Generating Stable Privacy-Enhanced Addresses with IPv6 SLAAC
(draft-gont-6man-stable-privacy-addresses)

Fernando Gont
on behalf of
UK CPNI

IETF 83
Paris, France. March 25-30, 2012

Modified EUI-64 format identifiers

- Privacy implications of EUI-64 format identifiers are well-known
  - They leak out node identity
  - They greatly simplify host scanning
- There seems to be general agreement that something should be done about them
  - For instance, Windows 7 does not use EUI-64 format identifiers

Privacy/Temporary addresses

- Aim to mitigate correlation of host activities
- They result in unpredictable and temporary addresses
- They are used **in addition** to MAC-derived addresses:
  - MAC-derived addresses for server-like functions
  - Privacy addresses for outgoing connections
- Some deem privacy addresses as difficult to manage

Summary of SLAAC-derived addresses

	Stable	Temporary
Predictable	Mod. EUI-64 I-IDs	None
Unpredictable	**NONE**	RFC 4941

- We lack of stable-privacy-enhanced IPv6 addresses
  - Used to replace MAC-derived addresses
  - Pretty much orthogonal to privacy addresses
  - Nodes with or without privacy addresses would benefit from them

Stable privacy-enhanced addresses

- We propose to generate IPv6 addresses as:

  F(Prefix, Modified_EUI64, Network_ID, secret_key)

- This function results in addresses that:
  - Are stable within the same subnet
  - Have different Interface-IDs when moving across networks

Moving forward

- Time to adopt it as a 6man wg document?

Feedback?

Fernando Gont

fgont@si6networks.com