IPv6 maintenance Working Group (6man)
Internet-Draft
Updates: 4861 (if approved)
Intended status: Standards Track
Expires: June 17, 2012

F. Gont
UK CPNI

December 15, 2011

Managing the Address Generation Policy for Stateless Address Autoconfiguration in IPv6
draft-gont-6man-managing-slaac-policy-00

Abstract

This document describes an operational problem that arises due to the impossibility of managing the address generation policy employed by hosts participating in IPv6 Stateless Address Autoconfiguration (SLAAC). Additionally, it specifies a new field in the Prefix Information option of Router Advertisement messages, such that routers can advertise, for each network prefix included in a Router Advertisement message, the desired address generation policy to be used for SLAAC.

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) that typically embeds a hardware address (using the Modified EUI-64 Format [RFC4291].

Since the identifiers (e.g. Ethernet MAC addresses) typically used for those addresses are usually globally unique, the IPv6 addresses generated as specified in [RFC4291] 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 random Interface Identifiers that are typically more difficult to leverage than their Modified EUI-64 Format counterpart. 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.

The impossibility of managing the address generation policy employed for SLAAC poses a problem when a site desires or requires a specific policy for the generation of IPv6 addresses. For example, some operating systems (notably FreeBSD) implement "Privacy Extensions", but do not enable them by default. And since there is currently no mechanism in IPv6 to convey the desired address-generation policy, administrators have no option other than manual configuration to enable such extensions. On the other hand, some implementations (notably Windows Vista and Windows 7) that enable "Privacy Extensions" by default might need to be deployed on sites that require the use of stable addresses (e.g. those resulting from Modified EUI-64 Format Identifiers [RFC4291]), for the ease of correlating network activities or enforcing simple access controls. However, since there is currently no mechanism to convey the desired address-generation policy for SLAAC, an administrator would need to manually-configure each of the attached nodes such that they employ the desired address generation policy.

Depending on manual configuration for enabling a specific and homogeneous address-generation policy may result in a lot of work on the side of the administrator, but may also be difficult to implement, particularly when considering mobile nodes such as laptops and mobile phones [Broersma]. Additionally, the lack of a mechanism for conveying address-generation policy information might preclude

the use of some technologies, such as "Privacy Extensions" [RFC4941], which are desirable in most general environments (e.g., a typical home network, or an Internet cafe), but are currently only enabled as a result of manual configuration.

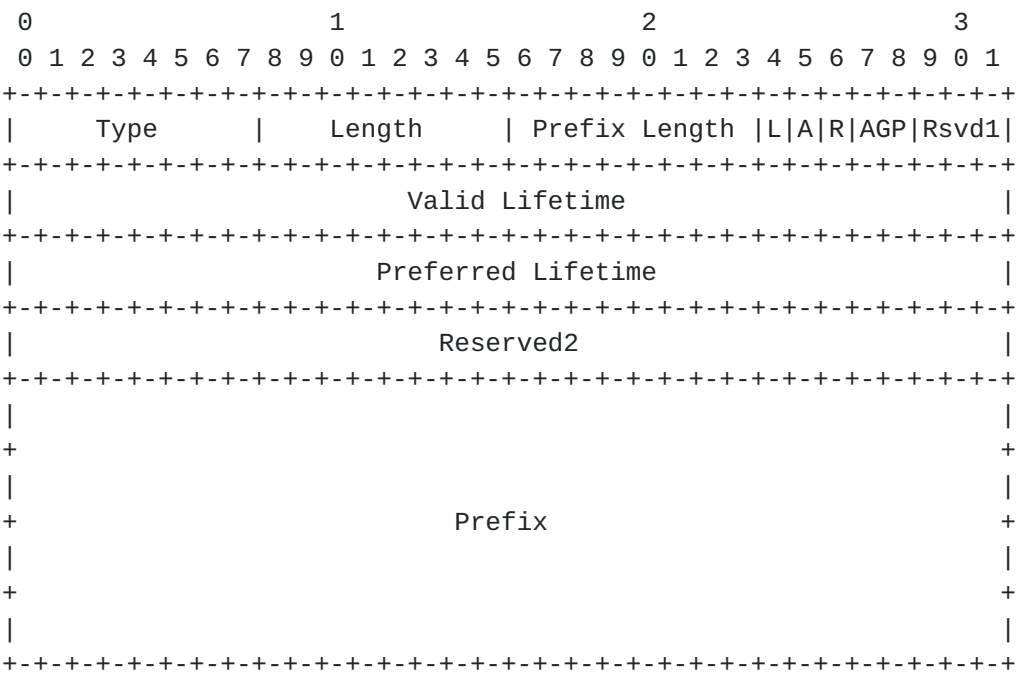
This document specifies a new field in the Prefix Information option of Router Advertisement messages, such that routers can advertise, for each network prefix to be used for SLAAC, the desired policy for the generation of IPv6 addresses. The policy information is simply "advisory" information, in the sense that hosts still have the final word on which address generation policy they use.

