6lo
Internet-Draft
Intended status: Standards Track
Expires: September 13, 2017

AR. Sangi
M. Chen
Huawei Technologies
C. Perkins
Futurewei

March 12, 2017

Designating 6LBR for IID Assignment
draft-rashid-6lo-iid-assignment-03

Abstract

In IPv6 Stateless Address Autoconfiguration (SLAAC), randomizing the interface identifier (IID) is a common practice to promote privacy. If there are a very large number of nodes, as has been discussed in several use cases, the effect will to proportionately increase the number of IIDs. A duplicate address detection (DAD) cycle is needed for each configured IID, introducing more and more overhead into the network. Each failed DAD requires the initiating node to regenerate a new IID and undergo the DAD cycle again. This document proposes an optimized approach when higher privacy is required in a given network by allowing a 6LBR (6LoWPAN Border Router) to provide a unique IID, avoiding any potential duplication. Such practice also prevents failure of time-critical applications, by enabling 6LBR to provide a unique IID, in case of address collision.

Further improvements are proposed to enable multiple concurrent DAD cycles, and to return the randomized IID from 6LBR to 6LN in a space-efficient manner.

Table of Contents

1. Introduction

IPv6 addresses in SLAAC are formed by concatenating a network prefix, acquired from Router Advertisement (RA) messages, with a locally generated IID [RFC4862], [RFC2464]. Since the best method for generating IIDs varies depending on the network, none of the proposed mechanisms [RFC4941],[RFC7217] is considered a default mechanism. Using neighbour discovery (ND), the uniqueness of newly a generated IID is verified [RFC6775]. 6LBR performs DAD, and replies with a status. A failed DAD would require the initiating 6LN (6LoWPAN node) to regenerate an IID and wait for another DAD cycle, until the 6LN successfully registers a unique address [RFC6775].

A locally generated IID can be derived either from an embedded IEEE identifier [RFC4941], or randomly (based on a few variables) [RFC7217]. Since MAC reuse is unfortunately far more common than usually assumed [RFC7217][MAC-Duplication], IIDs derived from MAC address are likely to cause more than the expected number of DAD failures. As soon as the 6LN generates an IID, it sends the NS (Neighbor Solicitation) message to 6LR (LLN Router). Then 6LR proceeds to send an ICMPv6 based DAR (Duplicate Address Request) message to 6LBR. An LN sends out a NS after checking its local cache for duplication; before proceeding with DAR, the 6LR also protects against address duplication within a locally maintained Neighbor Cache Entry (NCE) [RFC7217].

Use cases including huge numbers of nodes and vast scale networks are discussed in [RFC5548], [RFC5827]. The use of arbitrary IIDs can resolve privacy concerns for a participating node, but a simple NS intended to be targeted to a small group of nodes can pollute a great deal of wireless bandwidth [I-D.vyncke-6man-mcast-not-efficient]. Multicast NS and NA are much more frequent in large scale radio environment with mobile devices [I-D.ietf-6lo-backbone-router]. Since the IIDs may be sporadically changed for privacy, the probability further increases that a duplicate IIDs would result in DAD failure and repeated DAD cycles.

On the other hand, waiting for 6LN to regenerate another IID due to a failed DAD might lead to failure of a time-critical application.

Address assignment can also be done using DNS (Domain Name Server), but doing so typically requires multicast traffic and introduces more control overhead. Unlike DNS, the 6LoWPAN ND works on layer 2 and our proposed mechanism implicitly provides assistance to the DAD process.

This document describes improvements to 6LoWPAN ND which enable 6LBR to grant a unique IID for failed DAD, to enable multiple concurrent DAD cycles, and to return an IID to 6LN in a space-efficient manner.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]. This document uses terminology from [RFC6775], [RFC2464], [RFC8064], and [RFC7721].

SLLAO: Stateless Link-Local Address Option

RID: Random IDentifier

PRF: Pseudo Random Function

IID: Interface IDentifier

This document also uses the following terms:

EARO: Extended Address Registration Option

EDAR: Extended Duplicate Address Request

EDAC: Extended Duplicate Address Confirmation

LSB: Least Significant Bit

3. Likelihood of Address Collision

The following observations have motivated the design of this proposal:

- Manufacturer may not follow a fine grained randomness in MAC addresses.
- MAC addresses shorter than 64 bits are used in various constrained technologies.
- The frequency of an IID being changed depends on the degree of privacy that a particular application requires.
- Depending upon the method by which an IID is generated using MAC address, or with shorter MAC addresses, address collisions may become much more likely.

