IPv6 Maintenance (6man) Working Group
Internet-Draft
Updates: 4861, 4862 (if approved)
Intended status: Standards Track
Expires: November 19, 2020

F. Gont
SI6 Networks
J. Zorz
Go6 Institute
R. Patterson
Sky UK

May 18, 2020

Improving the Robustness of Stateless Address Autoconfiguration (SLAAC) to Flash Renumbering Events

draft-gont-6man-slaac-renum-08

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.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction 3
2. Terminology 3
3. SLAAC reaction to Flash-renumbering Events 4
3.1. Renumbering without Explicit Signaling 4
3.2. Renumbering with Explicit Signaling 5
4. Improvements to Stateless Address Autoconfiguration (SLAAC) . 6
4.1. More Appropriate Lifetime Values 7
4.1.1. Router Configuration Variables 7
4.1.2. Processing of PIO Lifetimes at Hosts 8
4.2. Honor Small PIO Valid Lifetimes 9
4.3. Interface Initialization 10
4.4. Conveying Information in Router Advertisement (RA) Messages 10
4.5. Recovery from Stale Configuration Information without Explicit Signaling 11
5. IANA Considerations 15
6. Implementation Status 15
6.1. More Appropriate Lifetime Values 16
6.1.1. Router Configuration Variables 16
6.1.2. Processing of PIO Lifetimes at Hosts 16
6.2. Honor Small PIO Valid Lifetimes 17
6.2.1. NetworkManager 17
6.3. Conveying Information in Router Advertisement (RA) Messages 17
6.4. Recovery from Stale Configuration Information without Explicit Signaling 17
6.4.1. dhcpcd(8) 17
6.5. Other mitigations implemented in products 17
7. Security Considerations 18
8. Acknowledgments 18
9. References 19
9.1. Normative References 19
9.2. Informative References 20
Appendix A. Analysis of Some Suggested Workarounds 21
A.1. On a Possible Reaction to ICMPv6 Error Messages 21
A.2. On a Possible Improvement to Source Address Selection . . 22
Authors' Addresses 24

1. Introduction

IPv6 network renumbering is expected to take place in a planned manner, with old/stale prefixes being phased-out via reduced prefix lifetimes while new prefixes (with normal lifetimes) are introduced. However, there are a number of scenarios that may lead to the so-called "flash-renumbering" events, where the prefix being employed on a network suddenly becomes invalid and replaced by a new prefix [I-D.ietf-v6ops-slaac-renum]. In such scenarios, hosts on the local network will continue using stale prefixes for an unacceptably long period of time, thus resulting in connectivity problems. [I-D.ietf-v6ops-slaac-renum] discusses this problem in detail.

In some scenarios, the local router producing the network renumbering event may try to deprecate the currently-employed prefixes (thus explicitly signaling the network about the renumbering event), whereas in other scenarios it may be unaware about the renumbering event and thus unable signal hosts about it.

From the perspective of a Stateless Address Autoconfiguration (SLAAC) host, there are two different (but related) problems to be solved:

- Avoiding the use of stale addresses for new communication instances

- Performing "garbage collection" for the stale prefixes (and related network configuration information)

Clearly, if a host has both working and stale addresses, it is paramount that it employs working addresses for new communication instances. Additionally, a host should also perform garbage collection for the stale prefixes/addresses, since they not only tie system resources, but also prevent communication with the new "owners" of the stale prefixes.

2. Terminology

The term "globally reachable" is used in this document as defined in [RFC8190].

The term "Global Unicast Address" (or its acronym "GUA") is used throughout this document to refer to "globally reachable" [RFC8190] addresses. That is, when used throughout this document, GUAs do NOT include Unique Local Addresses (ULAs) [RFC4193]. Similarly, the term "Global Unicast prefix" (or "GUA prefix") is employed throughout this document to refer to network prefixes that specify GUAs, and does NOT include the ULA prefix (FC00::/7) [RFC4193].

