IPv6 Maintenance (6man) Working Group
Internet-Draft
Updates: 4191, 4861, 4862, 8106 (if approved)
Intended status: Standards Track
Expires: 3 November 2023

F. Gont
SI6 Networks
J. Zorz
6connect
R. Patterson
Sky UK

2 May 2023

Improving the Robustness of Stateless Address Autoconfiguration (SLAAC) to Flash Renumbering Events
draft-ietf-6man-slaac-renum-07

Abstract

In renumbering scenarios where an IPv6 prefix suddenly becomes invalid, hosts on the local network will continue using stale prefixes for an unacceptably long period of time, thus resulting in connectivity problems. This document improves the reaction of IPv6 Stateless Address Autoconfiguration to such renumbering scenarios. It formally updates RFC 4191, RFC 4861, RFC 4862, and RFC 8106.

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 https://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 3 November 2023.

Copyright Notice

Table of Contents

1. Introduction

In scenarios where network configuration information becomes invalid without any explicit signaling of that condition, hosts on the local network will continue using stale information for an unacceptably long period of time, thus resulting in connectivity problems. This problem has been discussed in detail in [RFC8978].

This document updates the Neighbor Discovery specification [RFC4861], the Stateless Address Autoconfiguration (SLAAC) specification [RFC4862], and other associated specifications ([RFC4191] and [RFC8106]), such that hosts can more gracefully deal with the so-called flash renumbering events, thus improving the robustness of SLAAC.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. SLAAC reaction to Flash-renumbering Events

In some scenarios, the local router triggering the network renumbering event may try to deprecate the stale information (by explicitly signaling the network about the renumbering event), whereas in other scenarios the renumbering event may happen inadvertently, without the router explicitly signaling the scenario to local hosts. The following subsections analyze specific considerations for each of these scenarios.

3.1. Renumbering without Explicit Signaling

In the absence of explicit signalling from SLAAC routers (such as sending Prefix Information Options (PIOs) with small lifetimes to deprecate stale prefixes), stale prefixes will remain preferred and valid according to the Preferred Lifetime and Valid Lifetime parameters (respectively) of the last received PIO. [RFC4861] specifies the following default values for PIOs:

* Preferred Lifetime (AdvPreferredLifetime): 604800 seconds (7 days)

* Valid Lifetime (AdvValidLifetime): 2592000 seconds (30 days)

This means that, in the absence of explicit signaling by a SLAAC router to deprecate a prefix, it will take a host 7 days (one week) to deprecate the corresponding addresses, and 30 days (one month) to eventually remove any addresses configured for the stale prefix. Clearly, employing such long default values is unacceptable for most deployment scenarios that may experience flash-renumbering events.

NOTE:
[RFC8978] provides an operational recommendation for Customer Edge (CE) routers to override the standard default Preferred Lifetime

(AdvPreferredLifetime) and Valid Lifetime (AdvValidLifetime) to 2700 seconds (45 minutes) and 5400 seconds (90 minutes), respectively, thus improving the state of affairs for CE router scenarios.

Similarly, other Neighbor Discovery options employ unnecessarily long default lifetimes that are unacceptable for most deployment scenarios that may experience flash-renumbering events.

Use of more appropriate timers in Router Advertisement messages can help limit the amount of time that hosts will maintain stale configuration information. Thus, Section 4.1 formally specifies the use of more appropriate (i.e., shorter) default lifetimes for Neighbor Discovery options.

3.2. Renumbering with Explicit Signaling

In scenarios where a local router is aware about the renumbering event, it may try to phase out the stale network configuration information. In these scenarios, there are two aspects to be considered:

* The amount of time during which the router should continue trying to deprecate the stale network configuration information.

* The ability of SLAAC hosts to phase out stale configuration.

Since the network could be become partitioned at any arbitrary time and for an arbitrarily long period of time, routers need to contemplate the possible scenario where hosts receive an RA message, and the network subsequently becomes partitioned. This means that in order to reliably deprecate stale information, a router would should try to deprecate such information for a period of time equal to the associated Neighbor Discovery option lifetime used when the information was advertised.

NOTE:
For example, it should try to deprecate a prefix (via a PIO) for a period of time equal to the "Preferred Lifetime" used when advertising the prefix, and try to invalidate the prefix for a period of time equal to the "Valid Lifetime" (see Section 12 of [RFC4861]) used when advertising the prefix.

