IPv6 Operations Working Group (v6ops)
Internet-Draft
Intended status: Informational
Expires: April 18, 2013

F. Gont
Huawei Technologies

October 15, 2012

Interoperability Problems of StateLess Address Auto-Configuration (SLAAC) Arising from Duplicate Link-layer Addresses draft-gont-v6ops-slaac-issues-with-duplicate-macs-00

Abstract

Traditional Stateless Address Auto-Configuration (SLAAC) typically involves producing a Modified-EU64 format identifier to be employed as the Interface-ID of the resulting address. In the case of Ethernet network interface cards, such identifier derived from the corresponding IEEE 802 address. IEEE 802 addresses are generally expected to be globally unique, thus resulting in non-duplicate addresses. However, in many real-world scenarios, these identifiers fail to be unique, thus resulting in duplicate IPv6 addresses. This document discusses the interoperability problems arising from duplicate IEEE 802 addresses with IPv6 Stateless Address Auto-Configuration (SLAAC), and how some popular implementations react when the such problems arise. Finally, it discusses possible mitigations for the aforementioned issue.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79. This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.

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 April 18, 2013.

Copyright Notice

Copyright (c) 2012 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

IPv6 Stateless Address Auto-Configuration (SLAAC) [RFC4862] for Ethernet network interface cards typically involves generating a Modified EUI64 format identifier derived from the IEEE 802 address of the underlying in network interface card. Such Modified EUI-64 format identifier is then employed as the Interface-ID part of the resulting IPv6 address. Since the IEEE 802 addresses are generally expected to be globally-unique, the aforementioned algorithm is expected to result in unique addresses.

In any case, in order to prevent two systems from configuring the same address on the same network segment, [RFC4862] specifies a mechanism called "Duplicate Address Detection" (DAD), which employs Neighbor Solicitation and Neighbor Advertisement messages to detect whether a candidate IPv6 address is already in use on the local network. DAD is meant only to *detect* an address conflict: it is up to the implementation what to do if/once such a conflict is detected -- and the current SLAAC specification [RFC4862] essentially leaves possible algorithms to resolve the aforementioned DAD failure unspecified.

In practice, virtually all implementation do not employ any algorithm for resolving duplicate address conflicts, and therefore such event leads to a failure of IPv6 stateless address configuration.

Section 2 discusses the occurrence of duplicate IEEE 802 addresses in some detail. Section 3 analyzes the pros and cons of generating Modified EUI-64 format identifiers by essentially embedding a IEEE 802 address in the aforementioned identifier. Section 4 provides some details regarding how different implementations behave in the presence of DAD failures. Finally, Section 5 discusses possible mitigations for the aforementioned issue.

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].

2. Duplicate IEEE 802 addresses in the real world

IEEE 802 addresses are, in principle, not necessarily unique: the U/L bit the in the IEEE Organizational Unique Identifier (OUI) implies, when clear, a globally-unique IEEE 802 address, but indicates a non-unique ("local") address when set. However, most products ship with IEEE 802 addresses that have the U/L bit set, thus implying globally-unique IEEE 802 addresses.

However, in practice, even if when the U/L bit is clear, the corresponding IEEE 802 address might be non-unique. There are a number of reasons for which duplicate IEEE 802 addresses might exist in a given network:

- Some vendors have been found to simply "reuse" IEEE 802 addreses

- Virtualization technologies, such as VirtualBox, essentially select IEEE 802 addresses randomly, from a specific IEEE OUI [VirtualBox]. This means that it is possible for two virtual machines to end up employing the same IEEE 802 address for their respective virtual interfaces.

Besides any assessment of whether duplicate IEEE 802 addresses are the product of poor engineering choices or not, truth is that deployed systems might already be employing duplicate addresses, and hence it is desirable that such scenarios are gracefully handled.

3. IEEE-derived Modified EUI-64 format identifiers

One might argue that the only motivation for producing Modified EUI-64 format identifiers as specified in [RFC2464] are:

- In theory, it is a simple algorithm to produce globally-unique Modified EUI-64 format identifiers.
- Until recently, it was the only algorithm to produce stable Interface-IDs that had so far been standardized.

  The privacy extensions specified in [RFC4941] are meant to be employed *in addition* to traditional SLAAC addresses, while [I-D.ietf-6man-stable-privacy-addresses] is a recent standardization effort.

