Internet Engineering Task Force (IETF)
Request for Comments: 8978
Category: Informational
ISSN: 2070-1721

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

March 2021

Reaction of IPv6 Stateless Address Autoconfiguration (SLAAC) to Flash-Renumbering Events

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), hosts 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 document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8978.

Table of Contents

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: old prefixes are deprecated (and eventually invalidated) via reduced prefix lifetimes and new prefixes are introduced (with longer lifetimes) at the same time. However, there are several scenarios that may lead to the so-called "flash-renumbering" events, where a 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 (and eventually invalidate) the currently employed prefix (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, hosts 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 router

may obtain (via DHCPv6-PD) a different prefix from the one previously leased and therefore advertise (via SLAAC) a new sub-prefix on the LAN side. Hosts will typically configure addresses for the new sub-prefix but will also normally retain and may actively employ the addresses configured for the previously advertised sub-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. For example, this is particularly true for implementations in which DHCPv6-PD is implemented in a different software module than SLAAC.

* A switch-port that a host is connected to is moved to another subnet (VLAN) as a result of manual switch-port reconfiguration or 802.1x reauthentication. There has been evidence that some 802.1x supplicants do not reset network settings after successful 802.1x authentication. If a host fails 802.1x authentication for some reason, it may be placed in a "quarantine" VLAN; if successfully authenticated later on, the host may end up having IPv6 addresses from both the old ("quarantine") and new VLANs.

* During a planned network renumbering event, a router is configured to send an RA including a Prefix Information Option (PIO) for the "old" prefix with the Preferred Lifetime set to zero and the Valid Lifetime set to a small value, as well as a PIO for the new prefix with default lifetimes. However, due to unsolicited RAs being sent to a multicast destination address, and multicast being rather unreliable on busy Wi-Fi networks, the RA might not be received by local hosts.

* An 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 withdraw it gracefully. If such a push results in changing the prefix configured on a particular subnet, hosts attached to that subnet might not get notified about the prefix change, and their addresses from the "old" prefix might not be deprecated (and eventually invalidated) in a timely manner. A related scenario is an incorrect network renumbering event, 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 (and eventually invalidate) the stale prefixes, hosts may continue to employ the previously configured addresses, which will typically result in packets being filtered or blackholed either on the CE router or within the ISP network.

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 communication 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 (and eventually invalidate) 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/multi-prefix 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 (and eventually invalidate) 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 events do not occur and that, when they do occur, 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 problem discussed in this document is 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 scenarios, the problem discussed in this document would be avoided if DHCPv6-PD leased "stable" prefixes. However, a recent survey [UK-NOF] indicates that 37% of the responding ISPs employ dynamic IPv6 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 get 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 reduce the effectiveness of "temporary addresses" [RFC8981].

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

* There might be scalability and performance drawbacks of either a disaggregated distributed routing topology or a centralized topology, which are often required to provide stable prefixes, i.e., distributing more-specific routes or summarizing routes at centralized locations.

For a number of reasons (such as the ones stated above), IPv6 deployments might employ dynamic prefixes (even at the expense of the issues discussed in this document), and there might be scenarios in which the dynamics of a network are such that the network exhibits the behavior 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 PIO Lifetime 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 PIOs, 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 when 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, since:

* In scenarios where SLAAC routers explicitly signal the renumbering event, hosts will typically deprecate, but not invalidate, the stale addresses, since item "e)" of Section 5.5.3 of [RFC4862] specifies that an unauthenticated RA may never reduce the valid lifetime of an address to less than two hours. Communication with the new "users" of the stale prefix will not be possible, since the stale prefix will still be considered "on-link" by the local hosts.

* In the absence of explicit signaling from SLAAC routers, SLAAC hosts will typically fail to recover from stale configuration information in a timely manner, since hosts would need to rely on the last Preferred Lifetime and Valid Lifetime advertised for the stale prefix, for the corresponding addresses to become deprecated and subsequently invalidated. Please see Section 2.2 of this document for a discussion of the default PIO lifetime values.

2.4. Lack of Explicit Signaling about Stale Information

Whenever prefix information has changed, a SLAAC router should advertise not only the new information but also the stale information with appropriate lifetime values (both the Preferred Lifetime and the 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 certain scenarios, such as when a CE router crashes and reboots, the CE router may have no knowledge about the previously advertised prefixes and thus might be unable to advertise them with appropriate lifetimes (in order to deprecate and eventually invalidate them).

