IPv6 SLAAC & Renumbering Events

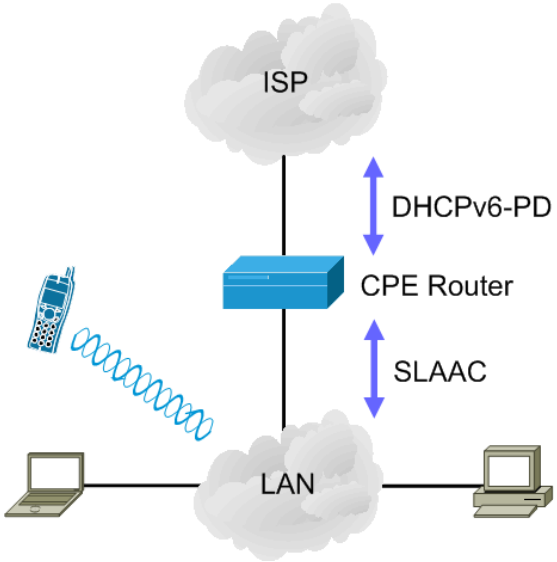
Fernando Gont

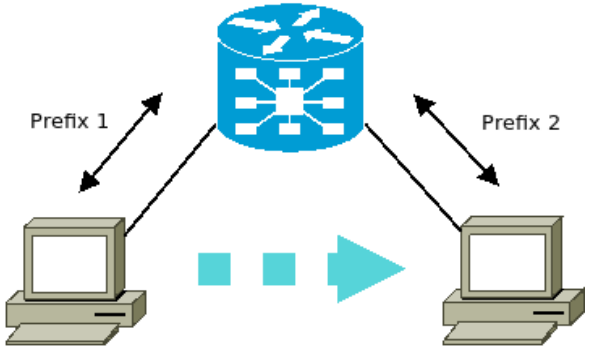
SI6 NETWORKS

RIPE 80, IPv6 WG. May 14th, 2020

IPv6 SLAAC & Renumbering Events

- Renumbering may make local prefixes change from one moment to another
- Nodes are often unaware that information has become stale
- Hosts end up with stale information for long period of time





Mitigations

- Operational
  - Do not do dynamic prefixes (RIPE-690)
  - Discussed in draft-ietf-v6ops-slaac-renum
- Protocol-based
  - Make SLAAC more robust to renumbering events
  - Discussed in draft-gont-6man-slaac-renum
- CPE-based
  - Improvements in CPEs that help mitigate this issue in a very common scenario
  - Discussed in draft-ietf-v6ops-cpe-slaac-renum

Protocol-based Mitigations

- Different signaling scenarios
  - 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: **7 days** (!)
  - Valid Lifetime: **1 month** (!)
- Proposal: Reduce default Lifetimes at routers
  - Default PIO Preferred Lifetime: Router Lifetime
  - Default PIO Valid Lifetime: N * Router Lifetime
- Proposal: cap received Lifetimes at hosts
  - Preferred Lifetime: min(Preferred Lifetime, Router Lifetime)
  - Valid Lifetime: min(Valid Lifetime, N * Router Lifetime)
- Even if router disappears, hosts recover in a timelier manner

Honor Small PIO Valid Lifetimes

- RFC4861 (Sec. 5.5.3, item e) **prevents** reducing Valid Lifetime < 2 hs
  - Considered an attack vector
- 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

- Goal: infer from received RAs if any information has become stale
- Router ceases advertising a previous prefix, and starts advertising a new one → **stale information!**
- If RA contains PIOs, but not the previous PIO:
  - Reduce PL= ~5 seconds, VL: 100's seconds **for missing prefix**
- If multiple routers announced prefix → just disassociate with router
- **Addresses only deprecated if there's another prefix**

CPE-based Mitigations

- DHCPv6-PD - SLAAC interface
  - PIO lifetimes must not span past DHCPv6-PD lifetimes
- Reduced LAN-side option lifetimes
  - PIO Preferred Lifetime = Router Lifetime
  - PIO Valid Lifetime = 2 * Router Lifetime
- Signal stale configuration information
  - Record announced prefixes on stable storage
  - Deprecate them e.g. upon bootstrap
- CPEs should not do DHCPv6-RELEASE upon reboot events

Questions?

Thanks!

Fernando Gont

fgont@si6networks.com

IPv6 Hackers mailing-list

http://www.si6networks.com/community/

www.si6networks.com