> Once the number of seconds in the original "Preferred Lifetime" have elapsed, all hosts will have deprecated the corresponding addresses, while once the number of seconds in the "Valid Lifetime" have elapsed, the corresponding addresses will be invalidated and removed.

Thus, use of more appropriate default lifetimes for Neighor Discovery options, as specified in Section 4.1, would reduce the amount of time stale options would need to be advertised by a router to ensure that the associated information is phased out.

In the case of Prefix Information Options (PIOs), in scenarios where a router has positive knowledge that a prefix has become invalid (and thus could signal this condition to local hosts), the current specifications will prevent SLAAC hosts from fully recovering from such stale information: Item "e)" of Section 5.5.3 of [RFC4862] specifies that an RA may never reduce the "RemainingLifetime" to less than two hours. Additionally, if the RemainingLifetime of an address is smaller than 2 hours, then a Valid Lifetime smaller than 2 hours will be ignored. The inability to invalidate a stale prefix may prevent communications with the new "owners" of a prefix, and thus is highly undesirable. However, the Preferred Lifetime of an address *may* be reduced to any value to avoid the use of a stale prefix for new communications.

Section 4.2 formally updates [RFC4862] to remove this restriction, such that hosts may react to the advertised "Valid Lifetime" even if it is smaller than 2 hours. Section 4.3 recommends that routers disseminate network configuration information when a network interface is initialized, such that new configuration information propagates in a timelier manner.

4. Improvements to Stateless Address Autoconfiguration (SLAAC)

The following subsections update [RFC4861] and [RFC4862], such that the problem discussed in this document is mitigated. The updates in the following subsections are mostly orthogonal, and mitigate different aspects of SLAAC that prevent a timely reaction to flash renumbering events:

* Reduce the default Valid Lifetime and Preferred Lifetime of PIOs (Section 4.1):

  This helps limit the amount of time a host may employ stale information, and also limits the amount of time a router needs to try to deprecate stale information.

* Honor PIOs with small Valid Lifetimes (Section 4.2):

This allows routers to invalidate stale prefixes, since otherwise [RFC4861] would prevent hosts from honoring PIOs with a Valid Lifetime smaller than two hours.

* Recommend routers to retransmit configuration information upon interface initialization/reinitialization (Section 4.3):

  This helps spread the new information in a timelier manner.

* Recommend routers to always send all options (i.e. the complete configuration information) in RA messages, and in the smallest possible number of packets (Section 4.4):

  This helps propagate the same information to all hosts.

4.1. More Appropriate Neighbor Discovery Option Lifetimes

This document defines the following variables to be employed for the default lifetimes of Neighbor Discovery options:

* ND_DEFAULT_PREFERRED_LIFETIME: max(AdvDefaultLifetime, 3 * MaxRtrAdvInterval)

* ND_DEFAULT_VALID_LIFETIME: 2 * ND_DEFAULT_PREFERRED_LIFETIME

where:

AdvDefaultLifetime:
: Router configuration variable specified in [RFC4861], which specifies the value to be placed in the Router Lifetime field of Router Advertisements sent from the interface, in seconds.

MaxRtrAdvInterval:
: Router configuration variable specified in [RFC4861], which specifies the maximum time allowed between sending unsolicited multicast Router Advertisements from the interface, in seconds.

max():
: A function that computes the maximum of its arguments.

NOTE:
: The expression above computes of maximum among AdvDefaultLifetime and "3 * MaxRtrAdvInterval" (the default value of AdvDefaultLifetime, as per [RFC4861]) to accommodate the case where an operator might simply want to disable one local router for maintenance, while still having the router advertise SLAAC configuration information.

> [RFC4861] specifies the default value of MaxRtrAdvInterval as 600 seconds, and the default value of AdvDefaultLifetime as 3 * MaxRtrAdvInterval. Therefore, when employing default values for MaxRtrAdvInterval and AdvDefaultLifetime, the default values of ND_DEFAULT_PREFERRED_LIFETIME and ND_DEFAULT_VALID_LIFETIME become 1800 seconds (30 minutes) and 3600 seconds (1 one hour), respectively. We note that when implementing BCP202 [RFC7772], AdvDefaultLifetime will typically be in the range of 45-90 minutes, and therefore the value of ND_DEFAULT_PREFERRED_LIFETIME will be in the range 45-90 minutes, while the value of ND_DEFAULT_VALID_LIFETIME will be in the range of 90-180 minutes.

