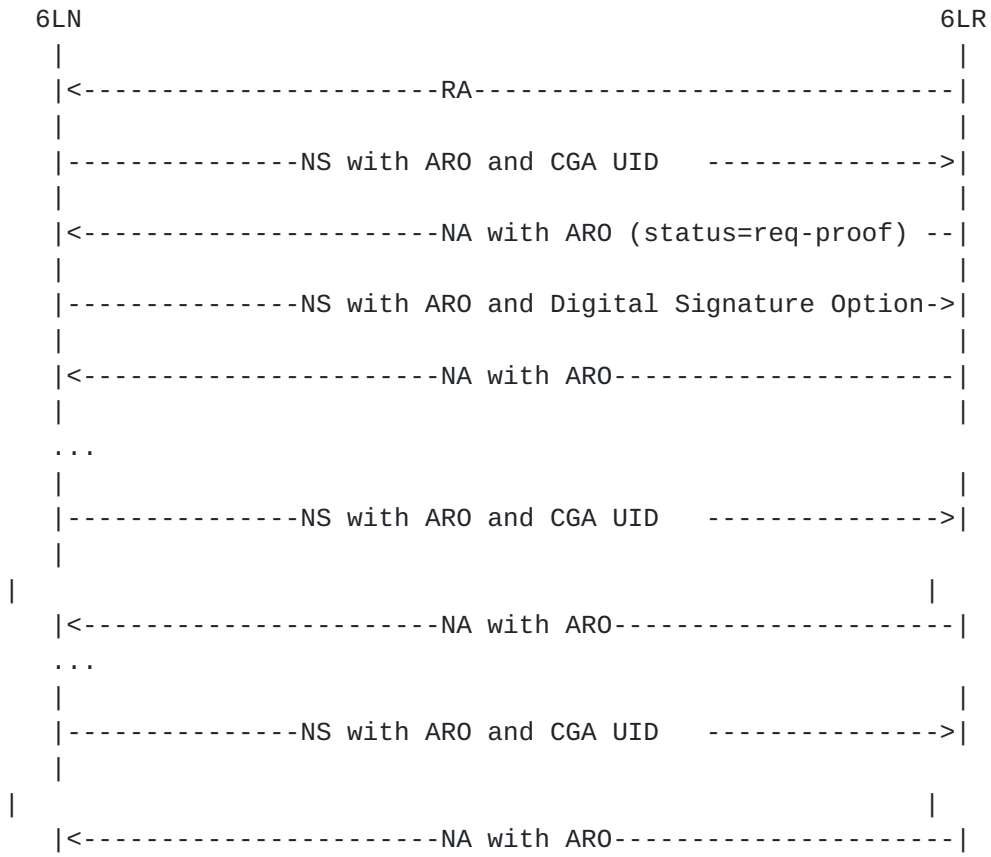


Figure 1: Lightweight SEND for LLN Protocol

6. Optimizations

In this section we present optimizations to the base LSEND defined above. We use EUI-64 identifier instead of source address in CGA calculations. We also extend LSEND operation to 6LoWPAN multihop network.

6.1. 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].

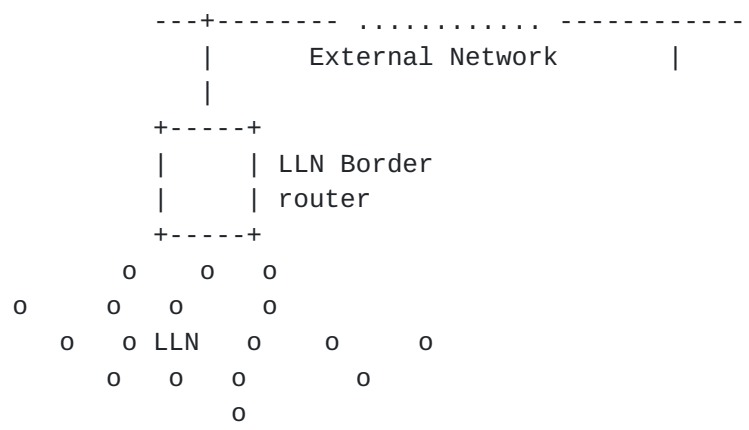


Figure 2: Basic Configuration

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 3:

