IPv6 maintenance Working Group (6man)
Internet-Draft
Updates: 2464, 2467, 2470, 2491, 2492, 2497, 2590, 3146, 3572, 4291, 4338, 4391, 4944, 5072, 5121 (if approved)
Intended status: Standards Track
Expires: February 20, 2016

F. Gont
SI6 Networks / UTN-FRH
A. Cooper
Cisco
D. Thaler
Microsoft
W. Liu
Huawei Technologies

August 19, 2015

Recommendation on Stable IPv6 Interface Identifiers
draft-ietf-6man-default-iids-06

Abstract

The IPv6 addressing architecture defines Modified EUI-64 format Interface Identifiers, and the existing IPv6 over various link-layers specify how such identifiers are derived from the underlying link-layer address (e.g., an IEEE LAN MAC address) when employing IPv6 Stateless Address Autoconfiguration (SLAAC). The security and privacy implications of embedding link-layer addresses in the Interface Identifier have been known and understood for some time now, and some popular IPv6 implementations have already deviated from such schemes to mitigate these issues. This document changes the recommended default Interface Identifier generation scheme for SLAAC to that specified in RFC7217, and recommends against embedding link-layer addresses in IPv6 Interface Identifiers. It formally updates RFC2464, RFC2467, RFC2470, RFC2491, RFC2492, RFC2497, RFC2590, RFC3146, RFC3572, RFC4291, RFC4338, RFC4391, RFC4944, RFC5072, and RFC5121, which require IPv6 Interface Identifiers to be derived from the underlying link-layer address. Additionally, this document provides advice about the generation of Interface Identifiers with other address configuration mechanisms, such as Dynamic Host Configuration Protocol version 6 (DHCPv6) and manual configuration.

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 February 20, 2016.

Copyright Notice

Copyright (c) 2015 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 3
3. Generation of IPv6 Interface Identifiers with SLAAC 4
4. Generation of IPv6 Interface Identifiers with DHCPv6 4
5. Generation of IPv6 Interface Identifiers with Manual Configuration 5
6. Future Work 5
7. IANA Considerations 5
8. Security Considerations 5
9. Acknowledgements 5
10. References 6
10.1. Normative References 6
10.2. Informative References 8
Authors' Addresses 9

1. Introduction

[RFC4862] specifies Stateless Address Autoconfiguration (SLAAC) for IPv6 [RFC2460], which typically results in hosts configuring one or more "stable" addresses composed of a network prefix advertised by a local router, and an Interface Identifier (IID) [RFC4291] that typically embeds a link-layer address (e.g., an IEEE LAN MAC address).

In some network technologies and adaptation layers, the use of an IID based on a link-layer address may offer some advantages. For

example, the IP-over-IEEE802.15.4 standard in [RFC6775] allows for compression of IPv6 addresses when the IID is based on the underlying link-layer address.

The security and privacy implications of embedding a link-layer address in an IPv6 IID have been known for some time now, and are discussed in great detail in [I-D.ietf-6man-ipv6-address-generation-privacy]; they include:

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

Some popular IPv6 implementations have already deviated from the traditional stable IID generation scheme to mitigate the aforementioned security and privacy implications [Microsoft].

As a result of the aforementioned issues, this document recommends the implementation of an alternative scheme ([RFC7217]) as the default stable IID generation scheme for SLAAC, such that the aforementioned issues are mitigated.

NOTE: [RFC4291] defines the "Modified EUI-64 format" for IIDs. Appendix A of [RFC4291] then describes how to transform an IEEE EUI-64 identifier, or an IEEE 802 48-bit MAC address from which an EUI-64 identifier is derived, into an IID in the Modified EUI-64 format.

Finally this document provides advice about the generation of Interface Identifiers with other address configuration mechanisms, such as Dynamic Host Configuration Protocol version 6 (DHCPv6) and manual configuration.

2. Terminology

Stable address:
An address that does not vary over time within the same network (as defined in [I-D.ietf-6man-ipv6-address-generation-privacy]).

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. Generation of IPv6 Interface Identifiers with SLAAC

Link layers MUST define a mechanism that provides mitigation of the security and privacy implications discussed in Section 1. Nodes SHOULD implement and employ [RFC7217] as the default scheme for generating stable IPv6 addresses with SLAAC. A link layer MAY also define a mechanism that is more efficient and does not address the security and privacy considerations discussed in Section 1. The choice of whether to enable privacy or not SHOULD be configurable in such a case.

