IPv6 maintenance Working Group (6man) Internet-Draft Intended status: Standards Track Expires: September 6, 2018

F. Gont SI6 Networks / UTN-FRH C. Huitema Private Octopus Inc. S. Krishnan Ericsson Research G. Gont SI6 Networks M. Garcia Corbo SITRANS March 5, 2018

Recommendation on Temporary IPv6 Interface Identifiers draft-gont-6man-non-stable-iids-02

Abstract

This document specifies a set of requirements for generating temporary addresses, and clarifies the stability requirements for IPv6 addresses, allowing for the use of 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 https://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 6, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to <u>BCP 78</u> and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents

Gont, et al. Expires September 6, 2018

Temporary Interface-IDs

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

<u>1</u> .	Introduction	2
<u>2</u> .	Terminology	<u>3</u>
<u>3</u> .	Problem statement	<u>3</u>
<u>4</u> .	Stability Requirements for IPv6 Addresses	<u>4</u>
<u>5</u> .	Requirements for Temporary IPv6 Addresses	<u>4</u>
<u>6</u> .	Future Work	<u>6</u>
<u>7</u> .	IANA Considerations	<u>6</u>
<u>8</u> .	Security Considerations	<u>6</u>
<u>9</u> .	Acknowledgements	<u>6</u>
<u>10</u> .	References	<u>6</u>
Autl	hors' Addresses	<u>9</u>

1. Introduction

IPv6 StateLess Address AutoConfiguration (SLAAC) [<u>RFC4862</u>] 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). [<u>RFC4941</u>] originally implied, throughout the specification, that temporary addresses are generated and employed along with stable 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 Temporary address (e.g., a temporary address).

On the other hand, the lack of a formal set of requirements for temporary addresses led to a number of flaws in popular implementations and in the protocol specification itself, such as allowing for the correlation of network activity carried out with different addresses, reusing randomized identifiers across different networks, etc.

This document clarifies the requirements for stability of IPv6 addresses, such that nodes are not required to configure stable addresses, and may instead employ only temporary addresses. It also specifies a set of requirements for the generation of temporary addresses.

2. Terminology

This document employs the terms defined in [<u>RFC7721</u>].

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 <u>RFC 2119</u> [<u>RFC2119</u>].

3. Problem statement

When [RFC4941] was written, its authors wanted to prevent privacy and security attacks enabled by addresses that contain "an embedded interface identifier, which remains constant over time". They observed that "Anytime a fixed identifier is used in multiple contexts, it becomes possible to correlate seemingly unrelated activity using this identifier." They were concerned with both onpath attackers who would observe the IP addresses of packets observed in transit, and attackers that would have access to the logs of servers.

Since the publication of [<u>RFC4941</u>] in September 2007, our understanding of threats and mitigations has evolved. The IETF is now officially concerned with Pervasive Monitoring [<u>RFC7258</u>], as well as the wide spread collection of information for advertising and other purposes, for example through the Real Time Bidding protocol used for advertising auctions [<u>RTB25</u>].

3.1. Privacy requirements

The widespread deployment of encryption advocated in [RFC7624] is a response to Pervasive Monitoring. Encryption of communication reduces the amount of information that can be collected by monitoring data links, but does not prevent monitoring of IPv6 addresses embedded in clear text packet headers. Stable IPv6 addresses enable the correlation of such data over time.

MAC Address Randomization [IETFMACRandom] is another response to pervasive monitoring. In conjunction with DHCP Anonymity [RFC7844], it ensures that devices cannot be tracked by their MAC Address or their DHCP identifiers when they connect to "hot spots". However, the privacy effects of MAC Address Randomization would be nullified if a device kept using the same IPv6 address before and after a MACaddress randomization event.

Many Web Browsers have options enabling browsing "in private". However, if the web connections during the private mode use the same IPv6 address as those in the public mode, web tracking systems similar to [<u>RTB25</u>] will quickly find the correlation between the

Temporary Interface-IDs

public personna of the user and the supposedly private connection. Similarly, many web browsers have options to "delete history", including deleting "cookies" and other persistent data. Again, if the same IPv6 address is used before and after the deletion of cookies, web tracking systems will easily correlate the new activity with the prior data collection.

Using temporary address alone may not be sufficient to prevent all forms of tracking. It is however quite clear that some usage of temporary addresses is necessary to provide user privacy. It is also clear that the usage of temporary addresses needs to be synchronized with other privacy defining event such as moving to a new network, performing MAC Address Randomization, or changing the privacy posture of a node.

