Designating 6LBR for IID Assignment
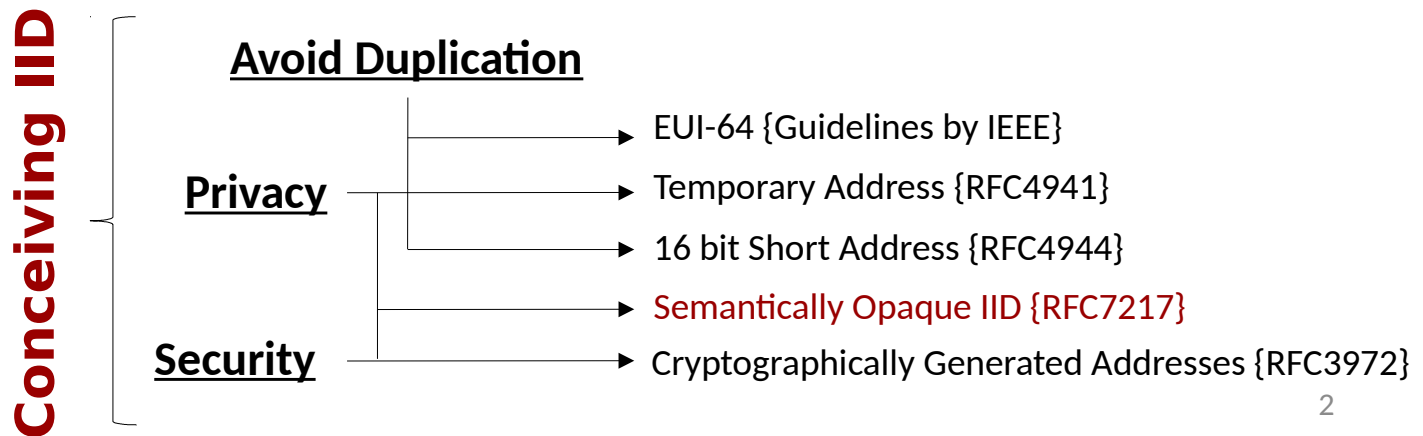
draft-rashid-6lo-iid-assignment-01

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

Privacy

Security

EUI-64 {Guidelines by IEEE}

Temporary Address {RFC4941}

16 bit Short Address {RFC4944}

Semantically Opaque IID {RFC7217}
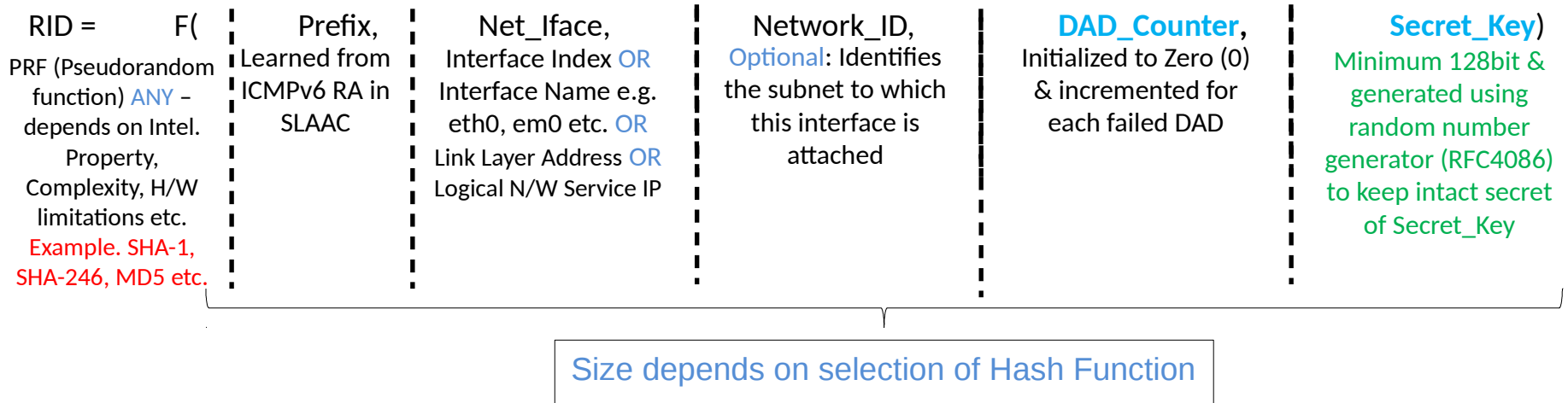
Cryptographically Generated Addresses {RFC3972}

