Designating 6LBR for IID Assignment

draft-rashid-6lo-iid-assignment-01

Abdur Rashid Sangi
Mach Chen
Charles Perkins
Purpose

• Heterogeneous nature of LLN devices use numerous methods to generate IIDs.
• Arbitrary use of IID to attain better privacy.
• Designating 6LBR to suggest a unique IID to avoid repeated DAD cycle for failed DAD.
• Using semantically opaque IID generation.

Conceiving IID

Avoid Duplication
- EUI-64 {Guidelines by IEEE}

Privacy
- Temporary Address {RFC4941}
- 16 bit Short Address {RFC4944}

Security
- Semantically Opaque IID {RFC7217}
- Cryptographically Generated Addresses {RFC3972}
History and status

• First version:
  – Proposed the usage of RFC7217 to generate IID by 6LBR during Neighbor Discovery process, on behalf of 6LNs. [16th March, 2016]

• Second version:
  – Delivering the suggested IID from 6LBR to 6LN in space-efficient manner. [16th June, 2016]
RFC7217 - Semantically opaque IID

• 2 steps procedure

1. Compute a random (but stable) identifier with the expression:

   \[ \text{RID} = F(\text{PRF (Pseudorandom function)} \text{ ANY - depends on Intel. Property, Complexity, H/W limitations etc. Example. SHA-1, SHA-246, MD5 etc.}) \]

   \[ \text{Prefix, Learned from ICMPv6 RA in SLAAC} \]

   \[ \text{Net_iface, Interface Index OR Interface Name e.g. eth0, em0 etc. OR Link Layer Address OR Logical N/W Service IP} \]

   \[ \text{Network_ID, Optional: Identifies the subnet to which this interface is attached} \]

   \[ \text{DAD.Counter, Initialized to Zero (0) & incremented for each failed DAD} \]

   \[ \text{Secret.Key}\] Minimum 128bit & generated using random number generator (RFC4086) to keep intact secret of Secret.Key

   Size depends on selection of Hash Function

2. Fetch 64 bit LSB for IID & consult DB holding previously used addresses.

   Not Unique: increment DAD.Counter & re-compute.

   Unique: continue using.

   Derived from Router Advertisement
Currently

- 6LN sends the ARO+SLLAO in NS.
- 6LR sends out extended DAR to 6LBR.

**Space efficient manner**

Modified
Make use of 4 reserved bits and elided 64 bits prefix.
In a space efficient manner:

- In case of failed DAD a suggested IID is aggregated with EUI-64.
- 6LN sends extended DAC.

Currently:

- Make use of 4 reserved bits, elided 128 bits of registered address and XoR aggregate the suggested IID with EUI-64.
Space efficient manner

- 6LR extracts XOR aggregated address to send out extended ARO to 6LN.

Currently

Modified

Suggested IID is XoR addregated with EUI-64.
Advantage over current ND

• Negating the need of repeated cycle in case of failed DAD.
• Semantically opaque IID throughout network.
• Space efficient way to deliver IID.
• Avoiding expansive mechanism of DHCP for same purpose.
• As mentioned in “draft-ietf-6lo-privacy-considerations-01” this draft suggests IID with 64 bits of entropy.
Next step

• Incorporating improvements as per the already available comments on mailing list.
• Adding further justifications for privacy that arbitrary IID brings as mentioned in “draft-gont-predictable-numeric-ids-00”
Thank you
Questions/Comments
Recap of 6LoWPAN ND

- **SLLAO**
  - RS
  - PIO-6CO-ABRO-SLLAO
  - RA

- **ARO-SLLAO**
  - NS

- **ARO with Status**
  - NR

Data flows

6LoWPAN Neighbor discovery

6lowpan topology

- 6lowpan host (6LH)
- 6lowpan router (6LR)
- 6lowpan border router (6LBR)