This document formally updates [RFC4861] to modify the default values of the Preferred Lifetime and the Valid Lifetime of PIOs as follows:

* AdvPreferredLifetime: ND_DEFAULT_PREFERRED_LIFETIME

* AdvValidLifetime: ND_DEFAULT_VALID_LIFETIME

This document formally updates [RFC4191] to specify the default Route Lifetime of Route Information Options (RIOs) as follows:

* Route Lifetime: Default: ND_DEFAULT_PREFERRED_LIFETIME

This document formally updates [RFC8106] to modify the default Lifetime of Recursive DNS Server Options as:

* Lifetime: Default: ND_DEFAULT_PREFERRED_LIFETIME

Additionally, this document formally updates [RFC8106] to modify the default Lifetime of DNS Search List Options as:

* Lifetime: Default: ND_DEFAULT_PREFERRED_LIFETIME

4.2. Honor Small PIO Valid Lifetimes

The entire item "e)" (pp. 19-20) from Section 5.5.3 of [RFC4862] is replaced with the following text:

> e) If the advertised prefix is equal to the prefix of an address configured by stateless autoconfiguration in the list, the valid lifetime and the preferred lifetime of the address should be updated by processing the Valid Lifetime and the Preferred Lifetime (respectively) in the received advertisement.

RATIONALE:

* This change allows hosts to react to the signal provided by a router that has positive knowledge that a prefix has become invalid.

* The behavior described in [RFC4862] had been incorporated during the revision of the original IPv6 Stateless Address Autoconfiguration specification ([RFC1971]). At the time, the IPNG working group decided to mitigate the attack vector represented by Prefix Information Options with very short lifetimes, on the premise that these packets represented a bigger risk than other ND-based attack vectors [IPNG-minutes].

  While reconsidering the trade-offs represented by such decision, we conclude that the drawbacks of the aforementioned mitigation outweigh the possible benefits.

  In scenarios where RA-based attacks are of concern, proper mitigations such as RA-Guard [RFC6105] [RFC7113] or SEND [RFC3971] should be implemented.

4.3. Interface Initialization

When an interface is initialized, it is paramount that network configuration information is propagated on the corresponding network (particularly in scenarios where an interface has been re-initialized, and the conveyed information has changed). Thus, this document replaces the following text from Section 6.2.4 of [RFC4861]:

> In such cases, the router MAY transmit up to MAX_INITIAL_RTR_ADVERTISEMENTS unsolicited advertisements, using the same rules as when an interface becomes an advertising interface.

with:

> In such cases, the router SHOULD transmit MAX_INITIAL_RTR_ADVERTISEMENTS unsolicited advertisements, using the same rules as when an interface becomes an advertising interface.

RATIONALE:

* Use of stale information can lead to interoperability problems. Therefore, it is important that new configuration information propagates in a timelier manner to all hosts.

NOTE:
[RFC9096] specifies recommendations for CPE routers to signal any stale network configuration information.

4.4. Conveying Information in Router Advertisement (RA) Messages

Intentionally omitting information in Router Advertisements may prevent the propagation of such information, and may represent a challenge for hosts that need to infer whether they have received a complete set of SLAAC configuration information. As a result, this section recommends that, to the extent that is possible, RA messages contain a complete set of SLAAC information.

This document replaces the following text from Section 6.2.3 of [RFC4861]:

> A router MAY choose not to include some or all options when sending unsolicited Router Advertisements. For example, if prefix lifetimes are much longer than AdvDefaultLifetime, including them every few advertisements may be sufficient. However, when responding to a Router Solicitation or while sending the first few initial unsolicited advertisements, a router SHOULD include all options so that all information (e.g., prefixes) is propagated quickly during system initialization.
>
> If including all options causes the size of an advertisement to exceed the link MTU, multiple advertisements can be sent, each containing a subset of the options.

with:

> When sending Router Advertisements, a router SHOULD include all options.
>
> If including all options would cause the size of an advertisement to exceed the link MTU, multiple advertisements can be sent, each containing a subset of the options. In all cases, routers SHOULD convey all information using the smallest possible number of packets, and SHOULD convey options of the same type in the same packet to the extent possible.

RATIONALE:

* Sending information in the smallest possible number of packets was somewhat already implied by the original text in [RFC4861]. Including all options when sending RAs leads to simpler code (as opposed to dealing with special cases where specific information is intentionally omitted), and also helps hosts infer when they have received a complete set of SLAAC

configuration information. Note that while [RFC4861] allowed some RAs to omit some options, to the best of the authors' knowledge, all SLAAC router implementations always send all options in the smallest possible number of packets. Therefore, this section simply aligns the protocol specifications with existing implementation practice.