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

As noted in Section 1, in some scenarios the router triggering the renumbering event may be able to explicitly signal the network about this event, while in other scenarios the renumbered hosts may need to infer a renumbering event is taking place. 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 the stale prefixes), stale prefixes will remain preferred and valid according to the Preferred Lifetime and Valid Lifetime values (respectively) of the last received PIO. IPv6 SLAAC employs the following default values for PIOs:

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

- o 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, for any practical purposes, employing such long default values is the equivalent of not using any timers at all, since taking 7 days or 30 days (respectively) to recover from a network problem is simply unacceptable.

Use of more appropriate timers in Router Advertisement messages can help limit the amount of time that hosts will maintain stale configuration information. Additionally, hosts are normally in a position to infer that a prefix has become stale -- for example, if a given router ceases to advertise an existing prefix and at the same time starts to advertise a new prefix.

Section 4.1.1 recommends the use of more appropriate lifetimes for PIOs, while Section 4.1.2 proposes to cap the accepted Valid Lifetime and Preferred Lifetime values at hosts, such that more appropriate values are employed even in the presence of legacy routers.

Section 4.5 specifies a local policy that SLAAC hosts can implement to heuristically infer that network configuration information has changed, such that stale configuration information can be phased out.

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 in a timelier manner.

In the absence of Router Advertisements (RAs) that include PIOs that would reduce the Valid Lifetime and Preferred Lifetime of a prefix, hosts would normally employ the lifetime values from PIO options of the last received RA messages. Since the network could be partitioned for an arbitrarily long period of time, a router would need to try to deprecate a prefix for the amount of time employed for the "Preferred Lifetime", and try to invalidate the prefix for the amount of time employed for the "Valid Lifetime" (see Section 12 of [RFC4861]).

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

Thus, use of more appropriate default lifetimes for PIOs, as proposed in Section 4.1.1, would reduce the amount of time a stale prefix would need to be announced as such by a router in order to make sure that it is deprecated/invalidated.

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 would prevent communication with the new

"owners" of the stale prefix, and thus is highly undesirable. On the other hand, the Preferred Lifetime of an address *can* be reduced to any value to avoid the use of a stale prefix for new communications.

Section 4.2 updates [RFC4862] such that this restriction in removed, and hosts react to the advertised "Valid Lifetime" (even if it is smaller than 2 hours).

Finally, Section 4.3 recommends that routers disseminate network configuration information when a network interface is initialized, such that possibly 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 aforementioned updates are mostly orthogonal, and mitigate different aspects of SLAAC that prevent a timely reaction to flash renumbering events.

o Reduce the default Valid Lifetime and Preferred Lifetime of PIOs (Section 4.1.1):
  This helps limit the amount of time a host will employ stale information, and also limits the amount of time a router needs to try to obsolete stale information.

o Cap the received Valid Lifetime and Preferred Lifetime of PIOs (Section 4.1.2):
  This helps limit the amount of time a host will employ stale information, even in the presence of legacy ([RFC4861]) routers.

o Honor PIOs with small Valid Lifetimes (Section 4.2):
  This allows routers to invalidate stale prefixes, since otherwise [RFC4861] prevents hosts from honoring PIOs with a Valid Lifetime smaller than two hours.

o Recommend routers to retransmit configuration information upon interface initialization/reinitialization (Section 4.3):
  This helps spread the new information in a timelier manner, and also deprecate stale information via host-side heuristics (see Section 4.5).

o 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, and also allows hosts to better infer that information missing in RA messages has become stale (see Section 4.5).

- o Infer stale network configuration information from received RAs (Section 4.5):
  This allows hosts to deprecate stale network configuration information, even in the absence of explicit signaling.

4.1. More Appropriate Lifetime Values

4.1.1. Router Configuration Variables

The default value for the "lifetime" parameters in PIOs is updated as follows:

AdvPreferredLifetime: max(AdvDefaultLifetime, 3 * MaxRtrAdvInterval)

AdvValidLifetime: 48 * max(AdvDefaultLifetime, 3 * MaxRtrAdvInterval)

where:

AdvPreferredLifetime:
Value to be included in the "Preferred Lifetime" field of the PIO.

AdvValidLifetime:
Value to be included in the "Valid Lifetime" field of the PIO.

