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

15 issues, but only 3 causes

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

13 solutions, 1 theme: host isolation

5 isolation mechanisms

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

How isolation deal with the 3 causes

- 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

Subnet + p2p	L3 isolation	Complete L2 isolation
Subnet + p2mp		Partial L2
Subnet + shared media		No L2
Proxy isolation	No L3 isolation	Complete or partial L2 isolation
GUA isolation		No L2, just GUA isolation
No isolation whatsoever		No L2, No GUA

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