IPv6 maintenance Working Group (6man)
Internet-Draft
Updates: 4861 (if approved)
Intended status: Standards Track
Expires: September 13, 2011

F. Gont
UTN/FRH
R. Broersma
DREN

March 12, 2011

Managing the Use of Privacy Extensions for Stateless Address Autoconfiguration in IPv6
draft-gont-6man-managing-privacy-extensions-01

Abstract

This document describes an operational problem that arises due to the impossibility of managing the use of "Privacy Extensions" for IPv6 Stateless Address Autoconfiguration (SLAAC) in network scenarios that employ SLAAC. Additionally, this document specifies new flag in the Prefix Information option of Router Advertisement messages, such that routers can advertise, for each network prefix to be used for SLAAC, whether the aforementioned "Privacy Extensions" should be used.

Table of Contents

1. Introduction

[RFC4862] specifies the Stateless Address Autoconfiguration (SLAAC) for IPv6, which typically results in hosts configuring one or more addresses composed of a network prefix advertised by a local router, and an Interface Identifier (IID) derived from a hardware address (such as an Ethernet MAC address).

Since e.g. Ethernet MAC addresses are typically globally unique, IPv6 addresses generated as specified in [RFC4862] could possibly be levareged 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 difficult the task of eavesdroppers and other information collectors to correlate the activities of a node, and basically result in random Interface Identifiers which may be more difficult to leverage than their hardware-derived counterpart. These "Privacy Extensions" have been implemented in a variety of systems, some of which (notably that in Microsoft Windows Vista and Microsoft Windows 7) enable them by default.

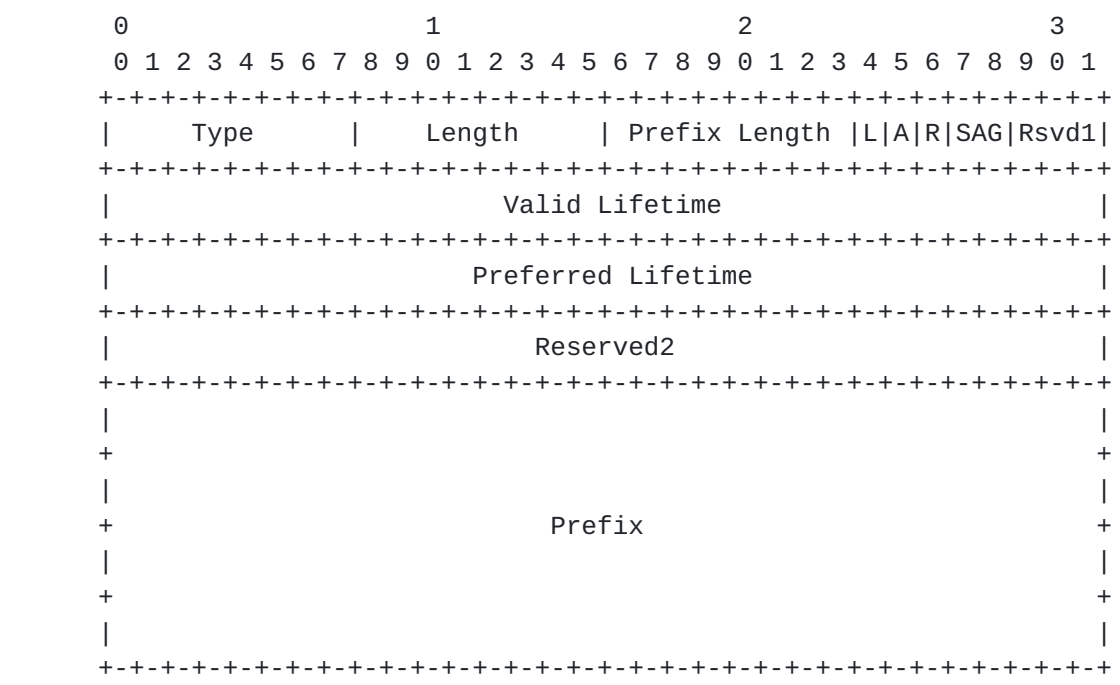
The imposibility of managing the use of "Privacy Extensions" poses poses a problem when a site has a specific policy for the generation of IPv6 Interface Identifiers. For example, if hosts that enable "Privacy Extensions" (by default) need to be deployed on sites that require the use of hardware-derived Interface Identifiers, an administrator may need to manually disable the use of "Privacy Extensions" in each of the attached nodes. This not only may result in a lot of work on the side of the administrator, but may also be difficult to implement (particularly when considering mobile computers such as laptops) [Broersma]. On the other hand, in some environments (e.g., a typical home network) the use of "Privacy Extensions" might be desirable. However, the imposibility to automatically enable "Privacy Extensions" may preclude their use (unless they are manually enabled by the administrator).

This document specifies a new flag in the Prefix Information option of Router Advertisement messages, such that routers can advertise, for each network prefix to be used for SLAAC, whether the aforementioned "Privacy Extensions" should be used.

