Temporary IPv6 Interface IID
draft-gont-6man-non-stable-iids-01

F. Gont, C. Huitema, G. Gont, M. Garcia Corbo

IETF 98

March 30, 2017

Revisiting RFC 4941?

- We learned a few things in the last 10 years
  - Is it OK to use the same IID for different prefixes?
  - Is it OK to only reset addresses based on fixed addresses?
  - Is it OK to regenerate IIDs periodically?
  - Do we actually need to also configure stable addresses?
- New requirements, e.g., resulting from address randomization

Stating the new requirements

- RFC 4941 had a fairly simple problem statement:
  - correlate seemingly unrelated activity using <the IID>.
- Our draft has a much more developed statement
  - Address structure – random bits
  - No correlation between different prefixes
  - Address lifetime – correlation with privacy events (next slide)

Privacy events and Address Changes

- Some events are important for privacy
  - Moving to a new network
  - MAC Address Randomization
  - User level event, e.g., “private mode” or “clear history”
- Need to avoid before/after correlation by IP addresses
  - Temporary addresses should change on such events

Proposed address generation

- Hash based mechanism, Random ID = F(
  - Prefix,
  - MAC_Address,
  - Network_ID,
  - Time,
  - DAD_Counter,
  - secret_key)
- Or, random number from appropriate generator (RFC 4086)

Next steps

- Prepare revision
  - Get feedback, additional input
  - Add text on address expiration
- Get working group consensus:
  - Adopt document as simple update to RFC 4941; or,
  - Make the document stand alone and obsolete RFC 4941.