Abstract

A very common IPv6 deployment scenario is that in which a CPE employs DHCPv6 Prefix Delegation to obtain an IPv6 prefix, and at least one prefix from within the leased prefix is advertised on a local network via SLAAC. In scenarios where e.g. the CPE crashes and reboots, nodes on the local network continue using outdated prefixes which result in connectivity problems. This document analyzes this problem scenario, and proposes workarounds.
1. Introduction

Probably 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 the ISP, and a prefix belonging to the leased prefix is advertised on the LAN-side of the CPE via Stateless Address Autoconfiguration (SLAAC) [RFC4862].

In scenarios such as that in which the CPE router crashes and reboots, the CPE may be leased (via DHCPv6-PD) a different prefix than the one previously leased and will therefore advertise such new prefix on the LAN side via SLAAC. 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. The default values, as specified in [RFC4861] are:

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

Lacking any explicit signaling to "obsolete" the previously-configured addresses (for the now invalid/outdated prefix), hosts may continue employing the previously-configured addresses which will typically result in packets being blackholed -- whether because of...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.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. Possible workarounds

The following subsections discuss possible workarounds for the aforementioned problem.

3.1. Improvement to SLAAC

This section specifies an improvement to SLAAC that improves robustness and that can mitigate the aforementioned problem.

The goal of this modification is that, when a router that was previously advertising a prefix for address configuration (PIO with the "A" bit set) is found to advertise other prefixes but not the previously-advertised prefixes, addresses configured for the "old" prefixes are marked as "not preferred" (i.e., their "Preferred Lifetime" is set to 0), thus allowing for a more timely-reaction to the problem described in Section 1.

Local information maintained for each prefix advertised by each router is augmented with one boolean flag named "deprecate" that defaults to "false". Note: 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] [I-D.ietf-6man-rfc6434-bis].

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

- The "deprecate" flag for each prefix advertised in the current Router Advertisement should be set to "false".
- For each prefix that had been previously advertised by this router but that does not have a corresponding PIO with the "A" flag set in the received RA, proceed as follows:
  - IF the "deprecate" flag is "true", then:
+ IF there is any address configured for this prefix with a "Preferred Lifetime" larger than 0, set its "Preferred Lifetime" to 0, and the "deprecate flag" of this prefix to "false".

+ ELSE (all addresses for this prefix have a "Preferred Lifetime" of 0), set the "Valid Lifetime" of any addresses configured for this prefix to 0, and the "deprecate" flag to "false". This will cause removal of all addresses for this prefix. Additionally, if the corresponding prefix had been advertised as on-link ("L"=1) by this router, remove any routes to this prefix associated with the network interface card on which the RA packet was received.

* ELSE (the "deprecate" flag is "false"):  

  + Set the "deprecate" flag of the corresponding prefix to "true".

Appendix B illustrates the packet exchange and operation of the algorithm for a typical scenario. Appendix A provides a flowchart for this algorithm.

NOTES:

- The aforementioned processing assumes that while network configuration information might be split into multiple RAs, PIOs will be spread among *at most* two RAs. This assumption avoids the use of any timers for this specific purpose.

- If the only prefix that has so far been advertised on the local network is the prefix that has become outdated, and there is no new prefix being advertised, the traditional processing is unaffected (the mechanism discussed in this document will *never* be triggered because no packets with PIOs with the "A" flag will be received). The logic here is that it’s better to have some address, than no address at all.

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

- The specified modification takes the conservative approach of first setting the "Preferred Lifetime" to 0 (such that addresses become non-preferred), and subsequently setting the "Valid Lifetime" to 0 (such as the addresses are completely removed). Once the addresses for this prefix have been removed, routes to this prefix associated with the network interface on which the RA packets were received are also removed.
3.2. Improved CPE behavior

The scenario discussed in Section 1 could be improved on the CPE-side as follows:

- A CPE MUST record, on stable storage, the list of prefixes being advertised on each LAN segment.
- Upon renewed information about the list of prefixes to be advertised on the LAN-side (whether as a result of DHCPv6-PD or manual configuration), then:
  
  * 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.

This improves the situation for hosts that do not implement the modification specified in Section 3.1 but would obviously make robustness dependent on the CPE, as opposed to the host itself.

3.3. Stable prefixes

The problem discussed in this document would be avoided if DHCPv6-PD would lease "stable" prefixes.

There are a number of possible issues associated with this option:

- 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.

Applicable legislation may require the ISP to deliver dynamic IPv6 prefixes *by default* (see e.g. [GERMAN-DP]).

4. Security Considerations

This document discusses a problem that may arise in scenarios where dynamic IPv6 prefixes are employed, and proposes workarounds that enable such usage while avoiding interoperability problems. The security and privacy implications of IPv6 addresses are discussed in [RFC7721].

An attacker that could impersonate a router could forge multiple RA packets that contain PIOs of prefixes that are currently not advertised on the local network, to trigger the mechanism specified in this document to cause addresses currently configured for the legitimate prefixes to be removed. However, an attacker that can impersonate a router could more easily achieve the same goal by advertising the legitimate prefixes with both the "Preferred Lifetime" and "Valid Lifetime" set to 0.

Attacks based on forged RA packets can be mitigated with technologies such as RA-Guard [RFC6105] [RFC7113].

5. Acknowledgments

The authors would like to thank (in alphabetical order) [TBD] for providing valuable comments on earlier versions of this document.

Fernando would like to thank Alejandro D‘Egidio, and Sander Steffan for a discussion of these issues.

The problem discussed in this document, and the recommendation to employ stable prefixes, have been previously documented in [RIPE-690].

6. References

6.1. Normative References


6.2. Informative References


Appendix A. Flowchart for Host Processing of RAs

Conceptually, the mechanism operates as follows:


Appendix B. Sample Timeline for Host Processing of RAs

The following example illustrates a sample packet exchange that illustrates the algorithm specified in Section 3.1:
Router
RA, PIO={2001:DB8:1::/64, L=1, A=1}
------------------------------------>
[Host configures addr
for this prefix]

RA, PIO={2001:DB8:1::/64, L=1, A=1}
------------------------------------>
[Normal proc. of RA]

[Router reboots]
RA, PIO={2001:DB8:2::/64, L=1, A=1}
------------------------------------>
deprecate=TRUE

RA, PIO={2001:DB8:2::/64, L=1, A=1}
------------------------------------>
Pref. Lftime=0
deprecate=FALSE

RA, PIO={2001:DB8:2::/64, L=1, A=1}
------------------------------------>
deprecate=TRUE

RA, PIO={2001:DB8:2::/64, L=1, A=1}
------------------------------------>
Valid Lftime=0
deprecate=FALSE
(Addr. Removed!)

Authors’ Addresses

Fernando Gont
SI6 Networks / UTN-FRH
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