Interface ID lifetime Algorithms
(Informational track)
draft-rafiee-v6ops-iid-lifetime

Authors:
Erik Nordmark
Arista Networks
Hosnieh Rafiee, Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Germany
Privacy vs. Operational Considerations

- The users want different levels of privacy
  - Changing/multiple IIDs is part of the solution
  - Solution might also include the applications

- Network operator want to limit the number of IIDs in use due to hardware constraints or for complexity reasons
  - Unlimited number of IID is not ideal
  - For instance, discussion on ipv6-ops@lists.cluenet.de about issues with many IIDs

- This draft is starting a discussion
  - Pointing out some possibilities in this tussle
Our Assumption & Purposes

- Our purpose is not how to generate IID but how to maintain the lifetime of the IIDs.
  - The node generates its interface ID (IID) by using RFC 4941, RFC 3972, draft ra-privacy, draft SSAS, etc.

- Comparison of the different ways of maintaining the IID lifetime

- Discuss when to remove deprecated IP addresses from the network adapter

- Offer a framework to control the number of valid IID in a certain time while provide user’s privacy
### Privacy in IPv4 vs IPv6

- Assume a host which remains on one network/location with lots of other hosts (Coffee shop, campus, etc)

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users cannot be identified via their IP address (NAT)</td>
<td>Users’ can be identified by their IP address (one of IPv6 features is end-to-end communications, of course NAT6 is possible)</td>
</tr>
<tr>
<td>Browsers’ cookies or other approaches to correlate users’ activities</td>
<td>IPv6 addresses is a way of identification in addition to cookies etc</td>
</tr>
</tbody>
</table>
Protecting Users’ Privacy

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using browsers in &quot;incognito mode&quot; or &quot;private browsing&quot;</td>
<td>The same approach applicable in IPv6</td>
</tr>
<tr>
<td>Future and optional: Browser asks for a separate IID for the “incognito” connections to better maintain users privacy</td>
<td></td>
</tr>
</tbody>
</table>

How can we control the number of IP address per applications? How can we enable applications to maintain their users privacy without any complexity?
Lifetime for an Interface ID (IID)

- RFC 4941
  - Maximum the IID is valid for a week
  - Cut the connections after this time
  - One new IID generated per day – 7 active IIDs

- Layer-4 lifetime
  - Makes problem for some services in application layer such as ftp

- Application based lifetime
Application based lifetime

- A framework that plays a role of intermediate between applications and network layer

- Increase the difficulty of correlating a user’s activities by using different IIDs for different applications, without negatively impacting the robustness of the applications.
  - Privacy-enabled Application ask a new IID from this framework

- Remove the deprecated IID when it is not used by any applications
Application based lifetime Algorithm

- Why we need to control the number of IID
  - To avoid multicast problem in networks that support limited number of IID
Do folks have operational data on the impact of large number of IID\$s?\$  
How we can connect the application layer privacy issues with the number of IID\$s?