4. IID Assignment by 6LBR

MAC driven IIDs [RFC2464] reduce or eliminate the need for DAD, but in practice such IID generation is discouraged ([RFC8064], [RFC7721]), as common privacy concerns still persist, for instance:

- Network activity correlation,
- Location tracking,
- Address scanning, and
- Device-specific vulnerability exploitation.

Multiple approaches are proposed to suit different network constraints. The mechanisms specified in [RFC4941], which are mainly

based on MAC address or an appropriate simple random number generation algorithm can also be used to generate IID.

Considering the scalability of a network and enabling 6LBR to randomize an IID, the method for IID generation specified in [RFC7217] SHOULD be used because this method is appropriate to support periodically changing IIDs.

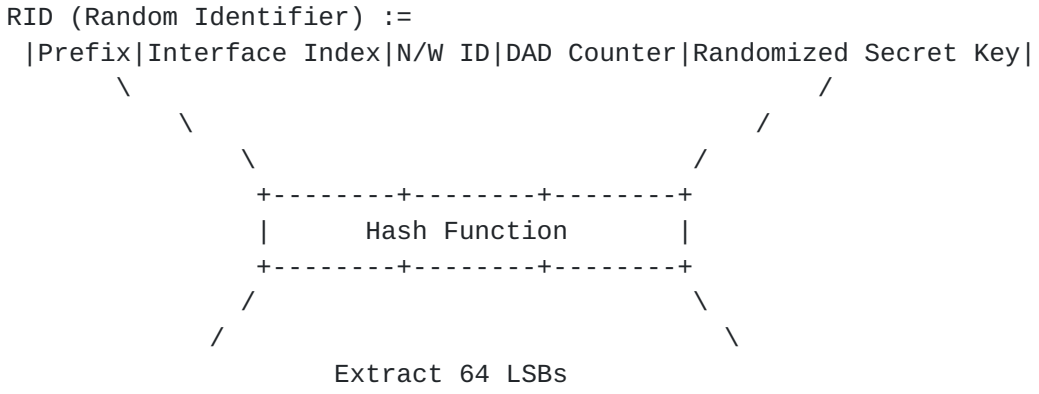

Figure 1: Using RFC7217 to generate IID

If DAD fails, the 6LBR will use public values for Prefix, Interface Index, and Network ID; the remaining two variables (DAD Counter, Randomized Secret Key) are local values. Neighbor solicitation using link-local address cannot be avoided, but only the newly generated IID needs to be forwarded to the LN.

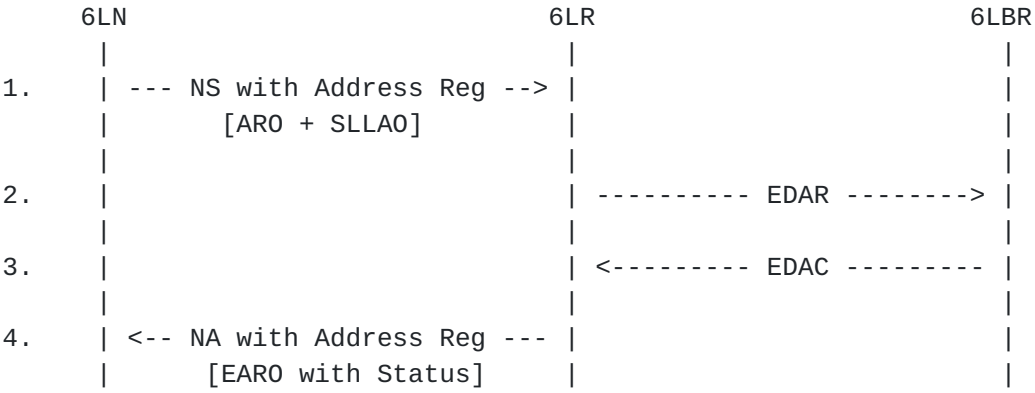

Figure 2: DAD cycle when 6LBR generates an IID

The approach in this draft is reactive rather than proactive; 6LBR only replies with a locally generated IID when DAD fails.