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. Updating the Prefix Information option

The syntax of the Prefix Information option is updated as follows:



An additional field, the two-bit "SAG" (Stateless Address Generation) field, is ispecified for the Prefix Information option. The semantics of each of the possible values are:

00:
No specific advice is provided for the generation of addresses for this prefix.

01:
When generating addresses for this prefix, the resulting addresses SHOULD be based on the underlying hardware address of the interface (e.g., the Ethernet MAC address).

10:
When generating addresses for this prefix, Privacy Extensions for SLAAC SHOULD be employed.

11:
Unused (reserved for future use).

The "R" bit was specified by [RFC3775]. The Rsvd1 field corresponds to the remaining reserved bits, and thus MUST be set to zero by the sender of this option, and ignored by the receiver.

Since the "SAG" bits correspond to a previously "reserved" field, implementations that predate this specification should be setting the SAG field to "00" when sending the option, and ignoring the SAG bits upon receipt.

2.1. Router specification

Routers that have no particular preference on the address generation policy MUST set the SAG bits to "00". Otherwise, they SHOULD set the SAG bits to "01" or "10" according to the preferred address generation policy. The special value "11" is reserved for future extensions, and MUST NOT be set by routers implementing this specification.

2.2. Host specification

When generating addresses for the prefix contained in the "Prefix Information Option", hosts SHOULD apply the policy specified by the "SAG" field. If no specific advice is provided (i.e., the SAG field is set to "00"), hosts are free with respect to which policy to employ when generating addresses for this prefix. Hosts that implement this specification MUST interpret the special value "11" in the same way as "00" (i.e., no specific advice is provided for address generation).

3. Security Considerations

An attacker could exploit the mechanism specified in this document to cause hosts in a given subnet to disable Privacy Extensions, thus causing their Interface Identifiers to be derived from hardware addresses, instead. Thus, the privacy of the victim hosts that would have enabled the Privacy Extensions could possibly be reduced.

However, it should be noted that this attack would require from an attacker the same effort as all the other Neighbor Discovery attack vectors that are based on crafted Router Advertisement messages, most of which are far more interesting for an attacker than this possible attack vector.

Among the possible options for mitigating this and other attack vectors based on crafted Router Advertisement messages is the deployment of the so-called "Router Advertisement guard" mechanism [I-D.ietf-v6ops-ra-guard].

SEND (SEcure Neighbor Discovery) [RFC3971] could be pontentially deployed to mitigate most Neighbor Discovery attacks. However, a number of issues (such as the requirement for Public Key Infrastructure) preclude the deployment of SEND in most general network scenarions. [CPNI-IPv6]

Finally, we note that while the value and effectiveness of privacy addreses have been questioned in a number of studies [I-D.dupont-ipv6-rfc3041harmful] [Escudero] [CPNI-IPv6], this document does not take a stance about their value and effectiveness: it limits itself to discussing the operational problem that arises due to the impossibility of managing the use of "Privacy Extensions", and updating the "Prefix Information" option such that "Privacy Extensions" can be more easily managed when IPv6 Stateless Address Autoconfiguration (SLAAC) is employed.

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. Acknowledgements

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

6. References

6.1. Normative References

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

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

[RFC3775] Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[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.

6.2. Informative References

[I-D.ietf-v6ops-ra-guard]
Levy-Abegnoli, E., Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", draft-ietf-v6ops-ra-guard-08 (work in progress), September 2010.

[I-D.dupont-ipv6-rfc3041harmful]
Dupont, F. and P. Savola, "RFC 3041 Considered Harmful", draft-dupont-ipv6-rfc3041harmful-05 (work in progress), June 2004.

[Broersma]
Broersma, R., "IPv6 Everywhere: Living with a Fully IPv6-enabled environment", Australian IPv6 Summit 2010, Melbourne, VIC Australia, October 2010, <http://www.ipv6.org.au/summit/talks/Ron_Broersma.pdf>.

[Escudero]
Escudero, A., "PRIVACY EXTENSIONS FOR STATELESS ADDRESS

AUTOCONFIGURATION IN IPV6 - "REQUIREMENTS FOR UNOBSERVABILITY", RVK02, Stockholm, 2002, <http://web.it.kth.se/~aep/PhD/docs/paper3-rvk2002.pdf>.