By default, nodes SHOULD NOT employ IPv6 address generation schemes that embed the underlying link-layer address in the IID. In particular, this document RECOMMENDS that nodes do not generate IIDs with the schemes specified in [RFC2464], [RFC2467], [RFC2470], [RFC2491], [RFC2492], [RFC2497], [RFC2590], [RFC3146], [RFC3572], [RFC4338], [RFC4391], [RFC4944], [RFC5121], and [RFC5072], and updates these documents with this recommendation.

Some link-layers support locally assigned link-layer addresses [IEEE-802], such as [IEEE-802.3] and [IEEE-802.11], or random addresses [BLUETOOTH]. Where IPv6 IIDs are to be derived from link-layer addresses, it is RECOMMENDED that the random addresses supported by the link-layer are used, or that pseudo-random locally assigned link-layer addresses are generated, assigned and used.

Future specifications SHOULD NOT specify IPv6 address generation schemes that embed the underlying link-layer address in the IID. In some cases, embedding the link-layer address in the IID may reduce resource requirements such as energy, bandwidth and number of frames to carry a given IPv6 packet by facilitating header compression in constrained devices. In such cases, future specifications MAY include IPv6 address generation schemes that embed the link-layer address in the IID, but MUST also specify an alternative IPv6 address generation scheme that provides mitigation of the security and privacy implications discussed in Section 1.

4. Generation of IPv6 Interface Identifiers with DHCPv6

By default, DHCPv6 server implementations SHOULD NOT generate predictable IPv6 addresses (such as IPv6 addresses where the IIDs are consecutive small numbers). [I-D.ietf-dhc-stable-privacy-addresses] specifies one possible algorithm that could be employed to comply with this requirement. Another possible algorithm would be to select a pseudo-random value chosen from a discrete uniform distribution, while avoiding the reserved IPv6 Interface Identifiers [RFC5453] [IANA-RESERVED-IID].

5. Generation of IPv6 Interface Identifiers with Manual Configuration

Network administrators should be aware of the security implications of predictable Interface Identifiers [I-D.ietf-6man-ipv6-address-generation-privacy], and avoid the use of predictable addresses when the aforementioned issues are of concern.

6. Future Work

At the time of this writing, the mechanisms specified in the following documents might require updates to be fully compatible with the recommendations in this document:

- RFC 6282 [RFC6282]
- RFC 4944 [RFC4944]
- RFC 6755 [RFC6775]

Future revisions or updates of these documents should take the issues of privacy and security mentioned in Section 1 and explain any design and engineering considerations that lead to the use of IIDs based on a node's link-layer address.

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 recommends [RFC7217] as the default scheme for generating IPv6 stable addresses with SLAAC, such that the security and privacy issues of IIDs that embed link-layer addresses are mitigated.

9. Acknowledgements

The authors would like to thank Erik Nordmark and Ray Hunter for providing a detailed review of this document.

The authors would like to thank (in alphabetical order) Fred Baker, Carsten Bormann, Scott Brim, Brian Carpenter, Samita Chakrabarti, Tim Chown, Lorenzo Colitti, Jean-Michel Combes, Greg Daley, Esko Dijk, Ralph Droms, David Farmer, Brian Haberman, Ulrich Herberg, Bob Hinden, Philip Homburg, Jahangir Hossain, Jonathan Hui, Christian Huitema, Ray Hunter, Sheng Jiang, Roger Jorgensen, Dan Luedtke, Kerry

Lynn, George Mitchel, Gabriel Montenegro, Erik Nordmark, Simon Perreault, Tom Petch, Alexandru Petrescu, Michael Richardson, Arturo Servin, Mark Smith, Tom Taylor, Ole Troan, Tina Tsou, Glen Turner, Randy Turner, and James Woodyatt, for providing valuable comments on earlier versions of this document.

10. References

10.1. 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>.

[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>.

[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>.

[RFC2467] Crawford, M., "Transmission of IPv6 Packets over FDDI Networks", RFC 2467, DOI 10.17487/RFC2467, December 1998, <http://www.rfc-editor.org/info/rfc2467>.

[RFC2470] Crawford, M., Narten, T., and S. Thomas, "Transmission of IPv6 Packets over Token Ring Networks", RFC 2470, DOI 10.17487/RFC2470, December 1998, <http://www.rfc-editor.org/info/rfc2470>.

[RFC2492] Armitage, G., Schulter, P., and M. Jork, "IPv6 over ATM Networks", RFC 2492, DOI 10.17487/RFC2492, January 1999, <http://www.rfc-editor.org/info/rfc2492>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <http://www.rfc-editor.org/info/rfc3315>.