Appendix A [RFC7217] states that a Net_Iface parameter can either be:

o Interface Index,

- Interface Name,
- Link-Layer Address, or
- Logical Network Service Identity.

EUI-64 of 6LN would be sent to 6LBR via 6LR within EARO and using that, a Link-Layer Address can be derived at 6LBR to input in PRF. For multiple interfaces, DAD_counter would be incremented as soon as the collision occurs.

4.1. Advantages of proposed algorithm

By reference to the algorithm in [RFC7217], the resulting IID offers the following advantages:

- For a given interface, same prefix and subnet would always result in same IID,
- It would always be a different IID generated when a different prefix is used, and
- The DAD_Counter parameter is incremented in case of address collision, so that the resulting address would be different than the previous address.

4.2. Extended Duplicate Address Request (EDAR)

The Prefix is the same throughout each LoWPAN network. This draft uses that feature to reduce the size of the DAR:

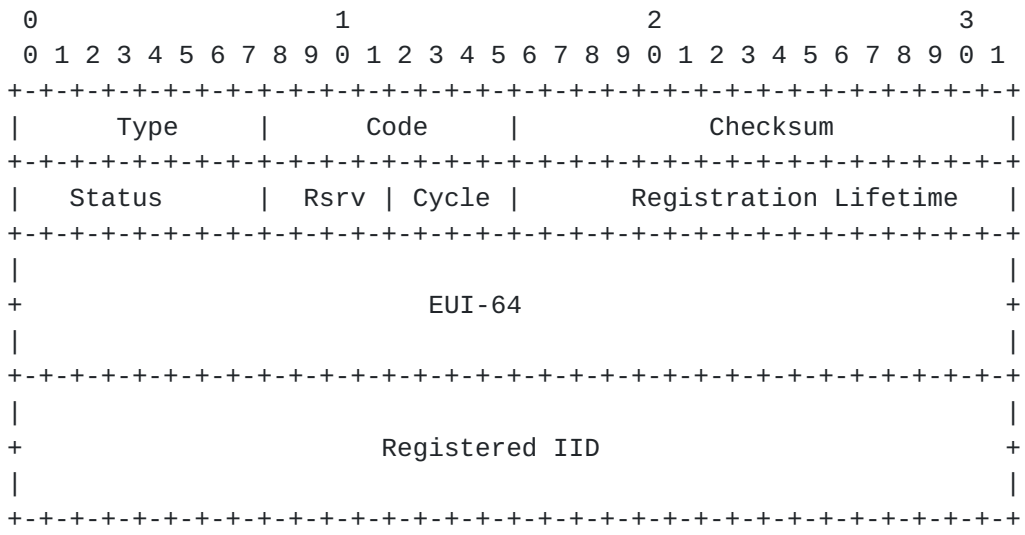

Figure 3: Extended Duplicate Address Request

The fields are similar to DAR in [RFC6775] except:

- Type: 159 (TBD)
- Cycle: 4 out of 8 reserved bits to identify the DAD cycle between given 6LR and 6LBR. The reference is used later by 6LR to extract IID provided by 6LBR.
- Unlike the DAR, the Registered IID (64 bit) is returned instead of Registered Address (128 bit).

4.3. Extended Duplicate Address Confirmation (EDAC)

EDAC reduces the space needed for returning the EUI-64:

