A method for Generating Stable Privacy-Enhanced Addresses with IPv6 Stateless Address Autoconfiguration (SLAAC)
draft-gont-6man-stable-privacy-addresses-00

Abstract

This document specifies a method for generating IPv6 Interface Identifiers to be used with IPv6 Stateless Address Autoconfiguration (SLAAC), such that addresses configured using this method are stable within each subnet, but the Interface Identifier changes when hosts move from one network to another. The aforementioned method is meant to be an alternative to generating Interface Identifiers based on IEEE identifiers, such that the same manageability benefits can be achieved without sacrificing the privacy of users.

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 This document may not be modified, and derivative works of it may not be created, and it may not be published except as an Internet-Draft.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 June 17, 2012.

Copyright Notice

Copyright (c) 2011 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
Table of Contents

1. Introduction ..................................................... 3
2. Design goals ..................................................... 5
3. Algorithm specification .......................................... 6
4. IANA Considerations .............................................. 8
5. Security Considerations .......................................... 9
6. Acknowledgements ................................................ 10
7. References ......................................................... 11
   7.1. Normative References ...................................... 11
   7.2. Informative References ...................................... 11
Author’s Address ..................................................... 12
1. Introduction

[RFC4862] specifies the Stateless Address Autoconfiguration (SLAAC) for IPv6, 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) that typically embeds a hardware address (using IEEE identifiers) [RFC4291].

Static addresses are generally considered to simplify network management, since they simplify ACLs and logging. However, since IEEE identifiers are typically globally unique, the resulting IPv6 addresses can be leveraged to track and correlate the activity of a node, thus negatively affecting the privacy of users.

The "Privacy Extensions for Stateless Address Autoconfiguration in IPv6" [RFC4941] were introduced to difficult the task of eavesdroppers and other information collectors to correlate the activities of a node, and basically result in temporary (and random) Interface Identifiers that are typically more difficult to leverage than those based on IEEE identifiers. When privacy extensions are enabled, "privacy addresses" are employed for "outgoing communications", while the traditional IPv6 addresses based on IEEE identifiers are still used for "server" functions (i.e., receiving incoming connections). Some flavor of these "Privacy Extensions" have been implemented in a variety of systems, some of which (notably Microsoft Windows Vista and Microsoft Windows 7) enable them by default.

Privacy addresses can be challenging in a number of areas. For example, from a network-management point of view, they tend to increase the complexity of enforcing access controls and event logging. As a result, some organizations disable the use of privacy addresses even at the expense of reduced privacy [Broersma]. Also, they result in increased complexity, which might not be possible or desirable in some implementations (e.g., some embedded devices).

In such scenarios in which "Privacy Extensions" are deliberately not used, addresses are generated using e.g. IEEE identifiers, and are subject to the privacy issues discussed above.

We note that even in those scenarios in which "Privacy Extensions" are not used, there is still no need or desire to negatively affect user privacy. As a result, this document specifies a method to generate interface identifiers that are stable/constant within each subnet, but that change as hosts move from one network to another, thus keeping the "stability" properties of the interface identifiers specified in [RFC4291], while still preventing to correlate the activities of a node as it moves from one network to another.
On the other hand, even in scenarios in which "Privacy Extensions" are employed, IPv6 addresses based on IEEE identifiers are still typically used for performing "server" functions. In such scenarios, implementation of the mechanism described in this document would still be desirable, such that the "stable" addresses used by hosts for "server" functions are not easily predictable (and hence difficult host-scanning).

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. Design goals

This document specifies a method for selecting interface identifiers to be used with IPv6 SLAAC, with the following goals:

- The resulting interface identifier remains constant/stable for each prefix used with SLAAC within each subnet. That is, the algorithm generates the same interface identifier when configuring an address belonging to the same prefix within the same subnet.

- The resulting interface identifier does change 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.

- It must be difficult for an outsider to predict the interface identifiers that will be generated by the algorithm, even with knowledge of the interface identifiers generated for configuring other addresses.

- The aforementioned interface identifiers are meant to be an alternative to those based on IEEE identifiers, as specified in [RFC4291].

