IPv6 Operations (v6ops) Working Group
Internet Draft
Intended status: Informational
Expires: July 2025

X. Xiao
E. Vasilenko
Huawei Technologies
E. Metz
KPN
G. Mishra
Verizon Inc.
N. Buraglio
Energy Sciences Network

January 30, 2025

Neighbor Discovery Considerations in IPv6 Deployments
draft-ietf-v6ops-nd-considerations-09

Abstract

The Neighbor Discovery (ND) protocol is a critical ~~part~~ component of the IPv6 architecture. ~~ND~~ The protocol uses multicast extensively. It also ~~and~~ assumes a security model where all nodes ~~trusts all hosts and routers~~on a link are trusted. Such a design might be inefficient ~~In~~ in some scenarios~~, such as~~ (e.g., use of multicast in wireless networks)~~, multicast can be inefficient~~. or when nodes~~In other scenarios, such as public access networks, some hosts or routers may not be~~are not trustworthy (e.g., public access networks). ~~Consequently, ND can have~~These security and operational issues in some scenarios jointly with a set of ~~. The issues and~~ mitigation solutions are documented in more than 20 RFCs. There is a need to structure tracking~~, making it challenging to track all~~ these issues and solutions. ~~Therefore, an overview document is helpful.~~

To that aim, ~~This~~ this document ~~first~~ summarizes the published ND issues ~~and the Solutions~~and ~~. This provides a one-stop reference as of the time of writing. This document~~ then ~~points out that these more than 20~~described how all these issues ~~issues~~ originate from ~~just~~ three causes. Addressing the issues is made simpler by addressing the causes. This document also analyzes the mitigation solutions ~~to~~ and ~~show~~ demonstrate that isolating hosts into different subnets and links can help to address the three causes~~, and thus prevent ND issues~~. ~~Three isolation methods and their applicability are described.~~ A ~~simple guideline~~ guidance is ~~suggested~~ provided for selecting a suitable isolation method to prevent potential ND issues.

Status of this Memo

Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire in July 2025.

Table of Contents

1. Introduction

Neighbor Discovery ~~[~~(ND~~]~~ ~~)~~ ~~is specified in~~ [RFC~~-~~4861]~~. It~~ defines how nodes (hosts and routers) on a link interact with each other. Stateless Address Autoconfiguration ~~(~~ ~~[~~SLAAC~~]~~ ~~)~~ [RFC4862] is closely related to ND and is mandatory for IPv6 ~~hosts and routers~~nodes. To understand the ND issues, it is useful to understand how ~~hosts and routers~~nodes interact to send, receive, and forward packets. Overall, ~~Below are~~ the ND procedure~~s~~ for a host is as follows:

1. LLA DAD: the host forms a Link-Local Address (LLA)~~,~~ and performs Duplicate Address Detection (DAD) using multicast Neighbor Solicitations (NSs).

2. Router Discovery: the host sends multicast Router Solicitations (RSs) to discover ~~the~~ a router on the link. The router responds with Router Advertisements (RAs), providing subnet prefixes and other information. The host installs a Neighbor Cache Entry (NCE) for ~~the~~ that router upon receiving the RAs. In contrast, the router cannot install an NCE for the host at this moment of the exchange because the host's global IP address is still unknown. When the router later needs to forward a packet to the host's global address, it will perform address resolution and install an NCE for the host.

3. GUA DAD: the host forms a Global Unicast Address (GUA) or a Unique Local Address (ULA~~), and~~) and uses multicast NSs for DAD. For description simplicity, this document will not further distinguish GUA and ULA.

4. Next-hop determination and address resolution: when the host ~~is~~has to send a packet, it will first determine whether the next-hop is a router or an on-link host (which is the destination). If the next-hop is ~~the~~ a router, the host already has the NCE for ~~the~~ that router. If the next-hop is an on-link host, it will use multicast NSs to perform address resolution for the destination host. As a result, the source host installs an NCE for the destination host.

5. Node Unreachability Detection (NUD): the host uses unicast NSs

to determine whether another node with an NCE is still reachable.

6. Link-layer address change announcement: if a host's link-layer address changes, it may use multicast NAs to announce its new link-layer address to other nodes.

~~For a router,~~T ~~t~~he procedure is ~~s~~ are ~~s~~ similar for a router, except ~~but~~ that there is no Router Discovery. Instead, routers ~~have~~ performs a Redirect procedure that hosts do not have. A router sends a Redirect to inform a host of a better next-hop for the host's traffic.

~~The above procedures show that~~ ND uses multicast in many messages, ~~ND~~ trusts messages from all nodes, and routers may install NCEs for hosts on demand when they are to forward packets to these hosts. These ~~can cause~~may lead to issues. Concretely, ~~Various~~ various ND issues and mitigation solutions have been published in more than 20 RFCs, including:

- ND Trust Models and Threats [RFC3756],
- Secure ND [SeND],
- Cryptographically Generated Addresses [CGA],
- ND Proxy [RFC4389],
- Optimistic ND [RFC4429],
- ND for mobile broadband [RFC6459][RFC7066],
- ND for fixed broadband [TR177],
- ND Mediation [RFC6575],
- Operational ND Problems [RFC6583],
- Wireless ND (WiND) [RFC6775][RFC8505][RFC8928][RFC8929][SND],
- DAD Proxy [RFC6957],
- Source Address Validation Improvement [SAVI],
- Router Advertisement Guard [RA-Guard][RA-Guard+],
- Enhanced Duplicate Address Detection [RFC7527],
- Scalable ARP [SARP],
- Reducing Router Advertisements [RFC7772],
- Unique Prefix Per Host [UPPH],
- ND Optimization for Transparent Interconnection of Lots of Links (TRILL) [RFC8302],
- Gratuitous Neighbor Discovery [GRAND],
- Proxy ARP/ND for EVPN [RFC9161], and
- Using DHCPv6 Prefix Delegation (DHCPv6-PD) to Allocate Unique IPv6 Prefixes per Client in Large Broadcast Networks [DHCP-PD].

~~Because of the large number of RFCs involved, it can be difficult to track the issues and solutions.~~ This document summarizes these RFCs into a one-stop reference (as of the time of writing) for easier access. This document also identifies ~~the~~ three causes of the issues, and ~~suggests~~ defines three host isolation methods ~~that help~~ to address the causes and, thus, prevent~~ing~~ potential ND issues.

1.1. Terminology

This document uses the terms defined in [ND]. Additional terms are defined in this section.

