Abstract

In scenarios where network configuration information related to IPv6 prefixes becomes invalid without any explicit signaling of that condition (such as when a CPE crashes and reboots without knowledge of the previously-employed prefixes), nodes on the local network will continue using stale prefixes for an unacceptably long period of time, thus resulting in connectivity problems. This document analyzes these problem scenarios, and discusses operational workarounds to improve network robustness.

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 January 7, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents
1. Introduction

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 a number of scenarios that may lead to the so-called "flash-renumbering", where the prefix being employed on a network suddenly becomes invalid and replaced by a new prefix. In some of these scenarios, the local router producing the network renumbering may be able and try to deprecate the currently-employed prefixes (thus 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 signaling of that condition, nodes on the local network will 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 deployment scenario for IPv6 in home networks is that in which a CPE 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 CPE router via Stateless Address Autoconfiguration (SLAAC) [RFC4862]. In scenarios where the CPE router crashes and reboots, the CPE may be leased (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 normally configure an address for the new prefix, but will normally retain and actively employ the previously-configured addresses, since their associated Preferred Lifetime and Valid Lifetime allow them to do so.

- 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. In particular there has been evidence that some 802.1x supplicants do not reset network settings after successful 802.1x authentication. So if a host had failed 802.1x authentication for some reason, was placed in a "quarantine" VLAN and then got successfully authenticated later on, it might end up having IPv6 addresses from both old ("quarantine") and new VLANs.

- During the planned network renumbering a router is configured to send an RA with the Preferred Lifetime for the "old" PIO set to zero and the new PIO having non-zero preferred lifetime. However, due to unsolicited RAs being sent as all-hosts multicast and multicast being rather unreliable on busy wifi network, the RA is not received by a host (or set of hosts).

- Automated device config management system performs periodical config push to network devices. If such a push results in changing /64 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 are not deprecated. The related case is incorrectly performed renumbering when a network administrator is renumbering a network by simply removing the "old" prefix from the configuration and configuring a new prefix instead.
Lacking any explicit signaling to "obsolete" the previously-configured addresses (for the now invalid/stale prefix), hosts may continue employing the previously-configured addresses which will typically result in packets being blackholed -- whether because of egress-filtering by the CPE or ISP, or because responses to such packets will be discarded or routed elsewhere.

The default values for the "Valid Lifetime" and "Preferred Lifetime" of Prefix Information Options (PIOs), as specified in [RFC4861], are:

- Valid Lifetime (AdvValidLifetime): 2592000 seconds (30 days)
- Preferred Lifetime (AdvPreferredLifetime): 604800 seconds (7 days)

This means that in the aforementioned scenarios, the stale addresses would be retained for unacceptably long period of time, thus leading to interoperability problems, instead of nodes transitioning to the newly-advertised prefix(es) in a timelier manner.

Some devices have implemented mechanisms to address this problem, such as sending RAs to invalidate the apparently stale prefixes when the device receives any packets employing a source address from a prefix not being advertised for address configuration [FRITZ]. However, this may introduce other interoperability problems, particularly in multihomed/multiprefix scenarios. This is 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 timelier manner. Clearly, it would be desirable that these flash-renumbering scenarios do not occur, and that, when they do occur, that hosts are explicitly notified of their occurrence. However, for robustness reasons it is also 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 notify hosts about such condition.

Section 2 analysis this problem in more detail. Section 3 proposes workarounds to improve network robustness.

2. Analysis of the Problem

As noted in Section 1, the problem discussed in this document exacerbated by a number of different parameters and behaviours. Each of the following sections analyze each of them in detail.
2.1. Default Timer Values in IPv6 Stateless Address Autoconfiguration (SLAAC)

Many protocols, from different layers, normally employ timers. The general logic is as follows:

- A timer is set with a value such that, under normal conditions, the timer does *not* go off.
- Whenever a fault condition arises, the timer goes off, and the protocol can perform fault recovery.

One common example for the use of timers is when implementing reliability mechanisms where a packet is transmitted, and unless a response is received, a retransmission timer will go off to trigger retransmission of the original packet.

For obvious reasons, the whole point of using timers is that in problematic scenarios, they will go off, and trigger some recovery action.