4. 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 Temporary, or both stable and temporary addresses.

5. Requirements for Temporary IPv6 Addresses

The requirements for temporary IPv6 addresses are as follows:

- Temporary addresses MUST have a limited lifetime, which should be different for different addresses. The lifetime of an address essentially limits the extent to which network activity correlation can be performed based on such address.
- The lifetime of an address MUST be further reduced when privacymeaningful events (such as a node attaching to a new network) takes place.
- 3. 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 that employ different prefixes, it must be difficult for an outside entity to tell whether the addresses correspond to the same network interface or even whether they have been generated by the same host.
- 4. The resulting interface identifiers MUST NOT embed layer-2 identifiers (e.g. MAC addresses).

- 5. 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.
- 6. The resulting Interface Identifiers MUST be semantically opaque [<u>RFC7136</u>] and MUST NOT follow any specific patterns.

By definition, temporary addresses have a limited lifetime. This is in contrast with e.g. stable addresses [RFC7217], that do not have have a limited lifetime. Having a variable maximum lifetime prevents an observer from synchronizing with the temporary address regeneration; that is, from being able to expect when address will be regenerated, and thus infer that one newly observed addresses is the result of regenerating a previously observed one.

The lifetime of an address should be further reduced by privacymeaningful events. For example, a host should not employ the same address across network attachment events. That is, a host that deattaches from a network and subsequently re-attaches to a (possibly different) network should regenerate all of its temporary addresses. Similarly, a host that implements MAC address randomization should regenerate all of its temporary addresses. Other events, such as those discussed in <u>Section 3.1</u> should also trigger the regeneration of all temporary addresses.

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 temporary 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 [<u>RFC7721</u>].

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.

6. Future Work

This document clarifies the requirements for stability requirements for IPv6 addresses, and specifies requirements for temporary addresses. A separate document ([<u>I-D.gont-taps-address-usage-problem-statement</u>]) discusses the tradeoffs involved when considering different stability properties of IPv6 addresses.

7. 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.

8. Security Considerations

This document clarifies the stability requirements for IPv6 addresses, and specifies requirements for the generation of temporary addresses.

The security and privacy properties of IPv6 addresses have been discussed in detail in [RFC7721] and [RFC7707].

9. Acknowledgements

The authors would like to thank (in alphabetical order) Brian Carpenter and Lorenzo Colitti for providing valuable feedback on earlier versions of this document.

<u>10</u>. References

<u>**10.1</u>**. Normative References</u>

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", <u>BCP 14</u>, <u>RFC 2119</u>, DOI 10.17487/RFC2119, March 1997, <<u>https://www.rfc-editor.org/info/rfc2119</u>>.
- [RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", <u>BCP 106</u>, <u>RFC 4086</u>, DOI 10.17487/RFC4086, June 2005, <<u>https://www.rfc-editor.org/info/rfc4086</u>>.

- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", <u>RFC 4291</u>, DOI 10.17487/RFC4291, February 2006, <<u>https://www.rfc-editor.org/info/rfc4291</u>>.
- [RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", <u>RFC 4862</u>, DOI 10.17487/RFC4862, September 2007, <<u>https://www.rfc-editor.org/info/rfc4862</u>>.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", <u>RFC 4941</u>, DOI 10.17487/RFC4941, September 2007, <<u>https://www.rfc-editor.org/info/rfc4941</u>>.
- [RFC7136] Carpenter, B. and S. Jiang, "Significance of IPv6 Interface Identifiers", <u>RFC 7136</u>, DOI 10.17487/RFC7136, February 2014, <<u>https://www.rfc-editor.org/info/rfc7136</u>>.
- [RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", <u>RFC 7217</u>, DOI 10.17487/RFC7217, April 2014, <<u>https://www.rfc-editor.org/info/rfc7217</u>>.
- [RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", <u>RFC 8064</u>, DOI 10.17487/RFC8064, February 2017, <<u>https://www.rfc-editor.org/info/rfc8064</u>>.

<u>10.2</u>. Informative References

[FIPS-SHS]

NIST, "Secure Hash Standard (SHS)", FIPS
Publication 180-4, March 2012,
<<u>http://csrc.nist.gov/publications/fips/fips180-4/</u>
fips-180-4.pdf>.

[I-D.gont-predictable-numeric-ids]

Gont, F. and I. Arce, "Security and Privacy Implications of Numeric Identifiers Employed in Network Protocols", <u>draft-gont-predictable-numeric-ids-02</u> (work in progress), February 2018.

