Privacy Extensions for Stateless Address Autoconfiguration in IPv6

(draft-ietf-6man-rfc4941bis)

F. Gont, S. Krishnan, T. Narten, R. Draves

IETF 104
Prague, Czech Republic. March 23-29, 2019

Generation of non-stable IIDs

- We propose two alternative algorithms:
  - Random IIDs
  - A la RFC7217:

    F(Prefix, MAC_Address, Network_ID, Time, DAD_Counter, secret_key)

Q: Algorithms

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

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
- Thoughts?

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
- Thoughts?

Q: When to change IIDs

- IIDs 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
- Reference DNA? Something else?