

IPv6 maintenance Working Group (6man)
Internet-Draft
Updates: [RFC4941](#) (if approved)
Intended status: Standards Track
Expires: November 24, 2016

F. Gont
SI6 Networks / UTN-FRH
W. Liu
Huawei Technologies
May 23, 2016

Recommendation on Non-Stable IPv6 Interface Identifiers
draft-gont-6man-non-stable-iids-00

Abstract

This document clarifies the stability requirements for IP6 addresses, and provides recommendations regarding the generation of non-stable addresses. Finally, it formally updates [RFC4941](#) such that nodes are allowed to configure only temporary addresses.

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 November 24, 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 (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents 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	2
2.	Terminology	2
3.	Stability Requirements for IPv6 Addresses	3
4.	Requirements for Non-Stable IPv6 Addresses	3
5.	Generation of Non-Stable IPv6 Addresses	4
6.	Update to existing RFCs	4
7.	Future Work	4
8.	IANA Considerations	5
9.	Security Considerations	5
10.	Acknowledgements	5
11.	References	5
	Authors' Addresses	6

[1.](#) Introduction

IPv6 Stateless Address AutoConfiguration (SLAAC) [[RFC4862](#)] has traditionally resulted in stable addresses, since the Interface Identifier (IID) has been generated by embedding a stable layer-2 numeric identifier (e.g., a MAC address). [[RFC4941](#)] implies, throughout the specification, that temporary addresses are generated and employed along with temporary addresses.

While the use of stable addresses (only) or mixed stable and temporary addresses can be desirable in a number of scenarios, there are other scenarios in which, for security and privacy reasons, a node may want to use only non-stable address (e.g., a temporary address).

This document clarifies the requirements for stability of IPv6 addresses, such that nodes are not required to configure stable addresses. It also specifies a set of requirements for the generation of non-stable addresses. Finally, it formally updates [[RFC4941](#)] such that temporary addresses can be employed without the need to configure a stable address along side.

[2.](#) Terminology

This document employs the terms defined in [[RFC7721](#)].

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 [RFC 2119](#) [[RFC2119](#)].

3. Stability Requirements for IPv6 Addresses

Nodes are not required to generate addresses with any specific stability properties. That is, the generation of stable addresses is OPTIONAL. This means that a node may end up configuring only stable addresses, only non-stable, or both stable and non-stable addresses.

4. Requirements for Non-Stable IPv6 Addresses

The requirements for non-stable IPv6 addresses are as follows:

1. The resulting Interface Identifiers MUST be different when addresses are configured for different prefixes. That is, if different autoconfiguration prefixes are used to configure addresses for the same network interface card, the resulting Interface Identifiers must be (statistically) different. This means that, given two addresses, it must be difficult for an outside entity to tell whether the addresses have been generated by the same host.
2. The resulting interface identifiers MUST NOT embed layer-2 identifiers (e.g. MAC addresses).
3. It must be difficult for an outside entity to predict the Interface Identifiers that will be generated by the algorithm, even with knowledge of the Interface Identifiers generated for configuring other addresses.
4. The resulting Interface Identifiers must be semantically opaque and must not follow any specific patterns.

The IIDs of addresses configured for different autoconfiguration prefixes must be different, such that traffic for those addresses cannot be correlated.

The reuse of identifiers that have their own semantics or properties across different contexts or scopes can be detrimental for security and privacy [[I-D.gont-predictable-numeric-ids](#)] [[RFC6973](#)] [[RFC4941](#)]. For example, if two different layer-3 protocols generate their addresses by embedding a layer-2 identifier (e.g., a MAC address), then the traffic for such protocols could be correlated (irrespective of whether the aforementioned layer-2 identifier has been randomized or not). Besides, a node that generates an IPv6 address by embedding a link-layer address in the IPv6 address will, when configuring addresses for different prefixes, result in the same IID being used for such prefixes, thus allowing the corresponding traffic to be correlated.

For security and privacy reasons, the IIDs generated for non-stable addresses must not be predictable. Otherwise, the node may be subject to many (if not all) of the security and privacy issues that are meant to be mitigated (please see [[RFC7721](#)]).

Any semantics or patterns in an IID might be leveraged by an attacker to e.g. reduce the search space when performing address-scanning attacks, infer the identity of the node, etc.

5. Generation of Non-Stable IPv6 Addresses

One possible algorithm for generating non-stable IPv6 addresses is that specified in [[RFC4941](#)].

Another possible approach would be to select a random IID when performing SLAAC. In this case, a node that disconnects from the network and subsequently reconnects would employ a (statistically different) IID for the same prefix. A different (random) IID should be employed for each autoconfiguration prefix. These addresses, as opposed to the temporary addresses specified in [RFC4941](#), would be stable for as long as the node stays attached (without disconnecting) to the network, but would change when a node reconnects.

6. Update to existing RFCs

The following subsections clarify how each of the RFCs affected by this document are updated.

6.1. Update to [RFC4941](#)

The temporary addresses specified in [[RFC4941](#)] MAY be used in replacement of the stable addresses [[I-D.ietf-6man-default-iids](#)]. That is, a node MAY configure temporary addresses only, without configuring any stable addresses.

7. Future Work

This document clarifies the requirements for stability requirements for IPv6 addresses. A subsequent document will discuss the tradeoffs involved when considering different stability properties of IPv6 addresses, and the different configuration setups such as: stable addresses only, non-stable addresses only, or mixed stable and non-stable addresses.

8. IANA Considerations

There are no IANA registries within this document. The RFC-Editor can remove this section before publication of this document as an RFC.

9. Security Considerations

This document clarifies the stability requirements for IPv6 addresses, and specifies requirements for the generation of non-stable addresses. Additionally, it formally updates [[RFC4941](#)] such that stable addresses are not required to be configured along with the temporary addresses.

10. Acknowledgements

The authors would like to thank (in alphabetical order) [TBD] for providing a detailed review of this document.

11. References

11.1. Normative References

- [I-D.ietf-6man-default-iids]
Gont, F., Cooper, A., Thaler, D., and S. LIU,
"Recommendation on Stable IPv6 Interface Identifiers",
[draft-ietf-6man-default-iids-11](#) (work in progress), April 2016.
- [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>>.
- [RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", [RFC 2460](#), DOI 10.17487/RFC2460, December 1998, <<http://www.rfc-editor.org/info/rfc2460>>.
- [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>>.
- [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>>.

11.2. Informative References

- [I-D.gont-predictable-numeric-ids]
Gont, F. and I. Arce, "Security and Privacy Implications of Numeric Identifiers Employed in Network Protocols", [draft-gont-predictable-numeric-ids-00](#) (work in progress), February 2016.
- [RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", [RFC 6973](#), DOI 10.17487/RFC6973, July 2013, <<http://www.rfc-editor.org/info/rfc6973>>.
- [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>>.

Authors' Addresses

Fernando Gont
SI6 Networks / UTN-FRH
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
Email: fgont@si6networks.com
URI: <http://www.si6networks.com>

Will Liu
Huawei Technologies
Bantian, Longgang District
Shenzhen 518129
P.R. China

Email: liushucheng@huawei.com

