Improving the Reaction of IPv6 SLAAC to Flash Renumbering Events

(draft-ietf-6man-slaac-renum-00)

Fernando Gont
Jan Zorz
Richard Patterson

6man Working Group
IETF 108. July 28, 2020

Mitigations

- Employ more appropriate PIO lifetimes
  - Use more appropriate lifetimes on the router/sending side
  - Cap received values on the host/receiving side
- Spread information in a timelier manner
  - Honor PIOs with small valid lifetimes
  - Propagate information when an interface becomes an “advertising interface”
- Deprecate/Invalidate stale information
  - Trigger detection of stale information
  - Deprecate/invalidate stale information if appropriate
- We propose improvements in all these areas

More appropriate Lifetimes (router side)

- **Current default PIO lifetimes**
  - Preferred Lifetime: **1 day** (!)
  - Valid Lifetime: **1 month** (!)
- **Proposal:**
  - Specify these values as a function of the Router Lifetime
- **Example**:
  - Default PIO Preferred Lifetime: Router Lifetime
  - Default PIO Valid Lifetime: N * Router Lifetime

More appropriate Lifetimes (host side)

- **Proposal: cap received Lifetimes at hosts**:
  - Preferred Lifetime: Router Lifetime
  - Valid Lifetime: N * Router Lifetime

  Only when:

  - Router Lifetime != 0 && Preferred Lifetime != 0xffffffff &&

    Valid Lifetime != 0xffffffff

  Since these values represent special cases:

  - Router Lifetime == 0 → don’t use this router as the default router
  - {Preferred, Valid} Lifetime == 0xffffffff → Infinity

Honor small PIO Valid Lifetimes

- Section 5.5.3, item e) of RFC4861 **prevents** reducing PIO Valid Lifetime < 2 hours
  - Considered an attack vector?
- **Attackers have a zillion other vectors!**
  - Flood hosts with bogus RIOs or PIOs
  - Spoof RA with Lifetime == 0 (disable router)
  - etc., etc., etc.
- You do first hop security, or you don’t
- **Proposal: honor all PIO Valid Lifetime** values
  - If router is aware of situation, it can signal it and avoid the problem

Interface Initialization

- Replace this section (Section 6.2.4) from 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.
  ```

- i.e., it is key that information propagates in a timely manner
- Jen also suggests that we should also recommend this when information changes on the router-side

Deprecating/invalidating stale info

- Section 4.5 contains an algorithm to detect, deprecate and invalidate stale information
- There have been objections to this algorithm
- Current proposed algorithm works as follows:
  - **Trigger**: An RA that advertises PIOs but misses a previous PIO
  - **Deprecation/Invalidation**: Upon the previous event, reduce the Preferred and Valid Lifetime (where Valid Lifetime >> Preferred Lifetime)
  - PIO will be quickly unpreferred, and will be eventually invalidated – or otherwise refreshed if it’s still valid

Deprecating/invalidating stale info (II)

- If RA contains GUA PIOs, but a previous GUA PIO is missing:
  - Reduce PL= ~5 seconds, VL: 100's seconds **for missing GUA prefix**
- If RA contains ULA PIOs, but a previous ULA PIO is missing:
  - Reduce PL= ~5 seconds, VL: 100's seconds **for missing ULA prefix**
- If multiple routers announced the prefix → just disassociate the prefix with the corresponding router

Other things that have been suggested

- Philip:
  - Have the host “sample” the server and see if it splits RA info
  - If it doesn’t, we can react more aggressively. If it does, wait extra time or poll server.
- Others:
  - Rather than passively deprecate information, perform some form of active testing
  - e.g. send a probe using the current prefix, or poll the router with an RS

A possible alternative

- No matter what we do, it seems to boil down to:
  - A condition that triggers detection of stale information
  - Possible Deprecation/Invalidation
- One possible approach:
  - An RA that misses a PIO triggers an unicast RS
    - possibly after a few seconds to accommodate split RAs
  - An unicast RS is sent to the router
    - and possibly retransmitted, if necessary
  - If previous information is not refreshed, it is deprecated and eventually invalidated