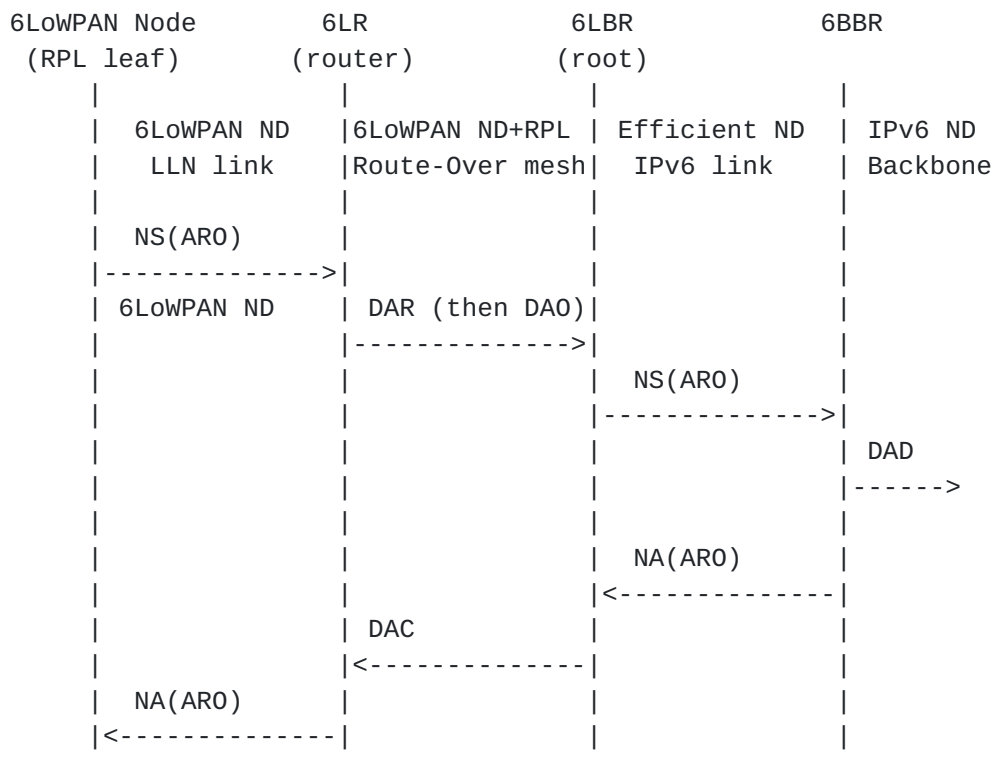


Figure 3: (Re-)Registration Flow over Multi-Link Subnet

A new device that joins the network auto-configures and 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 with 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 limit 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 Cryptographically Generated Address (CGA) [RFC3972] 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 based on CGA, so as to enforce that any update via a different 6LR is also based on CGA.

6.2. Protocol Operations

Digital signature and CGA are calculated over EUI-64 or interface id of the node. It is only done initially at once not repeated with every message the node sends. The calculation does not change even if the node has a new address since EUI-64 does not change. This means that this CGA can be used to claim multiple targets. The calculation is ECC based as described in Section 4.4.

Protocol interactions are as defined in Section 5. The address registration NS message contains CGA Parameters and Digital Signature Option defined in Section 4.2. The node MUST set the Extended Unique Interface IDentifier (EUI-64) field [Guide] in ARO to the crypotographically generated address. The Subnet Prefix field of CGA Parameters MUST be set to the 64-bit prefix in the RA message received from 6LBR. Source address MUST be set to the prefix concatenated with the node's crypotographically generated address. The Public Key field of CGA Parameters MUST be set to the node's ECC Public Key.