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:

RID = F(	Prefix,	Net_Iface,	Network_ID,	DAD_Counter,	Secret_Key)
PRF (Pseudorandom function) ANY – depends on Intel. Property, Complexity, H/W limitations etc. Example. SHA-1, SHA-246, MD5 etc.	Learned from ICMPv6 RA in SLAAC	Interface Index OR Interface Name e.g. eth0, em0 etc. OR Link Layer Address OR Logical N/W Service IP	Optional: Identifies the subnet to which this interface is attached	Initialized to Zero (0) & incremented for each failed DAD	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.
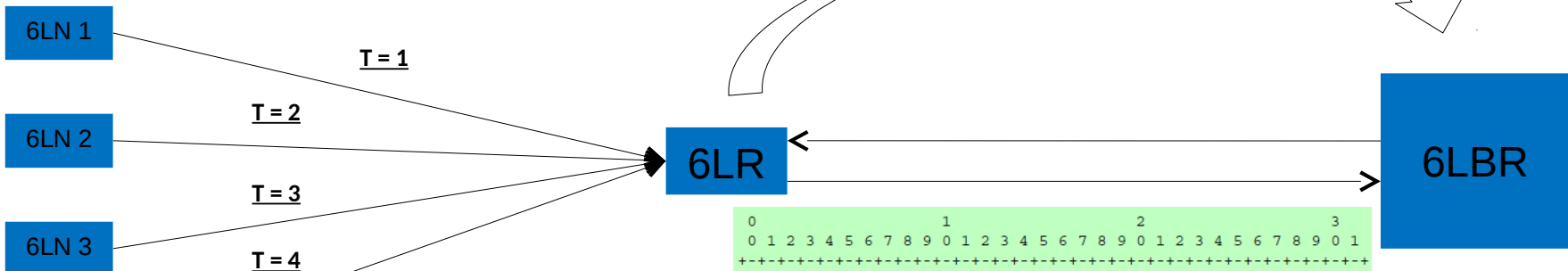
  Unique: continue using.