5. IANA Considerations

This document has no actions for IANA.

6. Implementation Status

[NOTE: This section is to be removed by the RFC-Editor before this document is published as an RFC.]

This section summarizes the implementation status of the updates proposed in this document. In some cases, they correspond to variants of the mitigations proposed in this document (e.g., use of reduced default lifetimes for PIOs, albeit using different values than those recommended in this document). In such cases, we believe these implementations signal the intent to deal with the problems described in [RFC8978] while lacking any guidance on the best possible approach to do it.

6.1. More Appropriate Lifetime Values

6.1.1. Router Configuration Variables

6.1.1.1. rad(8)

We have produced a patch for OpenBSD's rad(8) [rad] that employs the default lifetimes recommended in this document, albeit it has not yet been committed to the tree. The patch is available at: <https://www.gont.com.ar/code/fgont-patch-rad-pio-lifetimes.txt>.

6.1.1.2. radvd(8)

The radvd(8) daemon [radvd], normally employed by Linux-based router implementations, currently employs different default lifetimes than those recommended in [RFC4861]. radvd(8) employs the following default values [radvd.conf]:

* Preferred Lifetime: 14400 seconds (4 hours)

* Valid Lifetime: 86400 seconds (1 day)

This is not following the specific recommendation in this document, but is already a deviation from the current standards.

6.2. Honor Small PIO Valid Lifetimes

6.2.1. Linux Kernel

A Linux kernel implementation of this document has been committed to the net-next tree. The implementation was produced in April 2020 by Fernando Gont <fgont@si6networks.com>. The corresponding patch can be found at: <https://patchwork.ozlabs.org/project/netdev/patch/20200419122457.GA971@archlinux-current.localdomain/>

6.2.2. NetworkManager

NetworkManager [NetworkManager] processes RA messages with a Valid Lifetime smaller than two hours as recommended in this document.

6.3. Conveying Information in Router Advertisement (RA) Messages

We know of no implementation that splits network configuration information into multiple RA messages.

6.4. Recovery from Stale Configuration Information without Explicit Signaling

6.4.1. dhcpcd(8)

The dhcpcd(8) daemon [dhcpcd], a user-space SLAAC implementation employed by some Linux-based and BSD-derived operating systems, will set the Preferred Lifetime of addresses corresponding to a given prefix to 0 when a single RA from the router that previously advertised the prefix fails to advertise the corresponding prefix. However, it does not affect the corresponding Valid Lifetime. Therefore, it can be considered a partial implementation of this feature.

6.5. Other mitigations implemented in products

[FRITZ] is a Customer Edge Router that tries to deprecate stale prefixes by advertising stale prefixes with a Preferred Lifetime of 0, and a Valid Lifetime of 2 hours (or less). There are two things to note with respect to this implementation:

* Rather than recording prefixes on stable storage (as recommended in [RFC9096]), this implementation checks the source address of IPv6 packets, and assumes that usage of any address that does not correspond to a prefix currently-advertised by the Customer Edge

Router is the result of stale network configuration information. Hence, upon receipt of a packet that employs a source address that does not correspond to a currently-advertised prefix, this implementation will start advertising the corresponding prefix with small lifetimes, with the intent of deprecating it.

* Possibly as a result of item "e)" (pp. 19-20) from Section 5.5.3 of [RFC4862] (discussed in Section 4.2 of this document), upon first occurrence of a stale prefix, this implementation will employ a decreasing Valid Lifetime, starting from 2 hours (7200 seconds), as opposed to a Valid Lifetime of 0.

7. Security Considerations

The protocol update in Section 4.2 could allow an on-link attacker to perform a Denial of Service attack against local hosts, by sending a forged RA with a PIO with a Valid Lifetime of 0. Upon receipt of that packet, local hosts would invalidate the corresponding prefix, and therefore remove any addresses configured for that prefix, possibly terminating e.g. associated TCP connections. However, an attacker may achieve similar effects via a number other Neighbor Discovery (ND) attack vectors, such as directing traffic to a non-existing node until ongoing TCP connections time out, or performing a ND-based man-in-the-middle (MITM) attack and subsequently forging TCP RST segments to cause on-going TCP connections to be reset. Thus, for all practical purposes, this attack vector does not really represent any greater risk than other ND attack vectors. As noted in Section 4.2 , in scenarios where RA-based attacks are of concern, proper mitigations such as RA-Guard [RFC6105] [RFC7113] or SEND [RFC3971] should be implemented.