AdvDefaultLifetime:
Value of the "Router Lifetime" field of the Router Advertisement message that will carry the PIO.

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

NOTE:
[RFC4861] specifies AdvDefaultLifetime as 3 * MaxRtrAdvInterval (which defaults to 600 seconds). This means that, when employing default values for MaxRtrAdvInterval, the Router Lifetime would be set to AdvPreferredLifetime (1800 seconds). Thus, when employing the default values, or when manually setting AdvDefaultLifetime to a value smaller than 1800 seconds, AdvPreferredLifetime and AdvValidLifetime would be set to 1800 seconds (30 minutes) and 86400 seconds (1 day), respectively.

RATIONALE:

* The default values for PIO lifetimes should be such that, under normal circumstances (including some packet loss), the associated timers are refreshed/reset, but in the presence of network failures (such as network configuration information becoming stale), some fault recovering action (such as deprecating the corresponding addresses and subsequently removing them) is triggered.

* In the context of [RFC8028], where it is clear that the use of addresses configured for a given prefix is tied to the next-hop router that advertised the prefix, the "Preferred Lifetime" of a PIO should never be larger than the "Router Lifetime" of Router Advertisement messages. Some leeway should be provided for the "Valid Lifetime" to cope with transient network problems. As a result, this document updates [RFC4861] such that the default Valid Lifetime (AdvValidLifetime) and the default Preferred Lifetime (AdvPreferredLifetime) of PIOs are specified as a function of the default "Router Lifetime" (AdvDefaultLifetime) of Router Advertisement messages. In the absence of RAs that refresh information, addresses configured for advertised prefixes become deprecated in a timelier manner, and thus Rule 3 of [RFC6724] will cause other configured addresses (if available) to be preferred.

* The expression above computes the maximum between AdvDefaultLifetime and "3 * MaxRtrAdvInterval" (the default value for AdvDefaultLifetime, as per [RFC4861]) to cope with the case where an operator might simply want to disable one local router for maintenance, without disabling the use of the corresponding prefixes on the local network (e.g., on a multi-router network). [RFC4862] implementations would otherwise deprecate the corresponding prefixes. Similarly, [RFC8028] would likely behave in the same way.

4.1.2. Processing of PIO Lifetimes at Hosts

Hosts SHOULD cap the "Preferred Lifetime" and "Valid Lifetime" of PIOs as follows:

o IF (Router Lifetime != 0) AND (Preferred Lifetime != 0xffffffff) AND (Valid Lifetime != 0xffffffff), then:

```
Preferred Lifetime= MIN(Preferred Lifetime, "Router Lifetime")

Valid Lifetime= MIN(Valid Lifetime, 48 * "Router Lifetime")
```

RATIONALE:

* Capping the lifetimes in PIOs as suggested will not eliminate the problem discussed in this document, but will certainly reduce the amount of time it takes for hosts to converge to updated network configuration information, even when the SLAAC router advertises PIOs with the default values specified in [RFC4861] (as opposed to the new default values specified in Section 4.1.1) or when the corresponding router ceases to send RAs.

* A Router Lifetime of 0 has the special meaning of "this router is not to be employed as a default router", and may be employed only to advertise prefixes via SLAAC (but not as a default router). As a result, PIO lifetimes are not capped when Router Lifetime == 0.

* A PIO lifetime of 0xffffffff has the special meaning of "infinity", which means that these prefixes (and their corresponding addresses) should never time out. As a result, PIO lifetimes are not capped when the PIO Valid Lifetime == 0xffffffff or the PIO Preferred Lifetime == 0xffffffff.

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.

NOTE: "Processing" the Valid Lifetime and Preferred Lifetime includes capping the received values as specified in Section 4.1.2 of this document.

RATIONALE:

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

* Attacks aiming at disabling an advertised prefix via a Valid Lifetime of 0 are not really more harmful than other attacks that can be performed via forged RA messages, such as those aiming at completely disabling a next-hop router via an RA that advertises a Router Lifetime of 0, or performing a Denial of Service (DoS) attack by advertising illegitimate prefixes via

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

4.3. Interface Initialization

When an interface is initialized, it is paramount that network configuration information is spread 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 paramount that new configuration information propagates in a timelier manner to all hosts.

