IPv6 Operations Working Group (v6ops)
Internet-Draft
Intended status: Informational
Expires: May 6, 2021

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

November 2, 2020

Reaction of Stateless Address Autoconfiguration (SLAAC) to Flash-Renumbering Events
draft-ietf-v6ops-slaac-renum-05

Abstract

In scenarios where network configuration information related to IPv6 prefixes becomes invalid without any explicit and reliable signaling of that condition (such as when a Customer Edge router crashes and reboots without knowledge of the previously-employed prefixes), nodes on the local network may continue using stale prefixes for an unacceptably long time (on the order of several days), thus resulting in connectivity problems. This document describes this issue and discusses operational workarounds that may help to improve network robustness. Additionally, it highlights areas where further work may be needed.

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 May 6, 2021.

Table of Contents

1. Introduction 2
2. Analysis of the Problem 5
2.1. Use of Dynamic Prefixes 5
2.2. Default Timer Values in IPv6 Stateless Address Autoconfiguration (SLAAC) 6
2.3. Recovering from Stale Network Configuration Information . 7
2.4. Lack of Explicit Signaling about Stale Information . . . 7
2.5. Interaction Between DHCPv6-PD and SLAAC 8
3. Operational Mitigations 8
3.1. Stable Prefixes 8
3.2. SLAAC Parameter Tweaking 8
4. Future Work 9
5. IANA Considerations 10
6. Security Considerations 10
7. Acknowledgments 10
8. References 11
8.1. Normative References 11
8.2. Informative References 11
Authors' Addresses 13

1. Introduction

IPv6 Stateless address autoconfiguration (SLAAC) [RFC4862] conveys information about prefixes to be employed for address configuration via Prefix Information Options (PIOs) sent in Router Advertisement (RA) messages. IPv6 largely assumes prefix stability, with network renumbering only taking place in a planned manner, with old/stale prefixes being phased-out via reduced prefix lifetimes, and new prefixes (with longer lifetimes) being introduced at the same time. However, there are several scenarios that may lead to the so-called "flash-renumbering" events, where the prefix employed by a network

suddenly becomes invalid and replaced by a new prefix. In some of these scenarios, the local router producing the network renumbering event may try to deprecate the currently-employed prefixes (by explicitly signaling the network about the renumbering event), whereas in other scenarios it may be unable to do so.

In scenarios where network configuration information related to IPv6 prefixes becomes invalid without any explicit and reliable signaling of that condition, nodes on the local network may continue using stale prefixes for an unacceptably long period of time, thus resulting in connectivity problems.

Scenarios where this problem may arise include, but are not limited to, the following:

- The most common IPv6 deployment scenario for residential or small office networks, where a Customer Edge (CE) router employs DHCPv6 Prefix Delegation (DHCPv6-PD) [RFC8415] to request a prefix from an Internet Service Provider (ISP), and a sub-prefix of the leased prefix is advertised on the LAN-side of the CE router via Stateless Address Autoconfiguration (SLAAC) [RFC4862]. In scenarios where the CE router crashes and reboots, the CE may obtain (via DHCPv6-PD) a different prefix from the one previously leased, and therefore advertise (via SLAAC) the new prefix on the LAN side. Hosts will typically configure addresses for the new prefix, but will normally retain and may actively employ the addresses configured for the previously-advertised prefix, since their associated Preferred Lifetime and Valid Lifetime allow them to do so.

- A router (e.g. Customer Edge router) advertises autoconfiguration prefixes corresponding to prefixes learned via DHCPv6-PD with constant PIO lifetimes that are not synchronized with the DHCPv6-PD lease time (even though Section 6.3 of [RFC8415] requires such synchronization). While this behavior violates the aforementioned requirement from [RFC8415], it is not an unusual behavior, particularly when e.g. DHCPv6-PD is implemented in a different software module than the SLAAC router component.

- A switch-port the host is connected to is moved to another subnet (VLAN) as a result of manual switch-port reconfiguration or 802.1x re-authentication. There has been evidence that some 802.1x

supplicants do not reset network settings after successful 802.1x authentication. So if a host fails 802.1x authentication for some reason, is placed in a "quarantine" VLAN and is successfully authenticated later on, it might end up having IPv6 addresses from both the old ("quarantine") and the new VLANs.