MAC - To avoid confusion with link-local addresses, link-layer

Commenté [MB1]: Not sure we need to include this. A pointer to rfc4861#section-3 would suffice (and be more accurate)

Commenté [MB2]: I would Simply use the RFC numbers, through the document. Please update here and all similar uses in the document.

addresses are referred to as MAC addresses in this document.

Host Isolation - separating hosts into different subnets or links.

L3 Isolation - allocating a unique prefix per host [UPPH][DHCP-PD] so that every host is in a different subnet. This Layer 3 (L3) Isolation is also called Subnet Isolation in this document. ~~It should be noted that, due to the possibility of~~Given that ~~allocating~~ a unique prefix can be allocated per host on shared media, hosts in different subnets may be in the same link.

L2 Isolation - taking measures to prevent a host from reaching other hosts directly in Layer 2 (L2) so that every host is in a different link. This is also called Link Isolation. ~~It should be noted that, d~~Due to the existence of Multi-Link Subnet [MLSN], hosts in different links may be in the same subnet. Therefore, L2 Isolation does not imply L3 Isolation, and L3 Isolation does not imply L2 Isolation either.

L3 & L2 Isolation - applying L3 Isolation and L2 Isolation simultaneously so that every host is in a different subnet and in a different link. This is also called Subnet & Link Isolation.

Proxy Isolation - using an L3 ND proxy device to represent the hosts behind it to other hosts in the same subnet. Within the subnet, ND multicast exchange is ~~effectively~~ segmented into multiple smaller scopes, each represented by an ND proxy device. Proxy Isolation is Partial L2 Isolation.

2. Review of Inventoried ND Issues

2.1. Multicast May Cause Performance and Reliability Issues

In some cases, ND uses multicast for Node Solicitations ~~(~~NSs), Node Advertisements (NAs), Router Solicitations (RSs)~~,~~ and Router Advertisements (RAs). While multicast can be highly efficient in certain scenarios, especially in wired networks, multicast can also be inefficient in other scenarios ~~(,~~ e.g., in large L2 networks or wireless networks~~)~~.

~~In large L2 networks~~Typically, multicast can create a large amount of protocol traffic in large L2 networks. This can consume network bandwidth, create a processing burden, and ~~reduce~~ impact network performance [RFC7342].

In wireless networks, multicast can be inefficient or even unreliable due to higher probability of interference, lower data rate, and lack of acknowledgements~~, etc~~. [RFC9119].

~~Multicast is used in the following ND messages.~~ The ~~related m~~Multicast~~-related~~ performance issues of ND message are summarized below:

. Issue 1 LLA DAD Degrading Performance: in an L2 network of N

Commenté [MB3]: Why do we need two terms then. Please simplify

Commenté [MB4]: Idem as above

Commenté [MB5]: Idem as above

Commenté [MB6]: Do we have a pointer to cite here?

Commenté [MB7]: Idem as above

addresses (which can be much larger than the number of hosts as each host can have multiple addresses), there can be N such multicast messages. This may cause performance issues when N is large.

. Issue 2 Router's Periodic Unsolicited RAs Draining Hosts' Battery: multicast RAs are generally limited to one packet every MIN_DELAY_BETWEEN_RAS (3 seconds), and there are usually only one or two routers on the link, so it is unlikely to cause a performance issue. However, for battery-powered hosts, such messages may wake them up and create battery life issues [RFC7772].

. Issue 3 GUA DAD Degrading Performance: ~~in an L2 network of N addresses, there can be N such multicast messages. This may cause performance issues when N is large.~~Same as in Issue 1.

. Issue 4 Router's Address Resolution for Hosts Degrading Performance: Same as in Issue 1.~~in an L2 network of N addresses, there can be N such multicast messages. This may cause performance issues when N is large.~~

. Issue 5 Host's Address Resolution for Hosts Degrading Performance: Same as in Issue 1.~~in an L2 network of N addresses, there can be N-square such multicast messages. This may cause performance issues when N is large.~~

. (For Further Study) Hosts' MAC Address Change NAs Degrading Performance: with randomized and changing MAC addresses [MADINAS], there may be many such multicast messages. ~~As [MADINAS] is new and its impact to ND has not been fully evaluated, this issue is for further study.~~

In wireless networks, multicast is more likely to cause packet loss. Because DAD treats no response as no duplication, packet loss may cause duplicate addresses to be undetected. Multicast reliability issues are summarized below:

. Issue 6 LLA DAD Not Completely Reliable in Wireless Networks.
. Issue 7 GUA DAD Not Completely Reliable in Wireless Networks.

Note: IPv6 addresses have an extremely low probability of collisions. Therefore, these two issues are more theoretical than practical.

For description simplicity, multicast originated from hosts and routers will be called host multicast and router multicast hereafter.

Commenté [MB8]: Move to terminology section

2.2. Trusting-all-nodes May Cause On-link Security Issues

~~ND trusts all nodes.~~ In ~~some~~ scenarios~~,~~ such as public access networks, some nodes may not be trustworthy. An attacker on the link can cause the following security issues [RFC3756][RFC9099]:

. Issue 8 Source IP Address Spoofing: an attacker can use another node's IP address as the source address of its ND message to pretend to be that node. The attacker can then launch various Redirect or ~~Denial-of-~~Denial-of-Service (DoS) attacks.
. Issue 9 Denial of DAD: an attacker can repeatedly reply to a victim's DAD messages, causing the victim's address

configuration procedure to fail, resulting in a DoS to the victim.

. Issue 10 Forged RAs: an attacker can send RAs to victim hosts to pretend to be a router. The attacker can then launch various Redirect or DoS attacks.

. Issue 11 Spoofed Redirects: an attacker can send forged Redirects to victim hosts to redirect their traffic to the legitimate router to itself.

. Issue 12 Replay Attacks: an attacker can capture valid ND messages and replay them later.

2.3. Router-NCE-on-Demand May Cause Forwarding Delay, NCE Exhaustion, and Address Accountability Issues

~~In ND, w~~When a router ~~is~~ has to forward a packet to a node, but it still does not have an NCE for the node, it will create an NCE first and set its state to INCOMPLETE~~, .~~ ~~then~~ Then, the router will multicast NSs to all the nodes and wait for the destination node to reply with its MAC address to create the NCE. This is called Router-NCE-on-Demand in this document~~, and~~ .