NOTE:
[I-D.ietf-v6ops-cpe-slaac-renum] specifies recommendations for CPE routers to deprecate 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. To the best of the authors' knowledge, SLAAC routers always send all options in the smallest possible number of packets, so this section simply more clearly aligns the existing specifications with existing implementations.

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 causes 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.

RATIONALE:

* Sending information in the smallest possible number of packets was somewhat already implied from the original text in [RFC4861], and in this respect the proposed update just adds clarity. Including all options when sending RAs both leads to simpler code (as opposed to dealing with special cases where specific information is intentionally omitted), and also helps hosts infer network configuration changes in a timelier manner. Note that while [RFC4861] allowed some RAs to omit some options, the authors of this document know of no implementation of such behavior. Therefore, the proposed change simply reflects existing practice.

4.5. Recovery from Stale Configuration Information without Explicit Signaling

This section specifies an algorithm that allows hosts to infer when a previously-advertised prefix has become stale, such that previously-configured addresses are "phased-out" and the host can transition to the newly-advertised prefixes in a timelier manner. Most of the value of this algorithm is in being able to mitigate the problem discussed in [I-D.ietf-v6ops-slaac-renum] at hosts themselves, without relying on updates of local routers.

Hosts can normally infer when network configuration information has changed. For example, if a SLAAC router (as identified by its link-local address) has ceased to advertise a previously-advertised prefix and has also started to advertise new prefixes via PIOs, this should be considered an indication that network configuration information has changed. Implementation of this kind of heuristic allows a timelier reaction to network configuration changes even in scenarios where there is no explicit signaling from the network -- thus improving robustness.

The basic premise behind these algorithms is that, when a router advertises new prefixes for address configuration (i.e., PIOs with the "A" bit set), but fails to advertise the previously-advertised prefixes, this is an indication that previously-advertised prefixes have become stale. Therefore, if this was the only router advertising the prefix, configured addresses for the stale prefixes should be deprecated (such that they are not employed for new communication instances), and they should eventually be removed (if this condition persists). If other routers were advertising the same prefix, the prefix should simply be dis-associated with the router that ceased to advertise it, and the fate of the corresponding addresses should depend on the routers that continue advertising the prefix.

The algorithm specified in this section updates the state of configured addresses upon receipt of an RA that, while carrying PIOs, fails to advertise a previously-advertised prefix. Namely, such an RA reduces the "Preferred Lifetime" of the corresponding addresses, to cause such addresses to be quickly deprecated, while accommodating the case where the advertising router might be sending SLAAC options in multiple separate packets. Similarly, the "Valid Lifetime" of such addresses is reduced, such that the addresses are invalidated in a timelier manner, while still providing some leeway for the local router to re-advertise the corresponding prefix.

Local information maintained for each prefix advertised by each router is augmented with one variable named "LTA_LA" (Lifetime Avoidance_Last Advertised), that records the last time a given prefix has been advertised by a given router.

NOTE:

While not strictly required, we note that existing implementations may already record the last time a prefix has been advertised by a given router as a possible implementation approach to be able to compute the remaining lifetime of an address.

Hosts are already expected to keep track of which router has advertised which prefix in order to be able to properly select the

first-hop router in multiple-prefix networks [RFC8028] [RFC8504]. Throughout this specification, each router is identified by its link-local address.

This algorithm employs two configuration variables:

LTA_DEPRECATE:
A time value (in seconds) to set the "Preferred Lifetime" of addresses corresponding to a given prefix, when a received RA suggests that such addresses might have become stale. It defaults to LTA_DEPRECATE_DEFAULT, which this document specifies as 5 seconds. This value is a rough estimate of the maximum amount of time to send a "batch" of RA messages that advertise the complete set of SLAAC information. [NOTE: We believe this variable could be set to a value even smaller than this]

LTA_INVALID:
A time value (in seconds) to set the "Valid Lifetime" of addresses corresponding to a given prefix, and the "Valid Lifetime" of a prefix (for on-link determination), when a received RA suggests that such addresses and prefix might have become stale. It defaults to LTA_INVALID_DEFAULT, which this document specifies as 1800 seconds (which corresponds to the largest possible value for MaxRtrAdvInterval [RFC4861]). [NOTE: We believe that it would be possible to set this variable to smaller values, but just opted for the most conservative setting].