- During the planned network renumbering, a router is configured to send an RA with the Preferred Lifetime for the "old" Prefix Information Option (PIO) set to zero and the new PIO with a non-zero Preferred Lifetime. However, due to unsolicited RAs being sent to a multicast destination address, and multicast being

rather unreliable on busy wifi networks, the RA might not be received by local hosts.

- Automated device config management system performs periodic config pushes to network devices. In these scenarios, network devices may simply immediately forget their previous configuration, rather than withdrawing it gracefully. If such a push results in changing the subnet configured on a particular network, hosts attached to that network would not get notified about the subnet change, and their addresses from the "old" prefix will not be deprecated. A related scenario is the incorrect network renumbering where a network administrator renumbers a network by simply removing the "old" prefix from the configuration and configuring a new prefix instead.

Lacking any explicit and reliable signaling to deprecate the previously-advertised prefixes, hosts may continue to employ the previously-configured addresses, which will typically result in packets being blackholed (whether because of egress-filtering by the CE router or ISP) or the return traffic being discarded or routed elsewhere.

The default values for the "Preferred Lifetime" and "Valid Lifetime" of PIOs specified in [RFC4861] mean that, in the aforementioned scenarios, the stale addresses would be retained, and could be actively employed for new communications instances, for an unacceptably long period of time (one month, and one week, respectively). This could lead to interoperability problems, instead of hosts transitioning to the newly-advertised prefix(es) in a more

timely manner.

Some devices have implemented ad-hoc mechanisms to address this problem, such as sending RAs to deprecate apparently-stale prefixes when the device receives any packets employing a source address from a prefix not currently advertised for address configuration on the local network [FRITZ]. However, this may introduce other interoperability problems, particularly in multihomed/multiprefix scenarios. This is a clear indication that advice in this area is warranted.

Unresponsiveness to these "flash-renumbering" events is caused by the inability of the network to deprecate stale information, as well as by the inability of hosts to react to network configuration changes in a more timely manner. Clearly, it would be desirable that these flash-renumbering scenarios do not occur, and that, when they do occur, that hosts are explicitly and reliably notified of their occurrence. However, for robustness reasons, it is paramount for hosts to be able to recover from stale configuration information even

when these flash-renumbering events occur and the network is unable to explicitly and reliably notify hosts about such conditions.

Section 2 analyzes this problem in more detail. Section 3 describes possible operational mitigations. Section 4 describes possible future work to mitigate the aforementioned problem.

2. Analysis of the Problem

As noted in Section 1, the problems discussed in this document are exacerbated by the default values of some protocol parameters and other factors. The following sections analyze each of them in detail.

2.1. Use of Dynamic Prefixes

In network scenarios where dynamic prefixes are employed, renumbering events lead to updated network configuration information being propagated through the network, such that the renumbering events are gracefully handled. However, if the renumbering event happens along with e.g. loss of configuration state by some of the devices involved in the renumbering procedure (e.g., a router crashes, reboots, and

gets leased a new prefix), this may result in a flash-renumbering event, where new prefixes are introduced without properly phasing out the old ones.

In simple residential or small office scenario, the problem discussed in this document would be avoided if DHCPv6-PD would lease "stable" prefixes. However, a recent survey [UK-NOF] indicates that 37% of the responding ISPs employ dynamic prefixes. That is, dynamic IPv6 prefixes are an operational reality.

Deployment reality aside, there are a number of possible issues associated with stable prefixes:

- Provisioning systems may be unable to deliver stable IPv6 prefixes.

- While an ISP might lease stable prefixes to the home or small office, the Customer Edge router might in turn lease sub-prefixes of these prefixes to other internal network devices. Unless the associated lease databases are stored on non-volatile memory, these internal devices might be leased dynamic sub-prefixes of the stable prefix leased by the ISP. In other words, every time a prefix is leased there is the potential for the resulting prefixes to become dynamic, even if the device leasing sub-prefixes has been leased a stable prefix by its upstream router.

- While there is a range of information that may be employed to correlate network activity [RFC7721], the use of stable prefixes clearly simplifies network activity correlation, and may essentially render features such as "temporary addresses" [RFC4941] irrelevant.