In any case, 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 [RENUM-RXN]. 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 means of 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 lifetimes 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 period of time that is longer than the one they have been leased for 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, as noted in Section 2.1, 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 associated timers will be refreshed/reset, but in the presence of network faults (such as the one discussed in this document), the associated timers go off and trigger some fault recovering action (e.g., deprecate and eventually 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 those where the operator has complete control of prefix allocation and where

> hosts on the network may spend long periods of time 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 lifetimes of the corresponding prefixes do not extend past the DHCPv6-PD lease time [RENUM-CPE].

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 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; therefore, Rule 3 of [RFC6724] causes other configured addresses (if available) to be used instead.

* Reducing the Valid Lifetime of PIOs 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 invalidate them. Reducing the Preferred Lifetime of PIOs helps reduce the amount of time it takes for a host to prefer other working prefixes (see Section 12 of [RFC4861]). However, we note that 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

Improvements in Customer Edge routers [RFC7084], such that they can signal hosts about stale prefixes to deprecate (and eventually invalidate) them accordingly, can help mitigate the problem discussed in this document for the "home network" scenario. Such work is currently being pursued in [RENUM-CPE].

Improvements in the SLAAC protocol [RFC4862] and some IPv6-related algorithms, such as "Default Address Selection for Internet Protocol Version 6 (IPv6)" [RFC6724], would help improve network robustness. Such work is currently being pursued in [RENUM-RXN].

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 IANA actions.

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 problem. This document does not introduce any new security issues; therefore, the same security considerations as for [RFC4861] and [RFC4862] apply.

7. References

7.1. 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>.

7.2. Informative References

[DEFAULT-ADDR] Linkova, J., "Default Address Selection and Subnet Renumbering", Work in Progress, Internet-Draft, draft-linkova-6man-default-addr-selection-update-00, 30 March 2017, <https://tools.ietf.org/html/draft-linkova-6man-default-addr-selection-update-00>.

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

[GERMAN-DP] BFDI, "Einführung von IPv6: Hinweise für Provider im Privatkundengeschäft und Hersteller" [Introduction of IPv6: Notes for providers in the consumer market and manufacturers], Entschliessung der 84. Konferenz der Datenschutzbeauftragten des Bundes und der Lander [Resolution of the 84th Conference of the Federal and State Commissioners for Data Protection], November 2012, <http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/84DSK_EinfuehrungIPv6.pdf?__blob=publicationFile>.

[Linux-update] Gont, F., "Subject: [net-next] ipv6: Honor all IPv6 PIO Valid Lifetime values", message to the netdev mailing list, 19 April 2020, <https://patchwork.ozlabs.org/project/netdev/patch/20200419122457.GA971@archlinux-current.localdomain/>.

[RENUM-CPE] Gont, F., Zorz, J., Patterson, R., and B. Volz, "Improving the Reaction of Customer Edge Routers to IPv6 Renumbering Events", Work in Progress, Internet-Draft, draft-ietf-v6ops-cpe-slaac-renum-07, 16 February 2021, <https://tools.ietf.org/html/draft-ietf-v6ops-cpe-slaac-renum-07>.

[RENUM-RXN] Gont, F., Zorz, J., and R. Patterson, "Improving the Robustness of Stateless Address Autoconfiguration (SLAAC) to Flash Renumbering Events", Work in Progress, Internet-Draft, draft-ietf-6man-slaac-renum-02, 19 January 2021, <https://tools.ietf.org/html/draft-ietf-6man-slaac-renum-02>.

[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>.

[RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <https://www.rfc-editor.org/info/rfc8981>.

[RIPE-690] Žorž, J., Steffann, S., Dražumerič, P., Townsley, M., Alston, A., Doering, G., Palet Martinez, 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 Martinez, J., "IPv6 Deployment Survey and BCOP", UK NOF 39, January 2018, <https://indico.uknof.org.uk/event/41/contributions/542/>.

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, Éric Vyncke, Klaas Wierenga, Robert Wilton, and Dale Worley for providing valuable comments on earlier draft 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 [DEFAULT-ADDR] and also in [RIPE-690]. Section 1 borrows text from [DEFAULT-ADDR], authored by Jen Linkova.

Authors' Addresses

Fernando Gont
SI6 Networks
Segurola y Habana 4310, 7mo Piso
Villa Devoto
Ciudad Autónoma de Buenos Aires
Argentina

Email: fgont@si6networks.com
URI: https://www.si6networks.com

Jan Žorž

6connect, Inc.

Email: jan@6connect.com

Richard Patterson
Sky UK

Email: richard.patterson@sky.uk