After normal processing of Router Advertisement messages, Router Advertisements that contain at least one PIO MUST be processed as follows:

- For each prefix prefix advertised by a PIO with the "A" flag set, proceed as follows:

  * LTA_LA = current_time()

- If the RA advertises at least one Global Unicast Prefix then, for each Global Unicast prefix that had been previously advertised by this router but that is not advertised by a PIO in the received RA, proceed as follows:

  * IF current_time() >= (LTA_LA + LTA_DEPRECATE) && Preferred Lifetime > LTA_DEPRECATE && Valid Lifetime > LTA_INVALID, then:

    + IF this is the only router advertising this prefix, set the "Preferred Lifetime" and the "Valid Lifetime" of IPv6 addresses corresponding to this prefix to LTA_DEPRECATE and

LTA_INVALID, respectively. Additionally, set the "Valid Lifetime" associated with this prefix (for on-link determination) to LTA_INVALID.

+ ELSE IF this prefix has been advertised my multiple neighboring routers, simply disassociate this prefix with this particular router. This will cause the fate of this prefix to depend on the other routers.

- If the RA advertises at least one Unique Local [RFC4193] prefix then, for each Unique Local prefix that had been previously advertised by this router but that is not advertised by a PIO in the received RA, proceed as follows:

  * IF current_time() >= (LTA_LA + LTA_DEPRECATE) && Preferred Lifetime > LTA_DEPRECATE && Valid Lifetime > LTA_INVALID, then:

    + IF this is the only router advertising this prefix, set the "Preferred Lifetime" and the "Valid Lifetime" of IPv6 addresses corresponding to this prefix to LTA_DEPRECATE and LTA_INVALID, respectively. Additionally, set the "Valid Lifetime" associated with this prefix (for on-link determination) to LTA_INVALID.

    + ELSE IF this prefix has been advertised my multiple neighboring routers, simply disassociate this prefix with this particular router. This will cause the fate of this prefix to depend on the other routers.

NOTES:

- current_time() is a monotonically-increasing counter that is incremented once per second, and is employed to measure time.

- The processing of RAs that do not contain any PIOs with the "A" bit set remains unaffected.

- If the only prefix that has so far been advertised on the local network is the prefix that has become stale, and there is no other prefix being advertised, the traditional processing is unaffected (the mechanism discussed in this document will *never* be triggered because received RAs will not contain other PIOs with the "A" bit set). The rationale here is that it is better to have some address, than no address at all.

- Only RAs that advertise Global Unicast prefixes may deprecate Global Unicast Addresses (GUAs), while only RAs that advertise Unique Local prefixes may deprecate Unique Local Addresses (ULAs).

- The specified modification takes the conservative approach of setting the "Preferred Lifetime" to LTA_DEPRECATE to allow for SLAAC information to be conveyed in multiple RA messages (that can be sent during a window of LTA_DEPRECATE seconds), and setting the "Valid Lifetime" to LTA_INVALID (to accommodate for possible packet loss, and transient problems). Once the addresses for this prefix have been removed, associated routes incorporated by the original RA messages SHOULD also be removed.

- In cases where this scenario has been triggered by a CPE router crashing and rebooting, it would take hosts LTA_DEPRECATE seconds to mark the corresponding addresses as "not preferred", and LTA_INVALID to completely remove such addresses from the system -- that is, 5 seconds and 600 seconds, respectively.

- The pseudo-code above checks that "Preferred Lifetime > LTA_DEPRECATE && Valid Lifetime > LTA_INVALID" to prevent subsequent RA packets that do not contain a specific PIO PIO from resetting the corresponding Preferred Lifetime and Valid Lifetime to LTA_DEPRECATE and LTA_INVALID (respectively) once they have already been reduced by this algorithm. Otherwise, the Preferred Lifetime and Valid Lifetime might never get decremented to 0 as expected.