Given that IEEE 802 addresses have been found to fail the uniqueness criteria assumed above, IEEE-derived Modified EUI-64 format identifiers will also fail the same uniqueness criteria. Additionally, IEEE-derived identifiers have been found to result in addresses that are trivial to scan [I-D.gont-opsec-ipv6-host-scanning], and that negatively affect the privacy of users [I-D.ietf-6man-stable-privacy-addresses] [RFC4941]. While it is true producing modified EUI64 format identifiers is the only scheme that has so far been fully standardized, there is ongoing work at the 6man wg to standardize an alternative scheme for producing stable modified EUI-64 format identifiers, which does not suffer from any of the drawbacks of modified EUI-64 format identifiers based on IEEE-identifiers.

At lest discussions in IETF circles seem to indicate that the drawbacks of modified EUI-64 format identifiers based on IEEE-identifiers are well-understood, and that there seems to be agreement that "they should be replaced with some alternative scheme".

4. Duplicate Address Detection (DAD) implementations

Different IPv6 stacks differ in some DAD implementations details, and, most importantly, on how they handle DAD failures. For example, different IPv6 stacks may send a different number of DAD probes before DAD is considered to have succeeded. Additionally, they typically differ on how they handle DAD failures. For example, in the Linux IPv6 stack, if DAD fails for a link-local address, it results in a "permanent" SLAAC failure that requires the admin to reboot the system in order for SLAAC to be re-attempted. On the other hand, DAD failure for non-link-local addresses is more of a "soft failure", and hence SLAAC might succeed some time later when a new Router Advertisement message that triggers SLAAC is received.

5. Mitigations to the problem of SLAAC failures due to duplicate IEEE 802 addresses

5.1. Implementing some DAD-failure recovery algorithm

One simple algorithm to resolve DAD failures could be such that, in the event of such failures, simply generates a new IPv6 tentative address by incrementing the Interface-ID of the tentative IPv6 address that previously failed DAD.

5.2. Replacing Modified EUI-64 format identifiers based on IEEE 802 addresses

A different approach to solve the problems arising from DAD failures would be to realize that there are a number of factors that make modified EUI64 format identifiers based on IEEE 802 addresses undesirable, and hence recommend the implementation of [I-D.ietf-6man-stable-privacy-addresses] in replacement of the IEEE-derived modified EUI-64 format identifiers.

6. IANA Considerations

This document has no actions for IANA.

7. Security Considerations

This document discusses an interoperability problem that may arise as a result of employing duplicate IEEE 802 addresses in the same network segment. Failure to gracefully handle DAD failures may allow an attacker to perform a Denial of Service attack against the victim implementation.

Such attacks could be readily performed with packet-crafting tools such as [SI6-Toolkit] and [THC-IPv6].

A more resilient approach might be to perform DAD for some maximum number of tentative IPv6 addresses, and to not perform DAD at all for the last of those address.

Obviously, this might lead to undesirable results if such "last" address was a real duplicate of an address currently in use at the local network.

In any case, as noted earlier in this document, IEEE-derived modified EUI64 format identifiers have undesirable properties in the areas of host tracking and host privacy, and hence the interoperability problem discussed in this document could be considered as yet another reason to replace such identifiers with some alternative scheme, such as that specified in [I-D.ietf-6man-stable-privacy-addresses]

8. Acknowledgements

This documents has benefited from the input of a number of people in a discussion of this topic on the v6ops wg mailing-list [V6OPS-LIST].

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

9.2. Informative References

[I-D.ietf-6man-stable-privacy-addresses]
Gont, F., "A method for Generating Stable Privacy-Enhanced Addresses with IPv6 Stateless Address Autoconfiguration (SLAAC)", draft-ietf-6man-stable-privacy-addresses-01 (work in progress), October 2012.

[I-D.gont-opsec-ipv6-host-scanning]
Gont, F., "Network Reconnaissance in IPv6 Networks", draft-gont-opsec-ipv6-host-scanning-01 (work in progress), July 2012.

[VirtualBox]
VirtualBox, "Oracle VM VirtualBox User Manual, version 4.1.2", August 2011, <http://www.virtualbox.org>.

[V6OPS-LIST]
"V6OPS WG mailing-list", https://www.ietf.org/mailman/listinfo/v6ops.

[SI6-Toolkit]
"SI6 Networks' IPv6 toolkit", <http://www.si6networks.com/tools/ipv6toolkit>.

[THC-IPv6]
"The Hacker's Choice IPv6 Attack Toolkit", <http://www.thc.org/thc-ipv6/>.

Author's Address

Fernando Gont
Huawei Technologies
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

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