Router-NCE-on-Demand~~this~~ can cause multiple issues:

. Issue 13 NCE Exhaustion: ND resolves addresses by creating an NCE in the INCOMPLETE state and multicasting NS to discover the destination MAC address. This mechanism introduces a security vulnerability: an attacker can send a high volume of packets targeting non-existent IP addresses, causing the router to create numerous NCEs in the INCOMPLETE state. The resulting resource exhaustion may render the router unable to function. This vulnerability, described as "NCE Exhaustion" in this document, does not require the attacker to be on-link.

. Issue 14 Router Forwarding Delay: when a packet arrives at a router, the router ~~must~~ buffers it while attempting to determine the host's MAC address. This buffering delays forwarding and, depending on the router's buffer size, may lead to packet loss. ~~–~~This delay is referred to as "Router-NCE-on-Demand Forwarding Delay" in this document.

. Issue 15 Lack of Address Accountability: with SLAAC, hosts generate their own IP addresses. The router does not become aware of a host's IP address until an NCE entry is created. With DHCPv6 [RFC8415], the router may not know the host's addresses unless it performs DHCPv6~~-~~ snooping. In public access networks, where subscriber management often relies on IP address (or prefix) identification, this lack of address accountability poses a challenge [AddrAcc]. Without knowledge of the host's IP address, network administrators are unable to effectively manage subscribers, which is particularly problematic in public access networks. Additionally, once NCE entries are created on ~~the~~ a router, there is no standardized method to retrieve these

entries for management purposes, as highlighted in Section 2.6.1.4 of [RFC9099, ~~Section 2.6.1.4~~].

2.4. Summary of ND Issue

The ND issues ~~related to ND~~, as discussed in Sections 2.1 to 2.3, are summarized below. ~~It is important to note that t~~These issues stem from three primary causes: multicast, Trusting-all-nodes, and Router-NCE-on-Demand. Eliminating any of these causes would also mitigate the corresponding issues. These observations provide guidance for addressing and preventing ND-related issues.

~~.~~ 1. Multicast:

- Performance issues ~~caused by multicast~~
  - Issue 1: LLA DAD Degrading Performance.
  - Issue 2: Unsolicited RA Draining Host Battery Life.
  - Issue 3: GUA DAD degrading performance.
  - Issue 4: Router Address Resolution for Hosts Degrading Performance.
  - Issue 5: Host Address Resolution for Other Hosts Degrading Performance.

~~.~~ ~~*~~ Reliability issues ~~caused by multicast~~

  - Issue 6: LLA DAD Not Completely Reliable in Wireless Networks
  - Issue 7: GUA DAD Not Completely Reliable in Wireless Networks

~~.~~ (2) On-link security issues caused by Trusting-all-nodes

  - Issue 8: Source IP Address Spoofing
  - Issue 9: Denial of DAD
  - Issue 10: Forged RAs
  - Issue 11: Spoofed Redirects
  - Issue 12: Replay Attacks

~~.~~ (3) Router-NCE-on-Demand related issues

  - Issue 13: NCE Exhaustion
  - Issue 14: Router Forwarding Delay
  - Issue 15: Lack of Address Accountability

~~It is important to emphasize that t~~These issues are potential vulnerabilities and may not manifest in all usage scenarios.

When these issues are relevant to a specific deployment, it is advisable to consider the mitigation solutions available, which are described in the following section.

3. Review of ND Mitigation Solutions

Table 1 summarizes ~~Which~~ ND mitigation solutions ~~are~~ available for ~~which~~ each issue~~s are summarized in Table 1 below~~. Similar solutions are grouped together, beginning with those that address the most issues. Unrelated solutions are ordered based on the issues they address. Each solution corresponds to a section below, where abbreviations such as MBBv6 and FBBv6 are described.

	Multicast	Reli-	On-link	NCE	Fwd.	No A.

a mis en forme : Avec puces + Niveau : 1 + Alignement : 2,2 cm + Retrait : 2,83 cm

a mis en forme : Retrait : Gauche : 1,25 cm

a mis en forme : Retrait : Gauche : 1,25 cm

Commenté [MB9]: In order to ease correlating with 3 causes mention above, I would adjust the structure.

Commenté [BMI10]: expand

	performance					ability	security	Exhaust.	Delay	Acct.
Issue	1	2	3	4	5	6	7	8-12	13	14	15
MBBv6	All issues solved										
FBBv6	All issues solved										
UPPH		X		X	X		X		X	X	X
WiND	All issues solved for Low-Power and Lossy Networks (LLNs)										
SARP					X						
ND TRILL					X						
ND EVPN					X						
7772		X									
GRAND				X					Partly		
SAVI/ RA G/G+								X			
6583									X		
AddrR											X

Table 1. Solutions for the identified issues

3.1. ND Solution in Mobile Broadband IPv6

Mobile Broadband IPv6 (MBBv6) is defined in "IPv6 in 3GPP EPS" [RFC6459], "IPv6 for 3GPP Cellular Hosts" [RFC7066], and "Extending an IPv6 /64 Prefix from a Third Generation Partnership Project (3GPP) Mobile Interface to a LAN Link" [RFC7278]. The solution key points are:

. Putting every host~~, i.e., the mobile User Equipment (UE),~~ in a P2P link with the router ~~(, i.e., the mobile gateway~~e.g., PDN Gateway (PGW) or User Plane Function (UPF)). MBBv6 also simplifies ND to take advantage of this P2P architecture. As a result:

- o All multicast is effectively turned into unicast.
- o The P2P links in MBB do not have MAC address. Therefore, Router-NCE-on-Demand is not needed.
- o Trusting-all-nodes is only relevant to the router ~~(i.e., the mobile gateway)~~. By applying filtering at the router ~~(~~, e.g., dropping RAs from the hosts), even malicious hosts cannot cause harm.

. Assigning a unique /64 prefix to each host ~~(i.e., the UE)~~. Together with the P2P link, this puts each host in a separate link and subnet.

. Maintaining (prefix, interface) binding at the router for

Commenté [BMI11]: There is no such a thing per se. We simply need to reason about 3GPP architecture.

Commenté [MB12]: simplify

Commenté [MB13]: expand

Commenté [MB14]: Not defined

a mis en forme : Surlignage

Commenté [MB15]: simplify

forwarding purpose.

Since all the three causes of ND issues are addressed, all the ~~15 ND~~ issues discussed in Section 2.4 are addressed.