- There may be existing advice for ISPs to deliver dynamic IPv6 prefixes *by default* (see e.g. [GERMAN-DP]) over privacy concerns associated with stable prefixes.

For a number of reasons (such as the ones stated above), IPv6 deployments may employ dynamic prefixes (even at the expense of the issues discussed in this document), and that there might be scenarios in which the dynamics of a network are such that the network exhibits the behaviour of dynamic prefixes. Rather than trying to regulate

how operators may run their networks, this document aims at improving network robustness in the deployed Internet.

2.2. Default Timer Values in IPv6 Stateless Address Autoconfiguration (SLAAC)

The impact of the issue discussed in this document is a function of the lifetime values employed for the PIO lifetimes, since these values determine for how long the corresponding addresses will be preferred and considered valid. Thus, when the problem discussed in this document is experienced, the longer the PIO lifetimes, the higher the impact.

[RFC4861] specifies the following default PIO lifetime values:

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

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

Under problematic circumstances, such as where the corresponding network information has become stale without any explicit and reliable signal from the network (as described in Section 1), it could take hosts up to 7 days (one week) to deprecate the corresponding addresses, and up to 30 days (one month) to eventually invalidate and remove any addresses configured for the stale prefix. This means that it will typically take hosts an unacceptably long period of time (on the order of several days) to recover from these scenarios.

2.3. Recovering from Stale Network Configuration Information

SLAAC hosts are unable to recover from stale network configuration information for a number of reasons:

- Item "e)" of Section 5.5.3 of [RFC4862] specifies that an unauthenticated RA may never reduce the "RemainingLifetime" to less than two hours. If the RemainingLifetime of an address is

smaller than 2 hours, then a Valid Lifetime smaller than 2 hours will be ignored. The Preferred Lifetime of an address can be reduced to any value to avoid using a stale prefix for new communications.

- In the absence of explicit signalling from SLAAC routers (such as sending PIOs with a "Preferred Lifetime" set to 0), SLAAC hosts fail to recover from stale configuration information in a timely manner. However, when a network element is able to explicitly signal the renumbering event, it will only be able to deprecate the stale prefix, but not to invalidate the prefix in question. Therefore, communication with the new "owners" of the stale prefix will not be possible, since the stale prefix will still be considered "on-link".

2.4. Lack of Explicit Signaling about Stale Information

Whenever prefix information has changed, a SLAAC router should not only advertise the new information, but should also advertise the stale information with appropriate lifetime values (both "Preferred Lifetime" and "Valid Lifetime" set to 0). This would provide explicit signaling to SLAAC hosts to remove the stale information (including configured addresses and routes). However, in scenarios such as when a CE router crashes and reboots, the CE router may have no knowledge about the previously-advertised prefixes, and thus may be unable to advertise them with appropriate lifetimes (in order to deprecate them).

However, we note that, as discussed in Section 2.3, PIOs with small Valid Lifetimes in unauthenticated RAs will not lower the Valid Lifetime to any value shorter than two hours (as per [RFC4862]). Therefore, even if a SLAAC router tried to explicitly signal the network about the stale configuration information via unauthenticated RAs, implementations compliant with [RFC4862] would deprecate the corresponding prefixes, but would fail to invalidate them.

NOTE:
Some implementations have been updated to honor small PIO lifetimes values, as proposed in [I-D.ietf-6man-slaac-renum]. For example, please see [Linux-update].

2.5. Interaction Between DHCPv6-PD and SLAAC

While DHCPv6-PD is normally employed along with SLAAC, the interaction between the two protocols is largely unspecified. Not unusually, the two protocols are implemented in two different software components with the interface between the two implemented by some sort of script that feeds the SLAAC implementation with values learned from DHCPv6-PD.

At times, the prefix lease time is fed as a constant value to the SLAAC router implementation, meaning that, eventually, the prefix lifetime advertised on the LAN side will span *past* the DHCPv6-PD lease time. This is clearly incorrect, since the SLAAC router implementation would be allowing the use of such prefixes for a longer time than it has been granted usage of those prefixes via DHCPv6-PD.

3. Operational Mitigations

The following subsections discuss possible operational workarounds for the aforementioned problems.

