Selectively Applying Host Isolation to Simplify IPv6 First-hop Deployment

draft-xiao-v6ops-nd-deployment-guidelines-02

XiPeng Xiao, Eduard Vasilenko, Eduard Metz, Gyan Mishra

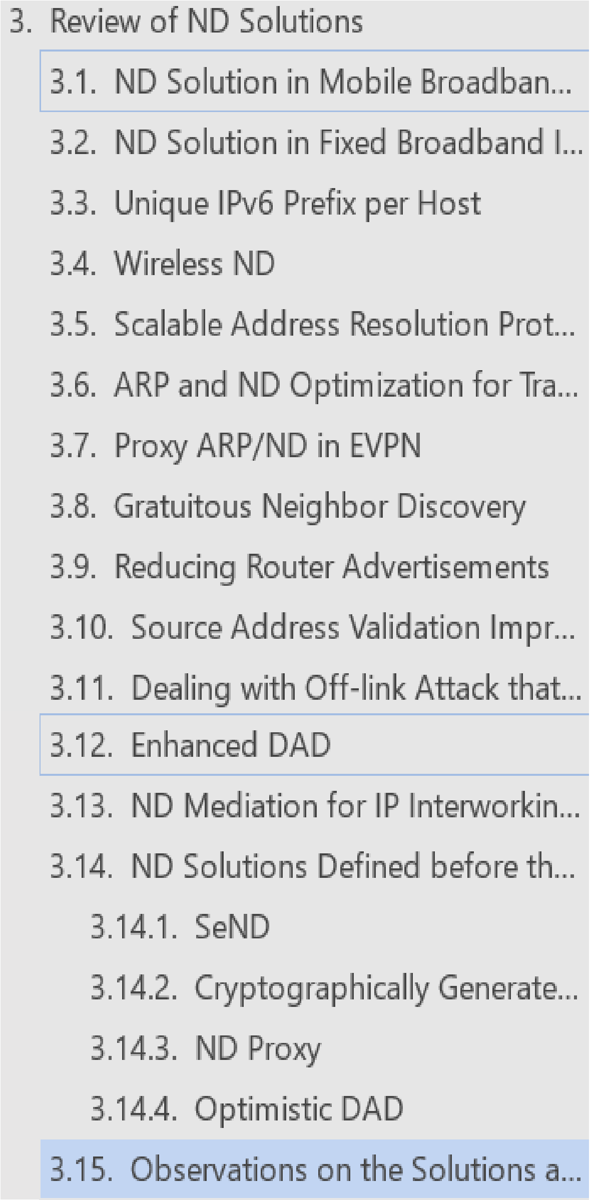
Problem Statement

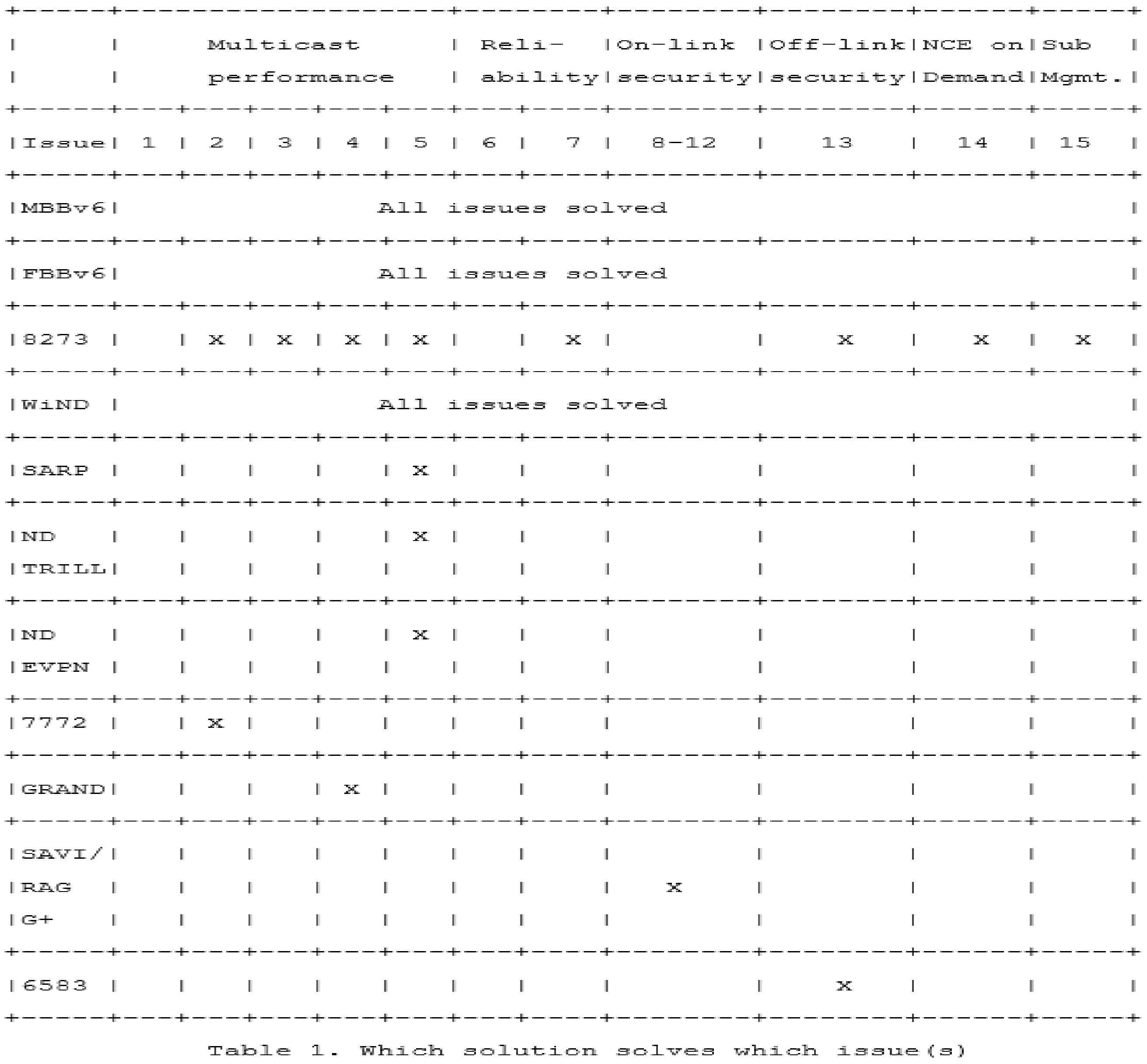
- 30+ RFCs on ND issues and solutions → difficult to keep track and understand → reluctant to deploy
  - SEND & CGA,
  - ND Proxy,
  - Optimistic ND,
  - ND for mobile broadband, ND for fixed broadband,
  - ND Mediation,
  - Operational ND Problems,
  - Wireless ND (WiND),
  - DAD Proxy,
  - SAVI/RA-Guard/RA-Guard+,
  - Enhanced DAD,
  - Scalable ARP,
  - Reducing Router Advertisements,
  - Unique Prefix Per Host,
  - GRAND,
  - Proxy ARP/ND for EVPN etc.

Summary of ND Issues

- 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

Overview of Existing ND Optimization Solutions





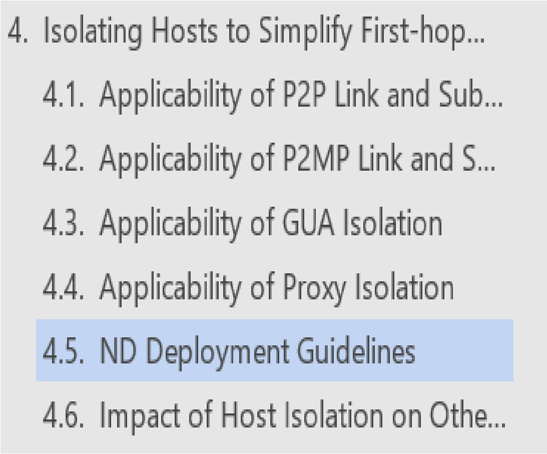
	Multicast performance					Reliability		On-link security	Off-link security	NCE on Demand	Sub Mgmt.
Issue	1	2	3	4	5	6	7	8-12	13	14	15
MBBv6	All issues solved										
FBBv6	All issues solved										
8273		x	x	x	x		x		x	x	x
WiND	All issues solved										
SARP					x						
ND TRILL					x						
ND EVPN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

Table 1. Which solution solves which issue(s)

An Insight from the Solutions

- Isolating hosts effective in solving ND issues.
- The stronger hosts are isolated, the more ND issues can be solved.
- 4 isolation methods
  - Link isolation (i.e. L2 isolation)
    - P2P
    - P2MP
  - Subnet isolation (i.e. Unique Prefix Per Host, RFC 8273)
  - GUA isolation (i.e. setting PIO L-bit=0)
  - Proxy isolation (i.e. use a proxy device to represent the hosts behind it)
- These isolation methods not independent, leading to only 4 meaningful combinations
  - P2P link + subnet isolation
  - P2MP link + subnet isolation
  - GUA isolation (without link or subnet isolation)
  - Proxy isolation

Guidelines on How to Select an Isolation Combination



4. Isolating Hosts to Simplify First-hop...

4.1. Applicability of P2P Link and Sub...

4.2. Applicability of P2MP Link and S...

4.3. Applicability of GUA Isolation

4.4. Applicability of Proxy Isolation

4.5. ND Deployment Guidelines

4.6. Impact of Host Isolation on Othe...

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

   a) 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.

   b) 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

Stronger isolation → fewer issues → simpler first-hop