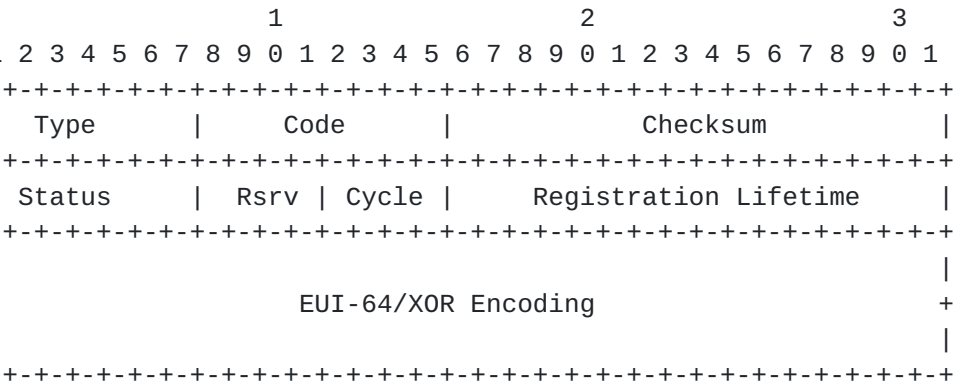

Figure 4: Extended Duplicate Address Confirmation

The fields are similar to DAC in [RFC6775] except:

- Type: 160 (TBD)
- Cycle: 4 out of 8 reserved bits identify the DAD cycle between the 6LR and 6LBR. These bits are used later by 6LR to extract the IID supplied by 6LBR.
- In case of a failed DAD, a 6LBR-generated IID is encoded using XOR with EUI-64; otherwise the same EUI-64 occupies the 64 bits.

4.4. Extended Address Registration Option

ARO and EARO can ONLY be initiated by host and 6LR, respectively. [RFC6775] expects the reply of a host initiated ARO from 6LR with the same ARO except for changing the status bit to indicate the duplication detection. EARO is introduced in this document; 6LR can send out this option if it receives EDAC instead of DAC from 6LBR.

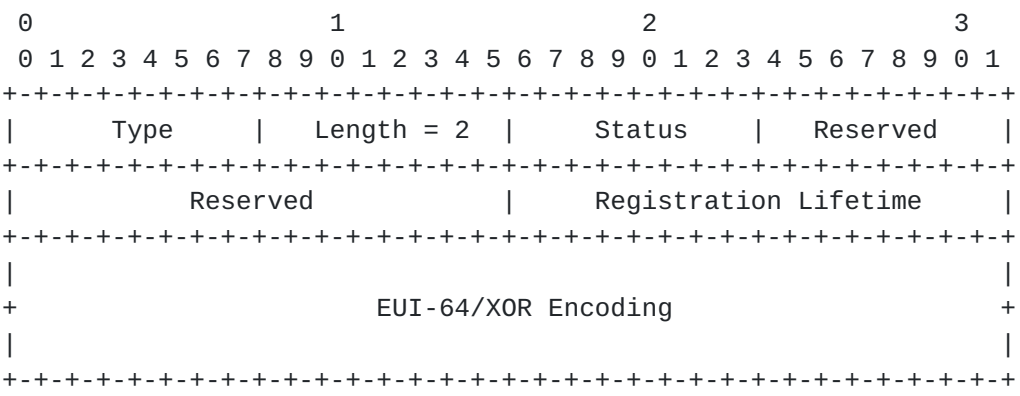

Figure 5: Extended Address Registration Option

- The fields are similar to ARO in [RFC6775] except:

- Type: 36 (TBD)

- EUI-64/XOR Encoding: a 64 bit IID generated by 6LBR is XOR'ed with EUI-64.

5. Multiple DAD cycles

In [RFC6775], 6LN is expected to generate an IID; so 6LR only acts on the first unique IID claim and silently discards any later claims for the same IID. In contrast, this document enables 6LBR to assign a unique IID in case of a duplicate IID claim by 6LR. For this purpose, a "Cycle" field is introduced to enable multiple concurrent DAD cycles that will be helpful for large-scale networks [RFC5548]. At 6LN, this "Cycle" field is also used when extracting both IID and EUI-64 that are XOR'ed by 6LBR. See Figure 3 and Figure 4 for the format of the Cycle field.

6. XOR Encoding

Each iteration of DAR and DAC [RFC6775] carries the entire 128 bit Registered Address during the DAD routine, even though the network Prefix is the same throughout each LoWPAN. This document enables eliding the network prefix part of the Registered Address as well in EDAC and EARO using simple XOR encoding. The encoded 64 bit field carries EUI-64 and randomized IID. See Figure 4 and Figure 5 for the format of the EUI-64/XOR encoding.

Under the proposed arrangement, 6LBR would only encode values, 6LN would only extract values and 6LR would do both.