3.1. Stable Prefixes

As noted in Section 2.1, the use of stable prefixes would eliminate the issue in *some* of the scenarios discussed in Section 1 of this document, such as the typical home network deployment. However, even in such scenarios, there might be reasons for which an administrator may want or may need to employ dynamic prefixes

3.2. SLAAC Parameter Tweaking

An operator may wish to override some SLAAC parameters such that, under normal circumstances, the timers will be refreshed/reset, but in the presence of network faults (such as the one discussed in this document), the timers go off and trigger some fault recovering action (e.g. deprecate and subsequently invalidate stale addresses).

The following router configuration variables from [RFC4861] (corresponding to the "lifetime" parameters of PIOs) could be overridden as follows:

AdvPreferredLifetime: 2700 seconds (45 minutes)

AdvValidLifetime: 5400 seconds (90 minutes)

NOTES:

The aforementioned values for AdvPreferredLifetime and AdvValidLifetime are expected to be appropriate for most networks. In some networks, particularly where the operator has complete control of prefix allocation and where hosts on the network may spend long periods sleeping (e.g., sensors with limited battery), longer values may be appropriate.

A CE router advertising a sub-prefix of a prefix leased via DHCPv6-PD will periodically refresh the Preferred Lifetime and the Valid Lifetime of an advertised prefix to AdvPreferredLifetime and AdvValidLifetime, respectively, as long as the resulting lifetime of the corresponding prefixes does not extend past the DHCPv6-PD lease time [I-D.ietf-v6ops-cpe-slaac-renum].

RATIONALE:

* In the context of [RFC8028], where it is clear that use of addresses configured for a given prefix is tied to using the next-hop router that advertised the prefix, it does not make sense for the "Preferred Lifetime" of a PIO to be larger than the "Router Lifetime" (AdvDefaultLifetime) of the corresponding Router Advertisement messages. The "Valid Lifetime" is set to a much larger value to cope with transient network problems.

* Lacking RAs that refresh information, addresses configured for advertised prefixes become deprecated in a more timely manner, and thus Rule 3 of [RFC6724] causes other configured addresses (if available) to be used instead.

* We note that lowering the default values for the "Valid Lifetime" helps reduce the amount of time a host may maintain stale information and the amount of time an advertising router would need to advertise stale prefixes to deprecate them, while reducing the default "Preferred Lifetime" would reduce the amount of time it takes for a host to prefer other working prefixes (see Section 12 of [RFC4861]). However, while the values suggested in this section are an improvement over the default values specified in [RFC4861], they represent a trade-off among a number of factors, including responsiveness, possible impact on the battery life of connected devices [RFC7772], etc. Thus, they may or may not provide sufficient mitigation to the problem discussed in this document.

4. Future Work

Improvement in Customer Edge Routers [RFC7084] such that they can

signal the network about stale prefixes and deprecate them accordingly can help mitigate the problem discussed in this document

for the "home network" scenario. Such work is currently being pursued in [I-D.ietf-v6ops-cpe-slaac-renum].

Improvements in the SLAAC protocol [RFC4862] and other algorithms such as "Default Address Selection for IPv6" [RFC6724] would help improve network robustness. Such work is currently being pursued in [I-D.ietf-6man-slaac-renum].

The aforementioned work is considered out of the scope of this present document, which only focuses on documenting the problem and discussing operational mitigations.

5. IANA Considerations

This document has no actions for IANA.

6. Security Considerations

This document discusses a problem that may arise in scenarios where flash-renumbering events occur, and proposes workarounds to mitigate the aforementioned problems. This document does not introduce any new security issues, and thus the same security considerations as for [RFC4861] and [RFC4862] apply.

7. Acknowledgments

The authors would like to thank (in alphabetical order) Brian Carpenter, Alissa Cooper, Roman Danyliw, Owen DeLong, Martin Duke, Guillermo Gont, Philip Homburg, Sheng Jiang, Benjamin Kaduk, Erik Kline, Murray Kucherawy, Warren Kumari, Ted Lemon, Juergen Schoenwaelder, Eric Vyncke, Klaas Wierenga, Robert Wilton, and Dale Worley, for providing valuable comments on earlier versions of this document.