[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>.

[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>.

[RFC2491] Armitage, G., Schulter, P., Jork, M., and G. Harter, "IPv6 over Non-Broadcast Multiple Access (NBMA) networks", RFC 2491, DOI 10.17487/RFC2491, January 1999, <http://www.rfc-editor.org/info/rfc2491>.

[RFC2497] Souvatzis, I., "Transmission of IPv6 Packets over ARCnet Networks", RFC 2497, DOI 10.17487/RFC2497, January 1999, <http://www.rfc-editor.org/info/rfc2497>.

[RFC2590] Conta, A., Malis, A., and M. Mueller, "Transmission of IPv6 Packets over Frame Relay Networks Specification", RFC 2590, DOI 10.17487/RFC2590, May 1999, <http://www.rfc-editor.org/info/rfc2590>.

[RFC3146] Fujisawa, K. and A. Onoe, "Transmission of IPv6 Packets over IEEE 1394 Networks", RFC 3146, DOI 10.17487/RFC3146, October 2001, <http://www.rfc-editor.org/info/rfc3146>.

[RFC3572] Ogura, T., Maruyama, M., and T. Yoshida, "Internet Protocol Version 6 over MAPOS (Multiple Access Protocol Over SONET/SDH)", RFC 3572, DOI 10.17487/RFC3572, July 2003, <http://www.rfc-editor.org/info/rfc3572>.

[RFC4338] DeSanti, C., Carlson, C., and R. Nixon, "Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel", RFC 4338, DOI 10.17487/RFC4338, January 2006, <http://www.rfc-editor.org/info/rfc4338>.

[RFC4391] Chu, J. and V. Kashyap, "Transmission of IP over InfiniBand (IPoIB)", RFC 4391, DOI 10.17487/RFC4391, April 2006, <http://www.rfc-editor.org/info/rfc4391>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <http://www.rfc-editor.org/info/rfc4944>.

[RFC5121] Patil, B., Xia, F., Sarikaya, B., Choi, JH., and S. Madanapalli, "Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks", RFC 5121, DOI 10.17487/RFC5121, February 2008, <http://www.rfc-editor.org/info/rfc5121>.

[RFC5072] Varada, S., Ed., Haskins, D., and E. Allen, "IP Version 6 over PPP", RFC 5072, DOI 10.17487/RFC5072, September 2007, <http://www.rfc-editor.org/info/rfc5072>.

[RFC5453] Krishnan, S., "Reserved IPv6 Interface Identifiers", RFC 5453, DOI 10.17487/RFC5453, February 2009, <http://www.rfc-editor.org/info/rfc5453>.

[RFC6282] Hui, J., Ed. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, DOI 10.17487/RFC6282, September 2011, <http://www.rfc-editor.org/info/rfc6282>.

[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>.

10.2. Informative References

[IEEE-802]
IEEE, "802-2014 - IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture", 2014, <https://standards.ieee.org/findstds/standard/802-2014.html>.

[IEEE-802.3]
IEEE, "802.3-2012 - IEEE Standard for Ethernet", 2012, <https://standards.ieee.org/findstds/standard/802.3-2012.html>.

[IEEE-802.11]
IEEE, "IEEE Standard for Information technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 2012, <http://standards.ieee.org/getieee802/download/802.11-2012.pdf>.

[BLUETOOTH]
Bluetooth SIG, "BLUETOOTH SPECIFICATION Version 4.2", 2014, <https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=286439>.

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

[I-D.ietf-6man-ipv6-address-generation-privacy]
Cooper, A., Gont, F., and D. Thaler, "Privacy Considerations for IPv6 Address Generation Mechanisms", draft-ietf-6man-ipv6-address-generation-privacy-07 (work in progress), June 2015.

[I-D.ietf-dhc-stable-privacy-addresses]
Gont, F. and S. LIU, "A Method for Generating Semantically Opaque Interface Identifiers with Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", draft-ietf-dhc-stable-privacy-addresses-02 (work in progress), April 2015.

[Microsoft]
Davies, J., "Understanding IPv6, 3rd. ed", page 83, Microsoft Press, 2012, <http://it-ebooks.info/book/1022/>.

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

Alissa Cooper
Cisco
707 Tasman Drive
Milpitas, CA 95035
US

Phone: +1-408-902-3950
Email: alcoop@cisco.com
URI: https://www.cisco.com/

Dave Thaler
Microsoft
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 425 703 8835
Email: dthaler@microsoft.com

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

Email: liushucheng@huawei.com