At 6LR before sending EDAR to 6LBR:

o 6LR would use the 4 out of 8 Reserved "Cycle" bits of EDAR to keep track of multiple DAD cycles. These iterations are recorded at 6LR and that information is used to extract IID/EUI-64 from EDAC to be forwarded to the appropriate 6LN.

At 6LBR before sending to 6LR:

o If Status = 0 (Success), then 6LBR returns EDAC using all the values as received from EDAR.

o If Status = 1 (Duplicate), then 6LBR generates IID and XORs it with EUI-64 to return in the EDAC to 6LR.

At 6LR before sending to 6LN:

o If Status = 0 (Success) then keep the claimed address of 6LN as Destination Address for ARO to 6LN.

o If Status = 1 (Duplicate), then match the "Cycle" bits of EDAC to extract (using XOR) the EUI-64 address and use the extracted address as the Destination Address for EARO to 6LN.

Finally, at 6LN:

o If Status = 0 (Success), 6LN starts using the address that it claimed.

o If Status = 1 (Duplicate) then 6LN XORs the received EUI-64 address with its claimed EUI-64, which results in the newly generated IID sent by 6LBR.

7. IANA Considerations

7.1. EDAR and EDAC Messages, and EARO Option

The document requires two new ICMPv6 type numbers under the subregistry 'ICMPv6 "type" Numbers':

o Extended Duplicate Address Request (159)

o Extended Duplicate Address Confirmation (160)

This document requires a new ND option type under the subregistry "IPv6 Neighbor Discovery Option Formats":

o Extended Address Registration Option (36)

7.2. Additions to Status Field

One new value is required for the "Address Registration Option Status Values" sub-registry under the "IPv6 Neighbor Discovery Option Formats":

Status	Description	
0	Success	
1	Duplicate Address	
2	Neighbor Cache Full	
3	6LBR generated IID	
4-255	Allocated using Standards Action [RFC5226]	

Addition to Status bits

8. Security Considerations

TBD

9. References

9.1. 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>.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998, <http://www.rfc-editor.org/info/rfc2464>.

[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>.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <http://www.rfc-editor.org/info/rfc4941>.

[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>.

[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>.

9.2. Informative References

[I-D.ietf-6lo-backbone-router] Thubert, P., "IPv6 Backbone Router", draft-ietf-6lo-backbone-router-03 (work in progress), January 2017.

[I-D.vyncke-6man-mcast-not-efficient] Vyncke, E., Thubert, P., Levy-Abegnoli, E., and A. Yourtchenko, "Why Network-Layer Multicast is Not Always Efficient At Datalink Layer", draft-vyncke-6man-mcast-not-efficient-01 (work in progress), February 2014.

[MAC-Duplication] Moore, HD., "The Wild West", September 2012, <https://speakerdeck.com/hdm/derbycon-2012-the-wild-west>.

[RFC5548] Dohler, M., Ed., Watteyne, T., Ed., Winter, T., Ed., and D. Barthel, Ed., "Routing Requirements for Urban Low-Power and Lossy Networks", RFC 5548, DOI 10.17487/RFC5548, May 2009, <http://www.rfc-editor.org/info/rfc5548>.

[RFC5827] Allman, M., Avrachenkov, K., Ayesta, U., Blanton, J., and P. Hurtig, "Early Retransmit for TCP and Stream Control Transmission Protocol (SCTP)", RFC 5827, DOI 10.17487/RFC5827, May 2010, <http://www.rfc-editor.org/info/rfc5827>.

[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, <http://www.rfc-editor.org/info/rfc7721>.

[RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <http://www.rfc-editor.org/info/rfc8064>.

Authors' Addresses

Abdur Rashid Sangi
Huawei Technologies
No.156 Beiqing Rd. Haidian District
Beijing 100095
P.R. China

Email: sangi_bahrian@yahoo.com

Mach(Guoyi) Chen
Huawei Technologies
No.156 Beiqing Rd. Haidian District
Beijing 100095
P.R. China

Email: mach.chen@huawei.com

Charles E. Perkins
Futurewei
2330 Central Expressway
Santa Clara 95050
USA

Email: charliep@computer.org