Recommendation on Non-Stable IPv6 Interface Identifiers

(draft-gont-6man-non-stable-iids)

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

IETF 100
Singapore. November 11-17, 2017

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
- Miscellaneous issues

Goals of this document

- Specify security/privacy requirements for non-stable addresses
- Suggest some possible algorithms to generate non-stable IIDs
- Clarify that hosts are not required to generate stable addresses
  - stable-only, temporary-only, or mixed stable/temporary become all possible
- Formally obsolete RFC4941

Requirements for non-stable IIDs

- Must have limited lifetime
- Lifetime must be further reduced by security-meaningful events
- Must be different for different prefixes
- Must not embed layer-2 addresses
- Must be difficult to predict by an outside entity
- Must be semantically opaque

Generation of non-stable IIDs

- Use any algorithm that complies with the specified requirements, e.g.:
  - Random IIDs that change upon network disconnection/attachment
  - A la RFC7217:

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

Moving forward

- Adopt as 6man WG item?