Designating 6LBR for IID Assignment
draft-rashid-6lo-iid-assignment-00

Abstract

In IPv6 Stateless Address Autoconfiguration (SLAAC), use of a random 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 be 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 that requires 6LBR (6LoWPAN Border Router) to provide a unique IID, avoiding the potential duplication.

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 September 17, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents
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 depends on the nature of networks, none of the proposed mechanisms is considered a default mechanism [RFC4941], [RFC7217]. Using neighbour discovery (ND), the uniqueness of newly generated IID is verified [RFC6775]. 6LBR ensures the duplication detection, and replies with a status. A failed DAD would require the initiating 6LN (6LoWPAN Node) to regenerate an IID and undergo another DAD cycle, until either 6LN succeeds or reaches its maximum number of retries [RFC6775].

A locally generated IID can be derived from embedded IEEE identifier [RFC4941] or randomly (based on a few variables) [RFC7217]. MAC reuse is far common than assumed [RFC7217], and 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) and 6LR proceeds with the address duplication request routine with 6LBR by sending an ICMPv6 based DAR (Duplicate Address Request) message. 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].

[RFC5548], [RFC5827] discuss use cases including huge numbers of nodes and vast scale networks. The arbitrary use of IIDs resolves the privacy concerns of participating node. A simple NS supposedly targeted to a very small group of nodes MAY ends-up polluting whole 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.thubert-6lo-backbone-router]. Additionally, as the IIDs are periodically changed for privacy, the probability becomes high for a duplicate IIDs that would results in DAD failure and repeated cycles.

This document describes optimization to 6LoWPAN ND by enabling 6LBR to grant a unique IID for failed DAD.

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]. Additionally, this document uses terminology from [RFC6775], [RFC2464], [I-D.ietf-6man-default-iids], and [I-D.ietf-6man-ipv6-address-generation-privacy]. This document also uses the following terms:

RID: Random identifier.

PRF: Pseudo random function.

LSB: Least significant bit.

EDAC: Extended duplicate address confirmation.

EARO: Extended address registration option.

3. IID Assignment by 6LBR

MAC driven IIDs [RFC2464] reduce or eliminate the the need for DAD, but in practice such IID generation is discouraged ([I-D.ietf-6man-default-iids], [I-D.ietf-6man-ipv6-address-generation-privacy]), as common privacy concerns still persist, for instance:

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

Moreover, multiple approaches are proposed to suit different network constraints. Considering the scalability of a network and enabling 6LBR to suggest an IID, this draft proposes another IID generating [RFC7217] approach to support periodically changing IIDs.

```
RID (Random Identifier) :=
   Prefix|Interface Index|N/W ID|DAD Counter|Randomized Secret Key|
   \    \          \         \           \            /         /
   \          \          \          \        /            +--------+--------+--------+
   \                                                            |      Hash Function       |
   \                                                            +--------+--------+--------+
   \                                                            /                            
   \                                                        /                                    
   \                                /                  /                                
   \                           /                              /                                
   \                          /                             /                                
   \                        /                            /                                
   \                      /                          /                                
   \                    /                        /                                
   \                  /                      /                                
   \                /                    /                                
   \              /                  /                                
   \            /                /                                
   \          /            /                                
   \        /        /                                
   \      /      /                                
   \    /    /                                
   \  /  /                                
   \|/|/                                
   \Extract 64 LSBs
```

**Figure 1:** Using RFC7217 to generate IID

In case DAD fails, the 6LBR will use public values for Prefix, Interface Index, and Network ID; the remaining two variables (DAD Counter, Randomized Private Key) are local values. Neighbor solicitation using link-local address cannot be avoided, but only the newly generated IID needs to be passed on to LN (by way of relevant 6LR).

```
6LN         6LR          6LBR
1. --- NS with Address Reg --> [ARO + SLLAO]
2.              -------------- DAR -------------->
3.              <------------ EDAC ---------->
4. <--- NA with Address Reg --- [EARO with Status]
```

**Figure 2:** DAD cycle when 6LBR generates an IID

The Approach in this draft is of reactive nature rather than proactive. 6LBR only replies with locally generated IID when DAD fails.
3.1. Extended Confirmation Message

The Prefix is the same throughout each LoWPAN network. This draft extends the DAC:

```
  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     |      Code     |            Checksum           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   Status      |    Reserved   |       Registration Lifetime   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                        EUI-64                             +       |
|                                                               |
|                                                               |
|                     6LBR Generated IID                        +       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3: Extended Duplication Address Confirmation

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

Type: 159

6LBR Generated IID: 64 bit IID generated by 6LBR.

3.2. 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 same ARO except the changed status bit to indicate the duplication result. EARO is introduced in this document and 6LR can send out this option if it receives EDAC instead of DAC from 6LBR.
The fields are similar to ARO in [RFC6775] except:

Type: 36

6LBR Generated IID: a 64 bit IID generated by 6LBR.

4. IANA Considerations

4.1. Additions of EDAC Message and EARO Option

The document requires one new ICMPv6 "type" number under the subregistry "ICMPv6 "type" Numbers":

- Extended Duplicate Address Confirmation (159)

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

- Extended Address Registration Option (36)

4.2. Additions to Status Field

IANA is required to assign two new values to the Status bit in Address Registration Option under the sub registry "IPv6 Neighbor Discovery Option Formats":

---

Figure 4: Extended Address Registration Option
<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Success</td>
</tr>
<tr>
<td>1</td>
<td>Duplicate Address</td>
</tr>
<tr>
<td>2</td>
<td>Neighbor Cache Full</td>
</tr>
<tr>
<td>3</td>
<td>6LBR generated IID</td>
</tr>
<tr>
<td>4-255</td>
<td>Allocated using Standards Action [RFC5226]</td>
</tr>
</tbody>
</table>

Supplementary to Status bits

5. Security Considerations

TBD

6. References

6.1. Normative References


6.2. Informative References


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

Email: rashid.sangi@huawei.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