We note that of use of the algorithm specified in this document is (to a large extent) orthogonal to the use of "Privacy Extensions" [RFC4941]. Hosts that do not implement/use "Privacy Extensions" would have the benefit that they would not be subject to the host-tracking issues discussed in the previous section. On the other hand, since hosts implementing "Privacy Extensions" still make use of IEEE-derived identifiers (mostly for performing "server" functions), implementation of this algorithm would still benefit such implementations, since it would prevent leakage of the Organizational Unique Identifier (OUI), which would be of help to attackers for host-scanning purposes [Gont-DEEPSEC2011] [CPNI-IPv6].
3. Algorithm specification

IPv6 implementations conforming to this specification MUST generate interface identifiers with the algorithm specified in this section. The aforementioned algorithm MUST be employed for generating the interface identifiers for all the IPv6 addresses configured with SLAAC for a given interface, including IPv6 link-local addresses.

1. Compute a random (but stable) identifier with the expression:

   \[ \text{RID} = F(\text{Prefix}, \text{Modified\_EUI64}, \text{Network\_ID}, \text{secret\_key}) \]

   Where:
   \[
   \begin{align*}
   \text{RID} & : \text{Random (but stable) identifier} \\
   F() & : \text{A pseudorandom function (PRF) that is not computable from the outside (without knowledge of the secret key). The PRF could be implemented as a cryptographic hash of the concatenation of each of the function parameters.} \\
   \text{Prefix} & : \text{The prefix to be used for SLAAC, as learned from an ICMPv6 Router Advertisement message.} \\
   \text{Modified\_EUI64} & : \text{The Modified EUI-64 format identifier corresponding to this network interface.} \\
   \text{Network\_ID} & : \text{Some network specific data that identifies the subnet to which this interface is attached. For example the IEEE 802.11 SSID corresponding to the network to which this interface is associated. This parameter is OPTIONAL.} \\
   \text{secret\_key} & : \text{A secret key that is not known by the attacker.}
   \end{align*}
   \]

2. The Interface Identifier is finally obtained by taking the leftmost 64 bits of the RID value computed in the previous step, and setting bit 6 (the leftmost bit is numbered 0) to zero. This creates an interface identifier with the universal/local bit indicating local significance only.

   Note that the result of \( F() \) in the algorithm above is no more secure than the secret key. If an attacker is aware of PRF is being used by
the victim (which we should expect), and the attacker can obtain enough material (i.e., addresses configured by the victim), the attacker may simply search the entire secret-key space to find matches. To protect against this, the secret key should be of a reasonable length. Key lengths of 128 bits should be adequate. The secret key can either be a true random number [RFC4086], or some per-host secret.

Including the optional Network_ID parameter when computing the RID value above would cause the algorithm to produce a different Interface Identifier when connecting to different networks, even when configuring addresses belonging to the same prefix. This means that a host would employ a different Interface ID as it moves from one network to another even for IPv6 link-local addresses.
4. 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.
5. Security Considerations

This document specifies an algorithm for generating interface identifiers to be used with IPv6 Stateless Address Autoconfiguration (SLAAC), in replacement of e.g. the Modified EUI-64 format identifiers. When compared to modified EUI-64 format identifiers, the identifiers specified in this document have a number of advantages:

- They prevent trivial host-tracking, since when a host moves from one network to another the prefix used for autoconfiguration will typically change, and hence the resulting interface identifier will also change.

- They mitigate host-scanning techniques which leverage predictable interface identifiers (e.g., known Organizational Unique Identifiers).

Finally, we note that this algorithm is meant to be an alternative for e.g. the Modified EUI-64 format identifiers, but not for temporary-address methods such as that specified in [RFC4941]. Clearly, temporary addresses can help reduce the attack exposure window, since the lifetime of each IPv6 address is reduced when compared to that of addresses generated with the method specified in this document. Additionally, they may be of help to correlate different activities performed by the same host while attached to the same network. However, we note that implementation of this algorithm would still benefit those hosts employing "Privacy Addresses", since it would prevent leakage of the IEEE Organizational Unique Identifier (OUI) when IEEE-identifier-derived addresses are used for serve-like functions, which can be of help to attackers for host-scanning purposes.
6. Acknowledgements

Fernando Gont would like to thank CPNI (http://www.cpni.gov.uk) for their continued support.
7. References

7.1. Normative References


7.2. Informative References

[Gont-DEEPSEC2011]

[Broersma]

[CPNI-IPv6]