The authors would like to thank (in alphabetical order) Mikael Abrahamsson, Luis Balbinot, Brian Carpenter, Tassos Chatzithomaoglou, Uesley Correa, Owen DeLong, Gert Doering, Martin Duke, Fernando Frediani, Steinar Haug, Nick Hilliard, Philip Homburg, Lee Howard, Christian Huitema, Ted Lemon, Albert Manfredi, Jordi Palet Martinez,

Michael Richardson, Mark Smith, Tarko Tikan, and Ole Troan, for providing valuable comments on a previous document on which this document is based.

Fernando would like to thank Alejandro D'Egidio and Sander Steffann for a discussion of these issues. Fernando would also like to thank Brian Carpenter who, over the years, has answered many questions and provided valuable comments that have benefited his protocol-related work.

The problem discussed in this document has been previously documented by Jen Linkova in [I-D.linkova-6man-default-addr-selection-update], and also in [RIPE-690]. Section 1 borrows text from [I-D.linkova-6man-default-addr-selection-update], authored by Jen Linkova.

8. References

8.1. Normative References

[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>.

[RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012, <https://www.rfc-editor.org/info/rfc6724>.

[RFC8028] Baker, F. and B. Carpenter, "First-Hop Router Selection by Hosts in a Multi-Prefix Network", RFC 8028, DOI 10.17487/RFC8028, November 2016, <https://www.rfc-editor.org/info/rfc8028>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters,

"Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

8.2. Informative References

[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/>.

[GERMAN-DP]
BFDI, "Einfuhrung von IPv6 Hinweise fur Provider im Privatkundengeschaft und Herstellere", Entschliessung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Lander am 7./8. November 2012 in Frankfurt (Oder), November 2012, <http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/84DSK_EinfuehrungIPv6.pdf?__blob=publicationFile>.

[I-D.ietf-6man-slaac-renum]
Gont, F., Zorz, J., and R. Patterson, "Improving the Robustness of Stateless Address Autoconfiguration (SLAAC) to Flash Renumbering Events", draft-ietf-6man-slaac-renum-01 (work in progress), August 2020.

[I-D.ietf-v6ops-cpe-slaac-renum]
Gont, F., Zorz, J., Patterson, R., and B. Volz, "Improving the Reaction of Customer Edge Routers to Renumbering Events", draft-ietf-v6ops-cpe-slaac-renum-05 (work in progress), September 2020.

[I-D.linkova-6man-default-addr-selection-update]
Linkova, J., "Default Address Selection and Subnet Renumbering", draft-linkova-6man-default-addr-selection-

update-00 (work in progress), March 2017.

[Linux-update]
Gont, F., "[net-next] ipv6: Honor all IPv6 PIO Valid Lifetime values", Post to the netdev mailing-list http://vger.kernel.org/vger-lists.html, April 2020, <https://patchwork.ozlabs.org/project/netdev/patch/20200419122457.GA971@archlinux-current.localdomain/>.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <https://www.rfc-editor.org/info/rfc4941>.

[RFC7084] Singh, H., Beebee, W., Donley, C., and B. Stark, "Basic Requirements for IPv6 Customer Edge Routers", RFC 7084, DOI 10.17487/RFC7084, November 2013, <https://www.rfc-editor.org/info/rfc7084>.

[RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", RFC 7721, DOI 10.17487/RFC7721, March 2016, <https://www.rfc-editor.org/info/rfc7721>.

[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>.

[RIPE-690]
Zorz, J., Zorz, S., Drazumeric, P., Townsley, M., Alston, J., Doering, G., Palet, J., Linkova, J., Balbinot, L., Meynell, K., and L. Howard, "Best Current Operational Practice for Operators: IPv6 prefix assignment for end-users - persistent vs non-persistent, and what size to choose", RIPE 690, October 2017, <https://www.ripe.net/publications/docs/ripe-690>.

[UK-NOF] Palet, J., "IPv6 Deployment Survey (Residential/Household Services) How IPv6 is being deployed?", UK NOF 39, January 2018, <https://indico.uknof.org.uk/event/41/contributions/542/attachments/712/866/bcop-ipv6-prefix-v9.pdf>.

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