3.2. ND Solution in Fixed Broadband IPv6

Fixed Broadband IPv6 (FBBv6) is defined in "IPv6 in the context of TR-101" [TR177]. FBBv6 has two flavors:

. P2P: every host, i.e., the Residential Gateway (RG), is in a P2P link with the router (~~, i.e.~~e.g.~~.~~, the Broadband Network Gateway (BNG)). In this case, the solution is functionally similar as MBBv6. All ND issues discussed in Section 2.4 are solved.

. P2MP: all hosts, i.e., the RGs, connected to an access device, ~~i.e.,~~(e.g., the Optical Line Terminal (OLT)), are in a P2MP link with the router, i.e., the BNG. This is implemented by aggregating all hosts into a single VLAN at the router and implementing L2 Split Horizon at the OLT to prevent direct host communication.

The key points of FBBv6-P2MP [TR177] are:

. Implementing DAD Proxy [RFC6957]: P2MP architecture with Split Horizon breaks normal ND's DAD procedure. Because all hosts are in the same interface from the router's perspective, the router must ensure that the hosts have different LLAs and GUAs. Otherwise, the router will not be able to distinguish them. However, because hosts cannot reach each other, normal DAD will not function as expected. Therefore, the router must participate in the hosts' DAD process and help hosts resolve duplication. With P2MP link and DAD Proxy:
  - o All host multicast to the router is effectively turned into unicast, as every host can only reach the router.
  - o Trusting-all-nodes is only relevant to the router. By applying some simple filtering at the router~~,~~ (e.g., dropping RAs from the host, even malicious hosts cannot cause harm).

. Assigning a unique /64 prefix to each host, as a result:
  - o The router can proactively create (IP prefix, MAC address) binding and use it for forwarding. There is no Router-NCE-on-Demand.
  - o Since different hosts are in different subnets, hosts will send traffic to other hosts via the router. There is no address resolution for other hosts.
  - o Without address resolution, router multicast to hosts consists only of unsolicited RAs. Because every host is in its subnet, unsolicited RAs will be sent individually to each host with the "host's MAC address replacing the multicast MAC address" approach specified in [RFC6085]. Therefore, router multicast is turned into unicast.

The following summarizes the key aspects of the FBBv6-P2MP architecture as described in [TR177]:

. Implementation of DAD Proxy [RFC6957]:

Commenté [MB16]: There is no such a thing per se.

Commenté [MB17]: The mobile case can also have a mobile RG/CE.

Commenté [MB18]: There are other nodes

Commenté [MB19]: Expand

Commenté [MB20]: This is just an example

In a P2MP architecture with Split Horizon, the normal ND DAD procedure is disrupted. Since all hosts appear on the same interface from the router's perspective:

- The router must ensure that all hosts have unique LLAs and GUAs, as address duplication would prevent the router from distinguishing between hosts.
- Due to the inability of hosts to reach each other directly, normal DAD cannot function. To address this, the router participates in the DAD process as a DAD Proxy to resolve address duplication.

With P2MP Links and DAD Proxy:

- Multicast traffic from all hosts to the router is effectively converted into unicast, as hosts can only communicate directly with the router.
- The Trusting-all-nodes model is limited to the router. By applying simple filtering (e.g., dropping RAs from hosts), the router can mitigate security risks, even from malicious hosts.

. Assigning a unique /64 prefix to each host:

Assigning each host a unique /64 prefix results in several operational improvements:

- The router can proactively install a forwarding entry for that prefix towards the host, eliminating the need for Router-NCE-on-Demand.
- Since each host resides in a different subnet, traffic between hosts is routed through the router, eliminating the need for hosts to perform address resolution for one another.
- Without address resolution, multicast from the router to hosts is limited to unsolicited RAs. As each host resides in its own subnet, these RAs are sent as unicast packets to individual hosts. This follows the approach specified in [RFC6085], where the host's MAC address replaces the multicast MAC address in the RA.

Since all three causes of ND issues are addressed, all ~~the~~ ND ~~15 ND~~ issues ~~discussed in~~ (Section 2.4) are also addressed.

3.3. Unique Prefix per Host

Unique Prefix per Host solutions are described in [UPPH] and [DHCP-PD]. Although [UPPH] relies on SLAAC for unique prefix allocation while [DHCP-PD] relies on DHCP-PD, for the discussions of this document, these two solutions are effectively the same. [UPPH]'s purpose is to "improve host isolation and enhanced subscriber management on shared network segments" such as Wi-Fi or Ethernet. The solution key points are:

. When a prefix is allocated to the host, the router can proactively install a forwarding entry for that prefix towards the host. There is no more Router-NCE-on-Demand.
. Without address resolution, router multicast to hosts consists

only of unsolicited RAs. They will be sent to hosts one by one in unicast because the prefix for every host is different.

. Since different hosts are in different subnets, hosts will send traffic to other hosts via the router. There is no host-to-host address resolution.

Therefore, ND issues caused by Router-NCE-on-Demand and router multicast are prevented.

[UPPH] ~~believes~~ indicates that a "~~A~~ network implementing a unique IPv6 prefix per host can simply ensure that devices cannot send packets to each other except through the first-hop router". But this may not be true when hosts are on a shared medium like Ethernet. In this case, hosts can still reach each other in L2 as they belong to the same Solicited-Node Multicast Group. Therefore, Trusting-all-nodes issues (i.e., On-link Security Issues 8-12) and host multicast issues may happen. Of the host multicast issues~~,~~ (i.e., Issues 1, 3, 5, 6, and 7), Unique Prefix per Host prevents Issues 5 and 7, because there is no need for address resolution among hosts, and there is no possibility of GUA duplication. But Issues 1, 3, and 6 may ~~happen~~occur.

3.4. Wireless ND and Subnet ND

Wireless ND (WiND) ~~is specified in a series of RFCs~~ [RFC6775][RFC8505][RFC8928][RFC8929]~~. WiND~~ defines a fundamentally different ND solution for Low-Power and Lossy Networks (LLNs) [RFC7102]. WiND changes host and router behaviors to use multicast only for router discovery. The solution key points are:

. Hosts use unicast to proactively register their addresses at the routers. Routers use unicast to communicate with hosts and become an abstract registrar and arbitrator for address ownership.

. The router also proactively installs Neighbor Cache Entries (NCEs) for the hosts. This avoids the need for address resolution for the hosts.

. The router sets PIO L-bit to 0. Each host communicates only with the router.

. Other functionalities that are relevant only to LLNs.

WiND addresses all ND issues ~~discussed in~~(~~Section~~ 2.4) in LLNs. However, WiND support is not mandatory for general-purpose hosts. Therefore, it cannot be relied upon as a deployment option without imposing additional constraints on the participating nodes.

