Selectively Isolating Hosts to Prevent Potential Neighbor Discovery Issues and Simplify IPv6 First-hops

draft-ietf-v6ops-nd-considerations
XiPeng Xiao, Eduard Vasilenko, Eduard Metz, Gyan Mishra, Nick Buraglio
3 Parts: (1) Potential ND Issues & Causes (2) Optimization Solutions & An Isolation Theme (3) How to Isolate Hosts to Prevent Potential Issues

<table>
<thead>
<tr>
<th>Performance issues caused by multicast</th>
<th>Reliability issues caused by multicast</th>
<th>On-link security issues caused by trusting all hosts</th>
<th>Off-link security issues caused by Router-NCE-on-Demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>• LLA DAD degrading performance</td>
<td>• LLA DAD not reliable for wireless networks</td>
<td>• Source IP address spoofing</td>
<td>• Router NCE exhaustion</td>
</tr>
<tr>
<td>• Unsolicited RA degrading performance</td>
<td>• GUA (or ULA) DAD not reliable for wireless networks</td>
<td>• DAD denial</td>
<td>• Performance issue caused by Router-NCE-on-Demand</td>
</tr>
<tr>
<td>• GUA (or ULA) DAD degrading performance</td>
<td>• Router address resolution for hosts degrading performance</td>
<td>• Fake RAs</td>
<td>• Subscriber management issue caused by Router-NCE-on-Demand</td>
</tr>
<tr>
<td>• Router address resolution for other hosts degrading performance</td>
<td>• Host Address resolution for other hosts degrading performance</td>
<td>• Fake Redirect</td>
<td>• Lack of subscriber management using ND with SLAAC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>15 issues, but only 3 causes</th>
<th>13 solutions, 1 theme: host isolation</th>
<th>How isolation deal with the 3 causes</th>
</tr>
</thead>
</table>

5 isolation mechanisms

- Subnet isolation
- P2P link isolation
- P2MP link isolation
- Proxy isolation
- GUA isolation

- Subnet isolation reduces multicast, hosts to trust & eliminates Router-NCE-on-demand
- P2P link isolation reduces multicast, hosts to trust & eliminate Router-NCE-on-demand
- P2MP link isolation reduces multicast, hosts to trust
- Proxy isolation reduces multicast, hosts to trust
- GUA isolation reduces multicast

Much easier to deal with 3 causes than to deal with individual issues
How to Select a Suitable Isolation Method

5 isolation mechanisms produce 6 methods. They cover all basis

<table>
<thead>
<tr>
<th>Method</th>
<th>L3 isolation</th>
<th>L2 isolation</th>
<th>GUA isolation</th>
<th>Proxy isolation</th>
<th>Shared Medium</th>
<th>P2P Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet + p2p</td>
<td>L3 isolation</td>
<td>Complete L2</td>
<td>No L3 isolation</td>
<td>Complete or partial L2</td>
<td>Partial L2</td>
<td>No L2</td>
</tr>
<tr>
<td>Subnet + p2mp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subnet + shared media</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proxy isolation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GUA isolation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No isolation whatsoever</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

How to apply 6 types of isolations: from strongest to weakest

1. If Subnet Isolation with P2P Link is feasible:
   a) Applicable scenarios:
      1) The medium is P2P.
      2) Direct host to host communication without going through the router is not needed.
      3) Multicast is not desirable (implying mDNS is not needed).
      4) Hosts may not be trustable.
      5) Subscriber management is needed.
      6) Privacy of hosts are not a major concern.
      Examples are public access networks such as MBBv6 or FBBv6 with PPPoE.
   a) Entry requirements:
      1) Hosts must be able to set up P2P links with the router.
      2) There are sufficient IPv6 addresses to provide Unique Prefix Per Host.
      3) The router must support a “Subnet Isolation with P2P Link” solution, e.g. MBBv6.
   b) Remaining ND issues and solutions:
      1) None.
2. Otherwise, if Subnet Isolation with P2MP Link is feasible
3. Otherwise, if Subnet Isolation with Shared Medium is feasible
4. Otherwise, if Proxy Isolation is feasible
5. If there are still multiple hosts in a same subnet and broadcast domain, if GUA Isolation (i.e. setting PIO L-bit=0) is feasible
6. Otherwise, no isolation to apply
Summary of Changes in this Version

- Added some text in Section 2.4 to point out that certain ND issues only happen in certain scenarios
  - To address Brian’s concern that this draft gives a negative impression on ND
- Modified the “Proxy Isolation” section
  - Proxy isolation divides a subnet into multiple multicast domains - can be considered as a kind of “L2 isolation without L3 isolation”.
  - Proxy isolation’s relationship with other L3/L2 isolation methods becomes clearer.
  - Promote proxy isolation before GUA isolation
- Pointed out that Unique Prefix Per Host reduces privacy

Draft relatively stable. Plan to request for WGLC