Selectively Applying Host Isolation to Simplify IPv6 First-hop Deployment

draft-ietf-v6ops-nd-considerations

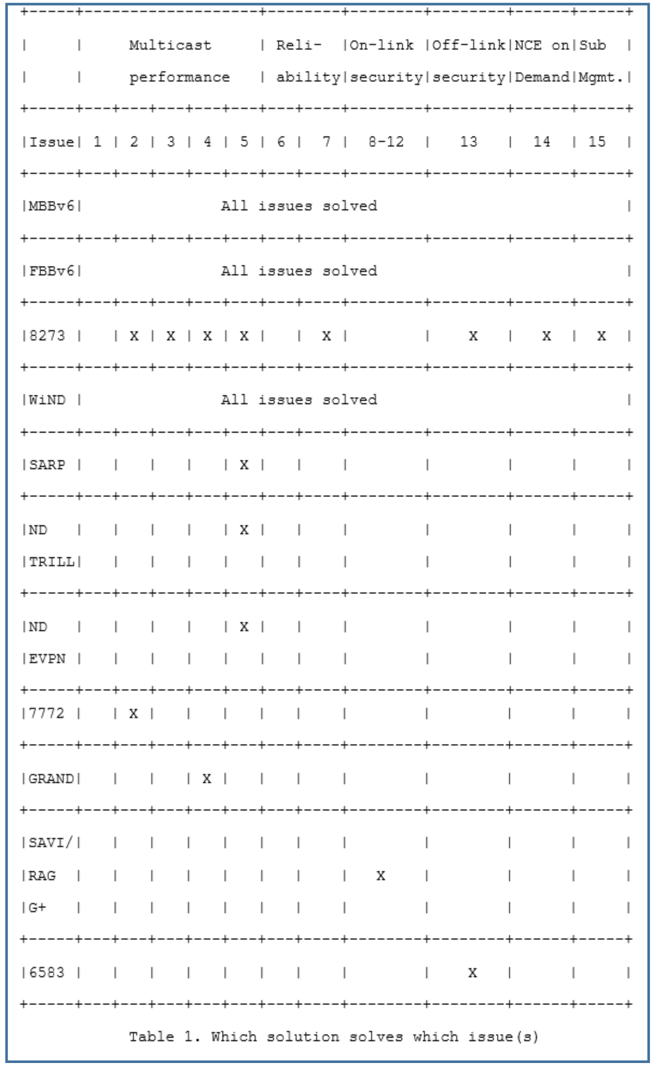
XiPeng Xiao, Eduard Vasilenko, Eduard Metz, Gyan Mishra, Nick Buraglio

Draft Contains 3 Parts: (1) Summary of Potential Issues & Causes (2) Summary of Optimization Solutions & Theme (3) How to Apply Host Isolation to Avoid 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 (isolation)



	Multicast performance					Reli-ability		On-link security	Off-link security	NCE on Demand	Sub Mgmt.
Issue	1	2	3	4	5	6	7	8-12	13	14	15
MBBv6	All issues solved										
FBBv6	All issues solved										
8273		X	X	X	X		X		X	X	X
WiND	All issues solved										
SARP					X						
ND TRILL					X						
ND EVPN					X						
7772		X									
GRAND				X							
SAVI/ RAG G+								X			
6583									X		

Table 1. Which solution solves which issue(s)

How to apply 4 types of isolations

1. If P2P Link and Subnet Isolation is feasible:
   a) **Applicable scenarios:**
      1) Direct host to host communication is not required.
      2) A P2P architecture is feasible.
      3) Multicast is not desirable (implying mDNS is not needed) for performance or reliability reasons, or
      4) Hosts may not be trustable, or
      5) Subscriber management is needed. Examples are public access networks such as MBBv6 or FBBv6 PPPoE
   b) **Entry requirements:**
      1) Hosts must be able to set up P2P links with the router.
      2) The router must have an optimized ND solution that avoids downstream multicast (i.e. DADs, unsolicited RAs, address resolution for hosts), like MBBv6 or FBBv6 or RFC 8273.
   c) **Remaining issues and solutions:**
      1. All ND issues are solved
      2. Filtering may be needed at the router to discard malicious/erroneous ND messages from hosts, e.g. RAs.
2. Otherwise, if P2MP Link and Subnet Isolation is feasible
3. Otherwise, if GUA Isolation (i.e. setting PIO L-bit=0) is feasible
4. Otherwise, if Proxy Isolation is feasible
5. Otherwise, no isolation to apply

Summary of Changes in this Version

- Changed draft name to: draft-ietf-v6ops-nd-considerations-00
  - To address Chongfeng's comment that ND is a single protocol that there is no such thing as a single protocol deployment;
- Added/modified text reduce impression that ND has many issues
  - To address Philipp Tiesel/Mike Ackermann's concern that this draft has a negative tone towards ND, and may scare people away from IPv6
- Editorial and some content change in Sections 3.3 (8273) and 3.4 (WiND) for clarity
  - To address Nick's comments that the original text is not clear enough
- Pointed out SARP and ND Proxy are experimental
  - To address Jen Linkova's comments in IETF 114 that some solutions we reviewed were experimental
- Highlight that assigning a prefix (e.g. /64 or /56) to each host is not an issue
  - Chongfeng requested that we pointed out the 8273 uses a lot of address prefixes.