Subnet Neighbor Discovery [SND] generalizes the solutions defined in WiND and defines a ~~new~~ protocol named Subnet Gateway Protocol (SGP). ~~It is being discussed in the IPv6 Maintenance (6man) WG.~~

Commenté [MB21]: Does not bring much.Simplify

3.5. Scalable Address Resolution Protocol (SARP)

Scalable Address Resolution Protocol [SARP] was an experimental solution that ended in 2017~~, two years after the RFC was published in 2015~~n. The usage scenario is Data Centers (DCs)~~DCs~~ ~~where~~ large L2 domains span across multiple sites. In each site, multiple hosts are connected to

Commenté [MB22]: simplify

Commenté [MB23]: expand

a switch. The hosts can be VMs so the number can be large. The switches are interconnected by a native or overlay L2 network.

The switch will snoop and install (IP, MAC address) proxy table for the local hosts. The switch will also reply to address resolution requests from other sites to its hosts with its own MAC address. ~~This way~~In doing so, all hosts within a site will appear to have a single MAC address to other sites. ~~Therefore~~As such, a switch only needs to build a MAC address table for the local hosts and the remote switches, not for all the hosts in the L2 domain. Consequently, ~~The~~ the MAC address table size of the switches is ~~therefore~~ significantly reduced. A switch will also add the (IP, MAC address) replies from remote switches to its proxy ND table so that it can reply to future address resolution requests for such IPs directly. This greatly reduces the number of address resolution multicast in the network.

Unlike MBBv6, FBBv6, and [RFC8372] which try to address all ND issues ~~discussed in~~ (Section 2.4), SARP focuses on reducing address resolution multicast to improve the performance and scalability of large L2 domains in DCs.

3.6. ARP and ND Optimization for TRILL

ARP and ND Optimization for TRILL ~~is specified in~~ [RFC8302]~~. The solution~~ is ~~very~~ similar to SARP ~~discussed in~~(Section 3.5). It can be considered as an application of SARP in the TRILL environment.

Like SARP, ARP and ND Optimization for TRILL focuses on reducing multicast address resolution. That is, it addresses Issue 5 ~~discussed in~~ (Section 2.1).

3.7. Proxy ARP/ND in EVPN

Proxy ARP/ND in EVPN is specified in [RFC9161]. The usage scenario is ~~Data Centers (~~DCs~~)~~ where large L2 domains span across multiple sites. In each site, multiple hosts are connected to a Provider Edge (PE) router. The PEs are interconnected by EVPN tunnels.

PE of each site snoops the local address resolution NAs to build (IP, MAC address) Proxy ND table entries. PEs then propagate such Proxy ND entries to other PEs via BGP EVPN. Each PE also snoops local hosts' address resolution NSs for remote hosts. If an entry exists in its Proxy ND table for the remote hosts, the PE will reply directly. Consequently, the number of multicast address resolution messages is significantly reduced.

Like SARP, Proxy ARP/ND in EVPN also focuses on reducing address resolution multicast.

3.8. Gratuitous Neighbor Discovery

Gratuitous Neighbor Discovery ~~is specified in~~ [GRAND]~~. GRAND~~ changes ND in the following ways:

. A node sends unsolicited NAs upon assigning a new IPv6 address

Commenté [MB24]: expand

Commenté [MB25]: Expand

to its interface.
. A router creates a new NCE for the node and sets its state to STALE.

Later, when the router receives traffic to the node, the existence of the NCE entry in the STALE state will cause the router to send unicast NS to the node to verify its reachability rather than sending multicast NS to resolve its MAC address. This can shorten the time the NCE entry reaches the REACHABLE state and improve forwarding performance. Therefore, GRAND provides an improvement but does not fully solve the Router-NCE-on-Demand issues. For example, NCE exhaustion can still happen.

3.9. Reducing Router Advertisements

Maintaining IPv6 connectivity requires that hosts be able to receive periodic multicast RAs [ND]. Hosts that process unicast packets while they are asleep must also process multicast RAs while they are asleep. An excessive number of RAs can significantly reduce the battery life of ~~portable~~ mobile hosts. [RFC7772] specifies a solution to reduce RAs:

. The router should respond to RS with unicast RA (rather than the normal multicast RA) if the host's source IP address is specified and the host's MAC address is valid. This way, other hosts will not receive this RA.
. The router should reduce multicast RA frequency.

[RFC 7772] addresses Issue 2 ~~discussed in~~ (Section 2.1).

Commenté [MB26]: Also fix similar occurrences

3.10. Source Address Validation Improvement and Router Advertisement Guard

Source Address Validation Improvement [SAVI] binds an address to a port on an L2 switch and rejects claims from other ports for that address. Therefore, a node cannot spoof the IP address of another node.

[RA-Guard] and [RA-Guard+] only allow RAs from a port that a router is connected to. Therefore, nodes on other ports cannot pretend to be a router.

[SAVI], [RA-Guard], and [RA-Guard+] address the on-link security issues.

3.11. RFC 6583 Dealing with NCE ~~Exhaution~~Exhaustion Attacks

[RFC6583] deals with the NCE ~~Exhaution~~Exhaustion attack issue discussed in Section 2.3. [RFC6583] recommends that:

. Operators should
  o Filter unused address space so that messages to such addresses can be dropped rather than triggering NCE creation.~~;~~
  o Implement rate-limiting mechanisms for ND message processing to prevent CPU and memory resources from being

overwhelmed.
. Vendors should
o Prioritize ND processing for existing NCEs over creating new NCEs

[RFC6583] RFC 6583 acknowledges that "some of these options are 'kludges', and can be operationally difficult to manage". [RFC6583] RFC 6583 partially addresses the Router NCE Exhaustion issue. In practical scenarios, network equipment vendors typically limit the number of NCEs on a router interface to prevent NCE Exhaustion. But this can have a side-effect. When more addresses are connected to that interface than the limit, irregular packet drops may result because the router does not maintain NCEs for all those IPv6 addresses [DHCP-PD].

3.12. Registering Self-generated IPv6 Addresses using DHCPv6

With In IPv4, network administrators can retrieve a host's IP address from the DHCP server, and use it for subscriber management. WithIn IPv6 and SLAAC, this is not possible, as discussed in Section 2.3.

[AddrReg] defines a method for informing a DHCPv6 server that a host has one or more self-generated or statically configured addresses. This enables network administrators to retrieve the IPv6 addresses for each host from the DHCPv6 server. [AddrReg] provides a solution for Issue 15 discussed in (Section 2.3).