CGA calculated may need to be modified before it is used as EUI-64. The b2 bit or U/L or "u" bit MUST be set to zero for globally unique and b1 bit or I/G or "g" bit MUST be set to zero for unicast before using it in IPv6 address as the interface identifier. In LSEND, senders and receivers ignore any differences in the three leftmost bits and in bits 6 and 7 (i.e., the "u" and "g" bits) in the interface identifiers [RFC3972].

The Target Address field in NS message is set to the prefix concatenated with the node's crypotographically generated address. This address does not need duplicate address detection as EUI-64 is globally unique. So a host cannot steal an address that is already registered unless it has the key for the EUI-64. The same EUI-64 can thus be used to protect multiple addresses e.g. when the node

receives a different prefix. The node adds CGA Parameters (including Public Key) and Digital Signature Option defined in Section 4.2 into NS message. The node sends the address registration option (ARO) which is set to the CGA calculated.

Protocol interactions given in Figure 1 are modified a bit in that Digital Signature option with the public key 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 cryptographical material 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 CGA 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 EUI-64 and have the 6LR/6LBR enforce first come first serve after that.

6.3. 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 LSEND we extend DAR/DAC messages to carry CGA Parameters and Digital Signature Option defined in Section 4.2.

In a multihop 6LoWPAN, the node exchanges the messages shown in Figure 3. 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 CGA (that it received in ARO) or the crypto information (that it received in CGA Parameters and Digital Signature Option). 6LR should be able to ask for it again. This is done by restarting the exchanges shown in Figure 1. The result enables 6LR to refresh CGA and public key information that was lost. 6LR MUST send DAR message with CGA Parameters and Digital Signature Option and 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 CGA and crypto information to make sure that the 6LR is not a fake.

7. 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.

8. IANA considerations

This document defines two new options to be used in neighbor discovery protocol messages and new type values for CGA Parameters and Digital Signature Option (TBA1) and Digital Signature Option (TBA2) need to be assigned by IANA.

This document defines 0xE8C47FB7FD2BB885DAB2D31A0F2808B4 for LSEND CGA Message Type Tag.

9. Acknowledgements

TBD.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC4903] Thaler, D., "Multi-Link Subnet Issues", RFC 4903, June 2007.

[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, August 2007.

[RFC5480] Turner, S., Brown, D., Yiu, K., Housley, R., and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information", RFC 5480, March 2009.

[RFC5889] Baccelli, E. and M. Townsley, "IP Addressing Model in Ad Hoc Networks", RFC 5889, September 2010.

[RFC6550] Winter, T., Thubert, P., 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, March 2012.

[RFC6775] Shelby, Z., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, November 2012.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, April 2014.

[SEC1] "Standards for Efficient Crtptography Group. SEC 1: Elliptic Curve Cryptography Version 2.0", May 2009.

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

[ANSIX9.62]
"American National Standards Institute (ANSI), ANS X9.62-2005: The Elliptic Curve Digital Signature Algorithm (ECDSA)", November 2005.

10.2. Informative references

[SEC2] "Standards for Efficient Crtptography Group. SEC 2: Recommended Elliptic Curve Domain Parameters Version 2.0", January 2010.

[FIPS-186-3]
"National Institute of Standards and Technology, "Digital Signature Standard"", June 2009.

[NIST-ST] "National Institute of Standards and Technology, "NIST Comments on Cryptanalytic Attackts on SHA-1"", January 2009, <http://csrc.nist.gov/groups/ST/hash/statement.html>.

[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., Watteyne, T., Struik, R., and M. Richardson, "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4e", draft-ietf-6tisch-architecture-06 (work in progress), March 2015.

Authors' Addresses

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

Email: sarikaya@ieee.org

Frank Xia
Huawei Technologies Co., Ltd.
101 Software Avenue, Yuhua District
Nanjing, Jiangsu 210012, China

Phone: ++86-25-56625443
Email: xiayangsong@huawei.com

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