0 --- 63

	Interface ID

Derived from Router Advertisement

64 --- 127
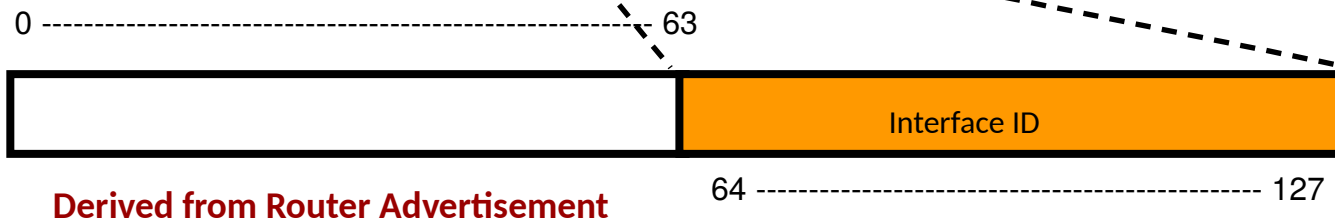
Space efficient manner

Currently

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |      Code     |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Status     |   Reserved    |     Registration Lifetime     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                            EUI-64                             |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Registered Address                       +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
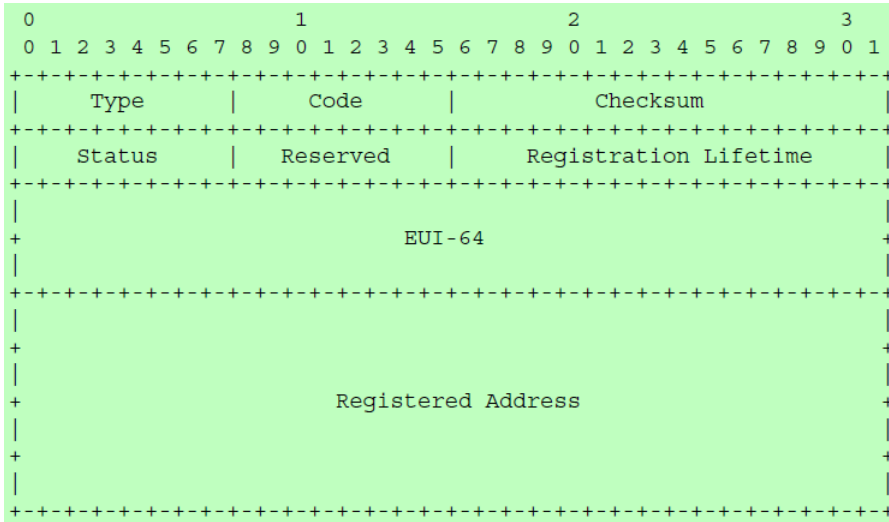
- 6LN sends the ARO+SLLAO in NS.
- 6LR sends out extended DAR to 6LBR.

| 6LN 1 |

T = 1

| 6LN 2 |

T = 2

| 6LR |

| 6LBR |

T = 3

| 6LN 3 |

T = 4

| 6LN 4 |

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |      Code     |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Status     | Rsrv | Cycle  |     Registration Lifetime     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                            EUI-64                             +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                         Registered IID                        +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