The aforementioned policy information basically indicates whether "stable" or "temporary" addresses are desired. We note that while the only address generation policies that have so far been standardized by the IETF are those based on e.g. IEEE identifiers and "Privacy Extensions for SLAAC", other address generation policies are possible. For example, [STABLE-PRIV] describes an address generation policy which results in interface identifiers that are stable for each prefix used for SLAAC, but that change from one autoconfiguration prefix to another.

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 "AGP" (Address Generation Policy) field, is specified 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 stable (i.e., not temporary). The resulting stable addresses may be based on Modified EUI-64 Format Identifiers [RFC4291], the stable private identifiers proposed in [STABLE-PRIV], or any other address generation policy specified in the future which results in IPv6 addresses that are stable/ constant for that autoconfiguration prefix/subnet.

10:
When generating addresses for this prefix, temporary addresses SHOULD be employed. The resulting addresses may be based on "Privacy Extensions for SLAAC" [RFC4941], or on any other policy which results in temporary Interface Identifiers. Address generation policies that result in stable addresses (such as those

specified in [RFC4941] and [STABLE-PRIV]) SHOULD NOT be used for this prefix.

11:
Unused (reserved for future use). The special value "11" is reserved for future extensions, and MUST NOT be set by routers implementing this specification. 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).

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

3. Router specification

3.1. Router configuration

This section specifies a variable that routers implementing this specification MUST support:

DesiredAddressPolicy:
This variable specifies the desired address generation policy for IPv6 addresses resulting from SLAAC. As of this specification, possible values are: "Default", "TemporaryAddresses", and "StableAddresses". This variable SHOULD default to "Default".

3.2. Router operation

A router sending a Prefix Information option MUST set the AGP bits according to the value of the variable DesiredAddressPolicy. The following table specifies which values must be used for the AGP field depending on the value of the DesiredAddressPolicy variable.

DesiredAddressPolicy	AGP field
Default	00
StableAddresses	01
TemporaryAddresses	10

Table 1: Correspondence between DesiredAddressPolicy and AGP bits

4. Host specification

4.1. Host configuration

This section specifies two new variables that hosts implementing this specification MUST support:

AddressPolicyConfiguration:
: This variable specifies whether the host should honor the advice conveyed in the AGP field of the received Prefix Information options. There are two possible values for this variable: "Enabled" and "Disabled". This variable SHOULD default to "Enabled".

DefaultAddressPolicy:
: This variable specifies the default IPv6 address generation policy that will be employed if AddressPolicyConfiguration is set to "Disabled", or if "AddressPolicyConfiguration" is set to "Enabled" but the AGP field of the received Prefix Information option is set to "00" (i.e., no specific advice is provided for the generation of addresses for this prefix). As of this specification, possible values are "TemporaryAddresses" (e.g. for [RFC4941]) and "StableAddresses" (for [RFC4291] or [STABLE-PRIV]). This variable SHOULD default to "TemporaryAddresses".

A host willing to ignore the advice of the router regarding which policy to use to generate IPv6 addresses MAY do so by setting AddressPolicyConfiguration to "Disabled".

It should be noted that the aforementioned variables might have different granularities. For example, a host could specify a set of EnableAddressPolicy and DefaultAddressPolicy variables on a global basis, on a "per network interface type" basis, on a "per wireless network" basis, etc.

4.2. Host Operation

When generating addresses for the prefix contained in a "Prefix Information Option", hosts implementing this specification MUST proceed as follows:

- If AddressPolicyConfiguration is set to "Enabled", the host SHOULD employ only the policy specified by the AGP field when generating addresses for this prefix. If no specific advice is provided (i.e., the AGP field is set to "00"), the host SHOULD employ only the policy specified by the DefaultAddressPolicy variable when generating addresses for this prefix.

- If AddressPolicyConfiguration is Disabled, the host SHOULD employ only the policy specified by the DefaultAddressPolicy variable when generating addresses for this prefix.

5. 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.

6. Privacy Considerations

As discussed in [RFC4941], IPv6 addresses generated using the Modified EUI-64 Format Identifiers [RFC4291] allow tracking of nodes across networks, since the resulting Interface-ID is a globally-unique value that will remain constant across all networks that the node may connect to.

As specified in Section 3 and Section 4 of this document, the default value for the AGP bits of a Prefix Information option is "01" (no specific advice is provided for the generation of addresses for this prefix), and the default address generation policy (DefaultAddressPolicy) for hosts is set to "TemporaryAddresses". This means that, unless the router or host default settings are overridden, the default settings resulting from this specification will enable the use of "temporary addresses" (such as those specified in [RFC4941]).

