Privacy Extensions for Stateless Address Autoconfiguration in IPv6
(draft-ietf-6man-rfc4941bis-00)
F. Gont, S. Krishnan, T. Narten, R. Draves

IETF 102
Montreal, Canada. July 14-20, 2018
Issues with RFC4941

• Prevents use of only temporary addresses
• Recommends reusing the same IID for multiple prefixes
• Reuses the same IID as host moves from one network to another
• Limits non-deprecated addresses to one per prefix
• Temporary addresses disabled by default
• Miscellaneous issues
Generation of non-stable IIDs

• We propose two alternative algorithms:
  - Random IIDs
  - A la RFC7217:
    \[
    F(\text{Prefix}, \text{MAC\_Address}, \text{Network\_ID}, \text{Time}, \text{DAD\_Counter}, \text{secret\_key})
    \]
Q: Algorithms

- There has been some discussion regarding what to do with the possible algorithms:
  - Improve the "a la rfc7217" algorithm -- done!
  - Recommend the simple randomization one?
  - Remove the "a la rfc7217" algorithm altogether?
  - Keep both algorithms as options, but do not recommend any specific one?
Q: Requirements for temporary IIDs

- Requirements were spelled out in draft-gont-6man-non-stable-iids and referenced in rfc4941bis
- There seems to be agreement to incorporate the requirements into rfc4941bis
  - Either in the body or in an appendix
Q: "On by default"

- rfc4941bis makes temporary addresses "on by default"
  - Probably out of question in the light of RFC7528
  - Is already the case for MS Windows systems

- Proposals to incorporate some text on how this might affect security devices
  - that assume many addresses per device is an attack
Q: When to change IID$s$

- IID$s$ change upon network (re-)attachment and other privacy-sensitive events
- Question was raised if/how we could prevent on-link glitches from triggering IID generation