    Figure 3: Extended Duplication Address Request
```

Modified
Make use of 4 reserved bits and
elided 64 bits prefix.

Space efficient manner

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Status     |   Reserved    |     Registration Lifetime     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                            EUI-64                             |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                     Registered Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

6LN 1

6LN 2

6LN 3

6LN 4

T = 1

T = 2

T = 3

T = 4

6LR

6LBR

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |           Checksum            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Status     | Rsrv | Cycle  |     Registration Lifetime     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                    EUI-64/XOR Aggregation                     +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

    Figure 4: Extended Duplication Address Confirmation
```
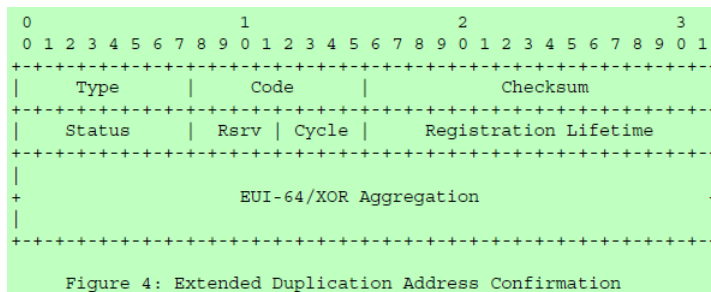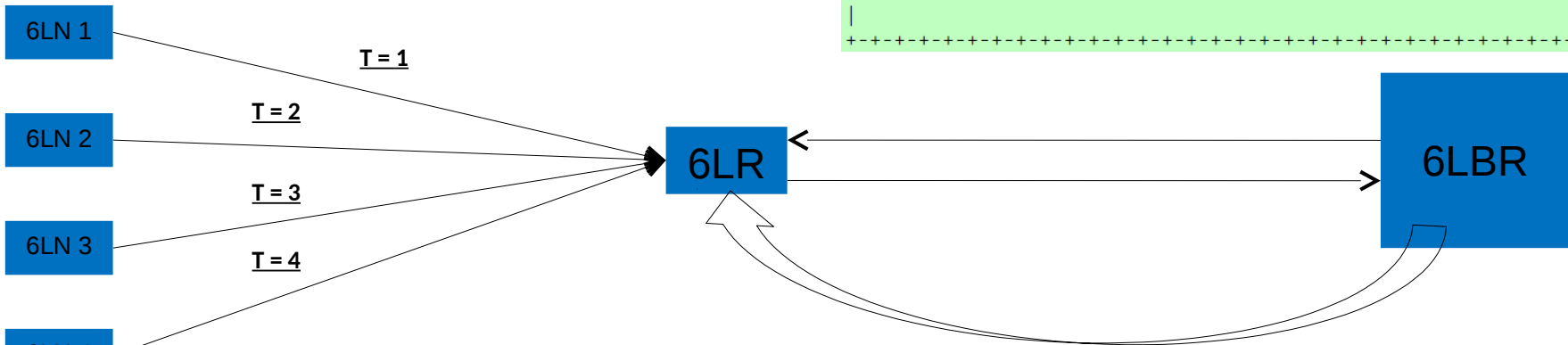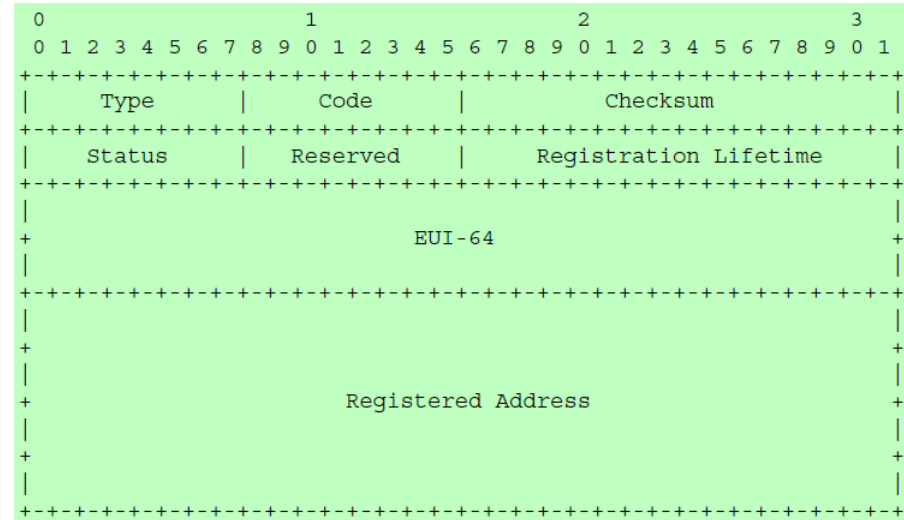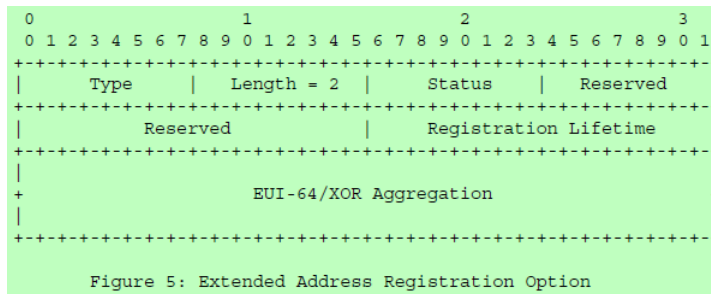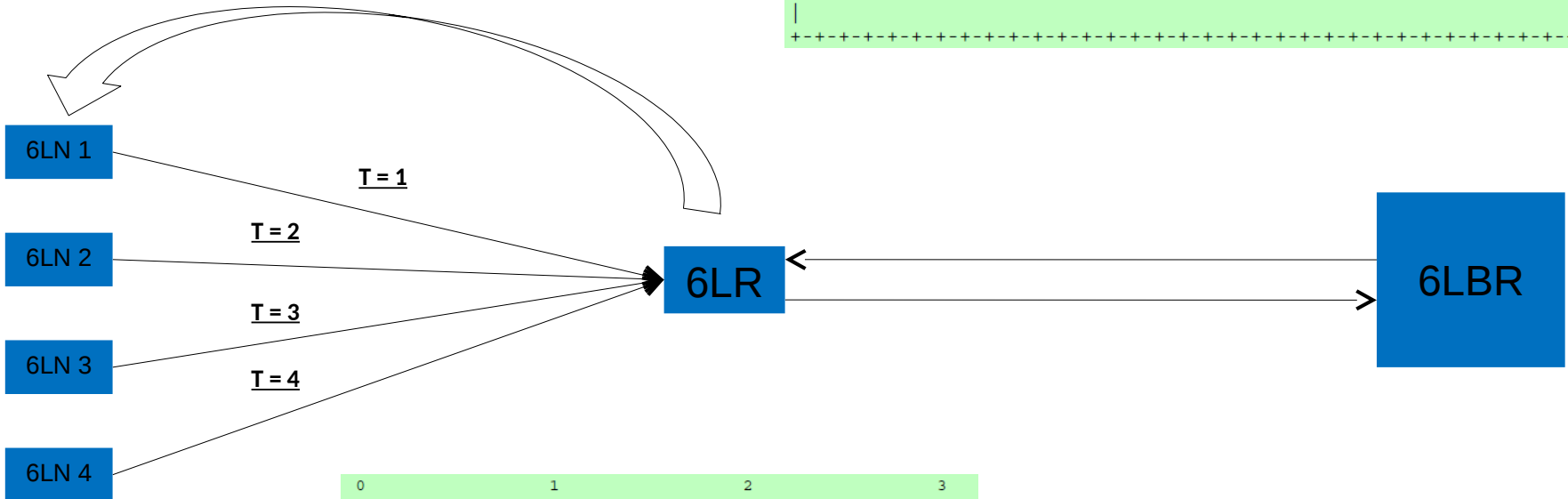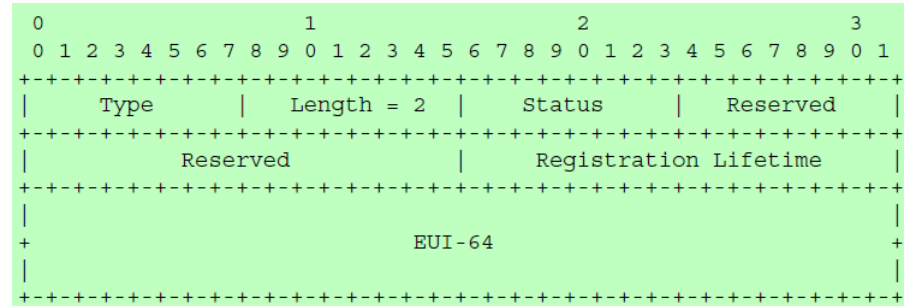
Modified
Make use of 4 reserved bits, elided 128 bits of registered address and XoR aggregate the suggested IID with EUI-64.

6

Space efficient manner

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length = 2   |    Status     |   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Reserved           |   Registration Lifetime       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                             EUI-64                            +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

6LN 1

6LN 2

6LN 3

6LN 4

T = 1

T = 2

T = 3

T = 4

6LR

6LBR

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length = 2   |    Status    |   Reserved    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Reserved          |    Registration Lifetime      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                     EUI-64/XOR Aggregation                    +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

      Figure 5: Extended Address Registration Option
```

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

6LoWPAN Neighbor discovery

6lowpan topology

6lowpan host (6LH)

6lowpan router (6LR)

6lowpan border router (6LBR)