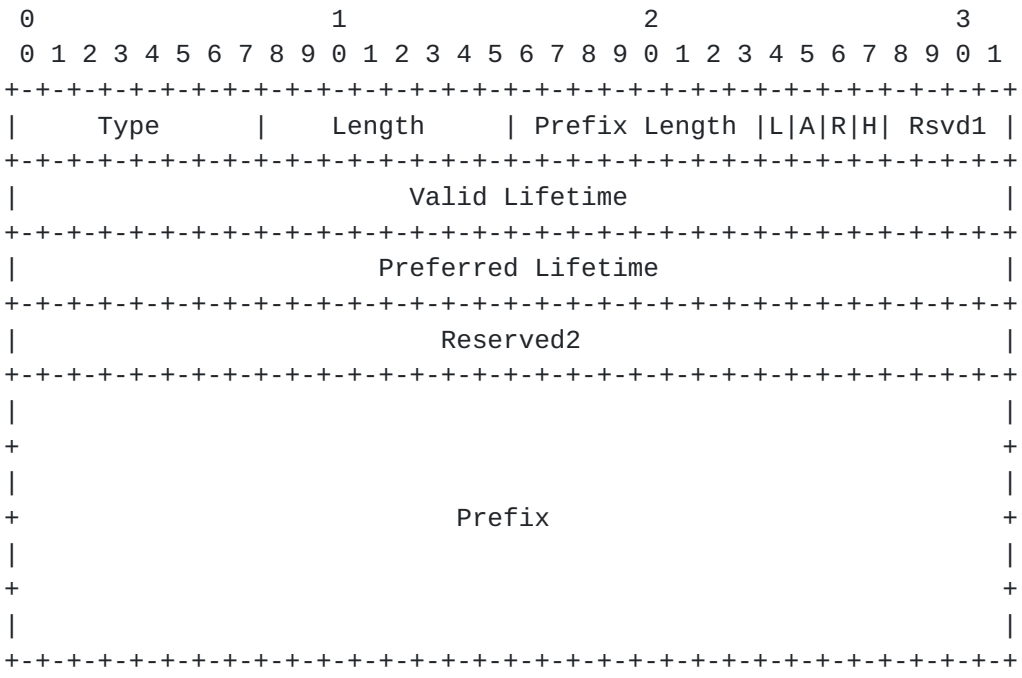
[CPNI-IPv6]
Gont, F., "Security Assessment of the Internet Protocol version 6 (IPv6)", UK Centre for the Protection of National Infrastructure, (to be published).

Appendix A. Possible alternatives

The following subsections describe possible alternatives (less optimal from the point of vew of the authors of this document). The main drawback is that if a single bit is specifed, then it's impossible to disambiguate between the case in which this specification is not supported (and thus the bit was "Reserved and set to "0"), and the case whether this specification is supported and the correspoding bit is meant to give specific advice on the desired address generation policy.

A.1. Specifying a 'hardware-addresses' bit

The syntax of the Prefix Information option is updated as follows:



An additional bit, "H" ("Hardware-derived addresses"), is specified for the Prefix Information option. When set, this bit indicates that hardware-derived addresses SHOULD be used when configuring IPv6 addresses as a result of Stateless Address Autoconfiguration. When not set, this bit indicates that Privacy Extensions SHOULD be enabled when configuring IPv6 addresses as a result of Stateless Address Autoconfiguration

The "R" bit was specified by [RFC3775]. The Rsvd1 field corresponds to the remaining reserved bits, and thus MUST be set to zero by the sender of this option, and ignored by the receiver.

Since the "H" bit was a previously reserved field, implementations that predate this specification should be setting this bit to zero when sending the option, and ignoring this bit upon receipt.

The following table illustrates the result of SLAAC depending on whether this specification is supported by the router and/or the host participanting in SLAAC.

Router / Host	Supported	Not Supported
Supported	As indicated by the "H" bit	As in current scenarios
Not Supported	Privacy Addresses	As in current scenarios

Table 1: Possible results of SLAAC scenarios

A.2. Specifying a 'privacy-addresses' bit

If rather than specifying an "H" bit, our I-D were to specify a "P" ("Privacy addresses") bit, the resulting possible scenarios would change as follows:

The following table illustrates the result of SLAAC depending on whether this specification is supported at the router and/or host participanting in SLAAC.

Router / Host	Supported	Not Supported
Supported	As indicated by the "P" bit	As in current scenarios
Not Supported	Hardware-derived addresses	As in current scenarios

Table 2: Alt. Possible results of SLAAC scenarios

As you may see, in this case only one scenario changes: when this spec is not supported by the router, but *is* supported by the host,

hardware addresses are used. This would mean that if e.g. MS were to implement this spec before e.g. Cisco, Privacy Addresses would be disabled.

Clearly, there's a tradeoff here.

Appendix B. Changes from previous versions of the draft (to be removed by the RFC Editor before publication of this document as a RFC

B.1. Changes from draft-gont-6man-managing-privacy-extensions-00

- Rather that specifying a single bit in the Prefix Information Options, a two-bit SAG field is specified -- with the previous options being moved to an appendix (Appendix A).

- Fixes writeos in the tables contained in Appendix A.1 and Appendix A.2.

Authors' Addresses

Fernando Gont
Universidad Tecnologica Nacional / Facultad Regional Haedo
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
Email: fernando@gont.com.ar

Ron Broersma
Defense Research and Engineering Network

Email: ron@spawar.navy.mil