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 [I-D.ietf-v6ops-slaac-renum] 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, bu is already a deviation from the current standards.

6.1.2. Processing of PIO Lifetimes at Hosts

6.1.2.1. NetworkManager

NetworkManager [NetworkManager], user-space SLAAC implementation employed by some Linux-based operating systems (such as Fedora or Ubuntu), caps the lifetimes of the received PIOs as recommended in this document.

6.1.2.2. slaacd(8)

slaacd(8) [slaacd], a user-space SLAAC implementation employed by OpenBSD, caps the lifetimes of the received PIOs as recommended in this document.

6.1.2.3. systemd-networkd

systemd-networkd [systemd], a user-space SLAAC implementation employed by some Linux-based operating systems, caps the lifetimes of the received PIOs as recommended in this document.

6.2. Honor Small PIO Valid Lifetimes

6.2.1. 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:

- o Rather than recording prefixes on stable storage (as recommended in [I-D.ietf-v6ops-cpe-slaac-renum]), 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.

- o 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

When it comes to the algorithm in Section 4.5, an attacker could impersonate the legitimate router and send an RA that does not advertise legitimate prefixes being employed in the local network. This cause the corresponding addresses to become deprecated. However, the addresses would not become invalid since normal unsolicited RA messages would refresh the "Preferred Lifetime" and "Valid Lifetime" of such addresses.

However, an attacker that can impersonate a router could more easily deprecate addresses by advertising the legitimate prefixes with the "Preferred Lifetime" set to 0, or perform a plethora of other possible of Denial of Service attacks based on forged RA messages. Therefore, when attacks based on forged RA packets are a concern, technologies such as RA-Guard [RFC6105] [RFC7113] should be deployed.

Capping the "Valid Lifetime" and "Preferred Lifetime" at hosts may help limit the duration of the effects of non-sustained attacks that employ forged RAs with PIOs, since hosts would now recover in a timelier manner.

8. Acknowledgments

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

The algorithm specified in Section 4.5 is the result of mailing-list discussions over previous versions of this document with Philip Homburg.

Fernando would like to thank Alejandro D'Egidio and Sander Steffann for a discussion of these issues, which led to the publication of [I-D.ietf-v6ops-slaac-renum], 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.

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].

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>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/info/rfc4193>.

[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>.

[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>.

[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>.

[RFC8190] Bonica, R., Cotton, M., Haberman, B., and L. Vegoda, "Updates to the Special-Purpose IP Address Registries", BCP 153, RFC 8190, DOI 10.17487/RFC8190, June 2017, <https://www.rfc-editor.org/info/rfc8190>.

[RFC8504] Chown, T., Loughney, J., and T. Winters, "IPv6 Node Requirements", BCP 220, RFC 8504, DOI 10.17487/RFC8504, January 2019, <https://www.rfc-editor.org/info/rfc8504>.

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, <http://blog.si6networks.com/2016/02/quiz-weird-ipv6-traffic-on-local-network.html>.

[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-02 (work in progress), May 2020.

[I-D.ietf-v6ops-slaac-renum]
Gont, F., Zorz, J., and R. Patterson, "Reaction of Stateless Address Autoconfiguration (SLAAC) to Flash-Renumbering Events", draft-ietf-v6ops-slaac-renum-02 (work in progress), May 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.

[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>.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, DOI 10.17487/RFC2827, May 2000, <https://www.rfc-editor.org/info/rfc2827>.

[RFC5927] Gont, F., "ICMP Attacks against TCP", RFC 5927, DOI 10.17487/RFC5927, July 2010, <https://www.rfc-editor.org/info/rfc5927>.

[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>.

[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>.

[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>.

[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>.

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

[systemd] systemd, "systemd web site", <https://systemd.io/>.

Appendix A. Analysis of Some Suggested Workarounds

[This section is to be removed before publication of this document as an RFC].

During the discussion of this document, some alternative workarounds were suggested on the 6man mailing-list. The following subsections analyze these suggested workarounds, in the hopes of avoiding rehashing the same discussions.

