Randomized MAC Addresses and IPv6 Address Assignment

Christian Huitema

Huitema@microsoft.com

IETF 93, Prague, July 2015

Random MAC Address Hypotheses

- Allow users to “hide” from the network
- Different at different locations
  - Prevent location tracking
- May or may not be constant per location over time
  - Arbitration between stability and privacy
  - Controlled by user preferences
  - Expected constant for the duration of a “session”
- Implemented using existing IEEE 802 rules
  - Preferred Format: U/L = 1, G=0, 46 random bits

Randomization and RFC 7217 Conflict

MAC Address Randomization

- Emphasis on Privacy
- Try to ensure "anonymity" when visiting a particular network
- User varies MAC Address over time if "hiding" from the network.

Stable, semantically opaque IIDs

- Emphasis on Stability
- Try to ensure that if hardware is replaced, IPv6 address remains stable.
- Defeats MAC Address Randomization

Proposal: Update RFC 7217

- Proposed revision of Section 5, Net_Iface selection
  - It ~~MUST~~ SHOULD be constant across system bootstrap sequences and other network events (e.g., bringing another interface up or down).
  - It MAY change if the system administrator decides so explicitly, e.g. by implementing Link Layer Address Randomization. This can be achieved by selecting the Current Link Layer Address for Net-Iface parameter.
- Proposed Addition to Appendix A, section A.3, Link-Layer Addresses
  - Link-Layer addresses will change dynamically in systems that implement Link Layer Address Randomization. This will cause IIDs to change whenever the Link Address changes, which is very desirable for privacy.

Other Address Assignment Methods

IEEE Based IID	Random MAC only unique on one link IPv6 Address discloses random MAC May (very rarely) collide with other random addresses	Bad idea.
Static ID	Remain static, defeat MAC randomization	Out of scope
Constant IID	Remain constant, defeat MAC randomization (Windows implementation are not actually constant, change if MAC address changes)	Should be replaced by RFC 7217 at some point
Temporary IIDs	Defeat MAC randomization if the lifetime overlaps.	Needs spec. Should update to variant of RFC 7217.
DHCPv6	Defeat MAC randomization if using stable DUID.	See DHCP anonymity profile
Embedded IPv4	Defeat MAC randomization if DHCP uses stable DUID, allocate constant value	

Feedback and proposal

- Feedback from Philip Homburg
  - Should be more explicit, no clear course of action.
  - Updating RFC 7217 should not be just a footnote.
  - Update or forward reference in draft-ietf-6man-default-iids
- Proposal
  - Revise the draft, clearer focus on RFC 7217
  - Adopt as WG item?
  - Not sure about draft-ietf-6man-default-iids