8. Acknowledgments

The authors would like to thank (in alphabetical order) Mikael Abrahamsson, Tore Anderson, Luis Balbinot, Brian Carpenter, Lorenzo Colitti, Owen DeLong, Gert Doering, Thomas Haller, Nick Hilliard, Bob Hinden, Philip Homburg, Lee Howard, Christian Huitema, Tatuya Jinmei, Erik Kline, Ted Lemon, Jen Linkova, Albert Manfredi, Roy Marples, Florian Obser, Jordi Palet Martinez, Michael Richardson, Hiroki Sato, Mark Smith, Hannes Frederic Sowa, Dave Thaler, Tarko Tikan, Ole Troan, Eduard Vasilenko, and Loganaden Velvindron, for providing valuable comments on earlier versions of this document.

Fernando would like to thank Alejandro D'Egidio and Sander Steffann for a discussion of these issues, which led to the publication of [RFC8978], and eventually to this document.

Fernando would also like to thank Brian Carpenter who, over the years, has answered many questions and provided valuable comments that has benefited his protocol-related work.

9. References

9.1. 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, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC7772] Yourtchenko, A. and L. Colitti, "Reducing Energy Consumption of Router Advertisements", BCP 202, RFC 7772, DOI 10.17487/RFC7772, February 2016, <https://www.rfc-editor.org/info/rfc7772>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

9.2. Informative References

[dhcpcd] Marples, R., "dhcpcd - a DHCP client", <https://roy.marples.name/projects/dhcpcd/>.

[FRITZ] Gont, F., "Quiz: Weird IPv6 Traffic on the Local Network (updated with solution)", SI6 Networks Blog, February 2016, <https://www.si6networks.com/2016/02/16/quiz-weird-ipv6-traffic-on-the-local-network-updated-with-solution/>.

[IPNG-minutes] IETF, "IPNG working group (ipngwg) Meeting Minutes", Proceedings of the thirty-eightt Internet Engineering Task Force , April 1997, <https://www.ietf.org/proceedings/38/97apr-final/xrtftr47.htm>.

[NetworkManager]
NetworkManager, "NetworkManager web site", <https://wiki.gnome.org/Projects/NetworkManager>.

[rad] Obser, F., "OpenBSD Router Advertisement Daemon - rad(8)", <https://cvsweb.openbsd.org/src/usr.sbin/rad/>.

[radvd] Hawkins, R. and R. Johnson, "Linux IPv6 Router Advertisement Daemon (radvd)", <http://www.litech.org/radvd/>.

[radvd.conf]
Hawkins, R. and R. Johnson, "radvd.conf - configuration file of the router advertisement daemon", <https://github.com/reubenhwk/radvd/blob/master/radvd.conf.5.man>.

[RFC1971] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 1971, DOI 10.17487/RFC1971, August 1996, <https://www.rfc-editor.org/info/rfc1971>.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005, <https://www.rfc-editor.org/info/rfc3971>.

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191, November 2005, <https://www.rfc-editor.org/info/rfc4191>.

[RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105, DOI 10.17487/RFC6105, February 2011, <https://www.rfc-editor.org/info/rfc6105>.

[RFC7113] Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", RFC 7113, DOI 10.17487/RFC7113, February 2014, <https://www.rfc-editor.org/info/rfc7113>.

[RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 8106, DOI 10.17487/RFC8106, March 2017, <https://www.rfc-editor.org/info/rfc8106>.

[RFC8978] Gont, F., or, J., and R. Patterson, "Reaction of IPv6 Stateless Address Autoconfiguration (SLAAC) to Flash-Renumbering Events", RFC 8978, DOI 10.17487/RFC8978, March 2021, <https://www.rfc-editor.org/info/rfc8978>.

[RFC9096] Gont, F., or, J., Patterson, R., and B. Volz, "Improving the Reaction of Customer Edge Routers to IPv6 Renumbering Events", BCP 234, RFC 9096, DOI 10.17487/RFC9096, August 2021, <https://www.rfc-editor.org/info/rfc9096>.

Authors' Addresses

Fernando Gont
SI6 Networks
Segurola y Habana 4310, 7mo Piso
Villa Devoto
Ciudad Autonoma de Buenos Aires
Argentina
Email: fgont@si6networks.com
URI: https://www.si6networks.com

Jan Zorz
6connect
Email: jan@connect.com

Richard Patterson
Sky UK
Email: richard.patterson@sky.uk