A.1. On a Possible Reaction to ICMPv6 Error Messages

It has been suggested that if configured addresses become stale, a CPE enforcing ingress/egress filtering (BCP38) ([RFC2827]) could send ICMPv6 Type 1 (Destination Unreachable) Code 5 (Source address failed

ingress/egress policy) error messages to the sending node, and that, upon receipt of such error messages, the sending node could perform heuristics that might help to mitigate the problem discussed in this document.

The aforementioned proposal has a number of drawbacks and limitations:

- It assumes that the CPE routers enforce ingress/egress filtering [RFC2827]. While this is desirable behaviour, it cannot be relied upon.

- It assumes that if the CPE enforces ingress/egress filtering, the CPE will signal the packet drops to the sending node with ICMPv6 Type 1 (Destination Unreachable) Code 5 (Source address failed ingress/egress policy) error messages. While this may be desirable, [RFC2827] does not suggest signaling the packet drops with ICMPv6 error messages, let alone the use of specific error messages (such as Type 1 Code 5) as suggested.

- ICMPv6 Type 1 Code 5 could be interpreted as the employed address being stale, but also as a selected route being inappropriate/ suboptimal. If the later, deprecating addresses or invalidating addresses upon receipt of these error messages would be inappropriate.

- Reacting to these error messages would create a new attack vector that could be exploited from remote networks. This is of particular concern since ICMP-based attacks do not even require that the Source Address of the attack packets be spoofed [RFC5927].

A.2. On a Possible Improvement to Source Address Selection

[RFC6724] specifies source address selection (SAS) for IPv6. Conceptually, it sorts the candidate set of source addresses for a given destination, based on a number of pair-wise comparison rules that must be successively applied until there is a "winning" address.

An implementation might improve source address selection, and prefer the most-recently advertised information. In order to incorporate the "freshness" of information in source address selection, an implementation would be updated as follows:

- The node is assumed to maintain a timer/counter that is updated at least once per second. For example, the time(2) function from unix-like systems could be employed for this purpose.

o The local information associated with each prefix advertised via RAs on the local network is augmented with a "LastAdvertised" timestamp value. Whenever an RA with a PIO with the "A" bit set for such prefix is received, the "LastAdvertised" timestamp is updated with the current value of the timer/counter.

o [RFC6724] is updated such that this rule is incorporated:

Rule 7.5: Prefer fresh information If one of the two source addresses corresponds to a prefix that has been more recently advertised, say LastAdvertised(SA) > LastAdvertised(SA), then prefer that address (SA in our case).

A clear benefit of this approach is that a host will normally prefer "fresh" addresses over possibly stale addresses.

However, there are a number of drawbacks associated with this approach:

o In scenarios where multiple prefixes are being advertised on the same LAN segment, the new SAS rule is *guaranteed* to result in non-deterministic behaviour, with hosts frequently changing the default source address. This is certainly not desirable from a troubleshooting perspective.

o Since the rule must be incorporated before "Rule 8: Use longest matching prefix" from [RFC6724], it may lead to suboptimal paths.

o This new rule may help to improve the selection of a source address, but it does not help with the housekeeping (garbage collection) of configured information:

* If the stale prefix is re-used in another network, nodes employing stale addresses and routes for this prefix will be unable to communicate with the new "owner" of the prefix, since the stale prefix will most likely be considered "on-link".

* Given that the currently recommended default value for the "Valid Lifetime" of PIOs is 2592000 seconds (30 days), it would take too long for hosts to remove the configured addresses and routes for the stale prefix. While the proposed update in Section 4.1 of this document would mitigate this problem, the lifetimes advertised by the local SLAAC router are not under the control of hosts.

As a result, updating IPv6 source address selection does not relieve nodes from improving their SLAAC implementations as specified in Section 4, if at all desirable. On the other hand, the algorithm

specified in Section 4.5 would result in Rule 3 of [RFC6724] employing fresh addresses, without leading to non-deterministic behaviour.

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
Go6 Institute
Frankovo naselje 165
Skofja Loka 4220
Slovenia

Email: jan@go6.si
URI: https://www.go6.si

Richard Patterson
Sky UK

Email: richard.patterson@sky.uk