3.13. Enhanced DAD

Enhanced DAD is specified in [RFC7527]. Enhanced DAD addresses a DAD failure issue in a specific situation: looped back interface. DAD will fail in a looped-back interface because the sending host will receive the DAD message back and will interpret it as another host is trying to use the same address. The solution is to include a Nonce option (defined in [SeND]) in each DAD message so that the sending host can detect that the looped-back DAD message is sent by itself.

Enhanced DAD does not solve any ND issue discussed in (Section 2). It extends ND to work in a new scenario: looped-back interface. It is reviewed here only for completeness.

3.14. ND Mediation for IP Interworking of Layer 2 VPNs

ND mediation is specified in [RFC6575]. When two Attachment Circuits (ACs) are interconnected by a Virtual Private Wired Service (VPWS), and the two ACs are of different media (e.g., one is Ethernet while the other is Frame Relay), the two PEs must interwork to provide mediation service so that a Customer Edge (CE) can resolve the MAC address of the remote end. [RFC6575] specifies such a solution.

ND Mediation does not address any ND issue discussed in (Section 2). It extends ND to work in a new scenario: two ACs of different media interconnected by a VPWS. It is reviewed here only for completeness.

3.15. ND Solutions Defined Bbefore the Latest Versions of ND

The latest versions of ND and SLAAC are specified in [RFCs 4861] and [RFC4862]. Several ND mitigation solutions were published before [RFC 4861]. They are reviewed in this section only for completeness.

3.15.1. SeND

The purpose of Secure Neighbor Discovery is specified in [SeND]. The purpose is to ensure that hosts and routers are trustworthy. SeND defined three new ND options (i.e., Cryptographically Generated Addresses [CGA], RSA public-key cryptosystem, and Timestamp/Nonce), an authorization delegation discovery process, an address ownership proof mechanism, and requirements for the use of these components in NDPND protocol.

SeND addresses the Trusting-all-nodes issues. But it has high requirements on the hosts and routers, especially to maintain the keys. There is no reported deployment.

3.15.2. Cryptographically Generated Addresses (CGA)

Cryptographically Generated Addresses is specified [CGA]The purpose of CGA. The purpose is to associate a cryptographic public key with an IPv6 address in [SeND]. The solution key point is to generate the Interface Identifier (IID) of the an IPv6 address by computing a cryptographic hash of the public key. The resulting IPv6 address is called a CGA. The corresponding private key can then be used to sign messages sent from the address.

Commenté [MB27]: Already introduced

CGA uses the factassumes that a legitimate host does not care about the bit combination of IID that would be created by some hash procedure. The attacker needs an exact IID to impersonate the legitimate hosts but then the attacker is challenged to do a reverse hash calculation that is a strong mathematical challenge.

CGA is part of SeND. There is no reported deployment.

3.15.3. ND Proxy

ND Proxy is specified in [RFC4389]. It is an Experimental solution. The purpose objective of such design is to enable multiple links joined by an ND- Proxy device to work as a single link.

Commenté [MB28]: Use consistent wording

- When a ND Proxy receives an ND request from a host in a link, it will "proxy" the message out the "best" outgoing interface. If there is no "best" interface, the ND- Proxy will "proxy" the message to all other links. Here "proxy" means acting as if the ND message originates from the ND- Proxy itself. That is, the ND- Proxy will change the ND message's source IP and source MAC address to the ND- Proxy's outgoing interface's IP and MAC address, and create an NCE entry at the outgoing interface accordingly.

- When ND- Proxy receives an ND reply, it will act as if the ND message is destined to itself, and update the NCE entry state at the receiving interface. Based on such state information,

the ND- Proxy can determine the "best" outgoing interface for future ND requests. The ND- Proxy then "proxy" the ND message back to the requesting host.

The idea of ND Proxy is widely used in SARP (Sections 3.5), ND Optimization for TRILL (Sections 3.6), and Proxy ARP/ND in EVPN which are discussed in (Sections 3.75) to 3.7.

3.15.4. Optimistic DAD

Optimistic DAD is specified in [RFC4429]. The purpose seeks is to minimize address configuration delays in the successful case and to reduce disruption as far as possible in the failure case. That is, Optimistic DAD lets hosts immediately use the newly formed address to communicate before DAD actually completes, assuming that DAD will succeed anyway. If the address turns out to be duplicate, Optimistic DAD provides a set of mechanisms to minimize the impact. Optimistic DAD modified the original ND [(RFC-2461)] and SLAAC [(RFC-2462)] but the solution was not incorporated into the latest specification of [ND] and [SLAAC]. However, implementations of Optimistic DAD exist.

Commenté [MB29]: Please fix all occurences

Optimistic DAD does not solve any ND issue discussed in (-Section 2). It is reviewed here only for completeness.

4. Guidelines for Preventing Potential ND Issues

By knowing the potential ND issues and associated mitigation solutions, network administrators of existing IPv6 deployments can assess whether these issues may occur in their networks and, if so, whether to deploy the mitigation solutions proactively. Deploying these solutions may take time and additional resources. Therefore, it is advisable to plan ahead.

Network administrators planning to start their IPv6 deployments can use the issue-solution information to help plan their deployments. Moreover, they can take proactive action to prevent potential ND issues.

4.1. Insights on Host Isolation from Existing Solutions

While various Neighbor Discovery (ND) solutions may initially appear unrelated, categorizing them into four distinct groups highlights an important observation: "host isolation" is an effective strategy for mitigating ND-related issues.

Group 1: L3 and L2 Isolation (Subnet and Link Isolation)

This group includes MBBv6 and FBBv6, which isolate hosts at both L3 and L2 by placing each host within its own subnet and link. This approach, referred to as "L3 & L2 Isolation" or "Subnet & Link Isolation", prevents ND issues caused by multicast and Trusting-all-nodes, as each host operates within its own isolated domain. Additionally, since routers can route packets to a host based on its unique prefix, the need for Router-NCE-on-Demand is eliminated,

thereby preventing ND issues arising from this mechanism.

Group 2: L3 Isolation (Subnet Isolation)

This group includes Unique Prefix per Host solutions like [UPPH] and [DHCP-PD], which isolate hosts into separate subnets while potentially leaving them on the same shared medium. This approach, termed "L3 Isolation" or "Subnet Isolation", mitigates ND issues caused by router multicast and eliminates the need for "Router-NCE-on-Demand", as detailed in Section 3.3.