However, IPv6 SLAAC employs, for PIOs, these default values:

- Preferred Lifetime (AdvPreferredLifetime): 604800 seconds (7 days)
- Valid Lifetime (AdvValidLifetime): 2592000 seconds (30 days)

Under normal network conditions, these timers will be reset/refreshed to the default values. However, under problematic circumstances such as where the corresponding network information has become stale without any explicit signal from the network (as described in Section 1), it will take a host 7 days (one week) to un-prefer the corresponding addresses, and 30 days (one month) to eventually remove any addresses configured for the stale prefix.

2.2. 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 RA may never reduce the "RemainingLifetime" more than to 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 the use of a stale prefix to be employed 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 "un-prefer" 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".

### 2.3. 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), such that there is explicit signaling to SLAAC hosts to remove the stale information (including configured addresses and routes).

However, as discussed in Section 2.2, PIOs with small Valid Lifetimes will not lower the Valid Lifetime to any value shorter than two hours (as per [RFC4862]). Therefore, even if a SLAAC router were to explicitly signal the network about the stale configuration information via RAs, such signaling would be mostly ignored.

### 2.4. 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.

### 2.5. Use of Dynamic Prefixes

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 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 the privacy concerns associated with stable prefixes.

The authors of this document understand that, 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 try to preclude how operators may run their networks, this document aims at improving network robustness in the deployed Internet.

3. Possible workarounds

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

Section 3.2 specifies the interaction between DHCPv6-PD and SLAAC, such that devices such as CPEs may be in a better position to convey current network information to hosts on the LAN-side. For obvious reasons (legacy CPEs, etc.), this improved behaviour cannot be relied upon for mitigating the problem described in Section 1. However, it does contribute to more robust IPv6 networks.

Finally, Section 2.5 analyzes the trade-offs of employing stable vs. dynamic network prefixes.

3.1. SLAAC Parameter Tweaking

An operator may wish to override some SLAAC parameters such that, under normal circumstances (including some packet loss), the timers will be refreshed/reset, but in the presence of network faults (such as network configuration information becoming stale without explicit signaling), the timers go off and trigger some fault recovering
action (such as un-preferring the corresponding addresses and subsequently removing them).

The following router configuration variables (corresponding to the "lifetime" parameters in PIOs) could be overridden as follows:

- AdvValidLifetime: 1.5 * AdvDefaultLifetime
- AdvPreferredLifetime: AdvDefaultLifetime

NOTE: A CPE router advertising a sub-prefix of a prefixed 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.

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, neither the "Preferred Lifetime" or the "Valid Lifetime" of a PIO should never be larger than the "Router Lifetime" (AdvDefaultLifetime) of Router Advertisement messages.

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

* Reducing the Valid Lifetime and Preferred Lifetimes of PIOs limits the amount of time hosts may use stale prefixes, and also limits the amount of time that a stale prefix needs to be advertised with a lifetime of "0" on the local network (see Section 12 of [RFC4861]).

3.2. Improved CPE behavior

This section specifies and clarifies requirements for CPE routers (particularly when they advertise prefixes learned via DHCPv6-PD) that can help mitigate the problem discussed in Section 1. This would obviously make robustness dependent on the CPE (on which the user or ISP may have no control), as opposed to the host itself.

The updated behaviour is as follows:
CPE routers MUST signal stale configuration information as specified in Section 3.2.1.

CPE routers MUST implement the DHCPv6-PD/SLAAC interface specified in Section 3.2.2.

CPE routers SHOULD NOT automatically send DHCPv6-PD RELEASE messages upon reboot events.

3.2.1. Signaling Stale Configuration Information

In order to phase-out stale configuration information:

- A CPE router sending RAs that advertise dynamically-learned prefixes (e.g. via DHCPv6-PD) on an interface MUST record, on stable storage, the list of prefixes being advertised on each network segment.

- Upon changes to the advertised prefixes, and after bootstrapping, the CPE router advertising prefix information via SLAAC should proceed as follows:

  * Any prefixes that were previously advertised via SLAAC, but that are not currently intended for address configuration, MUST be advertised with a PIO option with the "A" bit set to 1 and the "Valid Lifetime" and a "Preferred Lifetime" set to 0.

  * Any prefixes that were previously advertised via SLAAC as "on-link", but that are not currently not considered "on-link", MUST be advertised with a PIO option with the "L" bit set to 1 and the "Valid Lifetime" and a "Preferred Lifetime" set to 0.

  * If both of the previous conditions are met (a prefix was previously advertised with both the "A" and "L" bits set, but is currently *not* intended for address configuration and is *not* considered on-link), the prefix MUST be advertised with a PIO option with both the "A" and "L" bits set to 1 and the "Valid Lifetime" and a "Preferred Lifetime" set to 0. That is, the advertisements of the previous two steps can be coalesced into a single one with both the "A" and "L" bits set.