Nevertheless, it should be noted that the mechanism specified in this document simply provides the means for a router to convey *advisory* information regarding the desired policy for generating IPv6 addresses when SLAAC is employed: this specification allows hosts to ignore the aforementioned advice when deemed appropriate (by setting AddressPolicyConfiguration to "Disabled"). For example, hosts very concerned with the privacy implications of using interface identifiers that remain constant across networks may set AddressPolicyConfiguration to "Disabled" and DefaultAddressPolicy to "TemporaryAddresses" when connecting to untrusted networks, such that Temporary Addresses (such as those specified in [RFC4941]) are always employed (despite the advice provided by the local router).

Finally, we note that the value and effectiveness of some variants of Temporary Addresses (such as that specified in [RFC4941]) have been questioned in a number of studies [I-D.dupont-ipv6-rfc3041harmful] [Escudero] [CPNI-IPv6]. However, this document does not take a stance about their value and effectiveness.

7. Security Considerations

An attacker could exploit the mechanism specified in this document to cause hosts in a given subnet to disable "Temporary Addresses", thus usually leading to the generation of Interface Identifiers that embed the underlying hardware address (e.g. using Modified EUI-64 Format Identifiers), instead. Thus, in such cases, the privacy of the victim hosts that would have enabled the Privacy Extensions could possibly be reduced.

However, some considerations should be made about such possible attack. Firstly, such an attack would require from an attacker the same effort as any other Neighbor Discovery attack based on crafted Router Advertisement messages [RFC3756] [CPNI-IPv6], most of which would be far more interesting for an attacker than this possible attack vector. For example, a (possibly malicious) router could still cause a host to use Modified EUI-64 Format Identifiers if DHCPv6 [RFC3315] is required for address configuration, and the DHCPv6 server selects the IPv6 addresses to be leased to hosts based on e.g. the source link-layer address of the DHCP requests. Secondly, while the the only policy for generating stable IPv6 addresses that has so far been standardized by the IETF is that based on e.g. IEEE identifiers, there are other possible policies, such as that proposed in [STABLE-PRIV], that lead to stable addresses. That is, use of "stable" identifiers does not necessarily imply that such identifiers remain stable/constant across networks.

In those cases in which the network itself is trusted, but users connected to the same network are not, the possible options for mitigating this and other attack vectors based on crafted Router Advertisement messages include the deployment of the so-called "Router Advertisement guard" mechanism [RFC6104], with the implementation guidelines described in [I-D.gont-v6ops-ra-guard-evasion]. Additionally, SEND (SEcure Neighbor Discovery) [RFC3971] could be potentially deployed to mitigate these and other Neighbor Discovery attacks. However, a number of issues (such as the requirement for Public Key Infrastructure) difficult the deployment of SEND in most general network scenarios [CPNI-IPv6].

8. Acknowledgements

The author would like to thank (in alphabetical order) Mikael Abrahamsson, Ran Atkinson, Brian Carpenter, Christian Huitema, Mark Smith, Mark Townsley, and James Woodyatt, for providing valuable comments on [I-D.gont-6man-managing-privacy-extensions], on which this document is based.

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

9. References

9.1. 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.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[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.

[RFC6104] Chown, T. and S. Venaas, "Rogue IPv6 Router Advertisement Problem Statement", RFC 6104, February 2011.

9.2. Informative References

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3756] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.

[I-D.gont-v6ops-ra-guard-evasion] Gont, F. and U. CPNI, "IPv6 Router Advertisement Guard (RA-Guard) Evasion", draft-gont-v6ops-ra-guard-evasion-01 (work in progress), June 2011.

[I-D.gont-6man-managing-privacy-extensions]
Gont, F. and R. Broersma, "Managing the Use of Privacy Extensions for Stateless Address Autoconfiguration in IPv6", draft-gont-6man-managing-privacy-extensions-01 (work in progress), March 2011.

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

[STABLE-PRIV]
Gont, F., "A method for Generating Stable Privacy-Enhanced Addresses with IPv6 Stateless Address Autoconfiguration (SLAAC)", Work in Progress, December 2011, <http://tools.ietf.org/html/draft-gont-6man-stable-privacy-addresses>.

[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, (available on request).

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

A.1. Changes from draft-gont-6man-managing-privacy-extensions-01

- The address-generation policy information has been changed from "'Modified EUI-64' vs. 'Privacy Addresses'" to "'stable addresses' vs. 'temporary addresses'", thus noting that more than one possible policy exists for each category.

- The appendix on possible alternative specifications for the AGP bits has been removed.

- The document now focuses on a mechanism that would enable increased use of "temporary addresses" (such as "Privacy Extensions").

Author's Address

Fernando Gont
UK CPNI

Email: fgont@si6networks.com
URI: http://www.cpni.gov.uk