[I-D.gont-taps-address-usage-problem-statement]

Gont, F., Gont, G., Corbo, M., and C. Huitema, "Problem Statement Regarding IPv6 Address Usage", <u>draft-gont-taps-</u> <u>address-usage-problem-statement-00</u> (work in progress), February 2018.

[IANA-RESERVED-IID]

IANA, "Reserved IPv6 Interface Identifiers", <<u>http://www.iana.org/assignments/ipv6-interface-ids</u>>.

[IETFMACRandom]

Zuniga, JC., "MAC Privacy", November 2014, <<u>http://www.ietf.org/blog/2014/11/mac-privacy/</u>>.

[OPEN-GROUP]

The Open Group, "The Open Group Base Specifications Issue 7 / IEEE Std 1003.1-2008, 2016 Edition", <u>Section 4.16</u> Seconds Since the Epoch, 2016, <<u>http://pubs.opengroup.org/onlinepubs/9699919799/basedefs/</u> contents.html>.

[RAID2015]

Ullrich, J. and E. Weippl, "Privacy is Not an Option: Attacking the IPv6 Privacy Extension", International Symposium on Recent Advances in Intrusion Detection (RAID), 2015, <<u>https://www.sba-research.org/wp-</u> <u>content/uploads/publications/Ullrich2015Privacy.pdf</u>>.

- [RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", <u>RFC 1321</u>, DOI 10.17487/RFC1321, April 1992, <<u>https://www.rfc-editor.org/info/rfc1321</u>>.
- [RFC3041] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", <u>RFC 3041</u>, DOI 10.17487/RFC3041, January 2001, <https://www.rfc-editor.org/info/rfc3041>.
- [RFC6059] Krishnan, S. and G. Daley, "Simple Procedures for Detecting Network Attachment in IPv6", <u>RFC 6059</u>, DOI 10.17487/RFC6059, November 2010, <<u>https://www.rfc-editor.org/info/rfc6059</u>>.
- [RFC6151] Turner, S. and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", <u>RFC 6151</u>, DOI 10.17487/RFC6151, March 2011, <<u>https://www.rfc-editor.org/info/rfc6151</u>>.

- [RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", <u>RFC 6973</u>, DOI 10.17487/RFC6973, July 2013, <<u>https://www.rfc-editor.org/info/rfc6973</u>>.
- [RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", <u>BCP 188</u>, <u>RFC 7258</u>, DOI 10.17487/RFC7258, May 2014, <<u>https://www.rfc-editor.org/info/rfc7258</u>>.
- [RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", <u>RFC 7624</u>, DOI 10.17487/RFC7624, August 2015, <<u>https://www.rfc-editor.org/info/rfc7624</u>>.
- [RFC7707] Gont, F. and T. Chown, "Network Reconnaissance in IPv6 Networks", <u>RFC 7707</u>, DOI 10.17487/RFC7707, March 2016, <<u>https://www.rfc-editor.org/info/rfc7707</u>>.
- [RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", <u>RFC 7721</u>, DOI 10.17487/RFC7721, March 2016, <<u>https://www.rfc-editor.org/info/rfc7721</u>>.
- [RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity Profiles for DHCP Clients", <u>RFC 7844</u>, DOI 10.17487/RFC7844, May 2016, <<u>https://www.rfc-editor.org/info/rfc7844</u>>.
- [RTB25] Interactive Advertising Bureau (IAB), "Real Time Bidding (RTB) project, OpenRTB API Specification Version 2.5", December 2016, <<u>http://www.iab.com/wp-</u> <u>content/uploads/2016/03/</u> OpenRTB-API-Specification-Version-2-5-FINAL.pdf>.

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: <u>http://www.si6networks.com</u>

Christian Huitema Private Octopus Inc. Friday Harbor, WA 98250 U.S.A.

Email: huitema@huitema.net URI: <u>http://privateoctopus.com/</u>

Suresh Krishnan Ericsson Research 8400 Decarie Blvd. Town of Mount Royal, QC Canada

Email: suresh.krishnan@ericsson.com

Guillermo Gont SI6 Networks Evaristo Carriego 2644 Haedo, Provincia de Buenos Aires 1706 Argentina

Phone: +54 11 4650 8472 Email: ggont@si6networks.com URI: <u>https://www.si6networks.com</u>

Madeleine Garcia Corbo Servicios de Informacion del Transporte Neptuno 358 Havana City 10400 Cuba

Email: madelen.garcia16@gmail.com

Gont, et al. Expires September 6, 2018 [Page 10]