  * The aforementioned advertisement SHOULD be performed for at least the "Valid Lifetime" previously employed for such prefix.

The aforementioned improved behaviour assumes compliance with the following existing requirements from other specifications, which we reference here for clarity:
RFC7084 specifies (requirement LE-13, in Section 4.3) that when the delegated prefix changes (i.e., the current prefix is replaced with a new prefix without any overlapping time period), "the IPv6 CE router MUST immediately advertise the old prefix with a Preferred Lifetime of zero and a Valid Lifetime of either a) zero or b) the lower of the current Valid Lifetime and two hours (which must be decremented in real time) in a Router Advertisement message as described in Section 5.5.3, (e) of [RFC4862]."

### 3.2.2. Interaction Between DHCPv6-PD and SLAAC

The "Preferred Lifetime" and "Valid Lifetime" of PIOs corresponding to prefixes learned via DHCPv6-PD MUST NOT span past the lease time of the DHCPv6-PD prefixes. This means that the advertised "Preferred Lifetime" and "Valid Lifetime" MUST be dynamically adjusted such that the advertised lifetimes never span past the lease time of the prefixes delegated via DHCPv6-PD.

This is in line with these existing requirements from other specifications, which we reference here for clarity:

- RFC8415 specifies, in Section 6.3, that "if the delegated prefix or a prefix derived from it is advertised for stateless address autoconfiguration [RFC4862], the advertised preferred and valid lifetimes MUST NOT exceed the corresponding remaining lifetimes of the delegated prefix."

**Rationale:**

* The lifetime values employed for the "Preferred Lifetime" (AdvPreferredLifetime) and "Valid Lifetime" (AdvValidLifetime) should never be larger than the remaining lease time for the corresponding prefix (as learned via DHCPv6-PD).

* The lifetime values advertised for prefixes corresponding to a prefix leased via DHCPv6-PD should be dynamically updated (rather than static values), since otherwise the advertised lifetimes would eventually span past the DHCPv6-PD lease time.

## 4. Summary of Operational Mitigations

### 4.1. Networks

- Employ shorter values for the Preferred Lifetime and Valid Lifetime in PIOs

- Employ stable network prefixes where possible and desirable

---

4.2. CPE routers

- Implement the interface between DHCPv6-PD and SLAAC as appropriate
- Refrain from unnecessarily issuing DHCPv6-PD RELEASE commands upon reboots
- Record DHCPv6-PD leases on stable storage (when possible) and phase-out stale information when needed

5. Future Work

This document proposes operational mitigations to the discussed problem. Improvements in the SLAAC protocol and algorithms "Default Address Selection for IPv6" may achieve improved network robustness and should be considered by relevant Working Groups (see e.g. [I-D.gont-6man-slaac-renum]). Such work is considered out of the scope of this present document, which focuses on documenting the problem and proposing operational mitigations.

6. IANA Considerations

This document has no actions for IANA.

7. Security Considerations

This document discusses a problem that may arise in scenarios where dynamic IPv6 prefixes are employed, and proposes workarounds to mitigate the aforementioned problems. The security and privacy implications of IPv6 addresses are discussed in [RFC7721].

8. Acknowledgments

The authors would like to thank (in alphabetical order) Mikael Abrahamsson, Luis Balbinot, Brian Carpenter, Gert Doering, Nick Hilliard, Philip Homburg, Lee Howard, Christian Huitema, Albert Manfredi, Jordi Palet Martinez, Richard Patterson, Michael Richardson, Mark Smith, Tarko Tikan, and Ole Troan, for providing valuable comments on [I-D.gont-6man-slaac-renum], on which this document is based. Earlier versions of this document.

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 has 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.

9. References

9.1. Normative References


9.2. Informative References


[GERMAN-DP]

[I-D.gont-6man-slaac-renum]

[I-D.linkova-6man-default-addr-selection-update]


[RIPE-690]
<https://www.ripe.net/publications/docs/ripe-690>.

Authors’ Addresses

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

Phone: +54 11 4650 8472
Email: fgont@si6networks.com
URI: https://www.si6networks.com

Jan Zorz
Frankovo n. 165
Skofja Loka
Slovenia

Email: jan@go6.si

Richard Patterson
Sky UK

Email: richard.patterson@sky.uk