Group 3: Partial L2 Isolation (Proxy Isolation)

This group encompasses solutions such as WiND, SARP, ND Optimization for TRILL, and Proxy ND in EVPN. These solutions use a proxy device to represent the hosts behind it, effectively isolating those hosts into distinct multicast domains. While hosts are still located within the same subnet, their separation into multicast domains reduces the scope of ND issues related to multicast-based address resolution. This method is referred to as "Partial L2 Isolation" or "Proxy Isolation".

Group 4: Non-Isolating Solutions

The final group includes remaining solutions that do not implement host isolation. These solutions do not prevent ND issues but instead focus on addressing specific ND problems.

The analysis demonstrates that the stronger the isolation of hosts, the more ND issues can be mitigated. This correlation is intuitive, as isolating hosts reduces the multicast scope, minimizes the number of nodes that must be trusted, and may eliminate the need for "Router-NCE-on-Demand", the three primary causes of ND issues.

This understanding can be used to prevent ND issues.

4.2. Applicability of Various Isolation Methods

4.2.1. Applicability of L3 & L2 Isolation

Benefit:

- All ~~Neighbor Discovery (~~ND~~)~~ issues listed in Section 2.4 can be effectively mitigated.

Constraints:

1. L2 Isolation:

   Actions must be taken to isolate hosts in L2. In many cases, this can be difficult.

2. Prefix Allocation:

   A large number of prefixes will be required, with one prefix assigned per host. This is generally not a limitation for IPv6. For instance, members of a Regional Internet Registry (RIR) can obtain a /29 prefix allocation [RIPE738], which provides 32

billion /64 prefixes - sufficient for any foreseeable deployment scenario. Practical implementations, such as MBBv6 assigning /64 prefixes to billions of mobile UEs [RFC6459] and FBBv6 assigning /56 prefixes to hundreds of millions of routed RGs [TR177], demonstrate the feasibility of this approach.

3. Unique Prefix Identifiability:

   Assigning a unique prefix to each host may theoretically reduce privacy, as hosts can be directly identified by their assigned prefix. However, alternative host identification methods, such as cookies, are commonly used. Therefore, unique prefix identifiability may not make much difference. The actual impact on privacy is therefore likely to be limited.

4. Router Support for Subnet Isolation:

   The router must support an L3 Isolation solution, e.g., [UPPH] or [DHCP-PD].

5. Increased Router Interface Requirements:

   A large number of interfaces will be required at the router, with one interface dedicated to each host.

6. Router as a Bottleneck:

   Since all communication between hosts is routed through the router, the router may become a performance bottleneck in high-traffic scenarios.

7. Incompatibility with Host-Based Multicast Services:

   Services that rely on multicast communication among hosts, such as mDNS, will be disrupted.

Commenté [MB30]: Cite an authoritative reference

4.2.2. Applicability of L3 Isolation

Benefits:

. All ND issues ~~identified in~~ (~~Section~~ 2.4) are mitigated, with the exception of:

  o LLA DAD multicast degrading performance,

  o LLA DAD not reliable in wireless networks, and

  o On-link security

These remaining issues depend on the characteristics of the shared medium:

  o If the shared medium is Ethernet, the issues related to LLA DAD multicast are negligible.

  o If nodes can be trusted, such as in private networks, On-link security concerns are not significant.

. No need for L2 Isolation. Consequently, this method can be applied in a wide range of scenarios, making it possibly the most practical host isolation method.

Constraints:

1. Prefix Requirements:

   Similar to L3 & L2 Isolation, a large number of prefixes (one per host) will be required. However, as previously discussed, organizations with access to sufficient IPv6 address allocations from Regional Internet Registries (RIRs) should not face significant challenges.

2. Router Support for Subnet Isolation:

   The router must support an L3 Isolation solution, e.g., [UPPH] or [DHCP-PD].

3. Router as a Bottleneck:

   Since all communication between hosts is routed through the router, the router may become a performance bottleneck in high-traffic scenarios.

4. Privacy Considerations:

   Each host is identifiable by its unique prefix, potentially impacting privacy as discussed earlier.

4.2.3. Applicability of Partial L2 Isolation

Benefit:

. Reduced Multicast Traffic:

This method reduces multicast traffic, particularly for address resolution, by dividing the subnet into multiple multicast domains.

Constraint:

. Router Support for Proxy Isolation:

The router must implement Proxy Isolation to support this method effectively.

4.3. Guidelines for Applying Isolation Methods

Based on the applicability analysis provided in the preceding sections, network administrators can determine whether to implement an isolation method and, if so, which method is most appropriate for their specific deployment.

A simple guideline is to consider the isolation methods one by one in the order listed in Section 4.2, from the strongest isolation to the weakest. With stronger isolation, more ND issues can be prevented but the entry requirements will also be higher. All things

considered, L3 Isolation can be a good tradeoff because many ND issues can be prevented while the entry requirements are manageable.

Recommended approach:

. Consider the isolation methods in the order listed in the preceding sections, progressing from the strongest isolation to the weakest.

o Stronger isolation methods can prevent more ND issues but may also impose higher entry requirements.

o Weaker isolation methods have fewer entry requirements but may leave some ND issues unmitigated.

. L3 Isolation is often a practical tradeoff:

o It provides significant benefits by addressing most ND issues.

o Its entry requirements, such as prefix allocation and router support for Subnet Isolation, are generally manageable.

~~It is important to note that s~~Selecting an isolation method that is either too strong or too weak does not result in serious consequences:

. Choosing an overly strong isolation method may require the network administrator to meet higher entry requirements initially, such as measures for L2 Isolation, additional prefixes or additional router capabilities.

. Choosing a "weaker isolation method" may necessitate deploying supplemental ND mitigation techniques to address any unresolved ND issues.

In either case, the resulting solution can be functional and effective.

5. Security Considerations

This document is a review of known ND issues and solutions, including security. It does not introduce any new solutions. Therefore, it does not introduce new security issues.

6. IANA Considerations

This document has no request to IANA.

7. References

7.1. Informative References

[AddrAcc] T. Chown, C. Cummings, D.Carder, "IPv6 Address Accountability Considerations", Internet draft, Oct. 2024.

[AddrReg] W. Kumari, S. Krishnan, R. Asati, L. Colitti, J. Linkova, S. Jiang, "Registering Self-generated IPv6 Addresses using

DHCPv6", Internet draft, May 2024.

[CGA] T. Aura, "Cryptographically Generated Addresses (CGA)", RFC3972.

