

Improving the Reaction of IPv6 SLAAC to Flash Renumbering Events

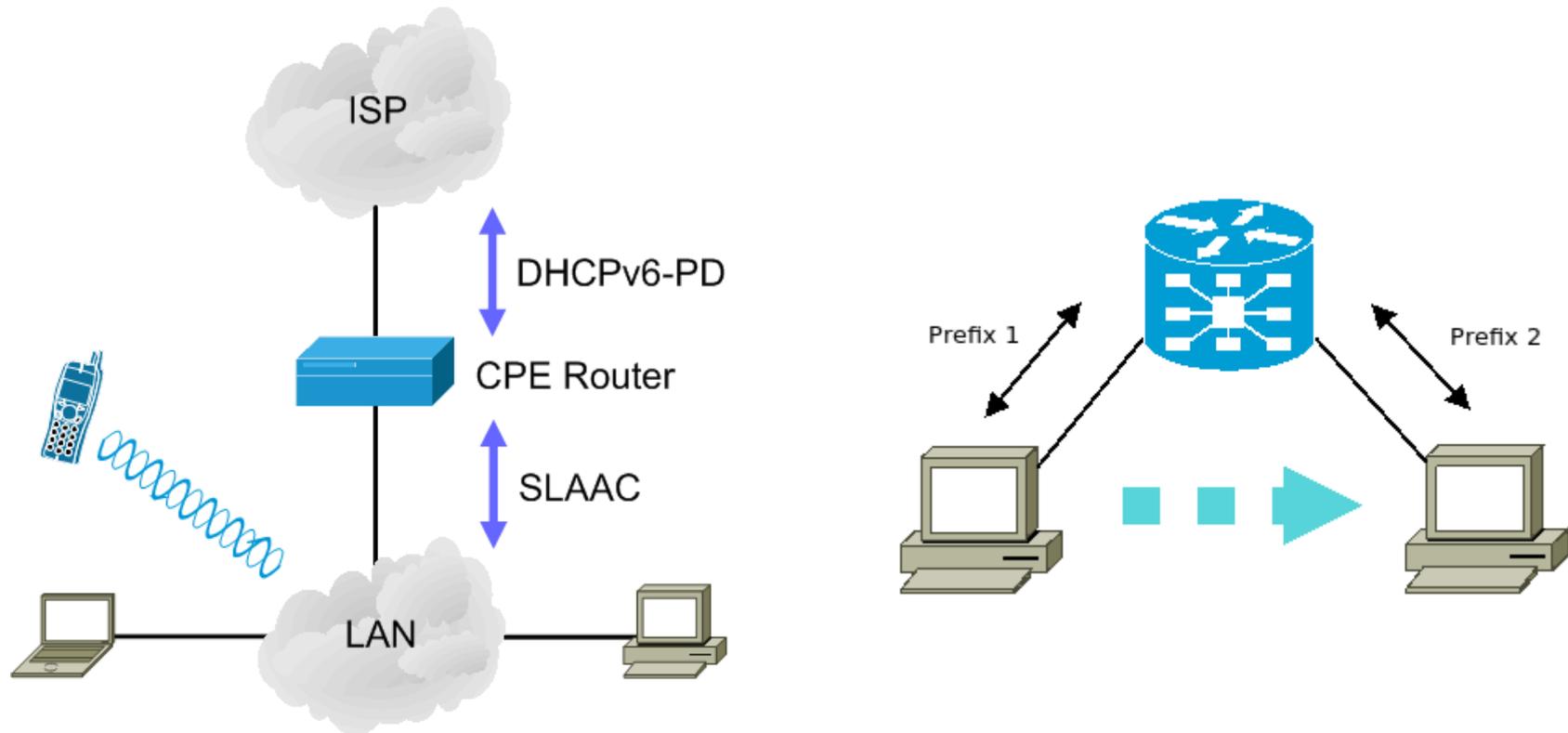
(draft-gont-6man-slaac-renum-05)

**Fernando Gont
Jan Zorz
Richard Patterson**

IETF 6man Interim Meeting
March 31, 2020

Problem statement

- Network configuration changes from one moment to another
- Routers often are unaware of the stale information
- Hosts end up with stale information for long period of time



Mitigations

- Signaling
 - Router continues operation
 - aware of stale information vs.
 - unaware of stale information
 - Router disappears
- Implementation – what needs to be updated?
 - Host side vs.
 - Router side
- We pursue improvements in all areas
- But it is key that hosts can recover from common scenarios even with “legacy” routers → **host smarts are good!**

More appropriate Lifetimes

- **Current PIO lifetimes**
 - Preferred Lifetime: **1 day (!)**
 - Valid Lifetime: **1 month (!)**
- **Proposal: Reduce default Lifetimes at routers:**
 - Default PIO Preferred Lifetime: Router Lifetime
 - Default PIO Valid Lifetime: $N * \text{Router Lifetime}$
- **Proposal: cap received Lifetimes at hosts:**
 - Preferred Lifetime: Router Lifetime
 - Valid Lifetime: $N * \text{Router Lifetime}$
- **Even if router disappears, hosts recover in a timelier manner**

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
 - RA-Guard, ND Inspection, etc.
- **Proposal: honor all PIO Valid Lifetime values**
 - If router is aware of situation, it can signal it and avoid the problem

Infer stale information

- Router ceases advertising a previous prefix, and starts advertising a new one → **stale information!**
 - Two possible algorithms (implementation details)
- If RA contains GUA PIOs, but not the previous GUA PIO:
 - Reduce PL= ~5 seconds, VL: 100's seconds **for missing GUA prefix**
- If RA contains ULA PIOs, but not previous ULA PIO:
 - Reduce PL= ~5 seconds, VL: 100's seconds **for missing ULA prefix**
- If multiple routers announced prefix → just disassociate with router
- **Addresses only deprecated if there's other prefix of same type**

Implementations

- Smaller default PIO Lifetimes (router side):
 - rad(8), radvd(8), rtadvd(8)
- Cap PIO Lifetimes (host side)
 - slaacd(8), NetworkManager(8), systemd-networkd(8)
- Honor small PIO Lifetimes:
 - slaacd(8), NetworkManager(8)
- Infer stale prefixes:
 - NetworkManager(8) (in the works)
 - systemd-networkd(8) (in the works)
 - dhcpcd(8) (partial implementation)

Moving forward

- Adopt as 6man wg item?