[DHCP-PD] L. Colitti, J. Linkova, X. Ma, "Using DHCP-PD to Allocate Unique IPv6 Prefix per Client in Large Broadcast Networks", RFC 9663.

[GRAND] J. Linkova, "Gratuitous Neighbor Discovery: Creating Neighbor Cache Entries on First-Hop Routers", RFC 9131.

[MADINAS] J. Henry, Y. Lee, "Randomized and Changing MAC Address: Context, Network Impacts, and Use Cases", draft-ietf-madinas-use-cases-19.

[mDNS] S. Cheshire, M. Krochmal, "Multicast DNS", RFC 6762.

[MLSN] D. Thaler, "Multi-Link Subnet Issues", RFC 4903.

[ND] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861.

[RA-Guard] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu, J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105.

[RA-Guard+] F. Gont, "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", RFC 7113.

[RFC3756] P. Nikander, J. Kempf, E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756.

[RFC4389] D. Thaler, M. Talwar, C. Patel, "Neighbor Discovery Proxies (ND Proxy)", RFC 4389.

[RFC4429] N. Moore, "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429.

[RFC6459] J. Korhonen, J. Soininen, B. Patil, T. Savolainen, G. Bajko, K. Iisakkila, "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)", RFC 6459.

[RFC6085] S. Gundavelli, M. Townsley, O. Troan, W. Dec, "Address Mapping of IPv6 Multicast Packets on Ethernet", RFC 6085.

[RFC6575] H. Shah, E. Rosen, G. Heron, V. Kompella, "Address Resolution Protocol (ARP) Mediation for IP Interworking of Layer 2 VPNs", RFC 6575.

[RFC6583] I. Gashinsky, J. Jaeggli, W. Kumari, "Operational Neighbor Discovery Problems", RFC 6583.

[RFC6775] Z. Shelby, S. Chakrabarti, E. Nordmark, C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775.

[RFC6957] F. Costa, J-M. Combes, X. Pougnard, H. Li, "Duplicate Address Detection Proxy", RFC 6957

[RFC7066] J. Korhonen, J. Arkko, T. Savolainen, S. Krishnan, "IPv6 for Third Generation Partnership Project (3GPP) Cellular Hosts", RFC 7066.

[RFC7102] JP. Vasseur, "Terms Used in Routing for Low-Power and Lossy Networks", RFC 7102.

[RFC7278] Extending an IPv6 /64 Prefix from a Third Generation Partnership Project (3GPP) Mobile Interface to a LAN Link", RFC7278.

[RFC7342] L. Dunbar, W. Kumari, I. Gashinsky, "Practices for Scaling ARP and Neighbor Discovery (ND) in Large Data Centers", RFC 7342.

[RFC7527] R. Asati, H. Singh, W. Beebee, C. Pignataro, E. Dart, W. George, "Enhanced Duplicate Address Detection", RFC 7527.

[RFC7772] A. Yourtchenko, L. Colitti, "Reducing Energy Consumption of Router Advertisements", RFC 7772.

[RFC8302] Y. Li, D. Eastlake 3rd, L. Dunbar, R. Perlman, M. Umair, "Transparent Interconnection of Lots of Links (TRILL): ARP and Neighbor Discovery (ND) Optimization", RFC 8302.

[RFC8505] P. Thubert, E. Nordmark, S. Chakrabarti, C. Perkins, "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery", RFC 8505.

[RFC8928] P. Thubert, B. Sarikaya, M. Sethi, R. Struik, "Address-Protected Neighbor Discovery for Low-Power and Lossy Networks", RFC 8928.

[RFC8929] P. Thubert, C.E. Perkins, E. Levy-Abegnoli, "IPv6 Backbone Router", RFC 8929.

[RFC9099] E. Vyncke, K. Chittimaneni, M. Kaeo, E. Rey, "Operational Security Considerations for IPv6 Networks", RFC 9099.

[RFC9119] C. Perkins, M. McBride, D. Stanley, W. Kumari, JC. Zuniga, "Multicast Considerations over IEEE 802 Wireless Media", RFC 9119.

[RFC9161] J. Rabadan, S. Sathappan, K. Nagaraj, G. Hankins, T. King, "Operational Aspects of Proxy ARP/ND in Ethernet Virtual Private Networks", RFC 9161.

[RIPE738] IPv6 Address Allocation and Assignment Policy, https://www.ripe.net/publications/docs/ripe-738

[SARP] Y. Nachum, L. Dunbar, I. Yerushalmi, T. Mizrahi, "The Scalable Address Resolution Protocol (SARP) for Large Data Centers", RFC7586.

[SAVI] J. Wu, J. Bi, M. Bagnulo, F. Baker, C. Vogt, "Source Address Validation Improvement (SAVI) Framework", RFC

7039.

[SeND] J. Arkko, J. Kempf, B. Zill, P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC3971.

[SLAAC] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862.

[SND] P. Thubert, M. Richardson, "Architecture and Framework for IPv6 over Non-Broadcast Access", Internet draft, June 2023.

[TR177] S. Ooghe, B. Varga, W. Dec, D. Allan, "IPv6 in the context of TR-101", Broadband Forum, TR-177.

[UPPH] J. Brzozowski, G. Van de Velde, "Unique IPv6 Prefix per Host", RFC 8273.

8. Acknowledgments

The authors would like to thank Eric Vyncke, Gunter Van de ~~Felde~~Velde, Lorenzo Colitti, Erik Kline, Warren Kumari, Pascal Thubert, Jen Linkova, Brian Carpenter, Mike Ackermann, Nalini Elkins, Ed Horley, Ole Troan, David Thaler, Chongfeng Xie, Chris Cummings, Dale Carder, Tim Chown, Priyanka Sinha, Aijun Wang, Ines Robles, Magnus Westerlund, Barry Leiba, and Paul Wouters for their reviews and comments. The authors would also like to thank Tim Winters for being the document shepherd.

Authors' Addresses

XiPeng Xiao
Huawei Technologies Dusseldorf
Hansaallee 205, 40549 Dusseldorf, Germany

Email: xipengxiao@huawei.com

Eduard Vasilenko
Huawei Technologies
17/4 Krylatskaya st, Moscow, Russia 121614

Email: vasilenko.eduard@huawei.com

Eduard Metz
KPN N.V.

Email: eduard.metz@kpn.com

Gyan Mishra
Verizon Inc.

Email: gyan.s.mishra@verizon.com

Nick Buraglio
Energy Sciences Network

Email: buraglio@es.net